

ArcSight ESM™ User's Guide

ArcSight ESM™ v5.0 SP2

September 2011



ArcSight ESM™ User's Guide ArcSight ESM™ v5.0 SP2

Copyright © 2000-2011 ArcSight, LLC. All rights reserved.

ArcSight and the ArcSight logo are registered trademarks of ArcSight in the United States and in some other countries. Where not registered, these marks and ArcSight Console, ArcSight ESM, ArcSight Express, ArcSight Manager, ArcSight Web, ArcSight Enterprise View, FlexConnector, ArcSight FraudView, ArcSight Identity View, ArcSight Interactive Discovery, ArcSight Logger, ArcSight NCM, SmartConnector, ArcSight Threat Detector, ArcSight TRM, and ArcSight Viewer, are trademarks of ArcSight, LLC. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:

<http://www.arcsight.com/copyrightnotice>

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

This document is ArcSight Confidential.

Revision History

Date	Product Version	Description
08/23/11	ArcSight ESM v5.0 SP2	Update for ESM v5.0 SP2.
09/14/10	ArcSight ESM v5.0 SP1	Update for ESM v5.0 SP1.
05/10	ArcSight ESM v5.0 GA	Update for ESM v5.0.
02/20/10	ArcSight ESM v5.0 Beta	Update for ESM v5.0 Beta.
01/26/10	ArcSight ESM v4.5 SP2	Update for ESM v4.5 SP2.
04/16/09	ArcSight ESM v4.5 SP1	Update for ESM v4.5 SP1.
11/11/08	ArcSight Express and ArcSight ESM v4.5	Update for ArcSight Express and ESM v4.5

Document template version: 1.0.2.9

ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	support@arcsight.com
Support Web Site	http://www.arcsight.com/supportportal/
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: What's New	41
Oracle 11G Support	41
Standard Content	41
Chapter 2: Getting Started	43
Quick Start Tools and Content	43
Network Model Wizard	44
Configuration and Using Standard Content	44
ArcSight Express	45
Getting Started Configuring ArcSight Express	45
ArcSight Express Documentation	46
ArcSight Web	46
Chapter 3: Standard Content	47
What is Standard Content?	47
Standard Content Foundations	48
ArcSight System Content	49
Shared Resources	50
Anti-Virus	50
Conditional Variable Filters	50
Network Filters	50
Standard Content Packages	51
Navigating to Standard Content	51
Set Up Connectors and Model the Network	52
Standard Content-Related SmartConnectors	53
Network Modeling	54
Apply Standard Asset Categories to Assets	54
Categorize Internal Assets	54
Determine the Protected Network	54
Categorize Critical Assets	55
Configure Notification Destinations	55
Configure Active Lists	56
Configure Asset Auto-Creation Filters	56
Configure Connector Asset Auto-Creation Controller Filter	57

Configure Device Asset Auto Creation Controller Filter	59
Configure SNMP Trap Forwarding Filter	60
Configure Rules to Send Notifications and Open Cases	62
Configure Rules with Notifications to the Cert Team	63
Configure Rules with Notifications to the SOC Operators	64
Schedule Reports	64
Default Trends Schedule	64
ArcSight Administration Trends	65
Configuration Monitoring Trends	65
Intrusion Monitoring Trends	66
Network Monitoring Trends	66
Workflow Trends	67
How to Enable/Disable Trends	67
Getting Started Using Standard Content	67
Monitoring with Standard Content	68
Active Channels	68
Dashboards	69
Investigating with Standard Content	70
Reporting with Standard Content	70
Chapter 4: ArcSight Express Solution	73
What is ArcSight Express Content?	73
How ArcSight Express Is Organized	74
Set Up Connectors and Model the Network	75
ArcSight Express-Related SmartConnectors	75
Network Modeling	76
Apply Standard Asset Categories to Assets	77
Categorize Internal Assets	77
Determine the Protected Network	77
Categorize Critical Assets	78
Create ArcSight Express Users	78
Configure Notification Destinations	78
Configure Asset Auto-Creation Filters	79
Configure Connector Asset Auto-Creation Controller Filter	79
Configure Device Asset Auto Creation Controller Filter	81
Configure Rules to Send Notifications and Open Cases	82
Schedule Reports	85
Tuning ArcSight Express Content	86
Chapter 5: Learning Paths	89
For the User	90
ArcSight User Certification Subjects	90
Active Channels	90

Login Process	90
For the Administrator	90
ArcSight Administrative Certification Subjects	90
Access Control Lists (ACLs)	90
Active List Resources	90
Dashboards	90
Data Monitor Resources (statistical)	91
Database Full Response	91
Filters	91
Reports	91
Resources and Resource Editors	91
Rules	91
Rule Actions	91
Shell Commands	91
Threat Level Formula	91
Users and User Groups (Administrator, Author, Operator)	91
Chapter 6: Working in the ESM Console	93
Navigating	94
Navigator Panel Resource Tree	95
Using SmartFolders	96
Creating a Case-Search SmartFolder	97
Creating a Reports SmartFolder	97
Editing Groups	97
Editing a Group	97
Categories Tab	97
Viewing Group Cases in a Grid View	98
Batch Editing	98
Batch-Editing Cases or Connectors	98
Cases Reminder	98
SmartConnector Reminders	99
Reconnecting to the Manager	99
Viewing	99
Viewer Panel	99
ESM Console Look-and-Feel	101
Inspecting and Editing	102
Overview of Inspect/Edit Features and Utilities	102
Searching for Fields in Event Inspector, Resource Editors or CCE	103
Controlling the ESM Console	105
Error and Warning Messages	107
Using the Network Tools	107
Running a Tools Command	107
Network Tool Default Options	108

Adding a Tool	108
Configure (Edit) a Tool	109
Deleting a Tool	110
Staying Informed	110
Acknowledging Notifications	110
Acknowledging a Page	111
Acknowledge a Cell Phone Message	111
Acknowledge an E-mail Message	111
Acknowledge Notifications at the ESM Console	111
Using Notes	111
Adding a Note	111
Viewing a Note	111
Deleting a Note	112
License Tracking	112
License Tracking Notifications	112
Standard Reports for License Status Tracking	113
Using the Menus	114
File Menu	114
Edit Menu	114
View Menu	115
Window Menu	116
Tools Menu	116
System Menu	117
Help Menu	117
Keyboard Shortcuts (Hot Keys)	119
Moving Copying, Linking, and Deleting Resources	120
Move, Copy, or Link a Resource	120
Delete a Resource	120
Printing from the Console	120
Printing Navigation Tree Views of Resources	121
Printing Resource Definitions	122
Saving as an HTML File	123
Printing Grid Views	123
Printing Conditions Tree Summary	123
Using Column Flip Limit to Format Grid View Printouts	125
Chapter 7: Monitoring Events	129
Monitoring Active Channels	129
Using Views	129
Selecting a View	129
Changing View Layouts	130
Floating a View	130
Closing One or All Views	130

Closing all Views Except the Current One	130
Viewing and Using Channels	130
Viewing an Active Channel	130
Sorting Events in an Active Channel	131
Creating an Active Channel	131
Applying a Field Set to an Active Channel	132
Adding a Column to the Channel	133
Using an Active Channel Header	134
Filtering an Active Channel	134
Saving Copies of Active Channels and Filters	135
Editing an Active Channel	135
Defining Grid Fields Options	136
Discovering Patterns in an Active Channel	137
Deleting an Active Channel	137
Adding a View Format	137
Changing View Layouts	137
Best Practices to Optimize Active Channel Performance	137
Investigating Views	140
Using an Event Attribute to Show a New Filtered View	141
Refining a Filter with an Event Attribute	141
Adding an Event Attribute to a Filtering Condition	142
Permanently Modifying an Active Channel	142
Showing an Exploited Vulnerability	143
Showing a Targeted Asset	143
Using Charts	143
Charting an Active Channel's Contents	143
Charting a Data Monitor's Contents	143
Exploring the Events Behind a Chart	144
Using Grids	145
Monitoring Events in the Grid View	145
Sorting Columns in the Grid View	145
Adding, Replacing, or Removing a Columns	145
Sizing a Column in the Grid View	146
Showing or Hiding Grid View Column Text and Icons	147
Exporting Events to a File	147
Choosing Grid View Menu Commands	148
Filtering Grid Views with Inline Filters	150
Customizing Grid Columns	152
Creating a Custom Column	152
Showing a Custom Column	153
Advanced Example: Creating a Custom Column with Velocity	153
Using Dashboards	153
Monitoring Dashboards	154

Loading Dashboards	154
Inspecting Events in Dashboards	154
Displaying Dashboards	155
Displaying Dashboards in a Slide Show Rotation	155
Rearranging Elements in Dashboard Layouts	156
Using Dashboard Menu Options	156
Zooming In or Out of Dashboards	156
Fitting all Dashboard Elements	156
Saving Dashboard Layouts	156
Closing a Dashboard	156
Editing Dashboard Elements	156
Changing a Dashboard's Layout	156
Managing Dashboards	156
Creating a Dashboard	156
Adding a Data Monitor to a Dashboard	157
Adding a Query Viewer to a Dashboard	157
Display Formats	158
Editing a Dashboard	158
Deleting a Dashboard	158
Managing Dashboard Groups	159
Creating a Dashboard Group	159
Renaming a Dashboard Group	159
Editing a Dashboard Group	159
Moving or Copying a Dashboard Group	159
Deleting a Dashboard Group	159
Using Data Monitors	160
Creating a Data Monitor	160
Editing a Data Monitor	161
Moving or Copying a Data Monitor	161
Deleting a Data Monitor	161
Enabling or Disabling a Data Monitor	161
Enabling or Disabling a Data Monitor from the Editor	162
Enabling or Disabling a Data Monitor in the Navigator	163
Overriding a Data Monitor's Last State	163
Data Monitor Types	164
Managing Data Monitor Groups	165
Creating a Data Monitor Group	166
Renaming a Data Monitor Group	166
Editing a Data Monitor Group	166
Moving or Copying a Data Monitor Group	166
Deleting a Data Monitor Group	166
Enabling or Disabling Data Monitor Groups	166
Using Query Viewers	167

Using Custom View Dashboards	167
Browser Environments for Custom View Dashboards	168
Displaying Custom View Dashboards	168
To Launch the Custom View Dashboard in a Separate Browser Window	169
To Refresh the Custom View Dashboard Layout	169
Custom View Dashboard Context Menu Options	169
To Revert to the Regular Dashboard View	170
Working with Custom View Dashboards	170
To Select View Mode	170
To Show Events in an Active Channel View	170
Arranging Custom View Dashboards	171
To Select Arrange Mode	171
To Load a Background Image	171
To Select a Previously Uploaded Background Image	172
Using Resource Graphs to Verify that a Background Image is Attached	173
Removing a Background Image	173
To Relocate, Resize, and Reshape Data Monitors	173
To Select Which Data Monitors to Display and How	173
Monitoring Active Lists	174
Viewing Active List Contents	174
Refreshing Active List Views	174
Adding to or Subtracting from an Active List	174
Filtering Active Lists	175
Editing Active Lists	175
Clearing Active List Views	175
Customizing Active View Grid Columns	175
Active List Grid Context Menu Commands	175
Graphing Attacks	176
Creating Static Event Graphs	176
Creating Live Event Graphs	176
Event Graph Notes	177
Chapter 8: Pattern Discovery	179
Pattern Discovery Overview	179
What Pattern Detection Provides	179
Pattern Components	180
How Pattern Discovery Works	181
Installing Pattern Discovery	181
Pattern Discovery Life Cycle	182
Creating or Editing a Profile	182
Editing Profile Attributes	183
Specifying Actions	185
Creating Local Variables	187

Adding Notes	188
Deleting a Profile	188
Taking a Snapshot	188
Exploring a Snapshot	190
Arranging Elements in Graphic View	191
Scheduling a Snapshot	192
Re-opening a Snapshot	193
Deleting a Snapshot	193
Investigating Patterns	193
Investigating Patterns in the Snapshots View	194
Investigating Patterns in the Patterns View	196
Viewing Patterns with Filter	196
Inspecting Patterns	197
Creating Rules from Patterns	198
Annotating Patterns	200
Deleting a Pattern	201
Usage Guidelines	201
Establishing a Baseline of Normal Patterns	201
Using Pattern Discovery in Routine Operations	201
Adjusting Pattern Discovery Memory	202
Chapter 9: Field Sets	203
Field Sets	204
Navigating to Field Sets	204
Creating and Using Field Sets	204
Creating a Field Set	205
Field Set Editor: Attributes Tab	205
Field Set Editor: Fields Tab	206
Field Set Editor: Local Variables Tab	210
Editing a Field Set	211
Sharing a Field Set	211
Deleting a Field Set	212
Where Field Sets can be Selected	212
About Global Variables	212
About Domains	212
Chapter 10: Selecting and Investigating Events	213
Handling Events in Grid Views	213
Selecting Events to Investigate in a Grid View	213
Inverting Event Selections in a Grid View	213
Selecting Events with Matching Cells in a Grid View	213
Exporting Data Fields to a CSV File	213
Showing Event Details and Rule Chains	214

Displaying Event Details	214
Displaying Simple Event Rule Chains	214
Displaying Detailed Event Rule Chains	215
Displaying Correlation-Event Rules	215
Executing or Clearing Rule Actions in a Grid View	215
Launching Event Details in a Browser	215
Hiding Empty Rows in the Event Inspector	215
Investigating Session Events	215
Investigating a Session Event	215
Collaborating on Events	216
Viewing Annotations for an Event	216
Annotating an Event	217
Event Annotation Fields	217
Comments Field	217
Mark Similar Events Fields	217
Creating New Stages	218
Stage Editor Fields	218
Editing Stages	219
Showing Event Payloads	219
Finding Payloads	220
Retrieving Payloads	220
Preserving Payloads	220
Discarding Payloads	220
Saving Payloads to Files	220
Viewing Payloads in Other Viewers	220
Getting Knowledge Base Articles	221
Displaying Articles from the Knowledge Base Window	221
Displaying Articles from a Grid View	221
Displaying Articles from the Event Inspector	221
Chapter 11: Filtering Events	223
Creating Filters	223
Creating a New Filter	223
Changing or Editing a Filter	224
Creating an Inline Filter	225
Moving or Copying Filters	226
Deleting Filters	227
Debugging Filters to Match Events	227
Applying Filters	231
Adding Filters to Resources	231
Applying Resources as Filters to Active Channels	231
Removing a Filter Condition or Resource	231
Importing and Exporting filters	232

Using Filter Groups	232
Creating Filter Groups	232
Renaming Filter Groups	232
Editing Filter Groups	232
Moving or Copying Filter Groups	233
Deleting Filter Groups	233
Investigating Views	233
Using an Event Attribute to Show a New Filtered View	234
Refining a Filter with an Event Attribute	234
Filtering Out ArcSight Events or Other Customizations	235
Adding an Event Attribute to a Filtering Condition	235
Permanently Modifying an Active Channel	236
Showing an Exploited Vulnerability	236
Showing a Targeted Asset	236
Modifying Views	236
Modifying a View Inline	237
Undoing an Inline Filter	237
Permanently Modifying a View	237
Chapter 12: Actors	239
About Actors	239
How the Actors Feature Works	241
About the Actor Model Import Connectors	243
Troubleshooting Errors with Actor Model Imports	244
Navigating to Actors	245
Configuring Actors (for Administrators)	245
Tuning Guide for Supporting Large Actor Models	247
Permissions Required to Use Actors and Actor-Related Data	248
About Exporting Actors	249
Viewing Actors in the ESM Console	249
Viewing Actors in the Navigator Panel	249
Viewing Actors in the Actor Editor	251
Viewing Actor Base Attributes	251
Viewing Actor Account Attributes	253
Viewing Actor Role Attributes	253
Viewing Actors in an Actor Channel	253
About the Actor Channel UI	255
Sorting Fields in Actor Channels	255
Actor Channel Options	255
Right-Click Options from the Grid View	256
Filtering Actor Channels	256
Adding a Local Filter to the Actor Channel Resource	256
Creating an Inline Filter	257

Saving Actor Channels	257
Editing Saved Actor Channels	258
Viewing Saved Actor Channels	258
Investigating Actors	258
Running Context Reports from an Actor Channel	258
Investigating an Actor from an Event Channel	260
Actor Context Reports in Standard Content	261
Creating and Editing Actors for Testing Purposes	262
Creating Actors for Testing Purposes	263
Editing Actors for Testing Purposes	264
Deleting Actors	265
Leveraging Actor Data Using Variables	265
Creating an Actor Global Variable	265
Creating an Actor-Based Variable in Another Resource	266
Creating and Using Category Models	266
Memory Recommendations for Using Category Models	267
Creating Category Models	267
Creating Actor-to-Actor Category Models	268
Creating Actor Attribute Category Models	270
Creating User-Defined Category Models	272
Editing a Category Model	274
Moving or Copying a Category Model	274
Deleting a Category Model	275
Viewing Category Models in Graphs	275
Working with Category Model Graphs	275
Leveraging Category Model Data Using Variables	277
Actor-Related Resources Provided in Standard Content	278
Actor Resource Framework Global Variables	278
Tracking Actor Configuration Changes Using Standard Content	281
Actor Configuration Changes: Monitoring	281
Actor Configuration Changes: Query Viewers	282
Actor Configuration Changes: Reports	283
Actor Configuration Changes: Global Variables	284
Chapter 13: Query Viewers	287
What are Query Viewers?	287
Navigating to Query Viewers	289
Pre-Built and Custom Query Viewers	289
Standard Content	289
Custom Query Viewers	290
Customizing Query Viewers as Needed	290
inActiveList Conditions for Queries	290
Query Viewers Need Base Queries	290

Running Queries and Viewing Results	291
Working with Query Viewer Results	294
Results in Table Format	295
Results in Chart Formats	299
Filtering Query Viewer Results	300
Adding a Filter	300
Viewing an Event or Resource Directly from the Query Viewer	301
Adding Query Viewers to Dashboards	302
Making Query Viewer Results Available to ArcSight Web	302
Adding Query Viewers as Startup Views	302
Generating Reports from Query Viewers	303
Defining and Using Baselines	304
Why Baselines are Useful	305
Planning for Baseline Comparisons	306
Adding a Baseline	306
Comparing Displayed Results to a Baseline	308
Show or Hide Baseline Columns	309
Sort Baseline Data	309
Filter Baseline Data	310
Removing a Baseline	310
Customizing Query Viewers	311
Creating a New Query Viewer	311
Defining Query Viewer Settings	312
Query Viewer Attributes	312
Query Viewer Fields	316
Query Viewer Variables	318
Query Viewer Drilldowns	319
Editing a Query Viewer	323
Deleting a Query Viewer	323
Example Queries for Common Scenarios	323
Basic Analysis High Level Summaries	324
Analyst's First View of Events	324
Drilldown Example	326
How the Drilldowns are Built	328
Non-Event Analysis Example	329
Baseline Analysis for Data Comparison	329
History Analysis Example	329
Chapter 14: Building Reports	331
Understanding Reporting Workflow	331
1. Build a Query	332
2. Build a Trend (Based on a Query)	332
3. Build a Query (Based on a Trend)	333

4. Select or Design a Report Template	333
5. Create a Report	333
6. Run a Report	334
7. Archive and Maintain Reports	334
Managing Dependencies for Reports Resources	335
Using Report Templates	335
Navigating to Templates	335
Using Standard Templates	336
Applying a Template to an Existing Report	336
Creating a New Report Based on a Template	337
Copying a Template	337
Opening the Designer to Edit a Template	338
Designing Custom Templates	338
Opening the Template Designer to Edit Existing Templates	338
Creating a New Template	338
Template Designer User Interface	339
Setting Report Page Options	346
Designing Report Flow Layout	347
Designing Report Tabular Layout	348
Building Report Elements into a Template	349
Building Queries	354
How Queries Work	355
Using Queries and Trends Together for Reports	355
Using Queries in Query Viewers	355
Building a Query	356
Creating a New Query	356
Defining Query Settings	357
General Attributes	357
Query Fields	359
SELECT Query Fields	360
GROUP BY Query Fields	362
ORDER BY Query Fields	364
Query Conditions	366
Creating Conditions on a Field	367
Editing a Query	368
Building Trends	369
How Trends Work	369
Snapshot Trend	369
Interval Trend	370
Query-Trend Relationships in Reporting	370
Building a Trend	371
Navigating to Trends	371
Creating a New Trend	371

Defining Trend Settings	372
Trend Attributes	372
Trend Schedule	376
Trend Parameters	377
Trend Actions (Add to Active List)	377
Testing a Trend	383
Viewing Trend Data	383
Refreshing Trend Data	384
Editing or Viewing a Trend Definition	385
Using a Trend in a Query or Report	385
Creating Reports	385
How Reports Work	385
Building a Report	386
Navigating to Reports	386
Creating a New Report	386
Defining Report Settings	387
Report Attributes	387
Report Templates	388
Report Data	391
Report Parameters	401
Setting Special Parameters for Running Large or Complex Reports	404
Setup and Parameters to Generate PDF Reports with Asian Fonts	406
Editing a Report	406
End-to-End Reporting Examples	407
Quick Start Example of Creating a Simple Report with the Wizard	407
Advanced Reporting Example Overview	410
1. Build the VPN Logins Outcome Query	411
2. Build the VPN Logins Outcome Hourly Trend	413
3. Filter the Trend Data (Login Attempts, Successes, Failures)	415
4. Create the VPN Logins Outcome Report on Trend Data	417
5. Run the Report	420
Chapter 15: Running and Managing Reports	423
Running Reports	423
Running a New or Archived Report	423
Running a Defined Report	424
Run-Report Options	425
Report Parameters	425
Displaying an Archived Report	426
Running a Delta Report	426
Running Reports from a Grid View	427
Running a Rule-Context Report from a Grid View	427
Running an Event Context Report from a Grid View	427

Running a Channel Report from a Grid View	427
Managing Reports	428
Editing a Report	428
Creating Focused Reports	428
Importing and Exporting Reports	429
Importing Reports	429
Exporting Reports	429
Moving or Copying a Report	429
Managing Report Groups	430
Creating a Report Group	430
Renaming a Report Group	430
Editing a Report Group	430
Moving or Copying a Report Group	430
Deleting a Report Group	431
Archiving and Scheduling Reports	431
Archiving a Report	431
Parameterized Report Entries	433
Viewing an Archived Report	433
Scheduling Report Tasks	433
Scheduling Individual-Report Archiving	433
Scheduling Report Archiving by Resource Group	435
Standard Time Transitions	436
Editing a Report Archiving Schedule	436
Editing Report Archiving Parameters	436
Deleting a Report Archiving Schedule	437
Chapter 16: Rules Authoring	439
Designing Rules	439
Managing Rules	440
Creating Rules	440
Editing Rules	440
Moving or Copying Rules	441
Deleting Rules	441
Managing Rule Groups	441
Creating Rule Groups	441
Renaming Rule Groups	441
Editing Rule Groups	441
Moving or Copying Rule Groups	442
Deleting Rule Groups	442
Specifying Rule Conditions	442
Creating New Rule Conditions	442
Adding Filter Conditions	443
Negating Event Conditions	444

Adding Asset Conditions	444
Adding Vulnerability Conditions	445
Adding Active List (InActiveList) Conditions	445
Creating Matching or Join Conditions	447
Editing or Deleting Join Data Field Conditions	448
Specifying Rule Thresholds and Aggregation	449
Setting or Changing Rule Thresholds	449
Aggregation Time Criteria	450
Deleting Aggregation from a Rule	451
Creating Rule Actions	451
Adding a Rule Action	452
Editing a Rule Action	452
Removing a Rule Action	452
Activating or De-activating a Rule Trigger	452
Enabling or Disabling a Rule Action	453
Threshold Triggering Options	453
Rule Actions Reference	455
Applying Rule Actions	460
More Rule Actions	460
Enabling and Disabling Rules	461
Enabling Rules	461
Disabling Rules	461
Automatically and Manually Disabled Rules	461
Disabling Rule Components	463
Importing and Exporting Rules	463
Scheduling Rules	463
Scenarios for Using Scheduled Rules	463
Scheduling a Rule Group	464
Example of a Scheduled Rule (Badge Swipes and Logins)	466
Testing Rules	468
Testing a Rule from the Rule Editor	469
Showing Rule Errors	470
Verifying Rule(s) with Events	470
Verify Rule(s) from the Resource Tree	471
Deploying Real-time Rules	473
Deploying a Rule	474
Removing or Un-deploying a Rule	474
Loading Rules	474
Automatic Disabling	475
Chapter 17: Global Variables	477
About Global Variables	477
Creating a Global Variable	478

Global Variable Editor: Attributes Tab	479
Global Variable Editor: Parameters Tab	479
Global Variable Editor: Local Variables Tab	479
Creating a Global Variable from a Domain Field	480
Promoting a Local Variable to a Global Variable	480
Editing a Global Variable	483
Moving or Linking a Global Variable	483
Deleting a Global Variable	483
Navigating to Global Variables	484
Adding a Global Variable to a Resource	484
Adding a Global Variable Using the CCE	485
Adding a Global Variable to a Data Monitor	485
Adding a Global Variable to a Field Set	487
Adding Global Variables to an Active Channel	488
Chaining a Global Variable	489
Global Variables in Standard Content	490
Actors Global Variables	490
Variables Library	490
Device, Protocol, and Total Bytes Global Variables	490
Asset Information Global Variables	490
Host Information Global Variables	490
Timestamp Formats Global Variables	490
User Information Global Variables	490
Chapter 18: Domain Field Sets	491
About Domain Field Sets	491
Anatomy of Domain Field Sets	491
How Domain Field Sets Work	492
Standard ESM Schema: the Static Schema	492
Device Custom Fields	493
Domain Fields: the Dynamic Schema	493
Example Scenarios for How to Apply Domain Field Sets	495
Implementing Domain Field Sets: Process Overview	496
Domain Modeling	497
Creating Domain Field Sets	498
Creating Domain Fields from the Console	498
Domain Field Editor: Attributes Tab	498
Domain Field Editor: Field Sets Tab	499
Deleting a Domain Field	500
Creating Domain Field Sets from the Console	500
Field Set Editor: Attributes Tab	501
Field Set Editor: Fields Tab	501
Field Set Editor: Local Variables Tab	501

Configuring FlexConnectors for Domains	501
Using Domain Field Sets in Correlation, Monitoring, and Investigation	503
Where to Find Domain Fields in the Event Inspector and Field Selectors	503
Where to Find Root Domain Fields in Field Selectors	503
Where to Find User-Created Domain Fields in Field Selectors	503
Using Domain Fields and Field Sets for Correlation	503
Using a Domain Field in a Global Variable	507
What Correlation Functions Support Which Data Types	509
Chapter 19: Use Cases	511
About Use Cases	511
Navigating to Use Cases	513
Master Use Cases	513
How Master Use Cases Work	514
Standard Use Cases	514
Pre-Installed Use Cases for ArcSight Express	514
ArcSight Jumpstart Use Cases	515
Installing Use Cases	516
Viewing and Using Use Cases	517
Accessing Resources from the Viewer Panel	518
Configuring Use Cases	518
Navigating the Use Case Configuration Wizard	519
Step 1 - Model Your Network	519
Step 2 - Install Use Case Package Bundles	520
Step 3 - Launch the Use Case Wizard	520
Step 4 - Introduction Panel	520
Step 5 - Prerequisites Panel	521
Step 6 - Confirm Event Sources Panel	521
Step 7 - Configuration Panels	523
Step 8 - Summary of Settings to Apply Panel	523
Step 9 - Configuration Complete Panel	525
Configuration Panels	525
Categorize Assets/Zones Panels	526
Populate Active List	527
Specify the Notification E-mail Address Panel	529
Set the Inactivity Time Period Panel	531
Set the Notification Rate Panel	531
Schedule Daily Report Panels	532
Schedule Weekly Report Panels	534
Schedule Monthly Report Panels	536
Schedule Yearly Report Panels	538
Enable Rules Panel	539
Enable Rule Actions Panel	540

Set Session List Entry Expiry Panel	541
Chapter 20: Identity Correlation	543
Understanding Session Correlation	543
How Session Correlation Works	543
Creating a Session List Rule	544
Creating a Variable	546
Managing Session Lists	547
Creating a Session List	547
Editing Session Lists	549
Moving or Copying Session Lists	549
Exporting Session Lists	550
Deleting Session Lists	550
Adding a Session List Entry	550
Adding a Session List Entry Based on an Existing Entry	550
Deleting a Session List Entry	550
Terminating a Session List Entry	551
Using Session Lists to Correlate Session Data on User Logins (Example)	551
Example Overview	551
1. Create a Session List to Store Windows Sessions	552
2. Create Rules to Populate the Session List with Windows Logins	553
Rule 1: Triggers on Windows Session Logins	554
Rule 2: Triggers on Termination of Windows Sessions	556
3. Verify Rules	558
4. Use the Session List in a Report	560
Using Active Lists to Correlate Users (Example)	561
Example Overview	562
1. Build and Populate the Active List with User IDs	562
Populating an Active List with User Data	563
2. Create a Rule that Uses Active List Values to Correlate User IDs	565
Chapter 21: List Authoring	571
Managing Active Lists	571
Creating an Active List	571
Case-Insensitive Lookup in Active Lists	573
Using Rules to Populate an Active List	574
Example	574
Editing Active List Entries	577
Editing an Active List	577
Move or Copy an Active List	577
Importing an Active List	577
Exporting an Active List	578
Deleting an Active List	578

Managing Active List Groups	578
Navigating to Active Lists	578
Creating an Active List Group	578
Renaming Active List Groups	579
Editing Active List Groups	579
Moving or Copying Active List Groups	579
Deleting Active List Groups	579
Managing Session Lists	579
Creating a Session List	580
Using Rules to Populate a Session List	582
Editing a Session List	582
Moving or Copying a Session List	582
Exporting a Session List	582
Deleting a Session List	582
Adding a Session List Entry Based on an Existing Entry	583
Adding a Session List Entry	583
Deleting a Session List Entry	583
Terminating a Session List Entry	583
Chapter 22: Case Management and Queries	585
Managing Cases	585
Create a New Case	586
Case Properties	586
Creating a Case from Displayed Events	587
Editing a Case	587
Finding Cases	588
Attaching a File to a Case	588
Viewing a Case Attachment	589
Adding Events to a Case	589
Showing Event Details for Cases in Channels	590
Deleting Events from a Case	590
Creating a Channel for a Case	590
Exporting a Case to an External System	591
Moving or Copying a Case	591
Deleting a Case	591
Managing Case Groups	591
Creating a Case Group	591
Renaming a Case Group	592
Editing a Case Group	592
Moving or Copying a Case Group	592
Deleting a Case Group	592
Running Case Queries	592
Setting Up an Automatic Case Query Group	592

Chapter 23: Integration Commands	595
What are Integration Commands?	595
Supported Command Types	596
Out-of-the-Box Commands for Logger and NSP TRM	596
Local Scripts and Commands to Other Applications	597
How it Works	597
Planning Checklist and Workflow	598
Navigating to Integration Command Resources	599
Quick Example	599
Defining Commands	602
Command Types and Attributes	603
Script Commands	603
URL Commands	604
Connector Commands	605
Adding and Editing Command Parameters	606
TRM CounterACT Connector Command Example	608
Using Configurations to Group Commands	610
Configurations Attributes	612
Configurations Contexts	613
How to Set Up Command Contexts	613
Configurations Commands	614
Adding a Command to a Configuration	615
Editing Commands in a Configuration	615
Removing Commands from a Configuration	615
Configuration Targets	615
Adding a Target to a Configuration	616
Editing Targets in a Configuration	616
Removing Commands from a Configuration	616
Specifying Targets	617
Target Attributes	617
Target Integration Parameters	618
Authorization and Authentication Settings	618
Setting User Login Parameters	619
Setting Login Credentials	619
Setting Login Credentials on Target Servers	619
Setting Logins and Other Parameters to Prompt for Values at Runtime	620
Access Control Lists (ACLs) on Integration Commands	621
Running Integration Commands	622
Entering/Saving Command Parameters at Runtime	622
Creating New Configurations On-the-Fly	623
Ready-Made ArcSight TRM Commands	623
Options for Up-Front or On-the-Fly Configuration	623
TRM Integration Commands	624

Enabling NSP TRM Commands	625
1. Set up the Command Targets	625
2. Set up the Command Configuration	626
3. Set up Users for TRM Access	626
Understanding NSP TRM Authentication	627
How to Get a TRM Authentication Token	627
Examples of Running TRM URL Commands	628
Attacker-Target Network Map	629
Investigate Node	629
Going Further with NSP TRM Command Results	630
ArcSight Logger Search Commands	630
Logger Integration Commands	631
Enabling Integrated Logger Searches	631
1. Set up Logger Command Targets	631
2. Set up the Logger Command Configuration	632
3. Set up Users for Logger Access	632
Example of Running a Logger Quick Search	633
Network Tools as Integration Commands	634
Chapter 24: Knowledge Base Authoring	637
Managing Knowledge Base Articles	637
Creating Knowledge Base Articles	637
Showing a Knowledge Base Article	638
Editing a Knowledge Base Article	638
Moving or Copying a Knowledge Base Article	638
Deleting a Knowledge Base Article	638
Managing Knowledge Base Article Groups	639
Creating a Knowledge Base Article Group	639
Renaming a Knowledge Base Article Group	639
Editing a Knowledge Base Article Group	639
Moving or Copying a Knowledge Base Article Group	639
Deleting a Knowledge Base Article Group	639
Getting Knowledge Base Updates	640
Refreshing the Knowledge Base Tree	640
Associating Knowledge Base Articles	640
Associating Resources with Knowledge Base Groups or Articles	640
Associating Grid View Elements with Knowledge Base Articles	640
Chapter 25: Managing Users and Permissions	641
Managing Users	641
Handling Users	641
Creating a User	641
Editing a User	643

Resetting User Passwords	643
Moving or Linking a User	644
Deleting a User	644
About the System User	645
Handling User Groups	645
Creating User Groups	645
Renaming User Groups	645
Editing User Groups	645
Moving or Linking User Groups	646
Deleting User Groups	646
Setting Startup Views	646
Managing Permissions and Resources	646
Editing Access Control Lists (ACLs)	646
Granting or Removing Resource Permissions	647
Granting or Removing Operations Permissions	649
Granting or Removing User Group Permissions	651
Granting or Removing Event Permissions	652
Granting or Removing Sortable Field Sets Permissions	654
Sharing Resources	656
Controlling Who Has Permissions to Deploy Data Monitors	656
How Upgrades Affect Data Monitor Deploy Permissions	658
Deployment Permissions on Imported Data Monitors	658
Managing Notifications	658
Managing Received Notifications	658
Managing Notification Groups and Levels	659
Creating Notification Groups	659
Renaming Notification Groups	660
Editing Notification Groups	660
Deleting Notification Groups	660
Adding Escalation Levels	660
Deleting Escalation Levels	660
Managing Notification Destinations	660
Creating Destinations	660
Editing Destinations	661
Moving or Copying Destinations	661
Deleting Destinations	661
Changing Notification and Acknowledgement Settings	662
Changing E-mail Settings	662
Adding New Pager Service Providers	663
Editing Pager Service Provider Settings	663
Deleting Pager Service Providers	663
Changing Wait Time Settings	663
Testing Notification Groups and Destinations	663

Testing Group Notifications	663
Testing Destination Notifications	664
Chapter 26: Managing Resources	665
Managing File Resources	665
Uploading Files and Creating a File Resource	666
Viewing Files	668
Downloading Files Locally	668
Editing File Resource Attributes	668
Replacing File Resource Contents	668
Deleting File Resources	668
Adding a File or Folder to a Package	669
Finding Files	669
Locking and Unlocking Resources	669
System Core Content	669
User Created Content	670
Unlocking a User-locked Resource	670
Selecting Resources	670
Finding Resources	671
Searching for System Resources	671
Search Field on Console Tool Bar	671
Query Options	673
Result Columns	673
Locating Specific Resources	674
Visualizing Resources	674
Graphing Resources	674
Using Graphs	675
Configuring Resource Graphs	676
Viewing Resources in Grids	677
Validating Resources	677
Valid and Invalid Resources	678
Fixing and Validating Resources	678
Troubleshooting (Requirements for Valid Resources)	680
Automatic and Manual Validation	682
Resource Validation During Upgrade	683
Extending Audit Event Logging	683
Saving Copies of Read-Only Resources	684
Common Resource Attribute Fields	684
Common	685
Assign	685
Parent Groups	685
Creation Information	686
Last Update Information	686

Managing Packages	686
Viewing Installed Packages	687
Viewing all Packages (with Dependencies)	687
Showing Package Archive Contents	687
Creating Packages	687
Importing Package Bundles	689
Exporting Packages	690
Installing Packages	690
Uninstalling Packages	691
Editing Packages	691
Adding Resources to Packages	691
Removing Resources from Packages	691
Deleting Packages	691
Resolving Package Conflicts	692
Chapter 27: Managing SmartConnectors	695
Selecting and Setting SmartConnector Parameters	695
Configuring the SmartConnector	695
Connector Editor Option Tabs	696
Connector Tab Configuration Fields	696
Default Content Tab Configuration Fields	697
SmartConnector Processing Categories	711
SmartConnector Time Interval Options	711
Managing SmartConnector Filter Conditions	712
Creating SmartConnector Filters	712
Adding SmartConnector Filter Conditions	712
Deleting SmartConnector Filter Conditions	713
Setting Special Severity Levels	713
Configuring a Conditional or Custom Severity Level	713
Sending Model Mappings to SmartConnectors	715
Sending Model Mappings to a Connector	715
Sending Control Commands to SmartConnectors	715
Getting Status Reports	715
Sending Flow-Control Commands	715
Managing SmartConnector Groups	722
Creating SmartConnector Groups	722
Renaming SmartConnector Groups	722
Editing SmartConnector Groups	723
Moving or Copying SmartConnector Groups	723
Deleting SmartConnector Groups	723
Managing SmartConnector Resources	723
Moving or Copying a SmartConnector Group	723
Deleting a SmartConnector Group	724

Importing and Exporting SmartConnector Configurations	724
Importing a SmartConnector Configuration	724
Exporting a SmartConnector Configuration	725
SmartConnector Filters	726
Upgrading SmartConnectors	726
Overview of the Upgrade Process	726
Upgrading SmartConnectors	728
Rolling back to a Previous Version	729
Troubleshooting	729
Getting Status and Versions on Installed SmartConnectors	729
Getting Status on a SmartConnector	729
SmartConnector Dashboards	730
Chapter 28: Modeling the Network	731
About the Network Model	731
Network Model	732
Assets	733
Asset Ranges	736
Zones	736
Networks	737
Asset Model	738
Locations	738
Vulnerabilities	738
Asset Categories	739
Populating the Network Model with Assets	740
ESM Console-Based Methods	741
Individually Using Network Modeling Resources	741
In a Batch Using the Network Modeling Wizard	741
SmartConnector-Based Methods	742
Automatically From a Vulnerability Scanner Report	743
ArcSight-Assisted Methods	743
As an Archive File From an Existing Configuration Database	743
Populating the Network Model Using the Wizard	744
Specifying CSV Column Types	744
Specify the Column Type Using a Header	745
Assign the Column Type in the Wizard	745
Zones CSV File Format	747
An Example of a Zones CSV File	748
Assets CSV File Format	748
An Example of an Assets CSV File	750
Static Addressing in a Dynamic Zone	750
Asset Ranges CSV File Format	750
An Example of an Asset Ranges CSV File	751

Increasing the Number of Rows Displayed	752
Summary of Data to Import	752
Network Data Imported into Manager	752
Auto-Zoning of Imported Assets	753
Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories	753
Managing Assets	754
Creating an Asset	754
Editing an Asset	755
Moving or Copying an Asset	755
Deleting an Asset	755
Showing Assets in a Channel	755
Auto Zoning an Asset	755
Managing Asset Groups	756
Creating an Asset Group	756
Renaming an Asset Group	756
Editing an Asset Group	756
Moving or Copying an Asset Group	756
Deleting an Asset Group	757
Asset Scalability	757
Viewing Assets in Active Channels	757
Finding Assets	757
Selecting Assets in the Common Conditions Editor	757
Managing Vulnerabilities	758
Vulnerability Editor	759
Creating a Vulnerability	759
Editing a Vulnerability	759
Moving or Copying a Vulnerability	760
Retrieving Vulnerable Assets	760
Adding an Asset to a Vulnerability	760
Deleting an Asset From a Vulnerability	760
Deleting a Vulnerability	760
Managing Vulnerability Groups	761
Creating a Vulnerability Group	761
Renaming a Vulnerability Group	761
Editing a Vulnerability Group	761
Moving or Copying a Vulnerability Group	761
Deleting a Vulnerability Group	761
Selecting Vulnerabilities in the Common Conditions Editor	761
Reporting on Output from Vulnerability Scanners	762
Reporting on Asset Vulnerabilities	763
Managing Zones	763
Managing Networks	764
Managing Asset Categories	764

Managing Locations	765
Managing Customers	766
Creating Customers	766
Editing Customers	766
Deleting Customers	766
Chapter 29: Managing Partitions	767
Getting Partition Information	767
Seeing a Partition Schedule	767
Archiving Partitions	768
Reactivating Archived Partitions	768
Reactivating Zipped or Large Archived Partitions	769
Deactivating Archived Partitions	769
Running Scheduled Tasks Right Away	769
Partition Properties	770
Chapter 30: Personalizing the ESM Console	771
Changing the Console Display	771
Resizing the Console	771
Showing or Hiding Menu Bars and Tools	771
Showing or Hiding the Status Bar	771
Showing or Hiding the Navigator Panel	771
Showing or Hiding the Viewer Panel	772
Showing or Hiding the Inspect/Edit Panel	772
Floating a Console Panel	772
Applying Translucency to a Console Panel	772
Docking a Console Panel	772
Closing a Console Panel	772
Changing User Preferences	772
Changing Your Password	773
Changing Other Users' Passwords	773
Setting Program Preferences	773
Changing Global Options Like Panel and Editor Characteristics	774
Setting Grid View Options	775
Setting Date and Time Formats	776
Configuring Event Graphs	777
Latitude and Longitude Options	777
Event Graph Options	778
Setting Notification Popups	779
Managing Hot Keys	779
Adding Shortcuts for Frequently Used Resources	779
Modifying a Custom Shortcut	781
Removing a Custom Shortcut	783

Activating a New Shortcut Schema	784
Sharing Custom Shortcut Schemas	785
Saving and Sending Settings	785
Saving a File	785
Saving a File to the ArcSight Manager	785
Loading a File From the ArcSight Manager	785
Sending a File by E-mail	786
Chapter 31: Reference Guide	787
Access Control Lists	787
Resource ACLs	787
Actions	788
Active Channels	788
Active Channel Views	789
Active Channel Headers	789
Comparisons	790
Active Channel Views for Assets and Cases	790
Active Lists	790
Uses of Active Lists	791
Active Lists for Long-Term State Retention	791
Optimize Data with Hash-Based Active Lists	792
Active List Audit Events	792
Active List Monitor Events	792
Active Lists with Values	793
Using Variables to Retrieve Data from Active Lists with Values	793
Example: Active List with Values to Store Directory Information	794
Working with Active Lists	796
Administrator	796
Advanced Editor	796
Aggregation	798
ArcSight Web	798
Assets	799
Assets Tab	799
Zones Tab	800
Networks Tab	800
Categories Tab	800
Vulnerabilities Tab	801
Locations Tab	801
Asset Auto-Creation	801
Creating Assets from a Vulnerability Scan Report	802
Creating Assets from a Vulnerability Scan Report for Static Zones	802
Creating Assets from a Vulnerability Scan Report for Dynamic Zones	802
Creating Assets for SmartConnectors	803

Creating Assets for SmartConnectors in Static Zones	804
Creating Assets for SmartConnectors in Dynamic Zones	805
Creating Assets for Network Devices	805
Creating Assets for Network Devices in Static Zones	806
Creating Assets for Network Devices in Dynamic Zones	807
Asset Names	807
Naming Assets from Scanner Events	807
Naming SmartConnector and Device Assets	808
Asset Auto-Creation Advanced Configuration Options	808
Asset Auto-Creation from Scanners in Dynamic Zones	808
Changing the Default Naming Scheme	810
Attack	811
Audit Events	811
Audit Event Categories	812
Resources (Configuration Events Common to Most Resources)	812
Active Channel	813
Active List	814
Actor	814
Authentication	815
Authorization	815
Connectors	816
Connector Connection	816
Connector Exceptions	816
Connector Login	817
Connector Registration and Configuration	817
Dashboard	817
Data Monitors	818
Last State Data Monitors	818
Moving Average Data Monitor	818
Reconciliation Data Monitor	818
Statistical Data Monitor	819
Top Value Counts Data Monitor	819
Domains (for Domain Fields)	819
Global Variables	819
Group Management	820
License Audit	820
Manager Activation	821
Manager Database Error Conditions	821
Manager External Event Flow Interruption	821
Notifications	822
Notification	822
Notification Acknowledgement, Escalation, and Resolution	822
Notification Testing	822

Pattern Discovery	823
Partition Archiver	823
Partition Manager	823
Query Viewers	824
Reports	824
Resource Quota	824
Rules	824
Rule Actions	824
Rule Activations	825
Rules Scheduled	825
Rule Firings	825
Rule Warnings	826
Scheduler	826
Scheduler Execution	826
Scheduler Scheduling Tasks	826
Scheduler Skip	827
Session Lists	827
Stress	827
Trends	828
Trends	828
Trend Partitions	828
User Login	828
User Management	829
Batching	829
Case Editor Tab Fields	829
Case Editor Events Tab	830
Case Editor Attachments Tab	831
Case Editor Final - Attack Agent Tab	831
Case Editor Final - Attack Mechanism Tab	831
Case Editor Final - Incident Information Tab	832
Case Editor Final - Other Tab	832
Case Editor Final - Vulnerability Tab	832
Case Editor Follow-Up Tab	833
Case Editor Initial - Attributes Tab	833
Case Editor Initial - Description Tab	834
Case Editor Initial - Security Classification Tab	834
Case Editor Notes Tab	835
Cases	835
Case Groups	836
Categories	836
Object Category	837
Behavior Category	839
Outcome Category	840

Device Group Category	841
Technique Category	841
Significance Category	843
Custom Event Categorization	844
Collaboration	845
Common Conditions Editor (CCE)	846
Editor Features	846
Condition Tree Command Buttons	848
Condition Tree Context Menu Commands	850
Adding Conditions	852
Search Box to Find Fields in the List	854
Field Comparisons with Variable or Static Values	855
Using Field Sets	855
Adding or Removing Global Variables Using the CCE	857
Testing for Zone Relevance	858
How to Create a Matching or Join Rule	859
Conditional Statements	859
ArcSight Variables	860
Conditions	860
Parameterized Conditions	860
ESM Console	862
Content	862
Content Packages	862
Custom Content	863
SmartConnector Content	863
Correlation	863
Correlation Rule	863
Customers	864
Dashboards	864
Dashboard Context Menu Commands	864
Database	865
Schema Design	865
Event Fields	865
More Efficient Field Usage	866
Precise Event Categorization	866
Data Fields	867
Connector Group	867
Attacker Group	870
Category Group	873
Destination Group	874
Device Group	877
Device Custom Group	880
Event Group	882

Event Annotation Group	886
File Group	889
Final Device Group	890
Flex Group	892
Manager Group	893
Old File Group	893
Original Connector Group	894
Request Group	896
Source Group	897
Target Group	900
Threat Group	903
Resource Attributes	904
Geographical Attributes	905
Data Monitors	905
Asset Category Count Data Monitor	906
Event Correlation Data Monitor	907
Event Graph Data Monitor	908
Event Reconciliation Data Monitor	909
Correlation-Event-Generating Fields	911
Geographic Event Graph Data Monitor	912
Hierarchy Map Data Monitor	913
Feature Enhancements	913
Use Cases	914
Defining a Hierarchy Map Data Monitor	914
Adding Variables	916
Specifying the Source Node Identifiers	916
Specifying Group Attributes	917
Hierarchy Map Display and Visualization Controls	918
Hourly Counts Data Monitor	922
Last <i>N</i> Events Data Monitor	923
Last State Data Monitor	924
Options for Table and Tile Views	926
Moving Average Data Monitor	928
Rules Partial Match Data Monitor	931
Session Reconciliation Data Monitor	931
Statistics Data Monitor	933
System Monitor Data Monitor	936
System Monitor Attribute Data Monitor	936
Top Value Counts Data Monitor	937
Data Monitor Expressions	938
Supported Data Monitor Expression Operators	939
Supported Data Monitor Expression Functions	939
Device	940

Event Inspector	940
Field Sets	940
Events	941
Field Sets	942
Filters	942
Filtering Options	943
Global Variables	943
Grid View	944
iDefense	944
Inspect/Edit Panel	945
Job Scheduler	945
Knowledge Base	946
Logical Operators	947
Managed Security Service Providers (MSSPs)	948
Manager	948
Navigator Panel	948
Notifications	949
Notification Operation	949
Testing Notification Escalations	950
Notification Destinations	950
Notification Acknowledgements	951
Packages	951
Partitions	951
Pattern Discovery	952
Pattern Concepts	953
Discovering Patterns	953
Pattern Analysis	953
Initial Phase	954
Routine Pattern Processing	954
Workflow Management	954
Pattern Analysis	954
Pattern Disposition	954
Pattern Expertise	955
Workflow	955
Visualization	955
Applications	956
Payload	956
Prioritization Fields	956
Priority Calculations and Ratings	957
Priority Elements	959
Priority Operators	960
MaxValue Attribute	960
Weight Attribute	960

Priority Rating	960
Queries	961
Queries and Trends	962
Building and Running Queries	962
Query Viewers	962
Reference Pages	962
Reports	963
Working with Report Templates, Queries, and Trends	963
Viewing and Managing Reports	963
Archived Reports	964
Report Groups	964
Delta Reports	964
Report Parameters	965
Running Reports	965
ArcSight-Provided Reports	965
Report Templates	966
Resources	967
Valid and Invalid Resources	967
Fixing and Validating Resources	967
Troubleshooting (Requirements for Valid Resources)	969
Automatic and Manual Validation	970
Resource Attributes	970
Rule Actions	972
Active List Rule Actions	972
Execute Connector Command Rule Actions	972
Rule Conditions	973
Rules	974
Rules Processing and Correlation	974
Rule Groups	976
Scheduled Rules	976
Rule-triggering Timing	976
Rule Chains	977
ArcSight Variables	977
Rules Editor	977
Scheduling Jobs	977
To schedule a job	978
To view all scheduled jobs	979
Troubleshooting Tips	979
Schema	979
Avoiding Field Naming Collisions	979
Send Logs	980
Guidelines for Using the Send Logs Utility	981
Options for Running Diagnostics and Sending Logs	981

Starting the Send Logs Wizard on the ESM Console	981
Session Correlation	983
Why Session Correlation Matters	983
Session Lists	983
SmartConnectors	984
Operational Status	984
Configuration	985
Zones	985
Upgrading	986
Filtering	986
SMTP	986
Sortable Field Sets	987
Using Sortable Columns in Grid Views	988
Status Monitor Events	988
Active Channel Statistics	988
Active List Statistics	989
Asset Statistics	990
Data Monitor Statistics	991
Event Broker Statistics	991
Filter Engine Statistics	992
Main Flow Statistics	992
Notification Statistics	992
Pattern Discovery Statistics	993
Report Statistics	993
Resource Framework Statistics	993
Rules Engine Statistics	994
Session List Statistics	995
Session Management Statistics	996
Side Table Statistics	996
SmartConnector Flow Statistics	998
Templates	999
Threat	999
Threat Evaluation	999
Evaluation Process	999
Evaluation Definitions	1000
Maintaining Model Confidence	1000
Using Threat Evaluation Information	1001
Limitations and Workarounds	1001
Thresholds	1001
Time Error Correction	1002
Timestamps	1002
Security Events	1002
Resources	1002

General Information	1002
Timestamp Variables	1003
Inclusive Timestamps	1003
Time Zone Correction	1003
Trends	1004
Understanding Trends and Queries	1004
Building Trends	1004
Upgrade SmartConnectors	1004
User Groups	1005
Users	1005
User Types	1006
Variables	1006
Local and Global Variables	1008
Variable Definition Fields	1009
Variable Functions	1009
Alias Functions	1010
Arithmetic Functions	1010
Category Model Functions	1012
Condition Functions	1012
Group Functions	1013
IP Address Functions	1014
List Functions	1014
String Functions	1014
Timestamps	1015
Type Conversion Functions	1016
Variable Availability and Contexts	1019
Velocity Templates	1019
Velocity Application Points	1020
Using Velocity Expressions to Retrieve Values from Event Fields or Variables	1021
Retrieving Values from Event Fields	1021
Using Variables in a Velocity Expression	1021
Using Velocity Expressions in Rule Actions	1022
Example of Rule Action that Uses Velocity Expressions to Retrieve Values	1022
Examples	1022
Usage Tips	1023
Velocity References for Reports	1023
Views	1028
View Types	1028
Other Views	1029
Dashboards	1029
Vulnerabilities	1029
Vulnerability Groups	1029
Standardized Vulnerability Tracking	1030

Web Browsers (Internal and External)	1030
Browser Preferences for HTML Displays	1030
Browser Preference Overrides for Specific Features	1030
External Browser Display Requirements	1031
Internal Browser Display Support	1031
Flash Plug-in and Setup Requirements for Internal Browser	1032
Index	1033

Chapter 1

What's New

ArcSight™ Enterprise Security Management (ESM) consolidates and normalizes data from devices and applications across your enterprise network in a centralized view. ArcSight ESM provides a comprehensive view of the security status of all relevant IT systems, and integrates security into your existing management processes and work flows to provide “forensics on the fly.” ESM provides solutions for compliance automation, identity monitoring, event collection and management, multi-variable correlation and pattern-matching, historical reporting, alert and frequency threshold notification, and more.

This topic describes the new features and enhancements added in this release, and explains where to find more information.

Oracle 11G Support

ESM v5.0 SP2 introduces Oracle Database 11g Release 2 for fresh installations, which supports upgrading from existing Oracle 10g on all supported platforms.

See the *ESM Installation and Configuration Guide*.

Standard Content

ESM v5.0 SP2 includes new and updated standard content packages.

- The ArcSight Administration Foundation Package monitors the function of ArcSight components. It now has updated Connector-Monitoring content, which includes connection and caching status for SmartConnectors.

In the *ESM Administrator's Guide*, see Appendix H, “Monitoring System Health” and find the topic “ESM Content Configuration” > “Configure Connector Monitoring Resources.”
- The NetFlow Monitoring Foundation Package leverages NetFlow session-level data to monitor and report on top bandwidth usage by source, destination and port.

The *NetFlow Monitoring Guide* is available for download from the ArcSight Customer Support site.

Chapter 2

Getting Started

ArcSight™ Enterprise Security Management (ESM) is a comprehensive software solution that combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. It consolidates and normalizes data from disparate devices across your enterprise network in a centralized view.

[“Quick Start Tools and Content” on page 43](#)

[“Network Model Wizard” on page 44](#)

[“Configuration and Using Standard Content” on page 44](#)

[“ArcSight Express” on page 45](#)

[“ArcSight Web” on page 46](#)

Quick Start Tools and Content

The ESM Console serves as the control point for administrators to configure content and resources, set up [ArcSight Web](#) access for Web users, and to manage, monitor, and respond to network security issues across the enterprise.



Use this information to better understand the ESM Console's features, layout, tasks, and key-concept details.

To learn more about other ArcSight publications, choose **Browse ArcSight Documentation** on the ESM Console's Help menu. If you are new to ESM, or would like to get hands-on experience with new and key features, please refer to the **ESM Reviewer's Guide**, which is also available on the Browse ArcSight Documentation page. The ESM Reviewer's Guide provides a thorough introduction to new and key features, along with examples of common authoring and monitoring tasks.

A [Network Model Wizard](#) is provided to facilitate the process of describing network devices and assets.

Also, a set of coordinated *Resources* (filters, rules, dashboards, reports, and so on) is provided to address common security and management tasks. [Standard Content](#) and [ArcSight Express Solutions](#) are designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box, with minimal configuration required on the ESM Console.

To get started using [ArcSight Express](#), see [“Getting Started Configuring ArcSight Express” on page 45](#).

- To get started, see [“Configuration and Using Standard Content” on page 44](#).
- To get started using [ArcSight Express](#), see [“Getting Started Configuring ArcSight Express” on page 45](#).

Network Model Wizard

The Network Model wizard enables you to quickly populate the network model by loading asset and zone information from Comma Separated Values (CSV) files. The following data can be imported into a Manager from CSV files:

- **Zones** define functional parts of a network, such as a wireless LAN, an engineering network, a VPN or a DMZ.
- **Assets** represent individual nodes on the network, such as servers and routers.
- **Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops.

For more about the Network Model wizard and instructions how to use it, see [“Populating the Network Model Using the Wizard” on page 744](#).

Configuration and Using Standard Content

For a complete guide to standard content (pre-packaged reports, rules, filters, channels, data monitors, and so on), refer to [Chapter 3, Standard Content, on page 47](#).

Configuration involves these tasks:

- 1 [“Set Up Connectors and Model the Network” on page 52](#). Modeling the network includes establishing event feeds into the Manager from SmartConnectors, setting up assets, zones, and networks for your key devices, and applying key asset categories used by your resources.
- 2 [“Apply Standard Asset Categories to Assets” on page 54](#). Applying categories to assets provides more information to the Manager about the criticality and business context of assets. Using categorization optimizes monitoring to the specifics of your enterprise.
- 3 [“Configure Notification Destinations” on page 55](#). Add notification information for users, such as e-mail addresses, contact numbers, and hours of availability.
- 4 [“Configure Asset Auto-Creation Filters” on page 56](#). Use predefined filters to make sure assets are accurately defined in the system.
- 5 [“Configure Rules to Send Notifications and Open Cases” on page 62](#). Configure key correlation rules that drive the notifications and case creation actions that communicate potential security risks to security operations personnel.
- 6 [“Schedule Reports” on page 64](#). Schedule reports that you want to make a central part of your regular reporting plan.
- 7 [“Default Trends Schedule” on page 64](#). Trends are special queries that can gather data over longer periods of time that can be leveraged for reports. For long-range queries such as end-of-month summaries, trends greatly reduce the burden on system resources.
- 8 [“Getting Started Using Standard Content” on page 67](#). Executive summaries, operational summaries, and other types of content summaries based are available as out-of-the-box, standard content. Using the tools and resources in ArcSight

Foundation content, you can get started right away monitoring, analyzing, and investigating network activity.



ArcSight Express

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

ArcSight Express is made up of the following components:

ArcSight Manager	Provides correlation and analytics
ArcSight Logger	Provides long-term storage for historical search and investigation.
ESM Console	The interface through which an administrator sets up ArcSight Express user accounts, and configures and tunes the content.
ArcSight Web	The ArcSight Web client is the primary interface for ArcSight Express users, providing access to daily security operations.

The administrator adds the ArcSight [SmartConnectors](#) required for the devices in your network to gather [Events](#).

ArcSight Express also comes with a series of coordinated [Resources](#) (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. ArcSight Express content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration using the Console.

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

Getting Started Configuring ArcSight Express

Configuring ArcSight Express involves the following tasks:

- 1 [Network Modeling](#). Modeling the network includes establishing event feeds into ArcSight Express from SmartConnectors, setting up assets, zones, and networks for your key devices, and applying key asset categories used by ArcSight Express content.
- 2 [Create ArcSight Express Users](#). Set up user accounts for the users who will access the ArcSight Express solution using the ArcSight Web.
- 3 [Configure Notification Destinations](#). Add notification information for users, such as e-mail addresses, contact numbers, and hours of availability.
- 4 [Configure Rules to Send Notifications and Open Cases](#). Configure key correlation rules that drive the notifications and case creation actions that communicate potential security risks to security operations personnel.

- 5 [Schedule Reports](#). Schedule reports that will be a central part of your regular reporting plan.
- 6 [Tuning ArcSight Express Content](#). After some use and testing, you may want to exclude certain devices or user scenarios from rule evaluation if they are part of a benign regular usage pattern in your environment.

ArcSight Express Documentation

- For complete instructions about how to configure the ArcSight Express content, see [“ArcSight Express Solution” on page 73](#).
- For instructions about installing and setting up the ArcSight Express appliance, see the *ArcSight Express Configuration Guide*.

ArcSight Web

[ArcSight Web](#) provides full event monitoring and drill-down capabilities in a streamlined interface. The Web server is pre-installed on the appliance.

The ArcSight Web interface can also be branded with your company logo.

Chapter 3

Standard Content

This ArcSight product comes with a series of coordinated resource systems that address common enterprise network security and management tasks. These resource systems are referred to collectively as *standard content*.

With some basic configuration, standard content enables you to get started right away to effectively manage enterprise security operations without having to create additional resources. This topic describes the standard content and provides instructions for administrators about how to configure it using the ArcSight Console.

- [“What is Standard Content?” on page 47](#)
- [“Standard Content Foundations” on page 48](#)
- [“Standard Content Packages” on page 51](#)
- [“Navigating to Standard Content” on page 51](#)
- [“Set Up Connectors and Model the Network” on page 52](#)
- [“Apply Standard Asset Categories to Assets” on page 54](#)
- [“Configure Notification Destinations” on page 55](#)
- [“Configure Asset Auto-Creation Filters” on page 56](#)
- [“Configure Rules to Send Notifications and Open Cases” on page 62](#)
- [“Schedule Reports” on page 64](#)
- [“Default Trends Schedule” on page 64](#)
- [“Getting Started Using Standard Content” on page 67](#)

What is Standard Content?

Standard content is a series of coordinated Resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration.

The content provided by ArcSight provides a full spectrum of security, network and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

The standard content is organized into functional groups called foundations. For more about the foundations, see the next topic, [“Standard Content Foundations” on page 48](#).

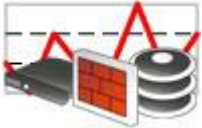


The standard content is installed using a series of packages, some of which are installed automatically with the Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.



Standard Content Foundations

Each foundation is a coordinated system of resources that provides real-time monitoring capabilities for its area of focus, as well as after-the-fact analysis in the form of reports, trends, and trend reports.

You can extend these foundations with additional resources specific to your needs, or you can use them as a template for building your own resources and tasks.

Several of the foundations rely on a series of common resources that provide core functions for common security scenarios. Resources that manage core functions are **locked** to protect them from unintended change or deletion.

Foundation	Description
Configuration Monitoring Foundation	 <p>The Configuration Monitoring foundation identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. Configuration monitoring is concerned mainly with monitoring hosts and user accounts for configuration-related activity, such as installing new applications, adding new systems to the network, anti-virus/network scanner/IDS engine and signature updates, and asset vulnerability postures.</p> <p>The configuration monitoring foundation helps you monitor how your networks change over time, measure daily statistics, understand the changes made, and know who's making them. Trends help you know what is normal and spot anomalies that should be investigated.</p>
Intrusion Monitoring Foundation	 <p>The focus of the Intrusion Monitoring foundation is to identify hostile activity and take appropriate action. This foundation provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting. As with previous releases, the essential security monitoring functions of the Intrusion Monitoring foundation make up the bulk of the standard content.</p> <p>The Intrusion Monitoring foundation targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and so on.</p>
Network Monitoring Foundation	 <p>The Network Monitoring foundation monitors the status of network throughput and network infrastructure.</p> <p>This foundation provides statistics about traffic and bandwidth usage that helps you identify anomalies and areas of the network that need attention.</p>

Foundation	Description
ArcSight Workflow Foundation	 <p>The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking using the incident response system.</p> <p>Qualifying events in the other foundation packages trigger notifications and cases that get escalated through the incident response stages.</p>
ArcSight Administration Foundation	 <p>The ArcSight Administration foundation provides statistics about the health and performance of ArcSight products. This foundation is installed automatically, and is essential for managing and tuning the performance of content and components.</p>

ArcSight System Content



The ArcSight System content consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.

System Function	Description
Internal ESM function	The system content contains sets of resources that manage network modeling, vulnerability handling, and other internal functions. These resources are leveraged by many basic systems and correlation tasks.
Correlation evaluation	System content rules, active lists, and filters help drive parts of the correlation engine, such as priority formula calculations and basic out-of-the-box event processing.
Security center operations and monitoring	The system content provides standard field sets and active channels to provide basic operations and monitoring functions.
Benchmarking and analysis	There are several benchmarking and analysis tools as add-on modules. Included as part of the system content, are two basic Pattern Discovery profiles. These profiles are active only if you have Pattern Discovery installed.

This content is installed automatically so that these functions and the infrastructure that supports them are immediately available. To safeguard against accidental damage or deletion, these resources are locked (read and write protected).

The core content infrastructure also serves the systems and solutions you deploy, and content you create yourself.

The diagram below shows system content usage.

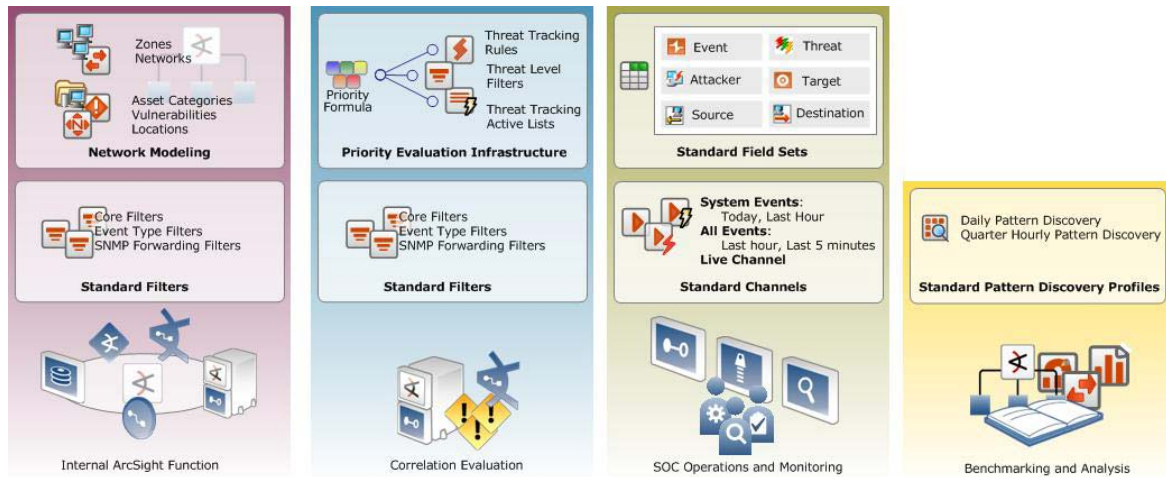


Figure 3-1 The standard features included in the core content support basic functions, such as network modeling, correlation, basic monitoring, and benchmarking.

Shared Resources



Common resources that support the five foundations are delivered in their own packages. Dependencies between these resources and the foundation packages they support are managed by the Package resource.

Anti-Virus

The Anti-Virus content is a set of filters, reports, and report queries used by other foundations, such as Configuration Monitoring and Intrusion Monitoring.

Conditional Variable Filters

The Conditional Variable Filters are a library of filters used by variables in standard content report queries, filters, and rule definitions. They express conditions that can also be used by any content in any package.

The Conditional Variable Filters are used by other standard content foundations, such as Anti Virus, Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow foundations.

Network Filters

Network filters are a set of filters required by other standard content foundations, such as Intrusion Monitoring and Network Monitoring. The Network Filters package is installed automatically.

Standard Content Packages

Standard content comes in a series of packages that are either installed automatically or presented as an install-time option. The following graphic outlines the packages and demonstrates their interoperability.

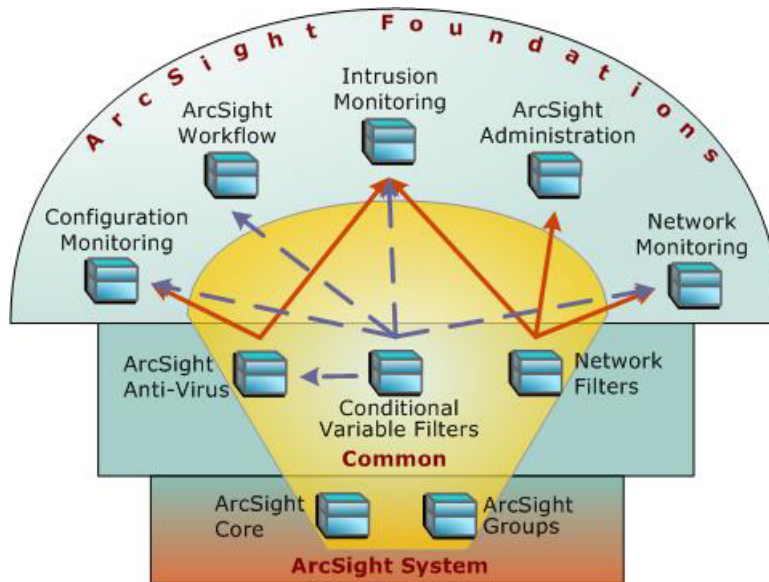


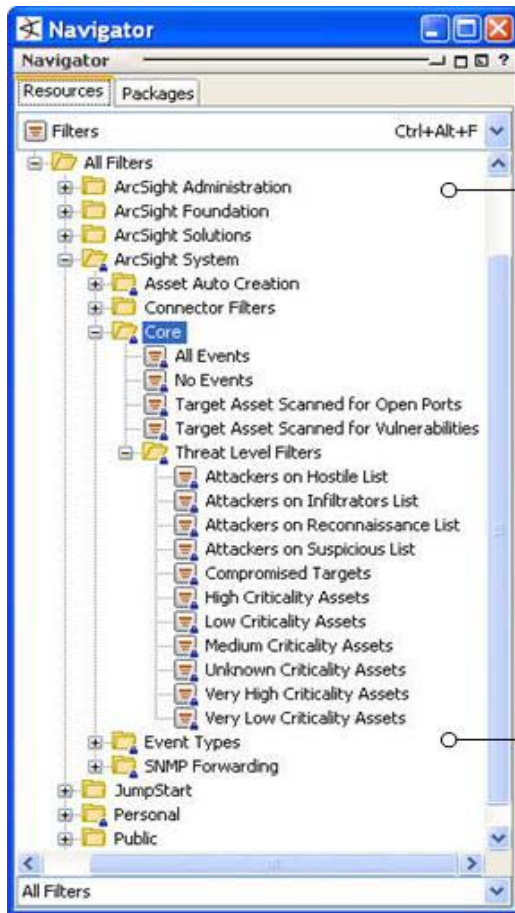
Figure 3-2 The ArcSight System packages at the base provide core content required for ArcSight operation. The Common packages in the center contain shared resources that support the foundation packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you select, you will see the ArcSight System resources and some or all of the other package content.

Navigating to Standard Content

Standard content consists of just about every kind of resource available. If you look in any resource menu, you will find standard content. The example below shows the Core filters in

the ArcSight system tree, and describes the standard content groups that are present when all the standard content is installed.



Standard Content

Standard content is presented in a series of groups that describe what they do.

Administration deals with administrative functions.

Foundation presents a series of coordinated resources that address fundamental security concerns, such as intrusion monitoring, configuration monitoring, and network monitoring.

Solutions holds a space for ArcSight solution packs that address specific business cases. Solution packs are available separately.

System supplies a series of resources that are used by the essential function of ArcSight correlation and network modeling.

Figure 3-3 Every resource in the resource menu contains standard content, a coordinated set of resources that address common security scenarios and facilitate basic functions. This sample shows the Core filters in the ArcSight System group in the Filters branch.

Set Up Connectors and Model the Network

The graphic below outlines the process for establishing the feeds necessary to drive the standard content:

- 1 Establish relevant SmartConnector feeds
- 2 Model the network
- 3 Assign networks to the appropriate SmartConnectors

4 Test feeds and configure content

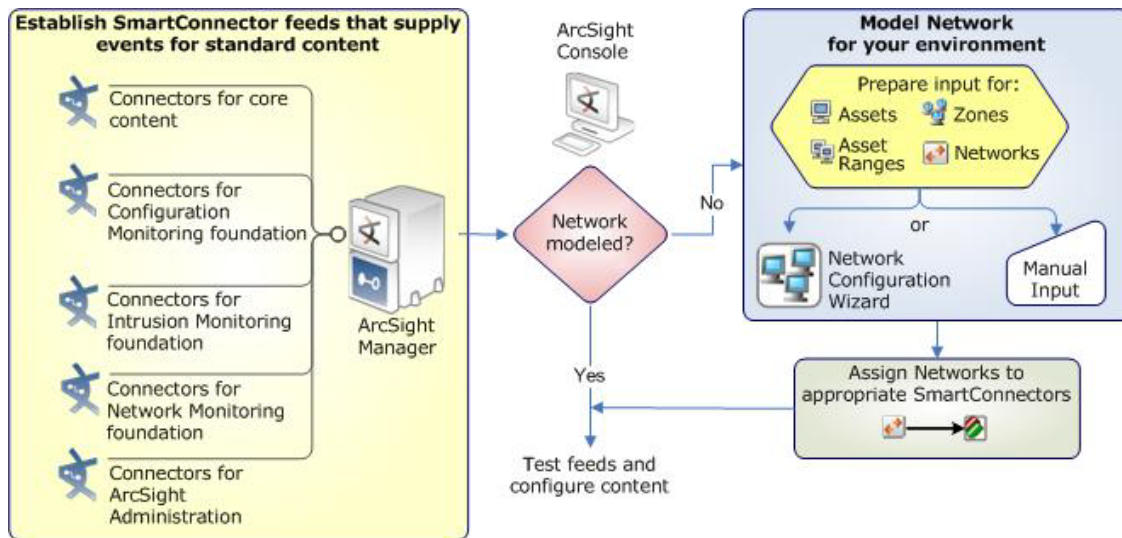


Figure 3-4 Configuring standard content starts with installing SmartConnectors and configuring zones and networks for devices that report to the Manager.

Standard Content-Related SmartConnectors

The standard content is designed to address event throughput, network health, and basic security-related scenarios. Depending on which packages you installed, verify that you have the minimum types of SmartConnectors reporting into the Manager.

Package	Device Types
Anti-Virus (required by Configuration and Intrusion Monitoring foundations)	Anti-virus software, such as: <ul style="list-style-type: none"> • Symantec EndPoint Protection • TrendMicro • McAfee AV
Configuration Monitoring	<ul style="list-style-type: none"> • Operating systems • Security applications (network and host-based IDS, anti-virus) • User management services (authentication, authorization, and accounting services) • Basic network devices (firewalls, routers, switches, VPN)
Intrusion Monitoring	<ul style="list-style-type: none"> • Network and host-based IDS • Intrusion Prevention Systems (IPS) • Anti-virus • Firewalls
Network Monitoring	<ul style="list-style-type: none"> • Routers • Firewalls • Switches • Real-time flow monitor

Network Modeling

A network model keeps track of the network nodes participating in the event traffic. Having your network modeled and critical assets categorized using the standard asset categories is what activates much of the standard content and makes it effective.

There are several ways to model your network, including the Network Modeling Wizard. If you are modeling the network using the Network Modeling wizard, review the next topic [“Apply Standard Asset Categories to Assets” on page 54](#) before creating the comma-separated values lists to load into the network model.

For more about the network model and how to populate it, see [Chapter 28, Modeling the Network, on page 731](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 744](#).

To learn more about the architecture of the ESM network modeling tools, see Chapter 4, “ArcSight Network Model” in *ArcSight 101*.

Apply Standard Asset Categories to Assets

Once your network model is populated with assets, apply the standard asset categories to them to activate standard content that uses these categories to apply criticality and business context to events. Asset categories can be assigned individually using the Asset editor, or in a batch using the Network Modeling wizard.

The asset categories most essential for engaging ESM standard content are discussed in this topic.

For more about asset categories and instructions about how to apply them using the Console tools, see [“Asset Categories” on page 739](#).

For more about the Network Modeling wizard, see [“Populating the Network Model Using the Wizard” on page 744](#).

Categorize Internal Assets

Internal Assets are considered to be assets inside the company network. Assets that are not categorized as specifically internal to the network are considered to be external. This includes assets with different asset categories, and those that are not categorized at all (such as external web sites, unknown external hosts, and so on).

For all assets that are internal to the network, classify them in the following asset category:

```
/All Asset Categories/Site Asset Categories/  
Address Spaces/Protected/
```

Determine the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

In general, assets do not inherit the categories applied to the zone to which they belong. However, any address contained in the Private Address Space Zones is categorized as *Protected*. For example, an asset with an IP address of [192.168.0.1](#) is not automatically

categorized as *Protected*, however, because it belongs to one of the Private Address Spaces zones, it is considered *Internal* because it belongs to a zone that is categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

Categorize Critical Assets

The asset categories most essential to basic event processing are those used by the Priority Formula to calculate an event's criticality. Asset criticality is one of the four factors used by the priority formula to generate an overall event priority rating.

Assets that are considered critical to protect, such as those that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations, should be classified as critical assets using the following criticality asset category:

[/All Asset Categories/System Asset Categories/Criticality/High](#)

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, see [“Priority Calculations and Ratings” on page 957](#).

Configure Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, the notifications are disabled in the standard content rules, so the admin user will need to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in standard content rules, see [“Configure Rules to Send Notifications and Open Cases” on page 62](#).

The standard content rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center.

- 1** In the Navigator panel, go to **Notifications > Destinations > Shared > All Destinations > CERT Team**.
- 2** Right-click **Level 1** and select **New Destination**.
- 3** In the Destination Editor, enter the following values in the Attributes tab and click **OK**:

Field	Value
Name	Enter a name for the destination, such as the user name of the contact; or the role, such as Investigator or Manager.
Start/End Time	If applicable, enter the start and end times of the period this person is available, for example, Start: 08:00:00 AM; End: 04:59:59 PM.

Field	Value
Destination Type	<p>From the drop-down menu, select the method by which the notification will be delivered:</p> <ul style="list-style-type: none"> • Console — Notification popup in this user's ArcSight account • E-Mail — User's e-mail account • Pager — User's pager. Enter the pager's PIN number and service provider. • Cell Phone — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.
User/Group	<p>From the drop-down menu, select the individual user or user group who will receive the notification. This field is required if you selected Console as the destination type, or if you want to use the contacts specified in the User's profile.</p>

- 4 Repeat steps 1, 2, and 3 for each escalation level you want to add. Add more escalation levels as needed.
- 5 Repeat steps 1, 2, 3, and 4 for the SOC Operators destination (**Notifications > Destinations > Shared > All Destinations > SOC Operators**).

Configure Active Lists

The ArcSight System content includes active lists that are designed to be populated manually with data specific to your environment. Once populated with values, these lists are cross-referenced by active channels, filters, rules, reports, and data monitors to give ESM more information about the assets in your environment. For details about active lists and how they work, see *ESM 101* and the topic *Active Lists* in the online Help.

The active lists that should be configured are **Trusted/Untrusted** active lists in ArcSight System (Lists | Active Lists | [All Active Lists/Arcsight System/Attackers](#)).

The ArcSight System content also includes active lists that are populated automatically during run-time by rules. These active lists do need not to have entries made to them manually before being used. You can, however, add manual entries to these lists.

You can manually add entries to active lists two ways:

- One by one using the Active List editor in the ArcSight Console. For instructions, see the topic *Editing Active List Entries* in the Console Help.
- In a batch by importing values from a CSV file. For instructions, see the topic *Importing an Active List* in the Console Help.

Configure Asset Auto-Creation Filters

A standard feature is automatic creation of assets in the ArcSight asset model for events whose devices are not already modeled either manually or using an asset scanner.

Depending on what devices you have reporting to ArcSight and what devices report in to your network, however, this can cause more individual assets to be added to your asset model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, ESM would model a new Connector, which falsely adds Connector nodes to the network model.

To limit how models are automatically modeled in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

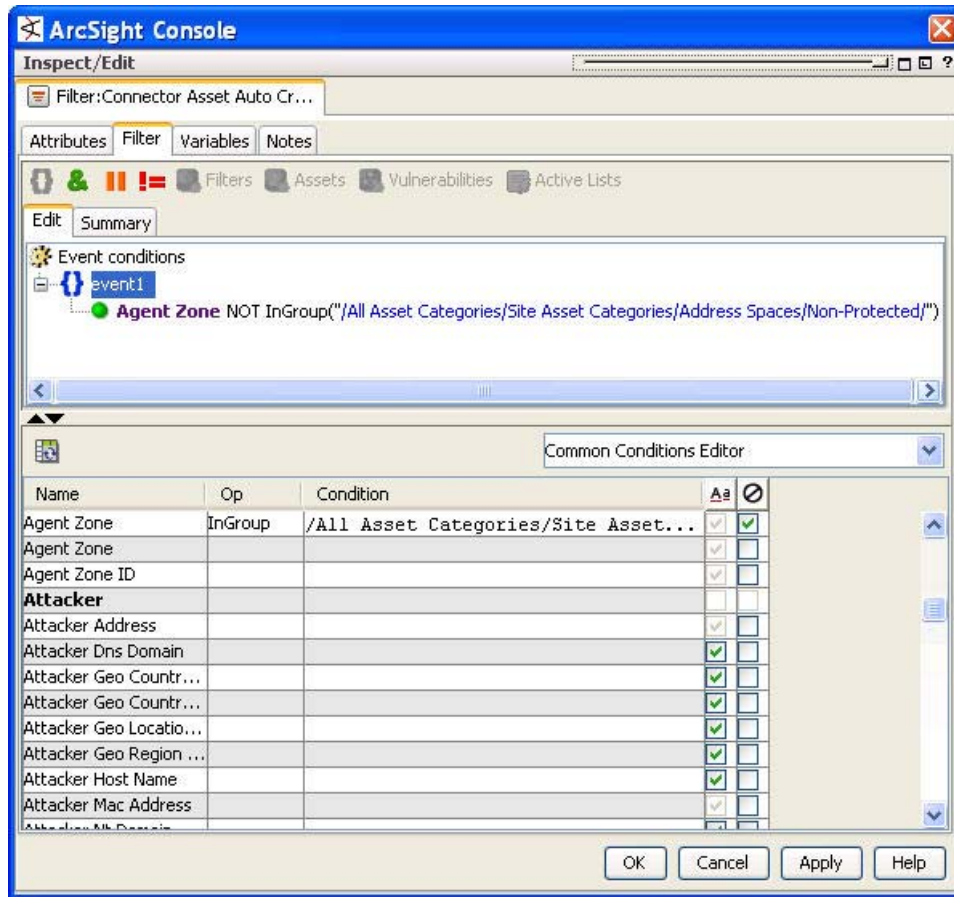
Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs the creation of an asset for network nodes represented in the events received from the SmartConnectors present in your environment.

By default, the *Connector Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to exclude connectors from a specific zone, such as a VPN zone, where the asset already exists, but traffic is coming into the network from an alternate VPN interface. You can also exclude traffic from different types of Connectors, such as from a particular device and vendor.

The example below shows the *Connector Asset Auto Creation Controller* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.

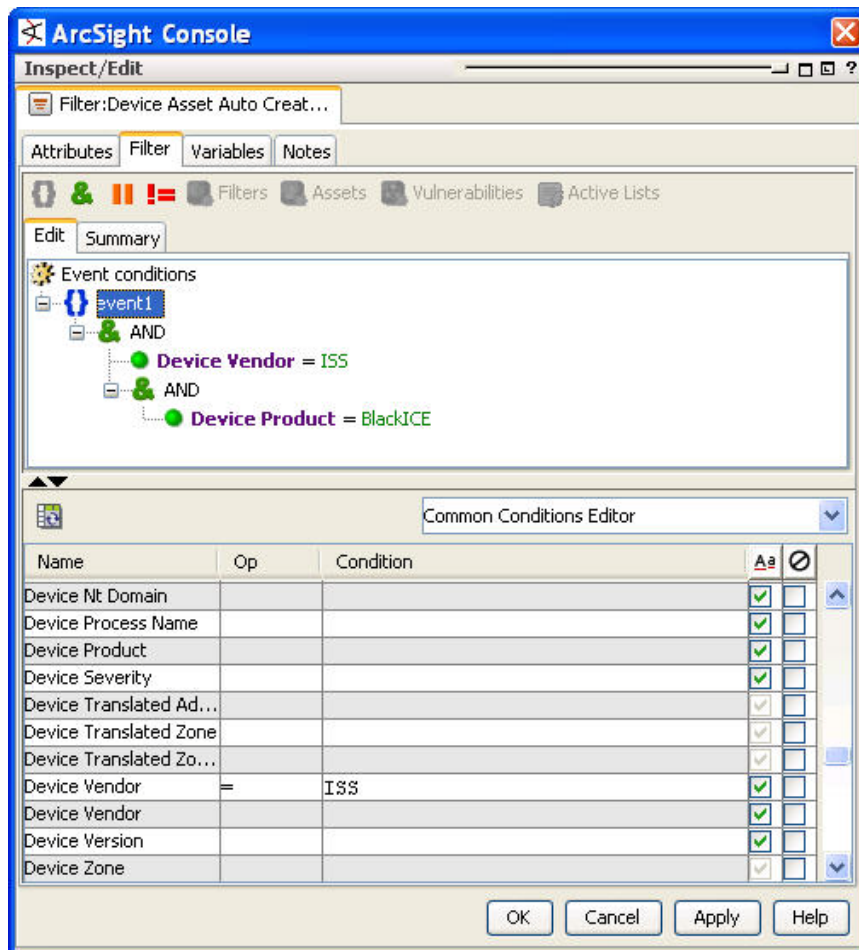



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.
- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊘).
- 7 Repeat from [Step 3](#) to [Step 5](#) for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.

Configure Device Asset Auto Creation Controller Filter

By default, the *Device Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify traffic from specific devices and device vendors, or event categories, such as **Hostile**. When you specify an event category, the filter directs the system to only create assets for events with this severity.

The example below shows the *Device Asset Auto Creation Controller* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 Select **event1** and add an AND operator (click the AND icon .
- 4 Select **event1** and use the event fields grid to build the condition, or right-click event1 and select **New Condition**. Navigate to **Device > Device Vendor**. In the Condition field, enter the vendor name, in this case **ISS**.
- 5 Add the device vendor and product you wish to include.

- a** If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to Device > Device Product. In the Condition field, enter the device name, in this case **BlackICE**.
- b** If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to Device > Device Product. In the Condition field, enter the device name.

For example, the condition would look like this:

OR

```
AND
    Device Vendor A
    Device Product 1
AND
    Device Vendor B
    Device Product 2
AND
    Device Vendor C
    Device Product 3
```

- 6** Repeat from [Step 3](#) through [Step 5](#) for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7** Click **OK** to apply changes and close the Filter editor.

Configure SNMP Trap Forwarding Filter

If you do not have SNMP traps enabled, you can skip this section and move on to [“Configure Rules to Send Notifications and Open Cases” on page 62](#).

The System filters group contains an SNMP Trap Sender filter ([All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#)). The SNMP Trap Sender filter only needs to be configured if you have the SNMP Trap Sender enabled to forward events through SNMP to a network management system, such as HP Openview.

By default, this filter is configured with the filter [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#). If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events will be trapped and forwarded to the network management system.

To configure this filter to forward certain events as an SNMP trap, you can do either of the following:

- Change the default condition in the SNMP Trap Sender filter so it expresses which events should be forwarded as traps. You can express this condition directly in the SNMP Trap Forwarding filter, or you can create another filter that expresses these parameters and point to it in the SNMP Trap Sender filter.
- Change the server configuration (via [server.properties](#)) to point the SNMP trap sender to another filter, and set that filter up as per your convenience.

Change Default Condition in SNMP Trap Forwarding Filter

- 1** In the Navigator panel, navigate to [All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#). Double-click the filter or right-click and select **Edit** to open it in the Filter editor in the Inspect/Edit panel.
- 2** At the Filter tab, change the default condition [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#) to list the type(s) of

events you want forwarded, or to point to another filter that expresses these parameters.

For example, you can create a filter that specifies all events with a priority greater than 8, or events from all Top Secret systems.

Change SNMP Trap Sender in `server.properties`

If you wish to use a filter other than the default `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender`, you must point the SNMP trap sender to the new filter in the ESM Manager `server.properties` file.



Note

These instructions apply **only** if you have SNMP forwarding already enabled at the Manager, *and* if you are using a filter other than the default SNMP Trap Sender filter to forward events.

If the SNMP forwarding feature is not already enabled at the Manager, the `server.properties` file will not contain the string that needs to be modified.

- 1 On the ArcSight ESM Manager machine at a command line, stop the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager stop`
 - ◆ Windows: Stop the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu
- 2 Make a backup copy of the file `$ARCSIGHT_HOME/config/server.properties`.
- 3 In a text editor, open the file `$ARCSIGHT_HOME/config/server.properties` and look for the following lines:

```
# -----
# SNMP Trap Sender configuration.
# -----
# Configuration for the SNMP trapsender. Copy these properties into
# your server.properties file and remove the '#'s (comments). By
# default, the SNMP trap sender is disabled.
#
# set the following property to true to enable trap sending
snmp.trapsender.enabled=false

# Filter that determines what arcsight events will be sent out as
# traps
snmp.trapsender.uri=/All Filters/ArcSight System/SNMP
Forwarding/SNMP Trap Sender
```

- 4 Change the `snmp.trapsender.uri` from `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender` to the URI for the filter you want to use.
- 5 Save and close the `server.properties` file.
- 6 Restart the Manager service.
 - ◆ Unix: `/etc/init.d/arcsight_manager start`
 - ◆ Windows: Start the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu

To enable the SNMP trap sender, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.

Configure Rules to Send Notifications and Open Cases

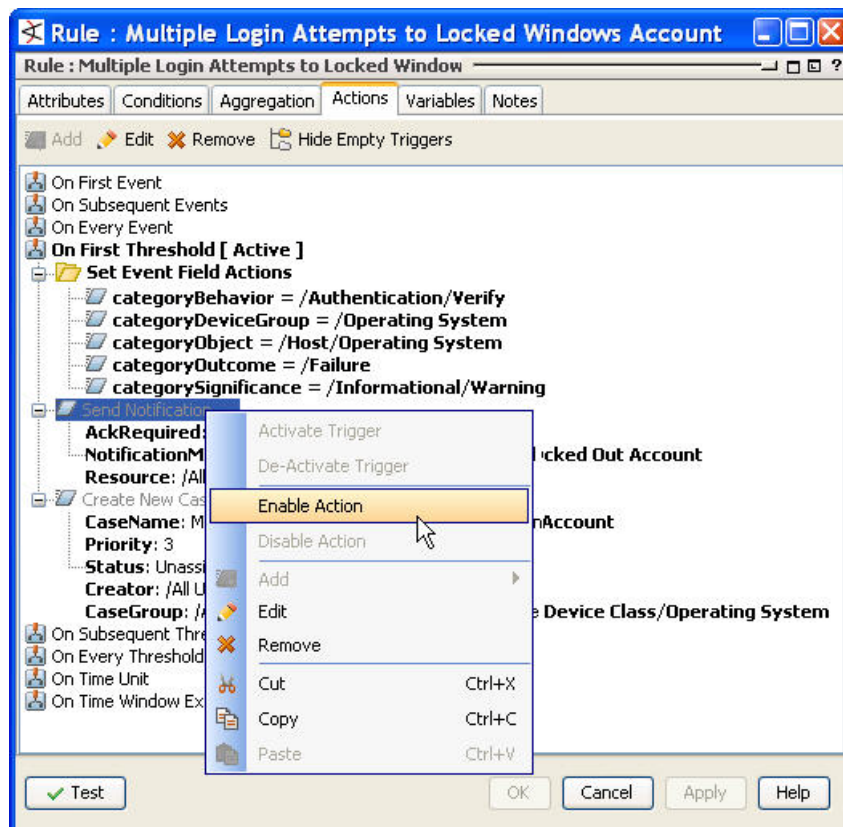
Standard content depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that the standard content is designed to find.

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group. For ESM administration scenarios, notifications are enabled, but case creation is disabled.

To enable standard content rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 55](#), then enable the notification and case actions in the rules.

- 1 In the Navigator panel, navigate to each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 63](#) and [“Configure Rules with Notifications to the SOC Operators” on page 64](#).
- 2 Open the rule for editing in the Inspect/Edit panel (double-click the rule or right-click it and select **Edit**).
- 3 In the Rule Editor in the Inspect/Edit panel, click the **Action** tab.
- 4 Find the *Send Notification* action. The disabled action will appear in grey text. To enable it, select the **Send Notification** action name, right-click it, and select **Enable**.

The example below shows the Action tab for the rule *Multiple Login Attempts to Locked Windows Account*.



- 5 To also create a case when the rule conditions are met, edit the action to give it an owner and enable the action.
 - a Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
 - b In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate ESM user. Click **OK**.
 - c Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.
- 6 Repeat from [Step 1](#) through [Step 5](#) for each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 63](#) and [“Configure Rules with Notifications to the SOC Operators” on page 64](#).

For more about working with Rule actions in the Rules Editor, see [“Creating Rule Actions” on page 451](#) and [“Applying Rule Actions” on page 460](#).

Configure Rules with Notifications to the Cert Team

The following security-related rules send notifications to the **CERT Team** notification group. In these rules, both the notification and case creation actions are disabled by default.

Cases created by these rules should be assigned to the appropriate user or user group in your organization.

Rule URI (File Path)	Rule Name
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Windows Account Locked Out Multiple Times
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Insecure Configuration
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Vulnerable Software
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/	Notify on Successful Attack

Configure Rules with Notifications to the SOC Operators

The following ArcSight Administration rules send notifications to the **SOC Operators** notification group. For these rules, the notification is enabled, and the case creation is disabled by default. Cases created by these rules are assigned to the Administrator.

Rule URI	Rule Name
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Excessive Rule Recursion
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Rule Matching Too Many Events
/All Rules/ArcSight Administration/ESM/System Health/Storage/	ASM Database Free Space - Critical

Schedule Reports

Reports can be run on demand, automatically on a regular schedule, or both. By default, reports are not scheduled to run automatically.

Evaluate the reports that come with the foundations you have installed, and schedule the reports that are of interest to your organization and business objectives.

For instructions about how to schedule reports, see [“Archiving and Scheduling Reports” on page 431](#).

Default Trends Schedule

Trends are a type of report query that can gather data over longer periods of time, which can be leveraged for reports. Trends streamline data gathering to the specific pieces of data you want to track over a long range, and breaks the data gathering up into periodic updates. For long-range queries, such as end-of-month summaries, trends greatly reduce the burden on system resources. Trends can also provide a snapshot of which devices report on the network over a series of days.

The standard content contains trends that monitor long-term conditions among the ArcSight foundations.

Based on the volume of data generated by some of these queries, only some of the trends are enabled by default at installation; the rest are disabled by default.

The enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually slower than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the Console.

Standard trends are listed below with their status on installation, and the time at which they are scheduled to run.

ArcSight Administration Trends

Both ArcSight Administration trends are enabled by default.

ArcSight Administration Trends	Status	Schedule
Trend Queries	Enabled	4:00 a.m.
ASM Database Free Space	Enabled	4:30 a.m.
ArcSight User Login Trends – Hourly	Enabled	5:00 a.m.

Configuration Monitoring Trends

Seven of the 13 Configuration Monitoring trends are enabled by default.

Configuration Monitoring Trends	Status	Schedule
Assets with Recent Configuration Modifications - Daily Trend	Enabled	12:40 a.m.
Host Configuration Modifications	Enabled	1:35 a.m.
Asset Startup and Shutdown Events - Daily Trend	Enabled	2:40 a.m.
Critical System Startup and Shutdown Events - Daily Trend	Disabled	N/A
Most Common Account Login Attempts - Daily Trend	Enabled	3:40 a.m.
User Account Login Failures	Enabled	4:40 a.m.
AAA User Account Creation	Disabled	N/A
AAA User Account Deletions	Disabled	N/A
Account Creation by Host	Disabled	N/A
Accounts Deleted by Host	Disabled	N/A
Local Windows User Creation - Disallowed Systems	Disabled	N/A
Password Modifications	Disabled	N/A
User Account Creation	Enabled	5:40 a.m.
User Account Modifications	Enabled	6:20 a.m.
User Removals	Enabled	1:15 a.m.
VPN User Account Creation	Disabled	N/A
Top Vulnerability Exposure of Critical Assets	Enabled	5:10 a.m.
Vulnerability Exposure by Asset Criticality (Snapshot)	Enabled	1:50 a.m. once a week
Vulnerability Exposure of Critical Assets (snapshot)	Enabled	3:30 a.m.

Configuration Monitoring Trends	Status	Schedule
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend (Snapshot)	Disabled	N/A

Intrusion Monitoring Trends

Eight of the 16 Intrusion Monitoring trends are enabled by default.

Intrusion Monitoring (8/16)	Status	Schedule
SANS Top 20 (v6.01) Attacked Systems	Disabled	N/A
Prioritized Attack Counts by Service	Disabled	N/A
Prioritized Attack Counts by Target Zone	Disabled	N/A
Inbound DoS Events	Disabled	N/A
Environment Status Events	Disabled	N/A
Port Scanning	Enabled	1:20 a.m.
Port Scanning Daily Top 20	Enabled	2:20 a.m.
Reconnaissance Activity	Disabled	N/A
Reconnaissance Types Detected	Disabled	N/A
Top 10 Reconnaissance Types Detected	Disabled	N/A
Zone Scanning Events by Priority	Enabled	4:20 a.m.
Brute Force Access Session Trends	Enabled	1:40 a.m.
Daily Top 10 Resource Access Trends	Disabled	N/A
Resource Access	Disabled	N/A
Asset Counts by Vulnerability (Snapshot)	Enabled	12:20 a.m. once a week
Prioritized Vulnerability Events by Zone	Enabled	5:20 a.m.
Top 10 Daily Vulnerability Events	Enabled	6:25 a.m.
Failed Logins per Hour	Enabled	6:00 a.m.
Top Users with Failed Logins per Day	Enabled	6:40 a.m.
Number of Vulnerabilities per Asset (Snapshot)	Enabled	3:20 a.m. once a week

Network Monitoring Trends

All three Network Monitoring trends are disabled by default.

Network Monitoring	Status	Schedule
Inbound Traffic by Application Protocol	Disabled	N/A
Outbound Traffic by Application Protocol	Disabled	N/A
Overall Traffic	Disabled	N/A

Workflow Trends

One Workflow trend is enabled by default, and the other is disabled by default.

Network Monitoring	Status	Schedule
Notification Events	Disabled	N/A
Notifications	Enabled	6:00 a.m.

How to Enable/Disable Trends



Caution

If you wish to enable a disabled trend, you must first **change the default start date** in the Trend editor, then enable it.

If the start date is not changed, the trend will take the default start date (which is derived from when the trend was first installed), and backfill the data from that time. For example, if you enable the trend 6 months after the first install, these trends will try to get all the data for the last 6 months, which would cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

To enable a disabled trend:

- 1 Edit the trend to change the default start date.
 - a Double-click the trend, or right-click it and select **Edit Trend** to open it in the Trend Editor in the Inspect/Edit panel.
 - b In the Trend editor, click the **Parameters** tab. In the *Query Parameters* section, find Start Time and uncheck the **Use Default** checkbox.
 - c In the *Value* drop-down menu, select a start date appropriate for the frequency at which the trend is scheduled to run. For example, if the trend is scheduled to run daily, select a start date of a week or less earlier than today. Click **Apply**.
- 2 Enable the trend.
 - ◆ If the Trend editor is still open, click the Attributes tab and check the **Enabled** checkbox. Click **OK** to apply changes and close the Trend editor.
 - ◆ If the Trend editor is closed, right-click the trend in the Navigator panel and select **Enable Trend**.

To disable an enabled trend:

- In the Navigator panel, right-click the trend you want to enable and select **Disable Trend**.

How to Monitor Trend Performance

The ArcSight Administration foundation contains resources that enable you to monitor the performance of your enabled trends. The Trends Status dashboard shows the run-time status for all enabled trends. The Trend reports show statistics about trend performance for all enabled trends.

Getting Started Using Standard Content

Whatever your role in the security operations center, you can get started right away using the standard content.

Each foundation is organized with content for different types of users.

- **Executive Summaries.** Executive summaries provide high-level analysis of event activity for management reports. These views show overall trends and long-term summaries.
- **Operational Summaries.** The operational summaries are intended for SOC operators and analysts for daily event monitoring and triage-level investigation.
- **Details.** The detailed content is intended for incident responders and analysts who need access to relevant event details in order to investigate situations that arise from monitoring reports in the operational summaries.
- **SANS Top 5 Reports.** Each foundation contains a set of reports that address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports.

Monitoring with Standard Content

You can use standard content to begin monitoring your network immediately when SmartConnectors are added and basic configuration is complete.

Active Channels

Each foundation provides high-level channels for observing general activity for its area of focus.

Foundation	Channel	Description
ArcSight System	System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	Today	Channel showing events received today since midnight. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	All Events / Last 5 Minutes and Last Hour	Channel showing events received during the last five minutes or the last hour. The channel includes a sliding window that always displays exactly the last five minutes of event data.
	Core / Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing correlation events.
Configuration Monitoring	Operational Summaries / High-Priority Scan Events Directed Toward High-Criticality Assets	This channel shows scan results in real time to give you a view into any high-priority vulnerabilities detected on highly critical assets.

Foundation	Channel	Description
Intrusion Monitoring	Intrusion Monitoring - Significant Events	<p>This channel provides an overview of hostile, compromise or high priority events. It continuously monitors events matching:</p> <ul style="list-style-type: none"> Not ArcSight Internal Events Priority greater than 8 or Category Significance Starts With /Compromise or /Hostile <p>Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).</p>
Network Monitoring	Argus Events	This active channel shows all the events coming from Argus SmartConnectors for the past 24 hours.
Workflow	Assigned Events	This channel shows events assigned today. The channel always displays events occurring since midnight of the current day up to the current time. A filter prevents the channel from showing correlated events. It shows only events that are not in closed stage and are assigned to a user.

Each foundation contains more channels that focus on events of different types. Explore the active channels to monitor the activity you are interested in.

For more about using active channels, see [“Monitoring Active Channels” on page 129](#).

Dashboards

Each foundation also includes general dashboards that provide a high-level view of activity for its area of focus.

Foundation	Dashboard	Description
Configuration Monitoring	Operational Summaries	This group contains four dashboards that provide an overview of configuration changes, database errors, host configuration modifications, and an overview of hosts with problems.
Intrusion Monitoring	Operational Summaries / Security Activity Statistics	<p>This dashboard is a window into the health of common avenues for security threats on the network, including transport protocols, address spaces, application protocols, and statistics involving the top target and attacker IPs, among others.</p> <p>The Intrusion Monitoring foundation contains many other dashboards that provide general executive-level summaries, and more detailed views on different focus areas for operations and investigations.</p>

Foundation	Dashboard	Description
Network Monitoring	General	<p>The dashboards in the General group provide an overview of the top traffic to mail and web servers, and moving average statistics for TCP, UDP, ICMP, and SYN transport protocols.</p> <p>The Network Monitoring foundation contains many more dashboards that provide more detail about network health, including bandwidth usage, inbound and outbound traffic, and activity from firewalls, network devices, and VPNs.</p>

Investigating with Standard Content

Each foundation contains resources that enable operators to view detailed activity and drill down, investigate, track, graph, map, and export, just to name a few.

Use **active channels** to view and sort event flows, investigate blocks of events, and drill down into single event details. For more about using active channels to investigate event activity, see [“Monitoring Active Channels” on page 129](#).

Use **dashboards** to view activity from many perspectives in a single screen. Dashboards are also fully drill-down enabled. For more about investigating using dashboards, see [“Using Dashboards” on page 153](#).

Use the Daily and Quarter Hourly **Pattern Discovery** profiles to find traffic patterns that are not easily detected using other methods. For more about investigating using Pattern Discovery, see [“Pattern Discovery” on page 179](#).

Reporting with Standard Content

Standard content supplies a robust set of reports for each foundation. The reports for each foundation are organized into different levels of detail depending on who the reports are for as outlined in [“Getting Started Using Standard Content” on page 67](#).

Foundation	Reports
Common	The Common group contains a set of anti-virus reports that apply to all the foundations.
Configuration Monitoring	<ul style="list-style-type: none"> • Detailed reports concentrate on configuration changes by device and by user, inventories of applications and assets by role, and vulnerabilities by asset, asset type, asset criticality, and so on. • Executive Summary reports focus on overall host configurations by zone, role, criticality, data role, and operating system. • Operational Summaries provide summaries of host configuration modifications by Customer, OS, and over the last 30 days; top user login successes and failures over recent time periods; and asset restarts over recent time periods. • SANS Top 5 Reports focus on SANS section 3: Unauthorized Changes to Users, Groups, and Services.

Foundation	Reports
Intrusion Monitoring	<ul style="list-style-type: none"> • Detailed reports are organized into types of activity: anti-virus; attack monitoring; environment state for applications, operating systems, and services; reconnaissance attempts; access events; user activity through device type; vulnerability activity by asset and by vulnerability; and worm outbreak activity. • Executive Summary reports provide an overall Security Intelligence Status Report, and summary views by business role and systems that are subject to regulations, such as the Sarbanes-Oxley Act. • Operational Summaries provide mid-level summaries organized into device types, such as anti-virus, attack monitoring, and reconnaissance. • SANS Top 5 Reports focus on SANS sections 1, 4, and 5: Attempts to Gain Access, Through Existing Accounts, Systems Most Vulnerable to Attack, and Suspicious or Unauthorized Network Traffic Patterns.
Network Monitoring	<ul style="list-style-type: none"> • Detailed reports provide views into traffic by host, by protocol, and by target, and activity over network devices and VPNs. • Executive Summary reports provide traffic summaries over daily, monthly, quarterly, and weekly time intervals. • Operational Summaries provide an overall traffic snapshot; bandwidth utilization statistics by device and by time interval; and statistics for inbound and outbound traffic by protocol and by host. • SANS Top 5 Reports focus on SANS section 5: Suspicious or Unauthorized Network Traffic Patterns.
Workflow	<ul style="list-style-type: none"> • Detailed reports provide statistics for all cases, notifications, and notification action events. • Executive Summary reports provide overall case statistics, such as average time to case resolution, number of cases at each escalation stage, and cases as they affect operations. • Operational Summaries provide detailed case statistics, including trends over time, notifications that reach level 3, the status of notifications by user, and so on.

Chapter 4

ArcSight Express Solution

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

With some basic configuration done using the ESM Console, ArcSight Express content enables you to get started using ArcSight Express right away to effectively manage enterprise security operations without having to create additional resources.

The Logger storage portion of the ArcSight Express solution comes with basic system-level filters and foundation reports. For more information about the standard Logger filters and reports, see the *Logger Administrator's Guide*.

[“What is ArcSight Express Content?” on page 73](#)
[“How ArcSight Express Is Organized” on page 74](#)
[“Set Up Connectors and Model the Network” on page 75](#)
[“Apply Standard Asset Categories to Assets” on page 77](#)
[“Create ArcSight Express Users” on page 78](#)
[“Configure Notification Destinations” on page 78](#)
[“Configure Asset Auto-Creation Filters” on page 79](#)
[“Configure Rules to Send Notifications and Open Cases” on page 82](#)
[“Schedule Reports” on page 85](#)
[“Tuning ArcSight Express Content” on page 86](#)

What is ArcSight Express Content?

ArcSight Express content is a series of coordinated [Resources](#) (filters, rules, dashboards, reports, and so on) that address common security and management tasks. ArcSight Express content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration using the ESM Console.

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

The instructions in this topic describe how Administrators can configure the ArcSight Express content for the users of the ArcSight Web interface.

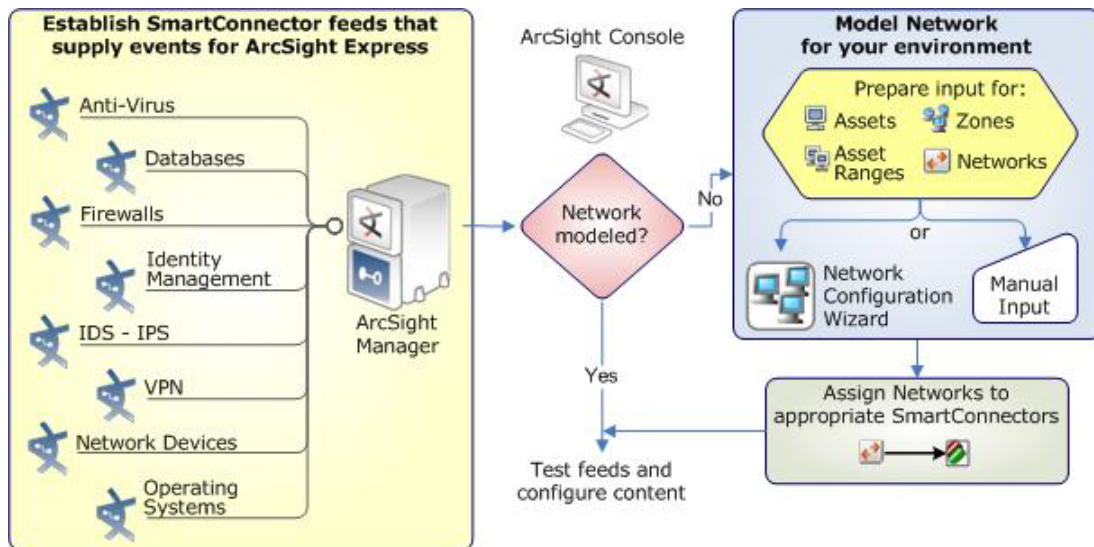
How ArcSight Express Is Organized

ArcSight Express content monitors and reports on activity relevant to the types of devices reporting into the Manager. The content is organized into the following device-specific groups:

Function	Description
Cross-Device	Functions that apply to multiple kinds of devices, such as login attempts, bandwidth usage, and configuration changes.
Anti-Virus	Activity involving anti-virus devices, such as update status, virus activity, and configuration changes.
Case Management	Activity and notifications involving cases opened in ArcSight as a result of events that warrant investigation.
Database	Database activity, such as configuration changes, database logins, errors and warnings.
Firewall	Firewall activity, such as network logins and logouts, denied connections, bandwidth usage, and configuration changes.
Identity Management	User activity, such as logins, user session durations, and configuration changes in order to identify who is doing what activity on the network.
IDS-IPS	Activity involving Intrusion Detection and Prevention Systems, such as signature updates, alerts, and statistics.
Network	Activity involving network infrastructure, including system up/down status, configuration changes, bandwidth usage, and login events.
Operating System	Activity involving operating systems, such as user logins, and user modification events.
VPN	Activity involving VPN connections, including authentication errors, logins, and connection status.
Vulnerabilities	Resources that monitor and report on exposed vulnerabilities by asset.

Set Up Connectors and Model the Network

The following graphic outlines the process for establishing the feeds necessary to drive the ArcSight Express content.



Configuring ArcSight Express content starts with installing SmartConnectors and configuring zones and networks for devices that report to the Manager.

- 1 Establish relevant SmartConnector feeds
- 2 Model the network
- 3 Assign networks to the appropriate SmartConnectors
- 4 Test feeds and configure content

ArcSight Express-Related SmartConnectors

The ArcSight Express content is designed to address event throughput, network health, and basic security-related scenarios. The ArcSight Express content supports feeds from the following types of SmartConnectors.

Device Group	Related Connectors
Anti-Virus	Most major anti-virus products, such as: <ul style="list-style-type: none"> • Symantec EndPoint Protection • TrendMicro • McAfee AV
Database	The database content for basic error reporting and user info that comes from most database connectors, such as: <ul style="list-style-type: none"> • Oracle 10g and 11g • MSSQL Server

Device Group	Related Connectors
Firewall	Firewall content picks up parsed and categorized events from specific firewalls, all-in-one devices, and client-side firewalls, such as those found on Windows. Examples include: <ul style="list-style-type: none">• Juniper Netscreen• CheckPoint• Cisco PIX
Identity Management	Identity management content picks up from identity management systems, such as: <ul style="list-style-type: none">• Juniper Steel-Belted Radius• Cisco Secure ACS• Windows AD
IDS - IPS	This content picks up events from any IDS/IPS system for which ArcSight supplies a Connector, including combination devices that may generate events of these types. For example: <ul style="list-style-type: none">• ISS Site Protector• Symantec Network Security• Cisco IPS
Network	This content works on events from networking devices, such as: <ul style="list-style-type: none">• Cisco IOS Devices• Juniper JunOS Devices
Operating System	This content picks up events from Windows and Unix-based systems that generate relevant events and for which ArcSight supplies supported connectors, such as: <ul style="list-style-type: none">• Linux OS Events (All major Versions)• MS Windows (2003/XP)
VPN	This content works on events from most VPN devices that report on errors, sessions established, and so on. For example: <ul style="list-style-type: none">• Juniper/Netscreen VPN• Cisco VPN• CheckPoint VPN-1
Vulnerabilities	Vulnerability content relies on the device model, which can be populated one by one, or by a vulnerability scanner for which ArcSight supplies a Connector.

Network Modeling

ArcSight uses a model of the network to keep track of the network nodes participating in the event traffic. Having your network modeled and critical assets categorized using standard asset categories is what activates much of the ArcSight Express content and makes it effective.

There are several ways to model your network, including the Network Modeling Wizard. If you are modeling the network using the Network Modeling wizard, review the topic [“Apply](#)

[Standard Asset Categories to Assets](#) on page 77 before creating the comma-separated values lists to load into the network model.

For more about the network model and how to populate it, see ["About the Network Model" on page 731](#).

For more about the Network Modeling wizard, see ["Populating the Network Model Using the Wizard" on page 744](#).

To learn more about the architecture of 's network modeling tools, see Chapter 4, "ArcSight Network Model" in 107.

Apply Standard Asset Categories to Assets

Once assets are added to the network model, or if you are adding them in bulk using the Network Modeling wizard, categorize relevant assets as internal to the network, and/or as critical assets.

Assets can be categorized individually using the Assets Editor, or in bulk using the Network Modeling wizard. Asset categories can also be applied to zones.

For more about asset categories and instructions about how to apply them using the Assets Editor, see ["Asset Categories" on page 739](#).

For more about the Network Modeling wizard, see ["Populating the Network Model Using the Wizard" on page 744](#).

Categorize Internal Assets

Internal Assets are considered to be assets inside the company network. Assets that are not categorized as specifically internal to the network are considered to be external. This includes assets with different asset categories, and those that are not categorized at all (such as external web sites, unknown external hosts, and so on).

For all assets that are internal to the network, classify them in the following asset category:

```
/All Asset Categories/Site Asset Categories/Address  
Spaces/Protected/
```

Determine the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

By default, the Private Address Space Zones are categorized as *Protected*. Assets within a zone that has been categorized do not inherit categories from the zone. For example, an asset with an IP address of 192.168.0.1 is not automatically categorized as *Protected*, but it belongs to one of the Private Address Spaces zones, so it is considered *Internal* because it belongs to a zone categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

Categorize Critical Assets

Assets that are considered critical to protect, such as those that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations, should be classified as critical assets using the following asset category:

[/All Asset Categories/System Asset Categories/Criticality/High](#)

Create ArcSight Express Users

ArcSight Express comes configured with a custom user group called ArcSight Express. Add users to this group with ArcSight Web privileges.

- 1 In the Navigator panel, go to **Users > Shared > Custom User Groups**
- 2 Right-click ArcSight Express and select **New User**
- 3 For each user you add, provide a User ID and Password, and set the User Type to **Web User** and click **OK**.

For more about creating users, see [Chapter 25, Managing Users and Permissions, on page 641](#).

Configure Notification Destinations

Configure notification destinations if you want to be notified when some of the ArcSight Express rules are triggered. By default, the notifications are disabled in the ArcSight Express rules. However, the admin user can configure the destinations AND enable the notification in the rules. For details about enabling the notifications in ArcSight Express rules, see [“Configure Rules to Send Notifications and Open Cases” on page 82](#).

The ArcSight Express rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center.

- 1 In the Navigator panel, go to **Notifications > Destinations > Shared > All Destinations > CERT Team**
- 2 Right-click **Level 1** and select **New Destination**.
- 3 In the Destination Editor, enter the following values in the Attributes tab and click **OK**:

Field	Value
Name	Enter a name for the destination, such as the user name of the contact; or the role, such as Investigator or Manager.
Start/End Time	If applicable, enter the start and end times of the period this person is available, for example, Start: 08:00:00 AM; End: 04:59:59 PM.

Field	Value
Destination Type	<p>From the drop-down menu, select the method for delivering notifications:</p> <ul style="list-style-type: none"> • Console — Notification popup in this user's ArcSight account • E-Mail — User's e-mail account • Pager — User's pager. Enter the pager's PIN number and service provider. • Cell Phone — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.
User/Group	<p>From the drop-down menu, select the individual user or user group who receives the notification. This field is required if you selected Console as the destination type, or if you want to use the contacts specified in the User's profile.</p>

- 4 Repeat steps 1, 2, and 3 for each escalation level you want to add. Add more escalation levels as needed.
- 5 Repeat steps 1, 2, 3, and 4 for the SOC Operators destination (**Notifications > Destinations > Shared > All Destinations > SOC Operators**).

Configure Asset Auto-Creation Filters

A standard feature of ArcSight is that it automatically creates assets in the ArcSight asset model for events whose devices are not already modeled either manually or using an asset scanner.

Depending on what devices you have reporting to ArcSight and what devices report in to your network, however, this can potentially cause a lot of unnecessary individual assets to be added to your asset model. For example, laptops with the intrusion detection system BlackICE from ISS can generate a new asset ID for that device every time the laptop logs onto the network. This situation also applies to VPN and wireless networks every time a device logs onto a new subnet.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, the Manager would model a new Connector, which falsely clutters the network model with Connector nodes.

To limit how the Manager automatically models assets in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

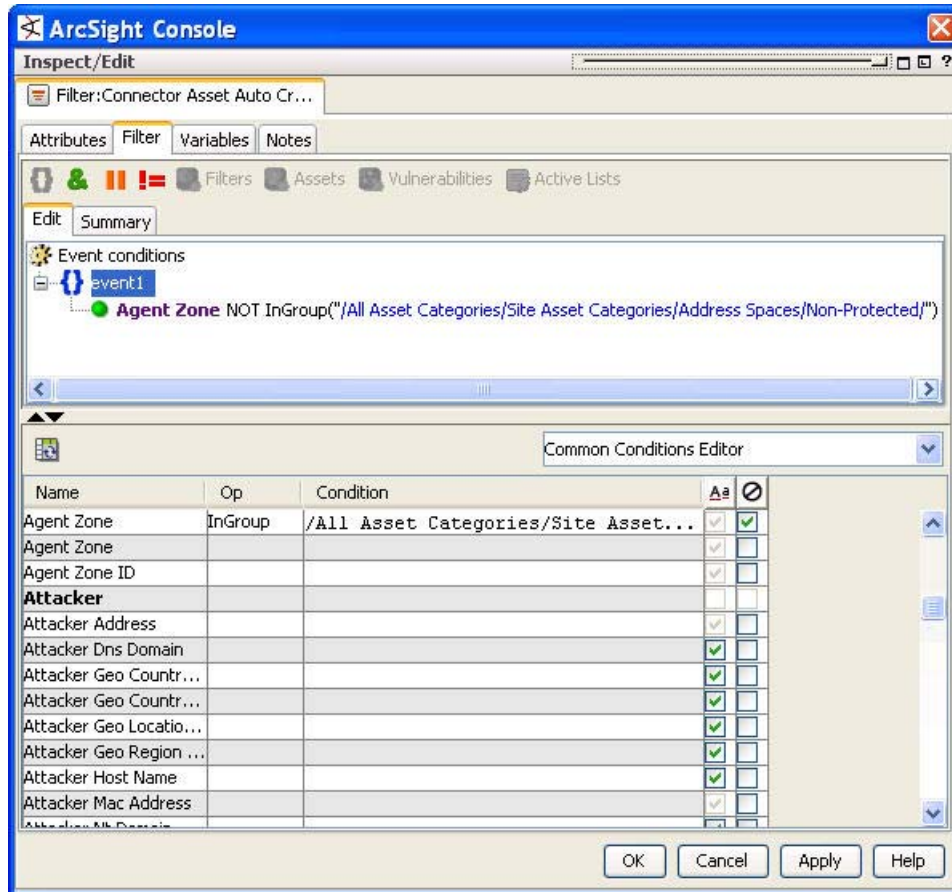
Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs the Manager to create an asset for network nodes represented in the events received from the SmartConnectors present in your environment.

By default, the *Connector Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to exclude connectors from a specific zone, such as a VPN zone, where the asset already exists, but traffic is coming into the network from an alternate VPN interface. You can also exclude traffic from different types of Connectors, such as from a particular device and vendor.

The example below shows the *Connector Asset Auto Creation Controller* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.



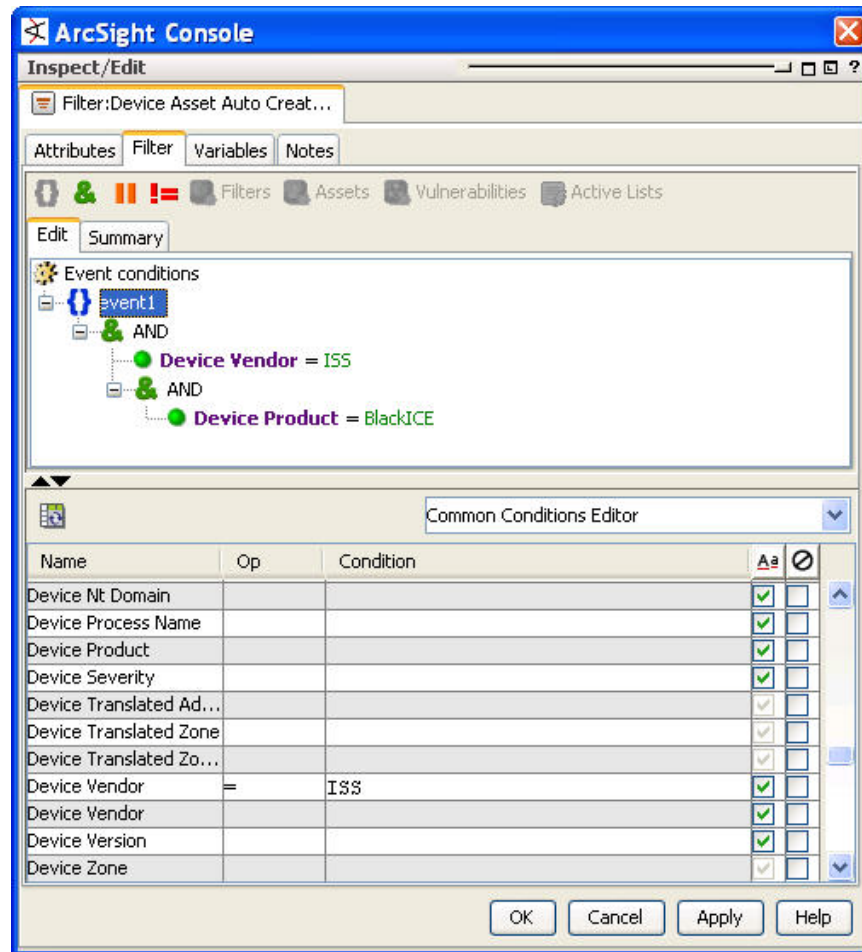
- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter (**All Filters/ArcSight System/Asset Auto Creation**) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.
- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊖).


- 7 Repeat steps 3 through 5 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.

Configure Device Asset Auto Creation Controller Filter

By default, the *Device Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can configure this filter to specify traffic from specific devices and device vendors, or event categories, such as **Hostile**. When you specify an event category, the filter directs the system to only create assets for events with this severity.

The example below shows the *Device Asset Auto Creation Controller* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 Select **event1** and add an AND operator (click the AND icon .

- 4 Select `event1` and use the event fields grid to build the condition, or right-click `event1` and select **New Condition**. Navigate to `Device > Device Vendor`. In the Condition field, enter the vendor name, in this case **ISS**.
- 5 Add the device vendor and product you wish to include.
 - a If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to `Device > Device Product`. In the Condition field, enter the device name, in this case **BlackICE**.
 - b If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to `Device > Device Product`. In the Condition field, enter the device name.

For example, the condition would look like this:

```
OR
  AND
    Device Vendor A
    Device Product 1
  AND
    Device Vendor B
    Device Product 2
  AND
    Device Vendor C
    Device Product 3
```

- 6 Repeat steps 3 through 6 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7 Click **OK** to apply changes and close the Filter editor.

Configure Rules to Send Notifications and Open Cases

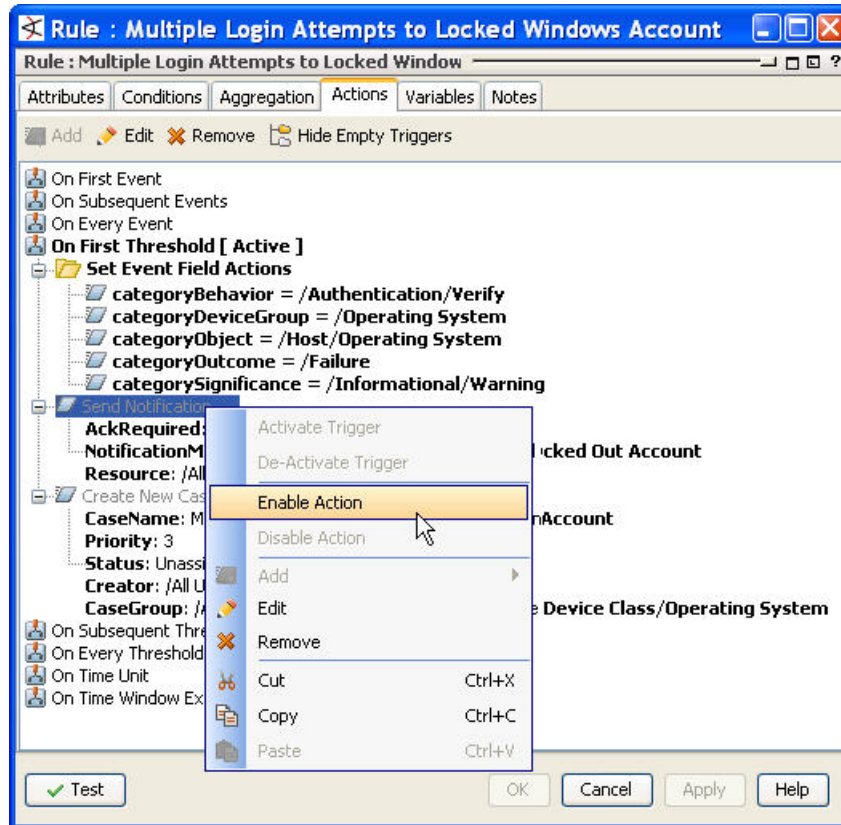
ArcSight Express depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that ArcSight Express is designed to find.

By default, the notifications and create case actions are disabled in the ArcSight Express rules that send notifications about security-related events to the Cert Team notification group. For administration scenarios, notifications are enabled, but case creation is disabled.

To enable ArcSight Express rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 78](#), then enable the notification and case actions in the rules.

- 1 In the Navigator panel, navigate to each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 83](#) and [“Configure Rules with Notifications to the SOC Operators” on page 84](#).
- 2 Open the rule for editing in the Inspect/Edit panel (double-click the rule or right-click it and select **Edit**).
- 3 In the Rule Editor in the Inspect/Edit panel, click the **Action** tab.
- 4 Find the *Send Notification* action. The disabled action appears in grey text. To enable it, select the **Send Notification** action name, right-click it, and select **Enable**.

The example below shows the Action tab for the rule *Multiple Login Attempts to Locked Windows Account*.



- 5 To also create a case when the rule conditions are met, edit the action to give it an owner and enable the action.
 - a Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
 - b In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate ArcSight Express user. Click **OK**.
 - c Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.
- 6 Repeat steps 1 through 6 for each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 83](#) and [“Configure Rules with Notifications to the SOC Operators” on page 84](#).

For more about working with Rule actions in the Rules Editor, see [“Creating Rule Actions” on page 451](#) and [“Applying Rule Actions” on page 460](#).

Configure Rules with Notifications to the Cert Team

The following security-related rules send notifications to the **CERT Team** notification group. In these rules, both the notification and case creation actions are disabled by default.

Cases created by these rules should be assigned to the appropriate user or user group in your organization.

Rule URI (File Path)	Rule Name
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Windows Account Locked Out Multiple Times
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Insecure Configuration
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Vulnerable Software
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/	Notify on Successful Attack

Configure Rules with Notifications to the SOC Operators

The following ArcSight Administration rules send notifications to the **SOC Operators** notification group. For these rules, the notification is enabled, and the case creation is disabled by default. Cases created by these rules are assigned to the ArcSight Express Admin user.

Rule URI	Rule Name
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Excessive Rule Recursion
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Rule Matching Too Many Events
/All Rules/ArcSight Administration/ESM/System Health/Storage/	ASM Database Free Space - Critical

Schedule Reports

Reports can be run on demand, automatically on a regular schedule, or both. By default, the reports that come with ArcSight Express are not scheduled to run automatically.

You may want to schedule certain reports that are based on cases, notifications, assets (not based on events). These non-event-based reports cannot be run for the previous day or the previous week, which means that their output is always the “current” state.

An example of an asset-based report that you may want to schedule would be *Exposed Vulnerability Count by Critical Asset*.

Reports on cases

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases by Operational Impact
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Case Stage Counts
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	All Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases per Target
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Open Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Today's Cases

Reports on notifications

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Statistics Summary
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	All Level 3 Notifications
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Status Report
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notifications By Acknowledgement Status
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Unacknowledged Level 3 Notifications

Reports on assets

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerabilities by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Critical Asset

For instructions about how to schedule reports, see [“Archiving and Scheduling Reports” on page 431](#).

Tuning ArcSight Express Content

ArcSight Express content is designed to find activity of concern that the staff of your security operations center should be notified about so they can follow up. There may be times, however, that a situation is actually a benign or routine condition in your environment.

In such a case, ArcSight Express provides the following active lists where you can store specific event and user situations that are determined to be low or no risk:

- /All Active Lists/ArcSight System/Tuning/**Event-based Rule Exclusions**
- /All Active Lists/ArcSight System/Tuning/**User-based Rule Exclusions**

The entries in these active lists are ignored by the rules that reference them. The *Event-based Rule Exclusions* active list is referenced by the event-based rules, and the *User-based Rule Exclusions* are referenced by the user-based rules:

Event-Based Rules	User-Based Rules
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ High Number of IDS Alerts for DoS	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Logout
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ SYN Flood Detected by IDS and Firewall	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Login
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/ High Number of IDS Alerts for Backdoor	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/ Multiple Windows Logins by Same User

These active lists store the following fields for the events and users:

Event-based Rule Exclusions	User-based Rule Exclusions
The following fields limit the rule exclusions to very specific events between two specific systems. <ul style="list-style-type: none"> • Device Event Class ID • Event Name • Attacker Zone Name • Attacker Address • Target Zone Name • Target Address 	The following fields limit the rule exclusions to user account activity that can be safely ignored. <ul style="list-style-type: none"> • Target NT Domain • Target User ID • Target User Name

There are three ways to add entries to these active lists:

- From an active channel
- Manually from the Active List editor
- In a batch from a CSV file

To add entries from an active channel:

- 1 In the active channel where the event appears, select and then right-click the event and select **Active List > Add to > Other...**
- 2 In the *Add to Active List* dialog box in the drop-down field, navigate to **/All Active Lists/ArcSight System/Tuning/Event-based Rule Exclusions** or **/All Active Lists/ArcSight System/Tuning/User-based Rule Exclusions** and click **OK**.
- 3 The *Add to Active List* dialog box displays the list of fields the active list saves from the selected event. If the selected event does not have a value for one or more of the fields, those fields remain empty.

To add entries to these active lists manually:

- 1** In the Navigator panel, go to **Lists > Active Lists > All Active Lists > ArcSight System > Tuning**.
- 2** Right-click the active list you want to populate and select **Edit Active List**.
- 3** In the Active List Editor in the Inspect/Edit panel, click **Add Entry**.
- 4** In the ActiveList Entry Editor, enter the appropriate event or user details and click **Add**.
- 5** Repeat steps 3 and 4 for every event or user situation you want to exclude from the event or user-based rules.

To populate Active Lists from an imported CSV file:

- 1** In the Navigator panel, navigate to the active list you want to configure ([Lists > Active Lists](#)).
- 2** Generate a CSV file with the values with which you wish to populate the active list, and save it to a directory on the Console system.
- 3** Right-click the active list you wish to import the values into and select **Import CSV File...**
- 4** In the Open dialog box, navigate to and select the CSV file and click **Open**.

For more about working with active lists, see ["Managing Active Lists" on page 571](#).

Chapter 5

Learning Paths

ArcSight ESM involves many different security functions, as presented through the ESM Console. Some of these functions are subjects of a certification process under various standards specified in the Common Criteria for Information Technology Security.

These topics are provided as a guide to help you locate and understand the ESM security functions related to certification. The User category applies to persons who, after logging in, would have only basic access to the system. The Author category applies to persons with analytic authoring privileges. The Administrator category applies to persons with both administrative and analytic authoring privileges in addition to basic access.

ArcSight ESM Roles	Topics and Tasks
Administrator	<p>ArcSight Administration: See Chapter 26, Managing Resources, on page 665.</p> <ul style="list-style-type: none">• Manages (creates, edits, and deletes) ArcSight groups and users• Manages user accounts, creating access control lists, and setting permissions• Establishes escalation procedures for automated notifications sent by e-mail, pager or cell phone
Author	<p>Analysis Authoring: See “Rules Authoring” on page 439, “Identity Correlation” on page 543, “List Authoring” on page 571, “Case Management and Queries” on page 585, “Knowledge Base Authoring” on page 637, and topics on creating and editing dashboards and data monitors in “Monitoring Events” on page 129. See also, reference topics on “Categories” on page 836, “Common Conditions Editor (CCE)” on page 846, “Data Fields” on page 867, and “Prioritization Fields” on page 956.</p> <ul style="list-style-type: none">• Creates rules that are correlated with events to generate responses with automated actions• Creates custom reports for Operators to summarize enterprise security activity or display information on devices, events, or users• Creates cases used by Operators to monitor suspicious events or situations that occur in the enterprise• Creates Knowledge Base content providing Operators with solutions and possible actions to security threats• Customizes Views used by Operators to capture network infrastructure displaying real-time events

ArcSight ESM Roles	Topics and Tasks
Operator	<p>Analysis Operations: See “Monitoring Events” on page 129, “Filtering Events” on page 223, “Building Reports” on page 331, “Running and Managing Reports” on page 423.</p> <ul style="list-style-type: none">Monitors, investigates, and analyzes events using Views, Event Inspector, Replay Controls, and other monitoring toolsAcknowledges notifications and responds to security threatsViews reports, cases, and Knowledge Base articles in order to proactively approach security issues

For the User

Users with an interest in certification issues can use the following subject matter list as a guide to relevant documentation topics.

ArcSight User Certification Subjects

Active Channels

- [“Monitoring Active Channels” on page 129](#)
- Reference topic: [“Active Channels” on page 788](#)
- Related topic: [“Viewing and Using Channels” on page 130](#).

Login Process

- Reference topic: [“Access Control Lists” on page 787](#)
- Related topics: [“Filters” on page 942](#), [“Users” on page 1005](#), and [“User Groups” on page 1005](#).

For the Administrator

ArcSight users with administrative privileges and an interest in certification issues can use the following subject matter list as a guide to relevant documentation topics. See also [Chapter 26, Managing Resources, on page 665](#).

ArcSight Administrative Certification Subjects

Access Control Lists (ACLs)

- Reference topic: [“Access Control Lists” on page 787](#)
- Related topics: [“Filters” on page 942](#), [“Users” on page 1005](#), and [“User Groups” on page 1005](#).

Active List Resources

- Reference topic: [“Active Lists” on page 790](#)
- Related topics: [“Rule Actions” on page 972](#) and [“Creating Filters” on page 223](#).

Dashboards

- Reference topic: [“Dashboards” on page 864](#)
- Related topics: [“Data Monitors” on page 905](#), [“Using Dashboards” on page 153](#), and [“Viewing and Using Channels” on page 130](#).

Data Monitor Resources (statistical)

- Reference topic: [“Data Monitors” on page 905](#)
- Related topics: [“Dashboards” on page 864](#) and [“Viewing and Using Channels” on page 130](#).

Database Full Response

- Reference topic: [“Database” on page 865](#)
- Related topics: [“Data Fields” on page 867](#), [“SmartConnectors” on page 984](#), and [“Sending Control Commands to SmartConnectors” on page 715](#).

Filters

- Reference topic: [“Filters” on page 942](#)
- Related topics: [“Using Grids” on page 145](#), [“Creating Filters” on page 223](#), and [“Applying Filters” on page 231](#).

Reports

- [“Reports” on page 963](#)
- [Chapter 14, Building Reports, on page 331](#)
- [Chapter 15, Running and Managing Reports, on page 423](#).

Resources and Resource Editors

The ESM Console offers editors for resources and resource components. Thus, there are many related topics. Since listing these topics would reiterate much of the Console documentation, it is more practical to summarize the resource groups and allow the reader to explore resource editing independently.

- [“Navigating” on page 94](#)
- [“Navigator Panel Resource Tree” on page 95](#) includes a table that describes all resources and gives cross-references to topics about them, where you can find information about editing each resource.

Rules

- Reference topic: [“Rules” on page 974](#)
- Related topics: [Chapter 16, Rules Authoring, on page 439](#), [“Rule Actions” on page 972](#), and [“Rule Conditions” on page 973](#).

Rule Actions

- Reference topic: [“Rule Actions” on page 972](#)
- Related topics: [Chapter 16, Rules Authoring, on page 439](#), [“Rule Conditions” on page 973](#), and [“Rules Editor” on page 977](#).

Shell Commands

Documentation for using operating system shell commands (command line commands) is included in the appropriate appendixes of the *Administrator's Guide*.

Threat Level Formula

- Reference topics: [“Threat Evaluation” on page 999](#)
- Related topics: [“Priority Calculations and Ratings” on page 957](#), [“Prioritization Fields” on page 956](#), and [“Threat” on page 999](#).

Users and User Groups (Administrator, Author, Operator)

- Reference topic: [“User Groups” on page 1005](#)

- Related topic: [“User Groups” on page 1005](#).

Working in the ESM Console

In addition to all the security analysis, forensic, response, and reporting capabilities built into the ArcSight ESM Console, the Console itself is a tool with its own characteristics and specialized controls. The Help topics in this section describe the basics of using ESM Console tools and controls to make the most of its features.

[“Navigating” on page 94](#)

[“Viewing” on page 99](#)

[“Inspecting and Editing” on page 102](#)

[“Controlling the ESM Console” on page 105](#)

[“Using the Network Tools” on page 107](#)

[“Staying Informed” on page 110](#)

[“Using the Menus” on page 114](#)

[“Keyboard Shortcuts \(Hot Keys\)” on page 119](#)

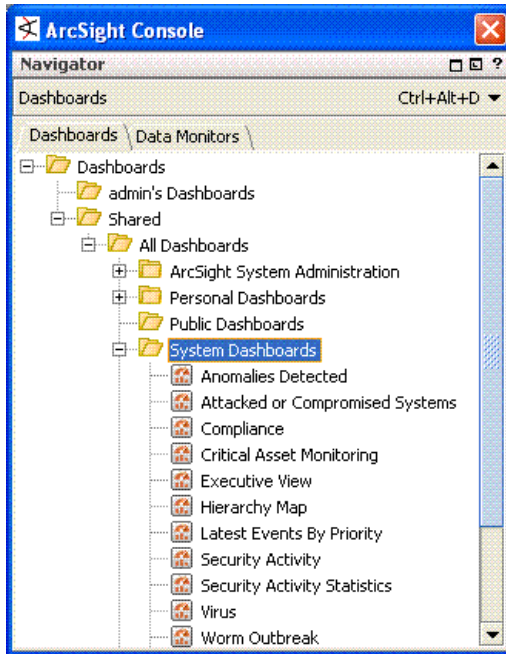
[“Moving Copying, Linking, and Deleting Resources” on page 120](#)

[“Printing from the Console” on page 120](#)

Navigating

The primary principle of navigating in the ESM Console is to use the Navigator panel to locate and manage security resources, and the Viewer and Inspect/Edit panels to analyze resource data and view or adjust the attributes of the resources producing the data.

Figure 6-1 The Navigator panel showing the Dashboards resource tree













Using the Navigator panel consists of:











- Choosing a resource tree from the drop-down list.
- Expanding (+) and collapsing (-) resource groups to locate particular subgroups or individual resources. (You can also use the keyboard **right arrow key to expand** and **left arrow key to collapse** the **Navigator resource trees**.)
- Right-clicking groups or individual resources to choose from their context menus.
- Using the Viewer or Inspect/Edit panels to see or act on the results of the context menu commands.

The resources available to you in the Navigator panel can be affected by your user type.

As a suggestion, browsing the resource trees established for your enterprise is a very good way to become familiar with both your environment and the ESM Console's capabilities.

Navigator Panel Resource Tree

Tree	Icon	Resource
Active Channels		Create, modify, and delete security-event views that actively and continuously evaluate the events they display, on the basis of time and other filter conditions. This view also includes the Field Sets resource tree for managing named field sets. See Chapter 7, Monitoring Events, on page 129 .
Assets		Security-sensitive devices and device groups installed in your enterprise, and the known exposures to potential threats those devices may represent. Assets also includes the related network, zone, location, category, and vulnerability information you use to manage network devices. See "About the Network Model" on page 731 .
Cases		Enterprise security incident cases, by status and priority. See Chapter 22, Case Management and Queries, on page 585 .
Connectors		The SmartConnectors currently installed at your enterprise. See Chapter 27, Managing SmartConnectors, on page 695 .
Customers		Manage resources that represent the security concerns of particular MSSP (Managed Security Services Provider) clients. See "Managing Customers" on page 766 .
Dashboards		Various event data monitors and their containing dashboards. See "Using Dashboards" on page 153 .
Files		The Files resource tree, when populated, lists files saved as resources on the Manager. This makes them accessible to all users of the system who are authorized for such access. File resources include Case file attachments, templates, and general-purpose shared files. See "Managing File Resources" on page 665 .
Filters		Event filtering definitions, organized in groups. See Chapter 11, Filtering Events, on page 223 and "Using Filter Groups" on page 232 .
Knowledge Base		A database of articles and groups of articles that aid problem-solving, analysis, and operation. See "Getting Knowledge Base Articles" on page 221 and Chapter 24, Knowledge Base Authoring, on page 637 .
Integrations		Application integration resources used to configure and launch commands, tools, and views in custom and third party applications and other ArcSight products from within the ESM Console. Provides the ability to configure custom scripts, URLs, and CounterACT SmartConnector commands, and integrate them into the Console UI in various contexts. Leverages velocity expressions and the UI contexts for pulling the content of event data, for example, as command parameter values. Provides support for ArcSight Network Synergy Platform (NSP) and Threat Response Manager (TRM). See Chapter 23, Integration Commands, on page 595 .

Tree	Icon	Resource
Lists		<p>Active Lists are lists of active source and target IP addresses of interest, as defined by enterprise rules. See “Managing Active Lists” on page 571 for more information.</p> <p>Session Lists are similar to active lists, but are optimized for time-based queries and monitoring of rule-driven combinations of event attributes or custom fields. See Chapter 20, Identity Correlation, on page 543 for more information.</p>
Notifications		Destinations and settings for the automatic messages that alert you to pre-defined situations or events. See “Acknowledging Notifications” on page 110 and “Managing Notifications” on page 658 .
Partitions		ArcSight Database archiving management. See Chapter 29, Managing Partitions, on page 767 .
Pattern Discovery		Profiles to capture, and snapshots of, potentially threatening event patterns. See “Pattern Discovery” on page 179 .
Query Viewers		A resource for defining and running SQL queries on other ESM resources (independent of reports), including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results. Query viewers can use the same queries as reports do, but can be run independently of them. See Chapter 13, Query Viewers, on page 287 .
Reports		Definitions for, and archived output from, various activity reports. See Chapter 15, Running and Managing Reports, on page 423 and Chapter 14, Building Reports, on page 331 .
Rules		Rules and groups of rules created for isolating, analyzing, and responding to events. See Chapter 16, Rules Authoring, on page 439 .
Stages		Workflow and annotation features for real-time analyst collaboration on security events.
Use Cases		Resource collections that address common security issues and business requirements. When use cases are installed, a Use Case tab is displayed in the Navigator panel. A wizard is available for configuration of the use case resources. See “Use Cases” on page 511 .
Users		ArcSight users and user groups. See Chapter 25, Managing Users and Permissions, on page 641 .

Using SmartFolders

ArcSight has special, automatically maintained folders to track the results of your case searches or to track your currently selected replay rules and currently running reports.

When you create them, these folders appear just below the root of each resource type in the Navigator, prefixed with your ArcSight user name.

Creating a Case-Search SmartFolder

To create a case-search SmartFolder:

- 1 Right-click a folder in the Cases tree and choose **New Search Group** in the context menu to open the Search Group Editor.
- 2 Use the Editor to define a search that updates dynamically each time a change occurs to one of your cases.

A given group contains the result of this search when it is applied to those cases.

Creating a Reports SmartFolder

The Reports tree in the Navigator panel shows a folder for each user name and the suffix "Reports." These folders list the reports that user is applying, and the right-click context menu offers the commands available for those reports. These folders are maintained automatically and you cannot change them.

You can use this feature to control report runs. For example, if a report is running too long and you would like to end it, right-click it and choose **Stop Report**.



Reports you run using the **Run** button in the Report Editor are initiated outside the usual Console processes and do not appear in, and are not controllable from, the Reports tree in the Navigator.

Editing Groups

You can group resource types in the Navigator panel to help you organize and manage them. Groups can also be hierarchical, resulting in "trees" of resources. Apart from the characteristics of the resources involved, such as assets or vulnerabilities, each group identity has certain properties you can edit in the Group Editor.

Editing a Group

To edit a group:

- 1 In the Navigator panel, right-click a resource group and choose **Edit Group**.
- 2 In the Group Editor, click the **Value** fields for the group attributes you want to change.
- 3 Click **Apply** to put your changes into effect but leave the editor open. Click **OK** to apply your changes and also close the editor.

Fields containing system information (like Creation Time) are not editable.

See ["Reference Pages" on page 962](#) for more about using the **Group Page** and **Member's Page** fields.

See ["Scheduling Jobs" on page 977](#) for information about scheduling tasks or "jobs" for reports (individually or by group), rules, or pattern discovery snapshots.

Categories Tab

The Group Editor for groups in the Assets tab of the Assets resource tree has an additional Categories tab. This tab has two sub panels: Local Asset Categories and Inherited Asset Categories. "Local" shows assets that are explicitly assigned to categories. "Inherited" shows assets whose category connections are presumptions based on a parent's group or a simple asset-range association.

Viewing Group Cases in a Grid View

When you right-click a case group in the Cases resource tree in the Navigator panel, and choose **View in Grid**, you see that group's cases listed in a Case Details view in the Viewer panel. Click any case in the grid to work with it individually. You can also:

- Right-click any column heading to get a menu of column configuration options.
- Right-click any individual case's fields to get a menu of case handling options, described below.

Option	Description
New	Create a new case.
Edit	Open a case in the Inspect/Edit panel for editing.
Delete	Delete the selected case.
Export to external system	Export the case to an external tracking system.
Edit case by ID	Find a case by its Display ID value.
Select rows with matching cell	Select cases where all values in a particular column have the same value or entry.
Invert selection	Reverse selection and highlighting of a previous selected group of cases.
Close	Clear the Case Details view.
Refresh	Refresh the Case Details view to reflect new or deleted cases and information updated in existing cases.
Knowledge Base	Show Knowledge Base information associated with cases.

Batch Editing

You can make common edits to multiple case or SmartConnector resources by selecting a set of either type in the Navigator panel and changing their common fields in the Case or Connector Editor.

Batch-Editing Cases or Connectors

To batch-edit cases or connectors:

- 1 **Ctrl+click** or **Shift+click** to select a set of individual cases or SmartConnectors in their respective resource trees in the Navigator panel.
- 2 **Right-click** the selected items and choose **Edit**.
- 3 Make changes to the appropriate common fields, such as **Description** or **Owner**.
- 4 Click **Apply** to record your changes and leave the editor open, or click **OK** to save and close. Saving affects only the fields you have changed, in each of the selected resources.

Cases Reminder

You can also lock and unlock cases in batches, using the **Lock Case** checkbox.

SmartConnector Reminders

Batch changes affect only default configurations, not alternates. However, you can add new alternate configurations by batch editing.

Note that if you make changes under the **Filters** tab, the entire tab's contents are saved to the selected SmartConnectors.

Only connectors of the same version can be batch-edited. Version is indicated by the color of the connector icons in the resource tree: blue for pre-v2.5 and green for v2.5 or later.

Reconnecting to the Manager

If your ESM Console loses its connection to the Manager, a dialog box enables you to **Retry** the connection, **Relogin**, or to **Cancel** the connection. Try these options in this order.

A connection to the Manager can't be re-established when the Manager has to be restarted or when a network problem prevents communication with the same Manager. In such cases click **Cancel** and start the Console again, using an appropriate Manager host name.

Viewing

This section provides information on using the Console Viewer Panel and choosing look-and-feel options (skins) for the ESM Console.

Viewer Panel

You see the products of security-event analyses in the Viewer panel, which can display several different types of views. (See also, ["Using Views" on page 129.](#))

Although there are some views that display information about resources, most views are active channels, which are continuously evaluated collections of security-event data. (See also, ["Monitoring Active Channels" on page 129.](#))

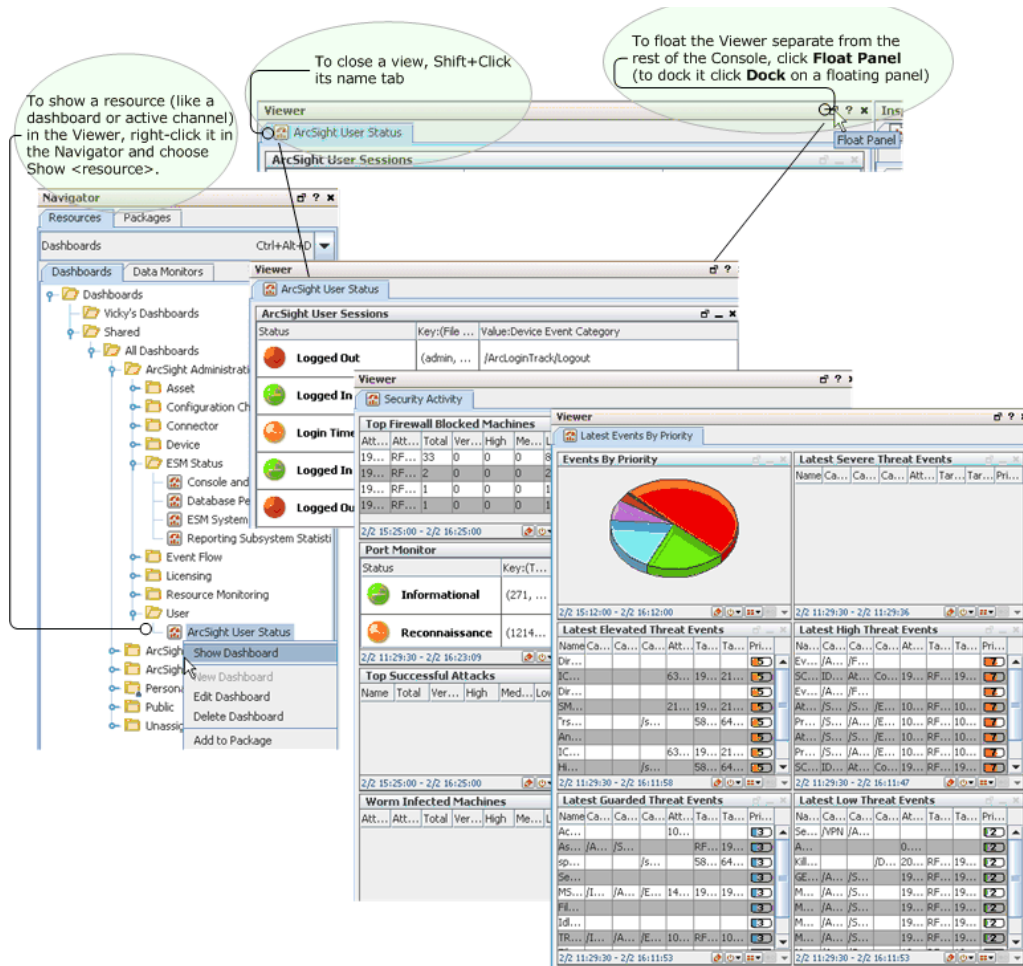


Tips:

- To show a resource (like a particular dashboard or active channel) in the viewer, right-click it in the Navigator tree and choose Show <resource>.
- To close individual views quickly, Shift+click their name tabs. (You can also right-click a view name tab and choose Close from the popup menu.)
- To float the Viewer panel, click the Float icon at the top left of the Viewer.

The Viewer panel can also internally render basic HTML, meaning that it automatically shows HTML-based reports, reference pages, results for the Web Search tool, and notification acknowledgements. More complex HTML that might include JavaScript, plug-ins, or other embedded objects is, for security reasons, still rendered in the external browser you specify through the Preferences dialog box. The external browser is also used by PDF document files.

The **Web Viewer** tabs in the Viewer panel have a live link at the top. You can click these links to open the contents in an external, fully functional browser window. You can also right-click the contents of a Web Viewer and use the standard browser commands to do basic functions such as going back or forward or reloading.



If your Console is not already displaying a default set of pre-defined views, or you want to change the views displayed, you can use these options:

- Choose **Window > Viewer Panel** to open the panel if it isn't open.
- Choose the **Active Channels**, **Dashboards**, or **Pattern Discovery** resource trees in the Navigator panel to find analysis tools or results to view.
- Right-click a resource in a tree and choose **Show <resource>** to open it in the Viewer panel.
- When multiple tabbed views are open in the panel, click the tabs at the **top** of the panel to choose the active channel you want to see, and the tabs at the **bottom** of the panel to choose which view of that active channel should be foremost.

To close an individual view, **Shift+click** its name tab. (You can also right-click a view name tab and choose **Close** from the popup menu.)

Using active channels and the many types of views they offer is fully covered in the topics under these headings:

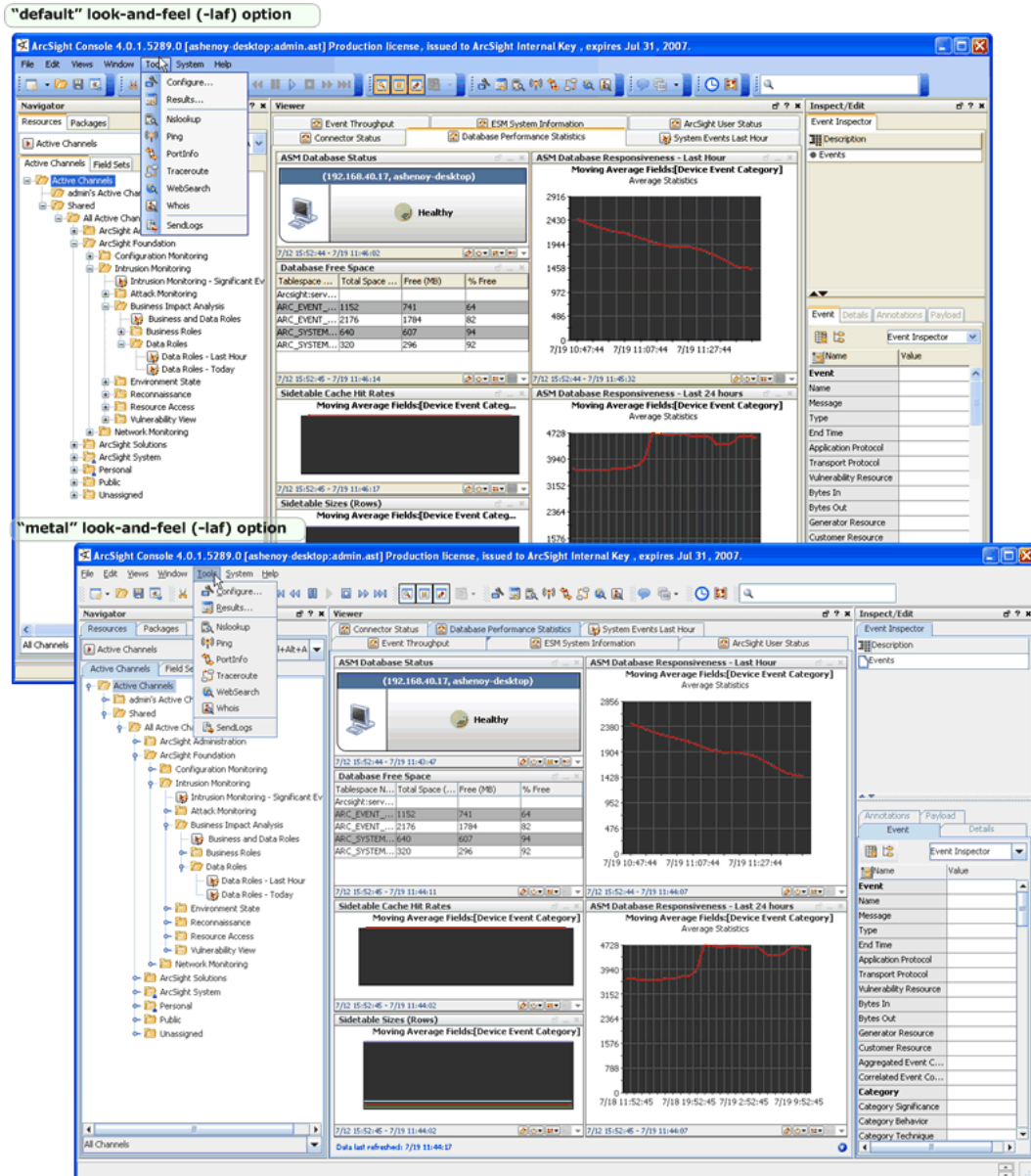
- Monitoring Events
- Selecting and Investigating Events
- Using Dashboards

ESM Console Look-and-Feel

If you start the ESM Console from the command line with the **arcsight console** command (in `ARCSIGHT_HOME/current/bin`), use the **-laf <style>** flag to specify a look-and-feel style. For example, the following command starts the Console with a "metal" look-and-feel:

```
arcsight console -laf metal
```

These styles modify the Console display and associated online help. The figure below shows what the ESM Console looks like when started with the default and metal styles.



The screen captures and illustrations used throughout the ESM Console online help show various look-and-feel styles. For more information about **arcsight console** command options, including **-laf**, see the "ArcSight Commands" appendix in the *Administrator's Guide*.

Inspecting and Editing

ESM provides the Inspect/Edit panel to examine the details of events that appear in active channels in the Viewer panel, or to modify the resource attributes in the Navigator panel. You can examine security events through the Inspect/Edit panel's Event Inspector, and edit resources using specialized editors, one for each specific resource type.



Press Enter to register edits made in editors and channel columns

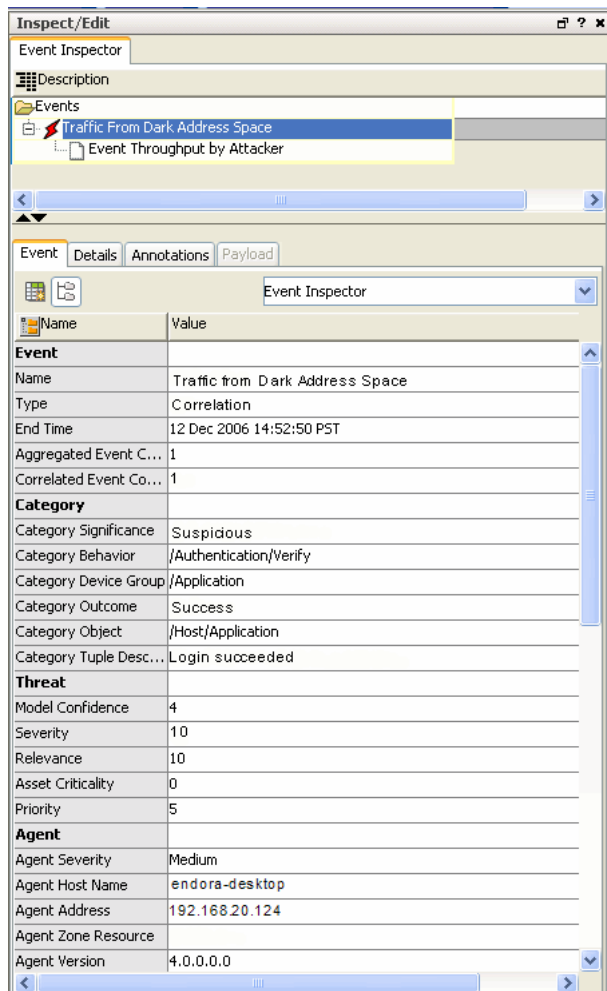
To ensure that ESM registers a change you make to a field in editor and channel columns, press the Enter key before clicking **Apply** or **OK**.

See also:




- [“Hiding Empty Rows in the Event Inspector” on page 215](#)
- [“Displaying Articles from the Event Inspector” on page 221](#)
- [“Retrieving Payloads” on page 220](#)
- [“Event Inspector” on page 940.](#)

Overview of Inspect/Edit Features and Utilities

Each editor has its own controls and attributes, described in the Help for its resource.

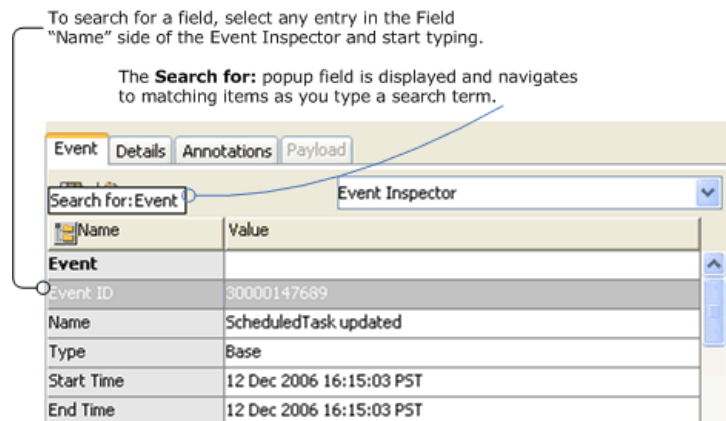


The Inspect/Edit panel opens automatically when you double-click an event in a grid view or choose to edit a resource in the Navigator panel. You can also right-click an event in a grid view and choose **Show Event Details**. To explore the Inspect/Edit panel, you can:

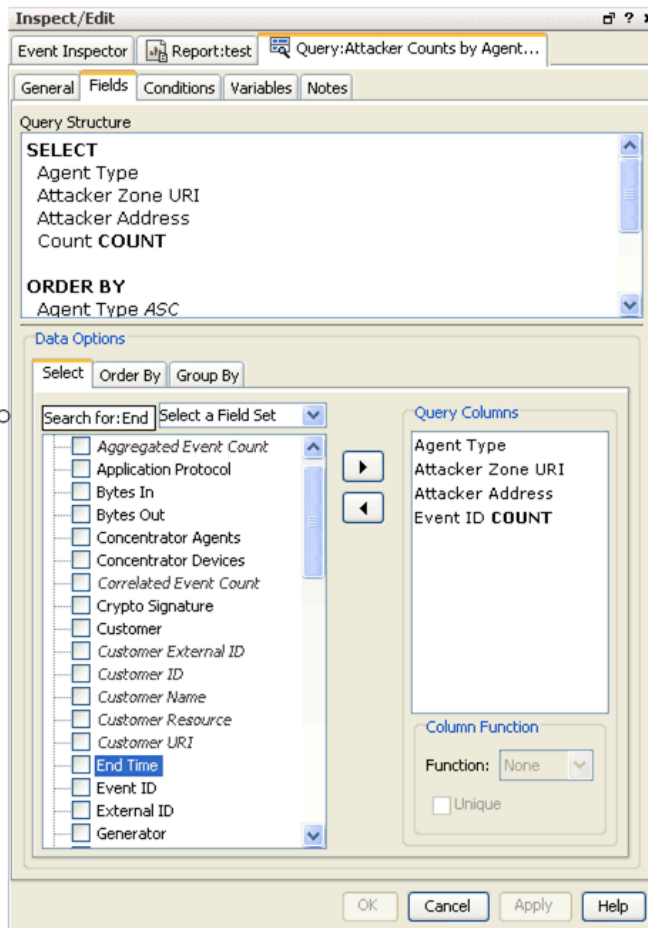
- Choose **Window > Inspect/Edit Panel** to open or restore the panel, if it already has inspectors or editors in it. If no inspectors or editors are open, the panel isn't available.
- When no editors or inspectors are open, or to work with different ones, double-click an event in a grid view or right-click an item in a Navigator panel resource tree and choose **Show <resource>**.
- To clear an editor from the Inspect/Edit panel, right-click its tab and choose **Close**.
- Click the **Hide Empty Rows** button () beside the **Select a Field Set** menu to see only populated fields.
- Click the New Field Set button () to create a new field set.
- Click the icon toggle button () to show/hide icons next to each field entry.

Searching for Fields in Event Inspector, Resource Editors or CCE

To find an item in a list of fields on the Event Inspector, any Resource Editor, or the [Common Conditions Editor \(CCE\)](#), click any field Name (on the left side of the field list) and start typing. A Search popup is displayed when you start typing, and shows the term as you type it. The search is predictive in that it will navigate to and select matching fields as you type. The Search utility works essentially the same way in the Event Inspector and in resource editors that use field sets and filters (and, by association, the CCE).



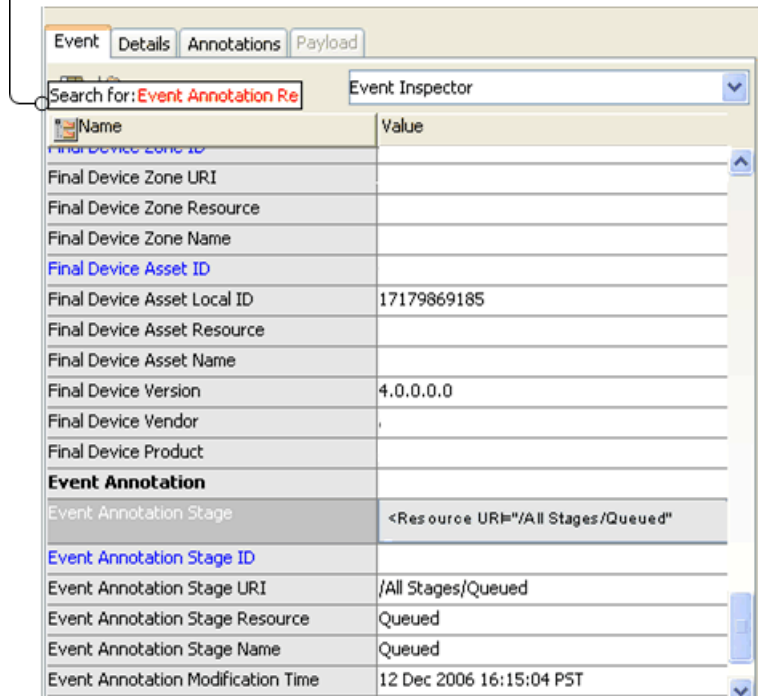
The popup Search on fields is available in all resource editors with Field tabs. To activate the Search, select the any field in the list and start typing.



If you start to type a term that is not in the field list, the Search popup text turns red. If you backspace out, the popup text will change from red to black when a matching field is found. Resume typing to find another matching term.

Predictive search updates as you type. If you start typing a term that is not in the list, your entry is highlighted in red.

You can backspace to erase letters in your search term. Your entry will show up in black again when it finds a match, and the Search utility will continue to jump to the first matching entry as you re-type.



To exit the Search, press the **Return** key.

To start a new Search, click into any entry under Name on the left side of the list again.

Getting More Help







The best way to learn more about the Event Inspector and each of the many resource editors is to click the question mark button (?) in the upper-right corner of the Inspect/Edit panel or **Help** button (Help) in the lower right of a resource editor.

Controlling the ESM Console

The ESM Console has certain common controls that you might use at any time to do basic tasks like copying and pasting, and showing or hiding panels or the status bar.

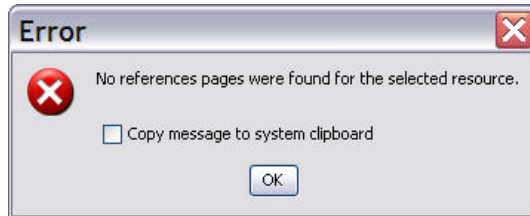
The controls you use the most are the toolbar buttons. There are four toolbars under the menus at the top of the Console. Each button has an identifying tooltip, but the full descriptions are as follows.

To show or hide toolbar components, right-click the toolbar and select or deselect the sections you want to change.

Tree	Icons	Resource
Standard application functions		The Save , Open , Cut , Copy , and Paste buttons operate as they do in any application. Saving and opening applies to ESM Console settings (.ast) files. Cutting, copying, and pasting applies to text and resources. (There is also a File > Save to Manager option available from the menus.)
Show or hide UI elements		Click the Show/Hide buttons to open/close the Navigator, Viewer, and Inspect/Edit panels and status or menu bars. Click the Floating button to bring floating windows forward.
Replay controls		The Replay buttons have essentially the same functions in certain views in the Viewer panel as their counterparts do on VCRs or CD players. From left to right, the buttons are: Rewind to Start , Rewind Incrementally , Pause , Play , Stop , Go Forward Incrementally , and Go Forward to End . You use the Replay buttons when working with channels configured for this mode.
Network tools		These buttons run standard IP-based network analysis tools as described in “Using the Network Tools” on page 107 .
Notifications		The Acknowledge Notifications button in the toolbar line tells you when you have messages to acknowledge. Click the button to open the Notifications manager in the Viewer panel so you can acknowledge the notification and resolve the issue.
Status Bar		<p>You can show or hide the status bar at the bottom of the Console window with this toolbar button, or use the Window > Status Bar menu command. When the status bar is showing, it displays Console operation messages. Normal status messages appear in blue and error messages are red.</p> <p>To view details on a message, click the message in the status bar. The ArcSight Messages dialog is displayed with the current message highlighted. From this dialog, you can access console messages, system messages and user notifications.</p> <p>To copy any message from the Messages dialog, highlight it and click Copy. The message is copied to the clipboard along with associated date and time. You can then paste the message into any other window, mail program, or editor that accepts ASCII text.</p>
Menu Bar		You use the menus in the menu bar as described in “Using the Menus” on page 114 .

Error and Warning Messages

Certain error messages, warnings, and notifications appear in a small dialog. To capture the error message and supporting data, click the Copy button or check **Copy message to system clipboard** to copy the entire message to the Clipboard. You can then paste the error message in text fields in the ESM Console, into the body of an e-mail message, or other applications.



Using the Network Tools

The network tools are the right-most set of buttons on the toolbar and are also available from the Tools menu. ArcSight provides **Ping**, **Traceroute**, **Nslookup**, **PortInfo**, **Whois**, **WebSearch**, and **Send Logs** as default utilities. Most of these tools are utilities you use to investigate events in grid views. In a grid view, you right-click an event to access these tools from a context menu. A new wizard-based utility called **Send Logs** gathers logs and diagnostic information for review or which you can email to ArcSight support.

You can add, copy, edit, or delete network tools using the Tools menu in the menu bar. The toolbar buttons and menu commands adjust automatically to such changes.



The Network Tools are also available as *integration commands* (see [“Network Tools as Integration Commands” on page 634 in Integration Commands](#)).

These tools are available in both places on the Console UI, but for future releases the legacy “network tools” feature described here will be phased out in favor of the integrations commands. The same, customizable tools and commands will be available (**ping**, **whois**, and so on), along with other new commands and a full set of application integration features.








To configure these tools, choose menu option **Tools > Local Commands > Configure**, as described in the following topics.

Running a Tools Command

To run a tools command:

- 1 In a grid view, select an IP address.
- 2 Right-click and select **Tools**, then one of the tool options described in [“Network Tool Default Options” on page 108](#).
- 3 Based on the tool selected, a window appears with the information.
- 4 In the window, click **Close**.

Network Tool Default Options

Tree	Icon	Resource
Nslookup		Resolve an IP address to a host or domain name or vice versa.
Ping		Determine whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response.
PortInfo		List standard usage, for example, WWW, FTP, and so on for a specified port number.
Traceroute		Show the path from the ESM Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between.
WebSearch		Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells.
Whois		Look up who is behind a given domain name; information might include addresses and telephone numbers.
Send Logs		Start the Send Logs wizard to gather logs and diagnostic information. Logs and diagnostics can be collected for all or a selected set of ArcSight components. (See “Send Logs” on page 980.)

Adding a Tool

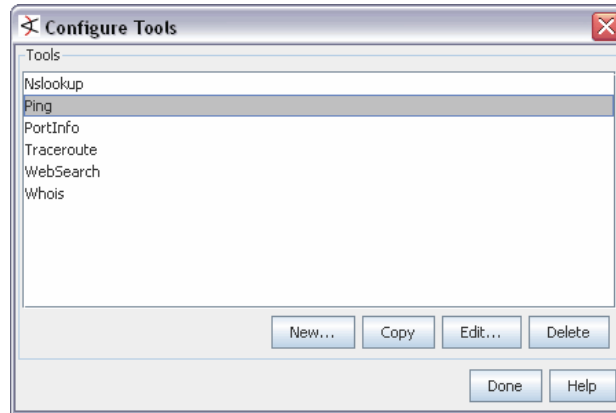
To add a tool:

- 1 Choose **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, click **New**.
- 3 In the Tool window, edit the Name, Program, Working Directory, Icon, and Program Parameters (command line parameters to be used for the program) text fields.
- 4 Click **OK**, then **Done**.

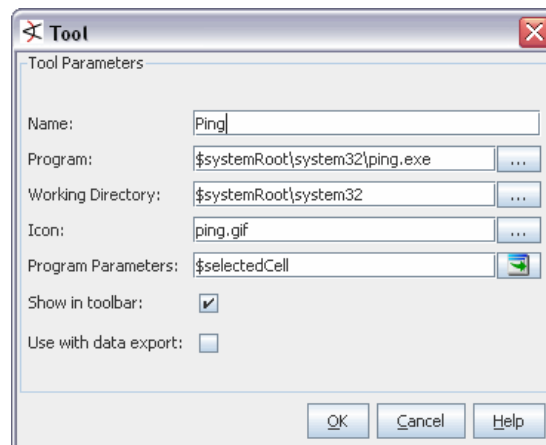
Configure (Edit) a Tool

To configure (edit) a tool:


- 1 Choose menu command **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, select an existing tool and click **Edit**.



- 3 In the Tool window, set these parameters and options:



Option	Description
Name	User-friendly name for this tool.
Program	Path to the executable file.
Working Directory	Default location assumed for arguments to the command. For example, to create a command (for example, <code>delete <file>.ast</code>) that acts on a file type that always resides in the same directory, specify the location here to save users from having to provide the full path to the file each time they use the command.
Icon	Path to the icon image file used to represent the tool.

Option	Description
Program Parameters	Provide any parameters needed for the command. You can type parameters in the field, or click the  button to get a pull-out menu where you can select Event Attributes to use as parameters, or add the selected cell or selected row as parameters to the command.
Show in toolbar	When Show in toolbar is on, the tool icon is shown in the Console toolbar. By default, this option is selected.
Use with data export	The purpose of this option is to separate tools that are run against events in channels and tools used as a destinations for event export. By default this option is not selected (off). If this tool is to be used as a destination for event export, select Use with data export . If this tool contains a command that will run against events in a channel, leave Use with data export off.

- 4 **Name, Program, Working Directory, Icon, and Program Parameters** (command line parameters to be used for the program) text fields. Also select whether you an the tool to show in the toolbar
- 5 Click **OK**, then **Done**.

Deleting a Tool

To delete a tool:

- 1 Choose menu command **Tools > Local Commands > Configure**.
- 2 In the Configure Tools window, select an existing tool and click **Delete**.
- 3 In the dialog box, click **Yes**.
- 4 Click **Done**.

Staying Informed

This topic discusses ways by which the Console helps you stay informed about developing situations involving events, and critical system status.

In addition to the security-event information ArcSight collects and analyzes, you can get, record, and pass other types of working information. This additional information falls into these categories:

Acknowledging Notifications

To be informed when certain defined events or circumstances occur. You might receive notifications by pager, or e-mail or similar means, but you can be sure to see an indicator in the **Notifications** button in the toolbar line of the Console.

Notifications can be sent as a result of a rule action, or by another user monitoring events in a grid. Clearing a notification requires that you acknowledge it. Whether or not you need to take other action depends on the circumstances. Acknowledgements are described briefly here, but for full detail, see ["Managing Notifications" on page 658](#).

Acknowledging a Page

Acknowledge a page by replying to it through your pager. All pagers must be configured to send replies. Your reply is sent to the pager service provider and then to ArcSight.

Acknowledge a Cell Phone Message

Acknowledge a call by replying to the e-mail sent through your cell phone. An e-mail enabled cell phone is required for receiving notifications and replying to them.

Acknowledge an E-mail Message

Acknowledge an e-mail by replying to the message. Reply to the e-mail address from which the notification was sent.

Acknowledge Notifications at the ESM Console

The ESM Console automatically alerts you of pending acknowledgements. The **Acknowledge Notifications** button is automatically enabled when you have one or more notification messages to be acknowledged. When you click the **Acknowledge Notifications** button, the Notifications manager opens in the Viewer panel so you can acknowledge and resolve the notification.

Using Notes

Each resource and resource group in the Navigator panel has an editor, and each editor has a Notes tab. The Notes tab retains all the text that you and others add to the resource.

Notes tabs have Table and List sub-tabs to show you tabular or text layouts of the notes accumulated for a resource. Notes are stored chronologically and you can sort them by clicking the **Date**, **Owner**, and **Text** headers.

Adding a Note

To add a note:

- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose **Edit Group**. If it is a resource, choose **Edit <resource>**.
- 4 In the Inspect/Edit panel, click the editor's **Notes** tab.
- 5 In the Notes space, type a note.
- 6 Click **Save** and then **OK**.

Viewing a Note

To view a note:

- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose **Edit Group**. If it is a resource, choose **Edit <resource>**.
- 4 In the Inspect/Edit panel, click the editor's **Notes** tab.
- 5 Right-click a note and choose **View**.

Deleting a Note

To delete a note:

- 1 Choose a resource tree in the Navigator panel.
- 2 Select a resource group or individual resource.
- 3 Right-click an item in the tree. If it is a group, choose **Edit Group**. If it is a resource, choose **Edit <resource>**.
- 4 In the Inspect/Edit panel, click the editor's **Notes** tab.
- 5 Right-click a note and choose **Delete**.

License Tracking

The product tracks the status of licenses for features you use, including actors, domains, ESM Console user limits, ArcSight Web user limits, device number limit, actor and asset number limit, and events-per-second limit.

Licenses for the features available to you are installed and configured at setup time. For details about setting up licenses during the installation and configuration process, see the *ESM Installation and Configuration Guide*.



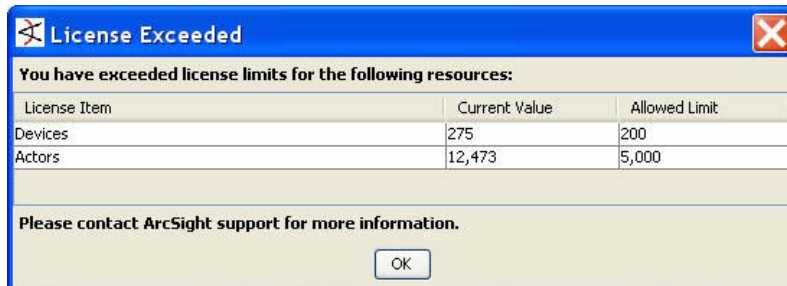
License tracking includes disabled and deleted actors

The ESM license tracking feature includes actors that are still in the ESM actor model with the status **Disabled** or **Deleted in IDM**. ESM's identity management feature preserves disabled and deleted actors in the actor model to track any unauthorized activity related to disabled or deleted actors.

If you do not want the ESM license tracking feature to evaluate actors with the status **Disabled** or **Deleted in IDM**, you can manually remove them from the ESM actor model. Manually removing disabled or deleted actors also removes the ability for ESM to track unauthorized activity related to these accounts. For details, see ["Deleting Actors" on page 265](#).

License Tracking Notifications



If your feature usage is close to or has exceeded the license agreements for your organization, you see a notification dialog when starting up the ESM Console, for example:



Your access to these features remains in place, even if the license limit has been exceeded.

Standard Reports for License Status Tracking

You can check on the status of your ESM feature licenses using the following reports and focused reports ([All Reports/ArcSight Administration/ESM/Licensing](#)):

Report	Type	Description
Licensing Report		This report shows the licensing history for one of the license types, and is the source report for the individual license focused reports. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
Licensing Report (All)		This report shows the licensing history for all the license types. The 6 charts show the current count and the count limit for each of the license types. The licensing history is over the last 7 days, by default.
Actors Licensing Report		This focused report shows the licensing history for actors. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
Assets Licensing Report		This focused report shows the licensing history for assets. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
Console Users Licensing Report		This focused report shows the licensing history for console users. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
Devices Licensing Report		This focused report shows the licensing history for devices. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
EPS Licensing Report		This focused report shows the licensing history for EPS. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.
Web Users Licensing Report		This focused report shows the licensing history for web users. The chart shows the current count and the count limit in a chart. The licensing history is over the last 7 days, by default.







For details about running reports, see [“Running Reports” on page 423](#).

Using the Menus

This section briefly describes the Console's menus and sub-menus.





File Menu




Keyboard shortcut **Alt+F** opens the **File** menu. Keyboard shortcuts for File menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 119](#).

Option	Icon	Resource	Shortcut
New		Create a new resource from the available submenu.	
Open		Open an existing Console settings file to use that configuration.	Ctrl-O
Save		Save your latest Console settings in the current configuration file.	Ctrl-S
Save As	None	Save your current Console settings in a different configuration file.	
Save to Manager		Save your current Console settings at the ArcSight Manager rather than locally, so you can get these settings at a different Console.	
Load From Manager		Load a preferred Console configuration file from the ArcSight Manager, so you can use it at this Console.	
Send To		Send a local Console configuration (.ast) file to an e-mail address so another user can save and use it at their Console.	
Log Out	None	Log out of the Console with your current user ID, without exiting, so someone else can log in.	
Exit	None	Log out of the Console and exit.	Alt-F4

Edit Menu






Keyboard shortcut **Alt+E** opens the **Edit** menu. Keyboard shortcuts for Edit menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 119](#).


Option	Icon	Resource	Shortcut
Cut		Cut selected text.	Ctrl-X
Copy		Copy selected text or resources.	Ctrl-C
Paste		Paste text or resources from the clipboard.	Ctrl-V
Delete		Delete selected text or resources.	Delete

Option	Icon	Resource	Shortcut
Select All		Select all text.	Ctrl-A
Preferences		Open the Preferences dialog box to make personal configuration changes.	
Find Resource		Use the Find Resource query editor to search for resources and review their details.	Ctrl-F

View Menu






Keyboard shortcut **Alt+V** opens the **View** menu. Keyboard shortcuts for View menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 119](#).

Option	Icon	Resource	Shortcut
New Active Channel		Open the New Active Channel dialog box so you can set up and start a new active channel in the Viewer panel.	Ctrl+Shift-D
Show Active Channel		Open the Active Channel Selector dialog box so you can choose an active channel to display in the Viewer panel.	Ctrl+Shift-S
Recent Active Channels		Choose a recently opened active channel to display in the Viewer panel again, if available.	
Resource Hotkeys		Shows currently programmed keyboard shortcuts for actions on the Console. These keyboard shortcuts are defined via in the Console Preferences dialog (Edit > Preferences > Manage Hotkeys). For more information, see “Keyboard Shortcuts (Hot Keys)” on page 119 .	
New Dashboard		Create a new, untitled and empty dashboard to populate with data monitors.	Ctrl+Shift-B
Show Dashboard		Open the Load Dashboards dialog box so you can select dashboards to open in the Viewer panel.	Ctrl+Shift-W
Recent Dashboards		Choose a recently opened dashboard to display in the Viewer panel again, if available.	
Notification Acknowledgment		Show all Notifications for the current user (pending, undeliverable, not acknowledged, acknowledged, and resolved)	Ctrl-N
Show Messages		Show all console messages, system messages, and user notifications in the ArcSight Messages dialog.	Ctrl-M
Next View		Take you to the next open view or tab in the Viewer.	Ctrl+Shift-N
Previous View		Take you to the previous open view in the Viewer.	Ctrl+Shift-P
Close All Views		Close all views that are open in the Viewer panel.	

Option	Icon	Resource	Shortcut
Slide Show		Show a continuous slide show of all open channels and dashboards.	F11 (Toggle to start or stop)








Window Menu


Keyboard shortcut **Alt+W** opens the **Window** menu. Keyboard shortcuts for Window menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 119](#).

Option	Icon	Resource	Shortcut
Navigator Panel		Show or hide the Navigator panel.	Ctrl-1
Viewer Panel		Show or hide the Viewer panel.	Ctrl-2
Inspect/Edit Panel		Show or hide the Inspect/Edit panel.	Ctrl-3
Status Bar		Show or hide the status bar.	Ctrl-4
Floating		Bring to the front one of the listed floating (undocked) windows, if available.	

Tools Menu



Keyboard shortcut **Alt+T** opens the **Tools** menu. Keyboard shortcuts for Tools menu options are included below. See also [“Keyboard Shortcuts \(Hot Keys\)” on page 119](#).

Option	Sub-menu	Icon	Resource	Shortcut
Local Commands	Configure		Add, copy, edit, or delete Network Tools.	Alt-C
	Results		Display the Tool Results dialog box.	Ctrl+Shift-R
	Nslookup		Resolve an IP address to a host name.	
	Ping		Determine whether an IP address is online.	
	PortInfo		List the default protocol usage for a specified port number (e.g., WWW, FTP, SMTP).	
	Traceroute		Show the path to an IP address.	
	WebSearch		Use Google to search the web for event-related keywords.	

Option	Sub-menu	Icon	Resource	Shortcut
	Whois		Find the registered owner of a given domain name.	
Network Model			Launch the Network Model wizard. See "Populating the Network Model Using the Wizard" on page 744 .	
Use Case			Launch the Use Case wizard. See "Configuring Use Cases" on page 518 .	
Send Logs			Launch the Send Logs wizard. See "Send Logs" on page 980 .	





System Menu


Keyboard shortcut **Alt+S** opens the **System** menu. See also ["Keyboard Shortcuts \(Hot Keys\)" on page 119](#).

Option	Icon	Resource
Scheduled Jobs		Open the Job Scheduler. For more information, see "Scheduling Jobs" on page 977 .
Categorize Event		Select a non ArcSight event in the grid, then select System > Categorize Event menu option to apply a category. For more information, see "Apply Standard Asset Categories to Assets" on page 54 and "Categories" on page 836 .

Help Menu

Keyboard shortcut **Alt+H** opens the **Help** menu. Keyboard shortcuts for Help menu options are included below. See also ["Keyboard Shortcuts \(Hot Keys\)" on page 119](#).

Option	Icon	Resource	Shortcut
Help Contents		Open the ESM Console Online Help. The online help's Welcome page provides more details about using the Help, including navigating, printing, getting PDFs, and more.	F1
What's New		Open the ESM Console Online Help "What's New" topic. See also Chapter 1, What's New, on page 41 .	
Browse ArcSight Documentation		Open an index page that offers pointers and links to other PDF-formatted documents concerning subjects such as SmartConnectors or upgrading.	
ArcSight Support		Open a browser window that displays the ArcSight Support login page, so you can sign in and use the ArcSight Support Center's User Forum and other features.	

Option	Icon	Resource	Shortcut
About		Show your ArcSight installation's legal notices and version information.	

Keyboard Shortcuts (Hot Keys)

You can accomplish many actions in the ESM Console by using the default keyboard shortcuts or *hot keys*, instead of menus and mouse navigation. The standard keyboard shortcuts and their associated actions is listed in the table below. Keyboard shortcuts associated with menu options are included here and also shown in [“Using the Menus” on page 114](#).



You can view the default keyboard shortcut schemas and set up custom shortcuts on the Hot Key tab in the Console Preferences dialog (Console menu option **Edit > Preferences**, click **Manage Hot Keys**). For information on how to view or configure Console keyboard shortcuts, see [“Managing Hot Keys” on page 779 in Chapter 30, Personalizing the ESM Console, on page 771](#).

Task	Keyboard Shortcut	Description
Annotate event (s)	Ctrl-T	Select one or more events in any grid view, and use Ctrl-T keyboard command (as an alternative to the right-click Annotate Events menu option). See “Annotating an Event” on page 217 .
Mark events reviewed	Ctrl-R	Select one or more events in any grid view, and use Ctrl-R keyboard command (as an alternative to right-click Mark as reviewed menu option). See “Collaborating on Events” on page 216 .
Copy	Ctrl-C	See “Edit Menu” on page 114
Cut	Ctrl-X	See “Edit Menu” on page 114
Delete	Delete key	See “Edit Menu” on page 114
Find	Ctrl-F	See “Edit Menu” on page 114
Open the Edit menu	Alt-E	See “Edit Menu” on page 114
Paste	Ctrl-V	See “Edit Menu” on page 114
Redo	Ctrl-Y	Re-do any text edit operation.
Select All	Ctrl-A	See “Edit Menu” on page 114
Undo	Ctrl-Z	Undo any text edit operation.
Exit/shut down the Console	Alt-F4	See “File Menu” on page 114
Open the File menu	Alt-F	See “File Menu” on page 114
Open the Edit menu	Alt-E	See “Edit Menu” on page 114
Open the View menu	Alt-V	See “View Menu” on page 115
Open the Window menu	Alt-W	See “Window Menu” on page 116
Open the Tools menu	Alt-T	See “Tools Menu” on page 116
Open the System menu	Alt-S	See “System Menu” on page 117
Open the Help menu	Alt-H	See “Help Menu” on page 117 and “About the Online Help” on page xxxvii .
Open the Help directly	F1	See “Help Menu” on page 117 and “About the Online Help” on page xxxvii .

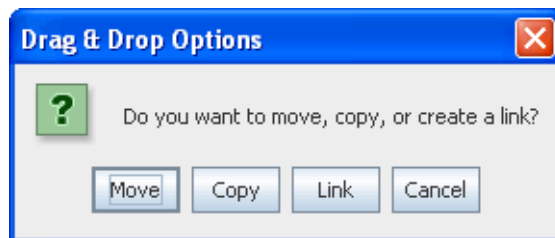
Moving Copying, Linking, and Deleting Resources

You may need to move or duplicate a resource to better organize your work or to make editable copies. You may also need to delete resource definitions you no longer need. These tasks are described here. For more information, see all topics in [Chapter 6, Working in the ESM Console, on page 93](#).

Move, Copy, or Link a Resource

To move, copy, or link a resource:

- 1 Choose the resource type you want to work with in the Navigator (Active Channels, Filters, Rules, and so on).
- 2 Navigate to and select a resource instance in the tree, and drag and drop it into another group of the same resource type. The system displays a dialog that provides options to move, copy, or link the resource.



Select **Move** to move the resource, **Copy** to make a separate copy of it, or **Link** to create a copy of the resource that is linked to the original.

If you select **Copy**, you create a separate copy of the resource definition that will not be affected when the original is edited. If you select **Link**, you create a copy of the resource definition that is linked to the original. Therefore, if you edit a linked resource definition, whether it be the original or the copy, all links are edited as well. When deleting linked resource definitions, you can either delete only the selected one or the selected one and all linked copies.

Delete a Resource

To delete a resource:

- 1 Navigate to the resource type you want to work with.
- 2 Select a resource instance in the tree, right-click and choose **Delete <Resource>** from the context menu.

Printing from the Console

You can print Navigator trees for all resources. You can print resource definitions for rules, filters, and cases, as well as conditions from the [Common Conditions Editor \(CCE\)](#) (for all resources with filters). You can print from all grid or channel views.



Note

As you would expect, you can also print any item for which the Console calls a Web browser, such as graphs, charts, and reports. This topic deals specifically with printing directly from the Console those resources or elements of resources that are not displayed in a web browser by default.

Printing Navigation Tree Views of Resources

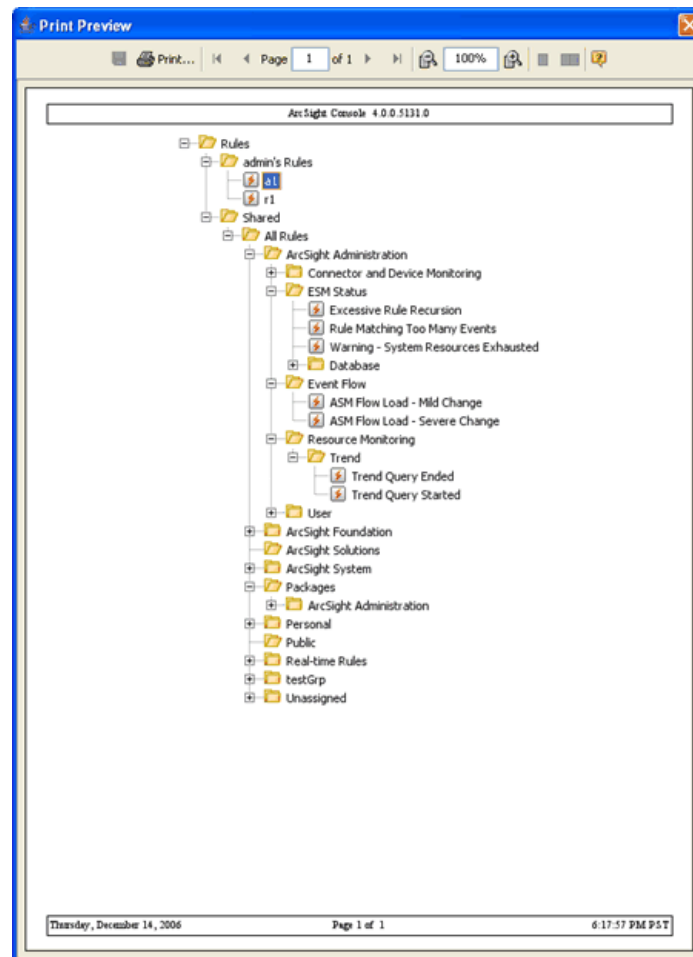
To print the Navigation tree for a resource:

- 1 In the Navigator, choose the resource you want to print.
- 2 Click items in the tree to expand or collapse folders in the tree depending on what you want to see in the printout.



A printout of the Navigation tree for a resource will show the tree exactly as it is displayed on the Console. Folders that are expanded or collapsed on the Console will show the same way in the printout. To print the tree showing the items contained in a particular folder, expand the folder in the Navigation tree before selecting the Print option.

- 3 Right-click any element in the Navigation tree for that resource and choose **Print <ResourceName> Tree**. (For example, Print Rule Tree.) Regardless of which item you select to access the right-click menu, the whole tree prints.
- 4 The system displays a print preview such as the preview of a Rules tree, as shown.



- 5 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 6 Click **OK** to print.

Printing Resource Definitions

You can print resource definitions for rules, filters, and cases. You can print a resource definition from the Navigator tree or from within the resource editor.

To print a resource definition:

- 1 In the Navigator, choose the type of resource you want to print.
- 2 Right-click an instance of that resource (a rule, filter, or case), and choose **Print <ResourceName> Definition** (for example, Print Rule Definition).

Or

Double-click a resource to open its editor in the Inspect/Edit panel, then right-click the topmost tab in the editor and choose **Print <ResourceName> Definition**.

The system displays a print preview such as the preview of a Rules definition.

From the Print Preview of a resource definition you can:

Export and save as an HTML file,

Or


Print.

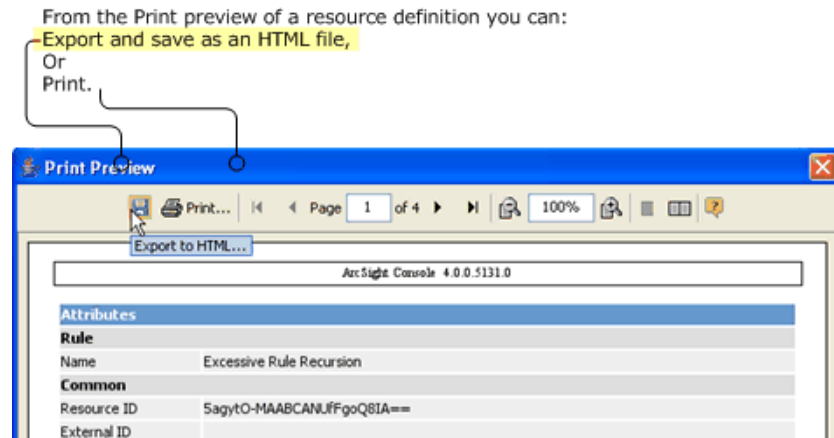


- 3 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 4 Click **OK** to print.

Saving as an HTML File

From the Print Preview dialog for a Resource Definition, you can save the definition as an HTML file.

- 1 On the Print Preview dialog, click the **Export to HTML** () tool button.



- 2 In the file browser, navigate to the location where you want to save the HTML file.
- 3 Enter a name for the file in the File Name field. The File Type is **Web Page (*.html)** by default.
- 4 Click **Save**.

Printing Grid Views

To print items from a grid view, (such as an active channel or active list):

- 1 Select one or more items in the grid. To select multiple, adjacent items, use the **Shift** key and mouse click, or click and drag. To select non-adjacent items, use the **Alt** key in combination with mouse clicks.
- 2 Right-click and choose **Print Selected Rows**.

The system displays a preview of the printout. (For examples, see [“Using Column Flip Limit to Format Grid View Printouts” on page 125.](#))
- 3 Click **Print** to open the Print dialog, and set these properties (which printer, page layout, and so on).
- 4 Click **OK** to print.



The format of a grid view printout is determined by the number of columns in the table and the configuration of the Column Flip Limit, which is set in the Console Preferences dialog. For more information, see [“Using Column Flip Limit to Format Grid View Printouts” on page 125.](#)

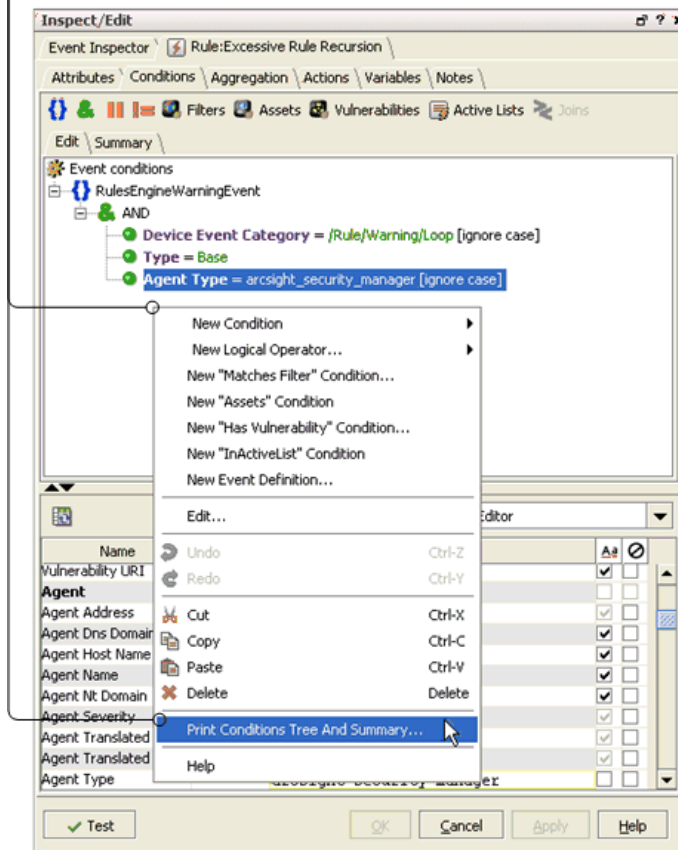
Printing Conditions Tree Summary

You can print Conditions for any resource with filters.

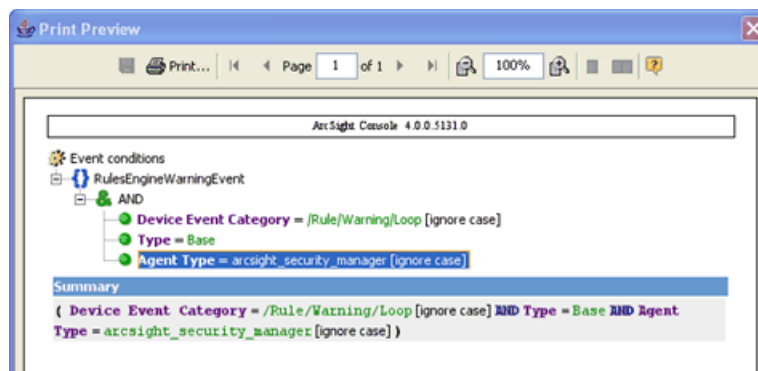
- 1 Open the resource in the Editor.
- 2 Click the **Conditions** tab.

- 3 Right-click anywhere on the Edit tab in the [Common Conditions Editor \(CCE\)](#).
- 4 Choose **Print Conditions Tree and Summary** from the context menu.

To print Conditions for any resource with filters, open the resource in the Editor, click the **Conditions** tab, and right-click anywhere on the **Edit** tab of the **Common Conditions Editor**. From the context menu, choose **Print Conditions Tree and Summary**.



The system displays a preview of the printout. For example, here is a Print Preview of the filter for a stock rule called Excessive Rule Recursion.



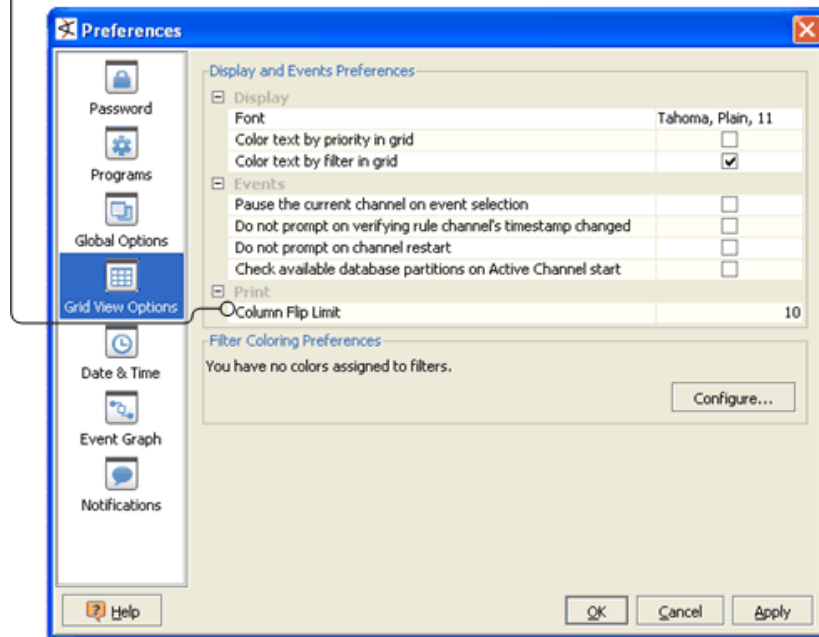
- 5 Click **Print** to bring up a standard Print dialog, and set these properties (which printer, page layout, and so on).
- 6 Click **OK** to print.

Using Column Flip Limit to Format Grid View Printouts

For printing tables from Grid Views (channels, lists, and so forth), you can configure the **Column Flip Limit** in the Console Preferences.

Choose **Edit > Preferences**, and click **Grid View Options**. The default is 10 columns.

For printing tables from Grid Views (channels, lists, and so forth), you can configure the **Column Flip Limit**. (Choose **Edit > Preferences** and click **Grid View Options**.) A grid view will print as a table or with details per row, depending on the number of columns it has and how the Column Flip Limit is configured.



Grid views with the same or fewer columns than the Column Flip Limit print as a table, the same as that shown in the UI on the Console grid view.

Grid views with the same or fewer columns than the Column Flip Limit print as tables, in the same format shown in the UI on the Console grid views.

Print Preview

Print... Page 1 of 2 100%

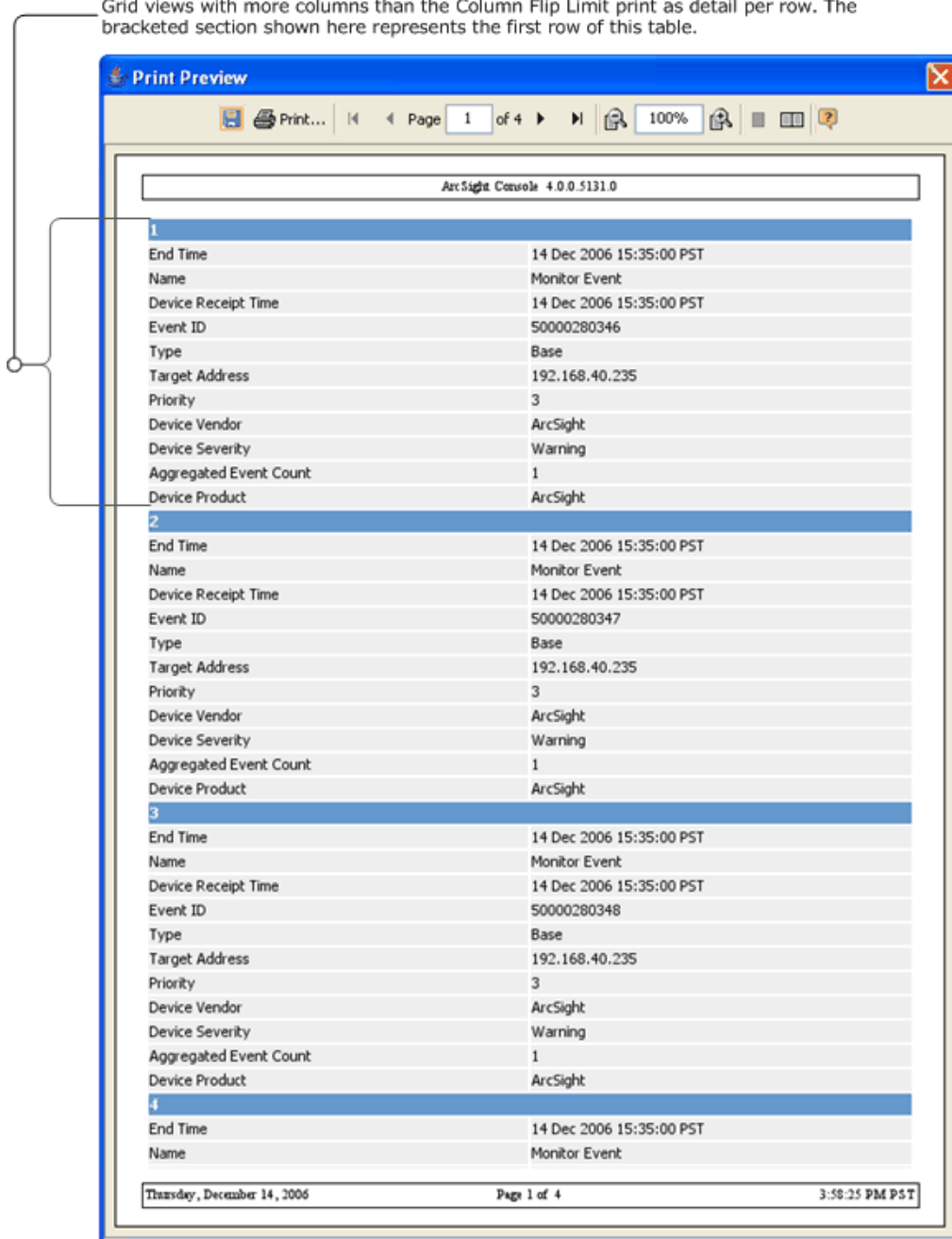
ArcSight Console 4.0.0.5131.0

End Time	Name	Device Receipt Time	Event ID	Type	Target Address	Priority	Device Vendor	Device Severity	Aggregated Event Count
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280345	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280346	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280347	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280348	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280349	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280350	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280351	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280352	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280353	Base	192.168.40.235	3	ArcSight	Warning	1
14 Dec 2006 15:35:00 PST	Monitor Event	14 Dec 2006 15:35:00 PST	50000280354	Base	192.168.40.235	3	ArcSight	Warning	1

Thursday, December 14, 2006 Page 1 of 2 4:53:19 PM PST

Grid views with more columns than the Column Flip Limit print details per-row rather in a normal table like that shown on the Console grid view.

Grid views with more columns than the Column Flip Limit print as detail per row. The bracketed section shown here represents the first row of this table.



The image shows a 'Print Preview' window from the ArcSight Console. The window title is 'Print Preview'. The toolbar includes a 'Print...' button, navigation arrows, 'Page 1 of 4', a magnifying glass, '100%', and other icons. The main content area displays a table of event details. The table has a header row with the title 'ArcSight Console 4.0.0.5131.0'. The table contains four rows of data, each representing an event. The first row is highlighted with a blue header. A bracket on the left side of the window points to the first row of the table.

ArcSight Console 4.0.0.5131.0	
1	
End Time	14 Dec 2006 15:35:00 PST
Name	Monitor Event
Device Receipt Time	14 Dec 2006 15:35:00 PST
Event ID	50000280346
Type	Base
Target Address	192.168.40.235
Priority	3
Device Vendor	ArcSight
Device Severity	Warning
Aggregated Event Count	1
Device Product	ArcSight
2	
End Time	14 Dec 2006 15:35:00 PST
Name	Monitor Event
Device Receipt Time	14 Dec 2006 15:35:00 PST
Event ID	50000280347
Type	Base
Target Address	192.168.40.235
Priority	3
Device Vendor	ArcSight
Device Severity	Warning
Aggregated Event Count	1
Device Product	ArcSight
3	
End Time	14 Dec 2006 15:35:00 PST
Name	Monitor Event
Device Receipt Time	14 Dec 2006 15:35:00 PST
Event ID	50000280348
Type	Base
Target Address	192.168.40.235
Priority	3
Device Vendor	ArcSight
Device Severity	Warning
Aggregated Event Count	1
Device Product	ArcSight
4	
End Time	14 Dec 2006 15:35:00 PST
Name	Monitor Event

Thursday, December 14, 2006 Page 1 of 4 3:58:25 PM PST

Instructions for setting the Column Flip Limit for grid views is also summarized in Setting Grid View Options in the [“Changing User Preferences”](#) on page 772, along with information about how to set other Console preferences.

Chapter 7

Monitoring Events

This topic describes how to monitor events coming from SmartConnectors using tools that are displayed in the Viewer panel.

[“Monitoring Active Channels” on page 129](#)
[“Using Dashboards” on page 153](#)
[“Using Data Monitors” on page 160](#)
[“Using Query Viewers” on page 167](#)
[“Using Custom View Dashboards” on page 167](#)
[“Monitoring Active Lists” on page 174](#)
[“Graphing Attacks” on page 176](#)

You can monitor events through a rich set of views, including active channel and grids, dashboard graphics and tables, and active lists, as described in the following topics.

Monitoring Active Channels

Active channels provide a streaming view of events coming into your system that can be viewed numerous ways using numerous types of filters and field sets.

Using Views

Views can vary in scope and scale, from broad to narrow, and from graphic to detailed, depending on how your enterprise is organized and monitored.

Selecting a View

In the Viewer panel, click a tab at the **top** to choose an active channel by name. When you've chosen a channel, you can select various instances of that channel (such as a grid view and bar chart of the same data) by clicking its tile, or its tab at the **bottom** of the panel.

Alternately, to quickly advance through each of the tabs in the Viewer panel, press **Ctrl+Shift+N** (next) or **Ctrl+Shift+P** (previous) to jump forward or backward. This applies to any type of view in the Viewer panel.

Changing View Layouts

You change individual view layouts with the **Layout** menu available from the blue icon at the lower-right corner of the Viewer panel. Click this icon to choose:

Layout Option	Result
Tab	Fill the active channel display with the current view and make other open views selectable by tabs at the lower border.
Tile Best Fit	Display all views in the active channel as variously shaped tiles, giving each a proportional amount of space.
Tile Horizontally	Display all views in the active channel horizontally, giving each a proportional amount of space.
Tile Vertically	Display all views in the active channel vertically, giving each a proportional amount of space.

Floating a View

In the active channel's name tab, right-click and choose **Float**.

Closing One or All Views

In the active channel's name tab, right-click and choose **Close** or **Close All**.

To close an individual view **Shift+click** its name tab. You can also right-click a view name tab and choose **Close** from the popup menu.

Closing all Views Except the Current One

In the active channel's name tab, right-click and choose **Close All But Current**.

Viewing and Using Channels

Viewing and using active channels includes creating them, filtering them, customizing contents, changing presentation formats or layouts, and deleting them.

Also, an action from a triggered rule can create a new active channel.



Press Enter to register edits made in editors and channel columns

To ensure that ESM registers a change you make to a field in editor and channel columns, hit the Enter key before clicking **Apply** or **OK**.

Viewing an Active Channel

To view an active channel:



- 1 Choose **Active Channels** in the Navigator.
- 2 Right-click a channel and choose **Show Active Channel**. The selected channel is displayed in the Viewer.



If a channel is open when Daylight Savings Time goes into or out of effect, the live channel will not reflect the correct start and end times until it is stopped and re-started.

Sorting Events in an Active Channel

The names of sortable fields in column headers are indicated with a double-arrow icon .

If a field is already sorted, an up  or down  arrow indicates the direction of the sort.

To sort events in an active channel:

- ◆ To sort the list by a column, right-click over the column and select **Sort Column**.
- ◆ To reverse the sort order, select **Sort Column** again on an already-sorted column. This makes the column the primary sort column.
- ◆ To remove a sort, right-click over a sorted column and select **Remove Sort**.

For more information, see [“Applying a Field Set to an Active Channel” on page 132](#) and [“Using Sortable Columns in Grid Views” on page 988](#). For information about how to create field sets that use sortable field sets, see [“Creating and Using Field Sets” on page 204](#).

Primary and secondary sort columns

When you select Sort Column, it becomes the primary sort column and the number 1 appears next to the sort arrow. The previous column by which the report was sorted becomes the secondary sort column and the number 2 appears next to the sort arrow.

This numbering applies to every column on which you sort, the newest sort is always 1 and the others change accordingly.

Sorting by primary and secondary time columns

When your primary and secondary sort columns are both time columns (such as Create Time and Modification Time), milliseconds become a factor in sort order.

Milliseconds are not displayed. This can create a situation where a number of items with the same primary time appear to show the secondary sort as in the wrong order. In reality the primary times are off by milliseconds, so they are *not* the same, and these milliseconds affect sort order before the secondary time is taken into account.

Creating an Active Channel

To create an active channel:

- 1 Choose the **File>New>Active Channel** menu command to open the **New Active Channel** dialog box, or right-click a group in the Active Channel resource tree and choose New Active Channel.
- 2 In the dialog box, name the channel and choose from the options described in [“To change an active channel's operating parameters, click the Attributes tab.” on page 135](#).
- 3 Click the **Examples** button to see how to specify commonly used channel values.

- 4 Click **OK** to save the new channel in your group in the Active Channels resource tree, and to open and run it in the Viewer panel.



Viewing Resources in Active Channels

You can view certain resources (in addition to events) in active channels, including Assets, Vulnerabilities, Asset Categories, Scanner Reports, Cases, and Stages. In the Navigator, right-click a resource or group, and choose **Show <ResourceName>**. The resource(s) are displayed in an active channel view.

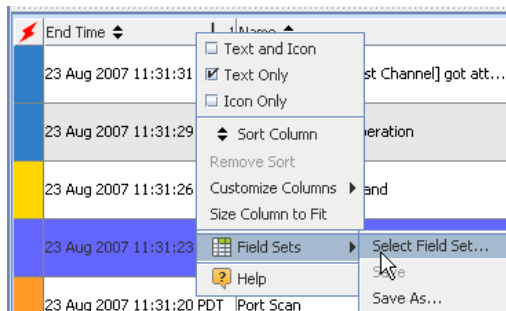
Using slightly different menu options, you can view the results of triggered Rules in channels as well. (For information on creating active channels for Rules, see [“Verifying Rule\(s\) with Events” on page 470.](#))

You can also create active channels from filters. In the Filters resource tree, right-click a filter and choose **Create Channel with Filter**. Many resources that have filters also provide this option. For example, you can right-click Connectors in the Navigator, and choose **Create Channel with Filter** to create a channel with the filter used by that connector. You can do the same with Assets (Assets, Vulnerabilities, Zones, Categories), Cases, and Stages. (For Cases, choose Case Details Channel as described in [“Creating a Channel for a Case” on page 590.](#) The case must include some events.)

Applying a Field Set to an Active Channel

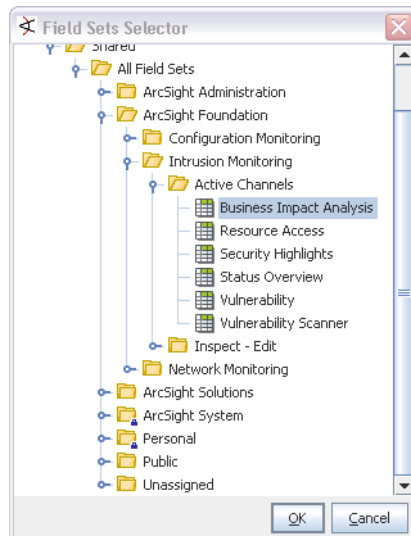
To apply a field set to an active channel:

- 1 Right-click over any field header and choose **Field Set > Select a Field Set** to open the Field Sets Selector dialog.



Field sets include any domain field sets you have created.

- 2 In the Field Sets Selector dialog, select a field set (or a domain field set you created) and click **OK**.



The active channel is displayed with the selected field set.



About ArcSight System Sortable Field Sets

The Sortable Field Sets under ArcSight System are not available for selecting in active channels. The ArcSight System sortable field sets are a special set marked for internal use to provide the sortable functionality and maintain consistency between the Console user interface, field sets, and database indexes.

For more information about sorting, see [“Sorting Events in an Active Channel” on page 131](#).

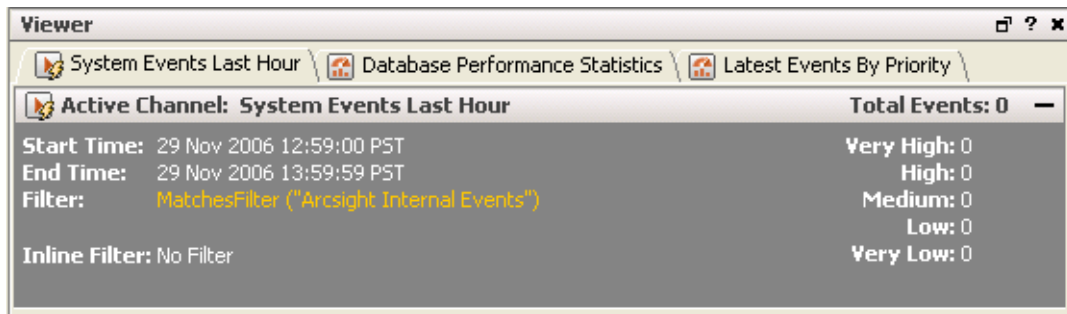
See [“Variable Availability and Contexts” on page 1019](#) for information about using variables in active channels.

Adding a Column to the Channel

You can add another column to the channel display to show additional fields.

Using an Active Channel Header

Each active channel has a header section with several features you can use to understand and manipulate what the channel displays.



Active Channel Header Features:

Feature	Usage
Name and Total	The top line of the header shows the channel's name and how many events it contains. You can also use the Plus (+) and Minus (-) buttons at the right end to open and close the header.
Priority Indicators	On the right border of the header is a column of event-priority statistic indicators. The numbers beside the Priority categories are the number of events in those categories. Click these indicators to filter the channel to show only the selected priority.
Time Span	The Start Time and End Time show the chronological range of the channel.
Filter status	This describes the filter that limits what the channel shows. Click a filter status name, such as <No Filter> , to open the Active Channel Editor and its Filters tab, where you can add, edit, or delete contents as described in "Creating Filters" on page 223 . You can also right-click the current filter status and choose to edit, save, or remove it.
Radar display button	Open and close the display with the Plus (+) and Minus (-) button at the right end of the Filter line.
Radar display operation	Click , Shift+click , Ctrl+click , or drag to select bars in the display. You can also drag a selection's borders left or right. The grid then shows just the events the selection represents. The display shows "This channel is active but temporarily empty" at any time, no matter how briefly, if there are no qualifying events. This also might show when a channel first opens.

Filtering an Active Channel

You can filter active channels through the Filter tab of the Active Channel Editor or inline using the blank fields in the top row of each grid view. Right-click the filter name in the header and choose **Edit Filter** to open the editor and create a filter as described in ["Creating Filters" on page 223](#). To use inline filters, see ["Using Grids" on page 145](#).



Understanding how to use the Common Conditions Editor (CCE) is integral to creating and editing filters. Please ["Common Conditions Editor \(CCE\)" on page 846](#) for more information.

Saving Copies of Active Channels and Filters

You can save copies of active channels or their filters to modify them later. This is useful to retain an original channel or filter as is, but use a copy of it for a new resource.

To save a copy of an active channel under a new name, right-click the filter name in the header, and choose **Save Active Channel As**. This brings up the Active Channels Selector dialog, which shows the Active Channels resource tree. Navigate to where you want to save the channel, enter a new name for it, and click **OK**.

You can use a copy of the filter for an active channel independently, or as a basis for other filters. Right-click the filter name in the header, and choose **Save Filter**. This opens the Filter Selector dialog, which shows the Filters resource tree. Navigate to where you want to save the filter, enter a new name for it, and click **OK**.

Editing an Active Channel

- 1 Right-click a channel in the Navigator panel's Active Channel resource tree and choose **Edit Active Channel**.
- 2 To change an active channel's operating parameters, click the **Attributes** tab.

Feature	Usage
Start Time	<p>The relative or absolute time reference that begins the period in which to track events in the channel. Edit the time expression, choose a common expression from the drop-down menu, or click the Selector button to choose an absolute date and time value. See "Timestamp Variables" on page 1003 for more expression options.</p> <p>Note: If a channel is open when Daylight Savings Time starts or ends, the live channel does not show the correct start time until you restart it.</p> <p>You can change the default start time for new channels by editing the <code>console.properties</code> file in the <code><ArcSight_ESM_Console_HOME>/current/config</code> directory. For example, add the this line...</p> <pre>console.channel.newChannel.defaultSubtractTime="\$Now - 2h"</pre> <p>... to change the start time to two hours ago. For a list of possible time values see the Start Time: field pull-down menu.</p>
End Time	<p>The relative or absolute time reference that ends the period in which to actively track the events in the channel. Edit the time expression, choose a common expression from the drop-down menu, or click the Selector button to choose an absolute date and time value. See "Timestamp Variables" on page 1003 for more expression options.</p> <p>Notes:</p> <ul style="list-style-type: none"> • If a channel is open when Daylight Savings Time starts/ends, the live channel does not show the correct start time until you restart it. • If setting the End Time results in the message "Invalid end date for sliding channel," this is because the channel is set to Continuously evaluate instead of Evaluate once at attach time. Either re-set the End Time or change the Time Parameters option for the channel to Continuously evaluate. • If possible, avoid creating active channels that query over more than 1 day. For active channels that query for more than 1 day, use Evaluate time parameters once at attach time instead of Continuously evaluate. Better yet, use trends for these types of active channels. See also "Best Practices to Optimize Active Channel Performance" on page 137.

Feature	Usage
Use as Timestamp	Choose the event-timing phase that best supports your analysis. End Time represents the time the event ended, as reported by the device. Manager Receipt Time is the event's recorded arrival time at the ArcSight Manager.
Time Parameters	Choose whether the channel will Continuously evaluate to show events that are qualified by Start and End times which are re-evaluated constantly while the channel is running, or Evaluate once at attach time to show only the events that qualify when the channel is first run. A channel set to Continuously evaluate is also known as a <i>sliding channel</i> , and typically has its End Time option set to \$Now .
Default Field Set	Choose an existing event field set for the events processed through the channel. The default field set is for users who view a channel for the first time. If no default is specified, the ArcSight system default is used. When a user closes a channel, ArcSight saves the field set (and all other console settings) to the user's <code>.ast</code> file. After a user has opened a channel once, the console does not use the default field set for that user again. Changing the default only affects other users who have never opened the channel before.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 684](#).

- 3 Click the **Filter** tab to edit the channel's filter condition as described in ["Creating Filters" on page 223](#).
- 4 Click the **Sort Fields** tab to explicitly set which fields to sort the channel on in grid views, the sort order for those fields, and whether sorting for each field is ascending (A to Z) or descending (Z to A).
- 5 Click the **Local Variables** tab to use ArcSight local variables with the active channel's filters.



You can create local variables which are available only to the resource you are creating (in this case, an active channel), or use global variables. For information on creating global variables, see ["Creating Filters" on page 223](#) and [Chapter 17, Global Variables, on page 477](#).

- 6 Click **Apply** or **OK** to save the updated channel.

Defining Grid Fields Options

In the New Active Channel dialog box you can choose from the **Select a Field Set** menu, or you can click the **Define** button to open the Define Grid Fields dialog box. See ["Creating and Using Field Sets" on page 204](#) for more information. To change these choices after creating a channel, use the steps described in ["Customizing Grid Columns" on page 152](#).

Feature	Usage
Fields	A name for the set.

Feature	Usage
Available Fields	Select the event fields (also called data fields or attributes) that you want the channel to process. As you make selections, they appear in the Fields to Show list at the right. Remember that not all fields are readily sortable.
Fields to Show	This list shows the selections you have made in the Available Fields list. The order you give to the fields in this list becomes their default presentation order in grid views. Once populated, you can select one or more fields (Shift+click and Ctrl+click apply) to rearrange with the Move Up , Move Down , and Remove buttons.
Move Up, Move Down, Remove	These buttons move or remove the fields you select in the Fields to Show list. The order you set becomes the presentation order in grid views.
Sort First By	After selecting and ordering fields, you establish their sorting order (also called their <i>group by</i> order). Use Sort First By to set the ascending (A to Z) or descending (Z to A) order of the first or most-significant column.
Then By	Use the first Then By sort-order field to set the second sorting order. Use the second Then By sort-order field to set the third sorting order.
More, Less	Click More if you need an additional Then By field. Click Less to remove one.

Discovering Patterns in an Active Channel

Right-click the channel in the Navigator panel's Active Channels resource tree and choose **Discover Patterns**. ArcSight takes a snapshot of the channel's current contents and examines it for patterns. You see the snapshot in the Viewer panel and the profile that generated the pattern appears in your personal folder in the Navigator panel's Pattern Discovery resource tree. For more information on pattern discovery, see ["Pattern Discovery" on page 179](#).

Deleting an Active Channel

Right-click the channel in the Navigator panel's Active Channels resource tree and choose **Delete Active Channel**.

Adding a View Format

To add another type of presentation (view) for the data in an active channel, click the **View Type** icon in the lower-right corner of the Viewer panel. Choose among grids and the various types of chart or graphic views.

Changing View Layouts

To change the visual arrangement of individual channels within a view container, such as data monitors within a dashboard, click the **Layout** icon and choose to show or arrange the views by **Tab**, or **Tile Best Fit**, **Tile Horizontally**, or **Tile Vertically**.

Best Practices to Optimize Active Channel Performance

The following topics compare active channels, reports, query viewers, and trends in terms of goals and optimal resources for various use cases.

Active Channels or Reports?

Active channels are the better choice if you would rather see results streaming in as the queries proceed, rather than wait for the results to appear in one view in a report.

However, if speed of results is your goal, you might want to run a report instead. The total completion time of an equivalent report would be faster than the total time it takes for the channel to load 100%. This is because the active channel runs multiple smaller queries instead of one large query to display initial results quicker.

See also, [“Building Queries” on page 354](#) [“Building Trends” on page 369](#), and [“Understanding Reporting Workflow” on page 331](#) in this guide, and “Query and Trend Performance Tuning” in the *Administrator’s Guide*.

Active Channels or Query Viewers?

[Query Viewers](#) behave more like reports (see [“Active Channels or Reports?” on page 138](#)) as they issue a single query and return all results in one go instead of the streaming progression of results from an active channel. Query viewers are most suitable if you have to slice and dice these query results further, for example, by changing the sort columns, changing types of charts/grid, and so on. These operations are performed on the client side with the results of the already-executed query. If you were using active channels instead, these types of changes would result in a re-run of the query.

See also [“Query Viewers” on page 287](#).

Active Channel Query Time Ranges

Take note of the query time range in one of your active channels. The more hours you are querying, the slower the results are to load. In terms of interactivity, an active channel shows results in minutes if you are querying a few hours of data. But the channel might start taking several hours to query larger time ranges that span more than 24 hours of data.

If you are querying over more than a day's worth of data, we recommend running a report (using queries and trends) or a query viewer instead of active channel.

Active Channel Filters

The more filter conditions you define in an active channel, the more work the channel has to do in the database to evaluate the conditions. In terms of interactivity, a channel that does not have any filter conditions will load data fastest. (This does not mean that the query will run on all events in the database. Only a subset of events are queried, based upon the page you are looking at in the channel.)

Filtering on Indexed Fields

Filtering on indexed fields is faster than filtering on non-indexed fields. You can find out which fields are indexed, by viewing these field sets:

/All Field Sets/ArcSight System/Sortable Field Sets/Field Set Based On ARC_E_ET Index

/All Field Sets/ArcSight System/Sortable Field Sets/Field Set Based On ARC_E_MRT Index

Filtering on Join Fields

The ESM event schema consists of a main **arc_event** table and several side tables. These side tables hold fields related to Annotation, Device fields, Agent fields, Resource References, and so on. If your query has a filter condition on a join field, the resulting channel would have to do more work to evaluate it.

Continuously-Updating Time Parameters

A channel that is “live” (querying against a moving time window and continuously updating the query time ranges) has to do more work than a channel based against fixed time windows. Performance will be better and faster on a channel with a fixed time window than on a live channel. (See also [“Use of the “Live” Channel from Standard Content” on page 139.](#))

End Time or Manager Receipt Time

Using “End Time” as the time field in your active channel is faster than using Manager Receipt Time. This is because End Time is used in the database as the partitioning key, so queries based on it query a smaller number of partitions.

Also, we recommend that you avoid creating channels that are based on one time field but sort on a different time field. A common cause of poor channel performance is user-created channels with this problem; that is, a channel based on End Time, but sorted on Manager Receipt Time (or vice versa).



When an event arrives at the Manager so late that the partition it belongs in is already beyond the retention period, the Manager adjusts the event's time range so that it is persisted in the second-to-oldest retained partition. The event is stored in the second-to-oldest partition because the oldest partition may be purged or archived anytime (such as during the data transfer).

This changes the events start and end times, which could cause correlation issues, but the chances of an event being delayed for longer than the retention period are low.

Sorting in Active Channels

By default, the channel has a sort order based upon the time field that was used for creating the channel (End Time or Manager Receipt Time). You have the option to sort on any other indexed columns defined in the two field sets referenced in [“Filtering on Indexed Fields” on page 138](#)). Note that the sorting operation is done in the database query, so every time you change sort by any column in your currently open active channel, effectively it has to re-create the complete channel. (You can use a query viewer instead, that does sorting on the client side with the data it has already queried.)

Also, the sorting operation can be very expensive, especially when millions of events match your filter conditions. Avoid sorting if your filter conditions are not restrictive. For example, the base channel with no filter conditions is normally fastest to load, but it would become the slowest to load if you change its default time based sort order.

Use of the “Live” Channel from Standard Content

If you are using [/All Active Channels/ArcSight System/Core/Live](#) or any similar channel, be aware that the performance of that channel is slower because it has several complex joins (Joins with Annotations, Resource Reference, Device), uses un-indexed fields, and performs additional bit-wise operations to evaluate its filter conditions. Depending upon your specific use-case, you can simplify and create your own “Live” channel that is more efficient.

Case Sensitive or Case-Insensitive Conditions?

Wherever possible, use case-sensitive conditions. That will save the extra computation needed for TOUPPER operation required for case-insensitive matches.

Query Execution Plan Issues

Sometimes, performance can degrade if Oracle Optimizer is choosing a suboptimal query execution plan. You can troubleshoot this with the help of ArcSight Customer Support. You can fix the most common execution plan issues by using these:

Regenerate event stats using this SQL script:

```
utilities/database/oracle/common/sql/RegenerateEventStats.sql
```

Capture system stats using this SQL script:

```
utilities/database/oracle/common/sql/GatherSystemStats.sql
```

For detailed steps, see [“Regenerate Event Statistics” on page 144](#) under [“Query and Trend Performance Tuning”](#) in the ESM Administrator Guide.

I/O Subsystem Performance

Channel query performance is typically limited by the performance of the I/O subsystem on the database. The more events you are inserting, the more load it would cause on the I/O. SAN performance, RAID levels, I/O caches, and so on play a role in how much performance we can obtain.

Database Parameters

Make sure that you are using the right-sized database template for your setup. You can seek ask ArcSight Customer Support for help on adjusting the database to make use of more available RAM, and so on.

To diagnose channel performance issues, start with the most basic active channel to see whether it meets your performance needs, and then keep refining/expanding to come to a point where you can tell what change is affecting performance. We recommend starting with the most basic active channel that has the following characteristics:

- Based upon End Time
- No filter conditions (also, make sure to run as an administrator user so that there is no access control filter)
- Query time is two hours ago to Now
- No continuous updates of time parameters

With above basic active channel, you should see less than a minute wait in starting the channel and doing random scrolls in the channel.

Investigating Views

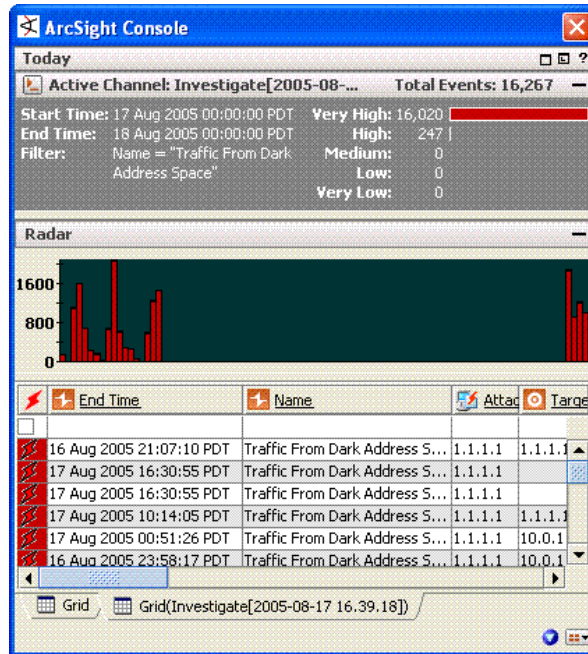
This topic explains how to use the Console's Investigate command to easily refine and explore channels contextually, using attributes of the events already being displayed in grid views. The Investigate command uses these attributes, and the values found in their events, to automatically formulate simple filters or conditions. When you create or refine a filter through Investigate, the Viewer panel automatically opens a new view of the channel with the filter applied. You explore the filter's effect in this view. You then have the option to keep the view by saving the channel under a new name, or discarding it by right-clicking in the grid and choosing **Close**.

When you use Investigate to add a condition to a resource editor such as Rules or Filters, the condition appears in the editor panel where you can modify it or click **Apply** to put it into effect.

The new or modified views you generate with the Investigate command can be grids, or you can choose to display them in applicable chart formats using the **Viewer Selector** icon in the lower-right corner of the Viewer panel.

To learn more about the event attributes these options use, please see [“Data Fields” on page 867](#).

Below is a temporary view created with the Investigate command



Using an Event Attribute to Show a New Filtered View

These options completely control the new view created, ignoring the filter in the original view. You most often use them to test and explore.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Create Filter [Attribute=Value]	Show only those events in which the selected attribute matches the value in the selected event.
Create Filter [Attribute!=Value]	Show only those events in which the selected attribute does not match the value in the selected event.
Create Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. Generally, attributes are considered related if they share a common focus such as IP addresses.

Refining a Filter with an Event Attribute

These options open a new view that uses a version of the prior filter modified to include the new filter component just selected. You usually apply these as part of a filter-refinement process.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add [Attribute=Value] to Filter	Show only those events that match both the prior and new filter elements.
Add [Attribute!=Value] to Filter	Show only those events that do not match both the prior and new filter elements.
Add to Filter [List of Related Attributes=Value, !=Value]	When the selected attribute type has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. This filtering element is applied in addition to any other already present. Generally, attributes are considered related if they share a common focus such as IP addresses.

Adding an Event Attribute to a Filtering Condition

The **Add condition to editor** options apply to the editor in the Inspect/Edit panel that currently has focus. If no editor is open, the default target is the Filters Editor.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add Condition [Attribute=Value] to Editor	In the current editor, insert a new condition in which the selected attribute matches the value in the selected event.
Add Condition [Attribute!=Value] to Editor	In the current editor, insert a new condition in which the selected attribute does not match the value in the selected event.
Add Condition to Editor [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, add a condition to the current editor using the available list of attribute-value pairs that do (or do not) equate. Generally, attributes are considered related if they share a common focus such as IP addresses.

To remove a condition from the editor, right-click it and choose **Delete**.

When you are using these options to affect a view that is subject to the editor in use, click **Apply** or **OK** in the editor to put the condition into effect.

Contextual filters (in contrast to conditions) are temporary unless you save the modified view as a named active channel. Condition statements are saved with their relevant editors.

Permanently Modifying an Active Channel

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

Showing an Exploited Vulnerability

The Investigate options include the ability to look for potentially exploitable vulnerabilities associated with an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Exploited Vulnerabilities**. Available information appears in the Vulnerabilities tab of the relevant Asset Editor.

Showing a Targeted Asset

You can also find out more about an asset targeted by an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Targeted Asset**. Available information appears in the Asset Editor.

Using Charts

The Console offers several chart view options for active channels and for data monitors. You can add chart views of the data in many active channels or data monitors simply by choosing a chart type from the **Format** pop-up menu in the view's lower-right corner.

ArcSight charts remain linked to the data they represent. You can immediately see a chart's events in a grid view that presents the data as charted, or filtered further using the options of the Investigate command. Charts use the same color for all values in a series. For example, if you are plotting successful and failed logins in a chart, successful logins as a series will have one color. Failed logins as another series will have a different color.

You can click and drag three-dimensional charts on their vertical or horizontal axes to tilt them for better viewing.

Charting an Active Channel's Contents


- 1 In the Navigator panel's Active Channels resource tree, right-click a channel and choose **Show Active Channel**.
- 2 In the Viewer panel, in the lower-right corner of the newly opened active channel, click the **Viewer Selector** icon to open its menu.
- 3 In the menu's **Chart** branch, choose one of the chart types described below.
- 4 The data in the view opens in an additional chart presentation, in the chosen format, within the active channel.
- 5 Click the **Layout** icon in the channel's lower-right corner to change the visual arrangement (tabbed or tiled) of the views within the channel, if needed.

Charting a Data Monitor's Contents

- 1 In the Navigator panel's Dashboards resource tree, double-click a dashboard or right-click it and choose **Show Dashboard**.
- 2 In the Viewer panel, in the lower-right corner of an applicable data monitor, click the **Viewer Selector** icon to open its menu.
- 3 In the chart menu, choose one of the types described below.
- 4 The data in the monitor switches to a chart presentation.

For data monitors, the **Chart Showing Priorities** submenu offers many of these same charting options, but with graphic elements such as pie wedges or bar segments that distinguish their priority-level components.

Contents of charts are affected by the things that affect active channels or data monitors, such as changing time parameters or filters. Not all charts are applicable to, or available for, all views.

For more about the format tools available for dashboards (), see [“Monitoring Dashboards” on page 154](#).

For more about custom view dashboards, see [“Using Custom View Dashboards” on page 167](#).

For more about working with dashboards, see [“Using Dashboards” on page 153](#).

Chart Type	Description
Area	A horizontal chart in which bands occupy various amounts of the displayed area to indicate relevant values.
Area Radar	A circular chart that shows proportional values as solid graphic extensions from a central zero point, outward to a higher-value border, and occupying relative numbers of degrees of the available circle.
Horizontal Bar	A horizontal chart that shows changes in relative quantities, usually by time units seen as solid rectangles, over a span of time.
Line	A horizontal chart that shows changes in relative quantities, usually by time units plotted on a line, over a span of time.
Pie	A circular chart with proportional wedges for the relevant values.
Radar	A circular chart that shows proportional values as a line plot from a central zero point, outward to a higher-value border, and occupying relative numbers of degrees of the available circle.
Scatter Plot	A horizontal chart that shows changes in relative quantities, usually by time units plotted as separate points, over a span of time.
Stacking Area	A horizontal chart in which stacked bands occupy various amounts of the displayed area to indicate relevant values.
Stacking Bar	A horizontal chart that shows changes in relative quantities, usually by time units seen as stacked solid rectangles, over a span of time.
3D Bar	A corner-anchored graph with height, width, and depth dimensions that can show three axes of categorical and quantitative information.

Exploring the Events Behind a Chart

To see a grid view of the events behind an active channel's chart, double-click the section of the graphic that represents those events. To filter those events further, right-click the relevant section of the chart and choose an Investigate command option. In charts that show color keys, such as Events by Priority, you can also double-click a color chip to open a grid view filtered by that key.

To see an active channel grid view of the events behind a data monitor's chart, double-click the section of the graphic that represents those events, or right-click and choose **Show**

Details, or choose **Show Detailed Channels** to see a view for each of the chart's components.

Using Grids

The tasks in this topic explain how to monitor events in grid views. To better understand the details in grid views, please read more about event grid data fields.

Monitoring Events in the Grid View

Click an active channel's tab at the top of the Viewer panel and select the **Grid** view of that channel using the tab at the bottom. When new events occur, they are displayed at the top of a grid view as a new row. Events can appear in ArcSight Severity or filter colors. You can set the color-code for events by using the steps described in ["Changing User Preferences" on page 772](#).

Sorting Columns in the Grid View

Right-click and select **Sort Column** on the grid column header of a particular column (for columns that support sorting) to sort the contents of that column. If the column contains numerals, it sorts from highest to lowest value (or vice versa). If the column contains words or alphabetic characters, it sorts alphabetically from A to Z (or vice versa).

You can also perform an advanced sort on one or more columns in the grid view. When selecting a secondary sort column, select the secondary column first, then the primary column. For example, to sort by Event Name then by Detect Time, sort **Detect Time** first, then **Event Name**.

After you sort a column it automatically pauses the current channel, stopping events from appearing in the grid view. Click the **Play** button in the Replay Controls to restart the channel and resume receiving events in the grid view.



Note

When you sort on time and on priority, you might observe cases where events with the same apparent time are not in priority order. Because events are timestamped to milliseconds, they may in fact be in time order although the milliseconds are not showing. In this case, you can show milliseconds to validate time order. Choose **Edit > Preferences**, then in the Date and Time panel change the **Date & Time** Format to also show milliseconds by adding "SS" to the seconds parameter, e.g., d MMM yyyy HH:mm:ss:SS z.

Adding, Replacing, or Removing a Columns

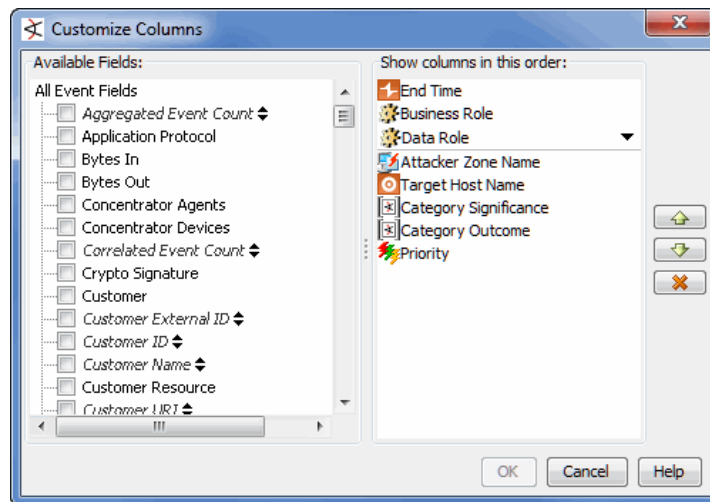
A quick way to add, replace or remove columns in a grid view (for example, active channel or list) is to right-click on the appropriate column header and select one of the following options:

- **Columns > Add/Remove Column > <Select a field from the menu>**
- **Columns > Replace This Column > <Select a field from the menu>**
- **Columns > Remove This Column**

These are context-dependent commands that apply to the column on which you launch the right-click menu. (To add a column, right-click on the header of the column you want to add the new column next to. Columns are added to the right of that header. To replace or remove a column, right-click on the header of the column you want to replace or remove.)


Alternatively, you can use the Customize Columns dialog to define the columns shown in the viewer as described here:

- 1 Right-click the column header and select **Columns > Customize Columns** to bring up the associated dialog. (Note that fields shown in italics are *derived* fields.)



Tip



Looking for information about custom columns? If you want to add a custom column, you need to create or define it first. After that, it shows up in the Available Fields list under *Custom Column*, and you can include it in grid views as with any other field. For information on creating custom columns, see [“Customizing Grid Columns” on page 152](#).

- ◆ **To add a column:** Select data fields (column titles) to add from the Available Fields list on the left. Check marks indicate selected columns. The selected columns show up in the list on the right as you select them. Alternatively, when you deselect or uncheck a data field on the left, the column is removed from the right-hand list.
- ◆ **To remove a column:** Select a field from the right-hand list and click the Delete button . Also, deselecting a data field from the Available Fields list on the left removes it from the right-hand list. Removing a column from a grid view does not delete the column information from the ArcSight Database.



Tip

You also can remove a column directly from the grid view without opening the Add/Remove Columns dialog. To do this, right-click a column header and select **Remove Column**.

- ◆ **To re-order the columns:** Select a data field (column title) in the right-hand list and click the Up  and Down  buttons to move it. The top-to-bottom order shown in the *Show columns in this order* list on the right translates to a left-to-right order when applied in the grid view. A column title at the top of this list will show as the first column in the grid view on the far left in the grid display. A column title at the bottom of this list will show as the last column in the grid view on the far right of the grid display.
- 2 Click **OK** to save changes you made on the Add/Remove Columns dialog. The grid view reflects added, replaced, removed, or re-sorted fields.

Sizing a Column in the Grid View

Right-click a column header and select **Size Column To Fit**.

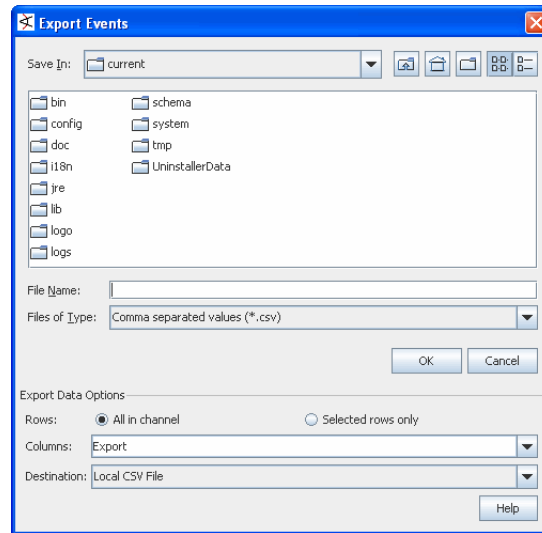
Showing or Hiding Grid View Column Text and Icons

Right-click a column header and select one of the following options:

Option	Display Result
Text and Icon	Display the column heading and its icon.
Text Only	Display only the column heading.
Icon Only	Display only the icon.

Exporting Events to a File

- 1 Right-click one or more events in the Viewer panel and choose **Export > Events** in channel. This brings up the Export Events dialog.



- 2 Use the file browser to navigate to the location where you want to save the file. You can use the buttons across the top right of the dialog to move up one directory level, go to your desktop, create a new folder, show files as a list or a list with details. Also, you can use the **Files of Type** drop-down menu to display only comma-separated values (CSV) format files or all files while you are browsing the directories.
- 3 In the **File Name** field, enter a name for the file to which you want to export the event(s).
- 4 Under **Export Data Options**:
 - ◆ Select **All in channel** to export all the events in the channel. The system will export all events in the channel to the specified file, regardless of which events you originally selected in the grid view. (This is option is selected by default.)
 - ◆ Select **Selected rows only** to export only the events you selected in the grid view.
 - ◆ From the **Columns** drop-down menu, choose a field set to use for the exported events. This limits the fields exposed in the exported events to the chosen field set. The default for "Columns" is the Export field set. You can keep the default, or select other field sets from a list of All Field Sets.

If you want to limit the exported columns (field sets) to only those showing in the current channel, you have a few options for doing this. See the tips on [How to Limit Export to Fields Visible in Channel](#).

- ◆ Select a **Destination** for the file. Local CSV File is selected by default, and is typically the only option.
- 5 Click **OK** to export the events to a file with the specified settings.



How to Limit Export to Fields Visible in Channel

The default "Export" field includes a large number of columns. Unless you have a pressing need to export all these fields for channel events, you might want to modify the export. Exporting a large field set for a large event set could be time- and resource-consuming.

If you want the exported file to include only the fields shown in the current channel, do either of these:

- If the channel is unmodified from its default (i.e., you have not added or removed fields), you can select the channel's default field set on the file export option. To find the default field set name, edit the channel and look at "Default Field Set" name or right-click any column header in the channel and choose Field Set > Selected Field Set. The default field set will be selected. (For example, for [/All Active Channels/ArcSight System/Core/Live](#) active channel, the default field set is [Standard-MgrRcpt](#). Selecting this field set on the export will give you that set of columns in the CSV file.)
- If you have modified the channel from its default (i.e., added or removed fields), you can save it as a custom field set and then choose your custom field set on the export dialog. To save a custom field set, right-click anywhere on the column headers in the active channel and choose Field Sets > Save As. On the Field Sets Selector, navigate to the group you want, name the new field set and click OK. Now it will be available to choose from on the export dialog.

The Export field set itself is also customizable. If you are sure you always want exported events to include a limited set of fields, you can edit the Export field set. (See ["Creating and Using Field Sets" on page 204](#) and ["Editing a Field Set" on page 211](#).)

Choosing Grid View Menu Commands

Right-click an event or event field in a grid in the Viewer panel to open a context menu. The commands available are those that apply to the current combination of event type, view, filter, and so forth.

Command	Description
Show Event Details	Use the Event Inspector to examine all the attribute details associated with the event.
Rule Options	<ul style="list-style-type: none"> • Simple chain: Show this event's base and correlated event tree in the Event Inspector. • Detailed chain: Show this event's base and correlated events in detail in a new grid view. • Show triggering resource: Show the rule that triggered this event in the Rule Editor. • Clear rule actions: Clears the list (if one is showing) of rule actions pending on the ArcSight Manager.

Command	Description
Investigate	Create a temporary filter as required based on the field's highlighted event. The Investigate command uses the event's attribute type (its column heading), and the particular event's field value (for example, an exact IP address), to formulate simple filters based on these two factors. The filter's operators can include Create Filter [X = Y] and Add Condition [X = Y] to Editor . The Investigate submenu also offers the Show Exploited Vulnerability and Show Targeted Asset commands to open detailed views of assets or vulnerabilities, if present in the selected event.
Active List	Add the selected event to, or remove it from an active list. This is explained further in "Active Lists" on page 790 and "Managing Active Lists" on page 571 .
Annotate Event	Open this event in the Annotate Events dialog box, where you can click the Stage field to set a collaboration workflow sequence for this event. When you select a stage you automatically place the event in the corresponding group in the Stages resource tree in the Navigator panel, where you and other analysts can collaborate on its investigation and resolution.
Move Timeline to Current Event	Reset the event timeline in the view to the time of the currently selected event.
Select Events with Matching Cell	Select any other events in the view that have values matching that in the currently selected cell.
Invert Selection	Select all events not currently selected, and deselect those that are currently selected.
Event Graph	Graph any logical relationships (i.e., source/target IP address connections) that exist among the currently selected events.
Rule Chain Graph	Graph the rule chain(s) behind the currently selected triggered events.
Geographic View	Geographically map the source and destination IP addresses of the selected events.
Tools	Run your choice of the standard network lookup tools, using field values from the selected events.
Create Rule	Use the Rule Editor to create an ArcSight rule to apply to the selected events.
Export	Export the selected events to an external event-tracking system, such as comma-separated-value (CSV) data in a report or for a spreadsheet, or save it as an HTML or a JPEG file.
Add to Case	Add the selected events to a new case for tracking.
Payload	Keep or discard the payload associated with a selected event.
Show Context Report	Output a report concerning rules and events within a specified time window.
Close	Close the current individual view within the selected view type.
Knowledge Base	Show the Knowledge Base pages associated with the selected events, or associate new pages.
Vendor Page	If available, show vendor Web page of the event's sensing device.


Command	Description
Help	Open the online Help to this topic.

Filtering Grid Views with Inline Filters

Active channels that display grid views have an inline means for creating simple filters. These filters are based on using a value found in one column, or creating AND conditions between values found in two or more columns. Inline filtering is a very rapid way to constrain detailed views.

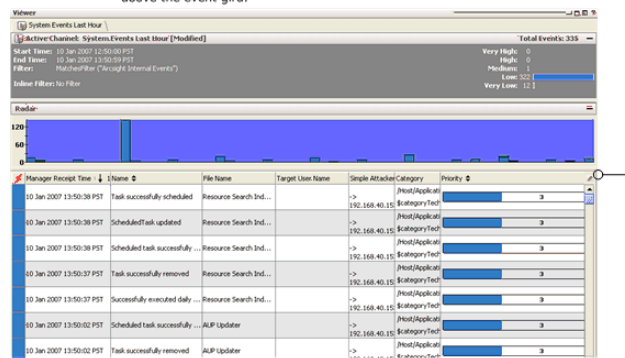
These filters are called *inline filters*. Also, note that while they are in effect, inline filters affect all views generated for the channel.

You can create, change, save, hide, and remove inline filters from the grid view. Also, you can create and manage multiple inline filters from this view.

- To create an inline filter, click the Inline Filter link in the event header or click the Edit Inline Filter  button at the top right of the grid view to display the inline filtering fields. Type a value by which you want to filter for one or more fields relating to a column in the grid. Click **Apply** to immediately apply the filter to the view. The inline filter is displayed in the header under the standard filter.
- To change an inline filter, click the **Edit Inline Filter** button again, and choose new values, and apply. The **Clear** button clears the inline filter fields, and **Cancel** closes the inline filtering window without saving current changes.
- To remove an inline filter, right-click over the Inline Filter name in the header for the selected event and choose **Remove Inline Filter**.
- To save an inline filter, right-click over the Inline Filter name in the header for the selected event and choose **Save Inline Filter**. This opens a Filters Selector dialog that shows the Filters tree. Navigate to the folder where you want to save the current filter, and click **OK**.
- To highlight the filtered events, click the **Highlight** checkbox (**on** is check marked) and use the drop-down color selector to select a color from the palette.
- To create and manage multiple inline filters, click the **+** button next to the Highlight options under the inline filters to add filter definition rows. (Click the **-** button to remove filter rows.) The potential uses of multiple inline filters are extensive, but essentially this provides a means of creating a filter with complex conditions, inline in an active channel. For example, in the Name column for an event, you could specify that the event name contains `ActiveList` on the first filter row and that the name does not contain `Successful`. You could extend this filter by specifying what you are looking for in some of the other fields or even add more qualifiers on the Name field.

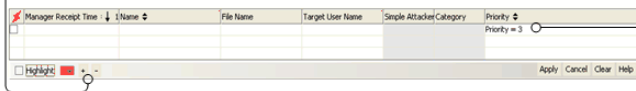
All fields can be narrowed down in this way, using multiple filter definition rows.

To add an inline filter, click the **Edit Inline Filter** button to the right of the viewer above the event grid.



Clicking the **Edit Inline Filter** button opens an inline filtering window. Type a value in one or more fields to further filter the event stream. In this example, we add an inline filter on the Priority field to specify showing only events of Priority 3. Click **Apply** to apply the inline filter.

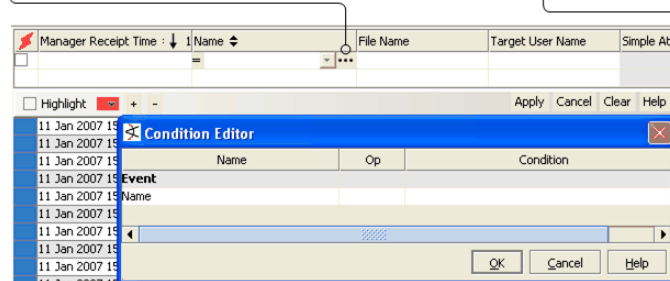
Also, you can click the + button to add filter definition rows and create multiple inline filters. Click the - button to remove rows.



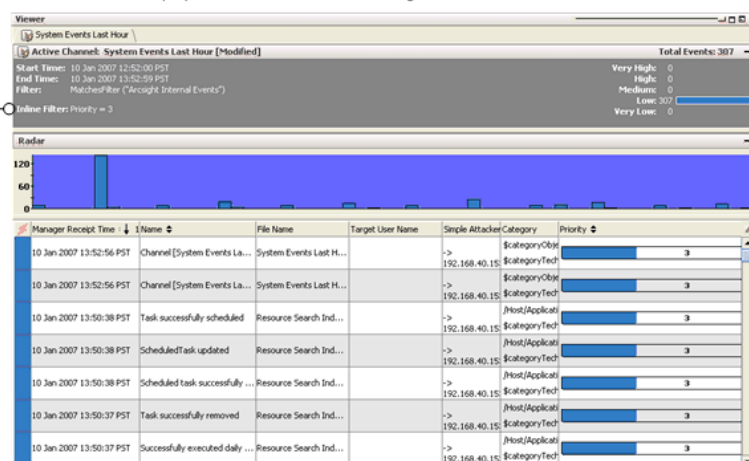
When you click into a field, you get an equals operator, a drop-down list of available values for that field based on the events currently displayed, and an ellipsis (...) indicating another dialog is available.

If these inline options are not enough to create the filter, click the ellipsis (...)

to bring up a Conditions Editor dialog in which to create the filter for the selected field.



Once the inline filter is applied, only events that match current filter and the inline filter are shown. The inline filter used is displayed in the header under the original filter.



Custom columns are not available as arguments for inline filtering.

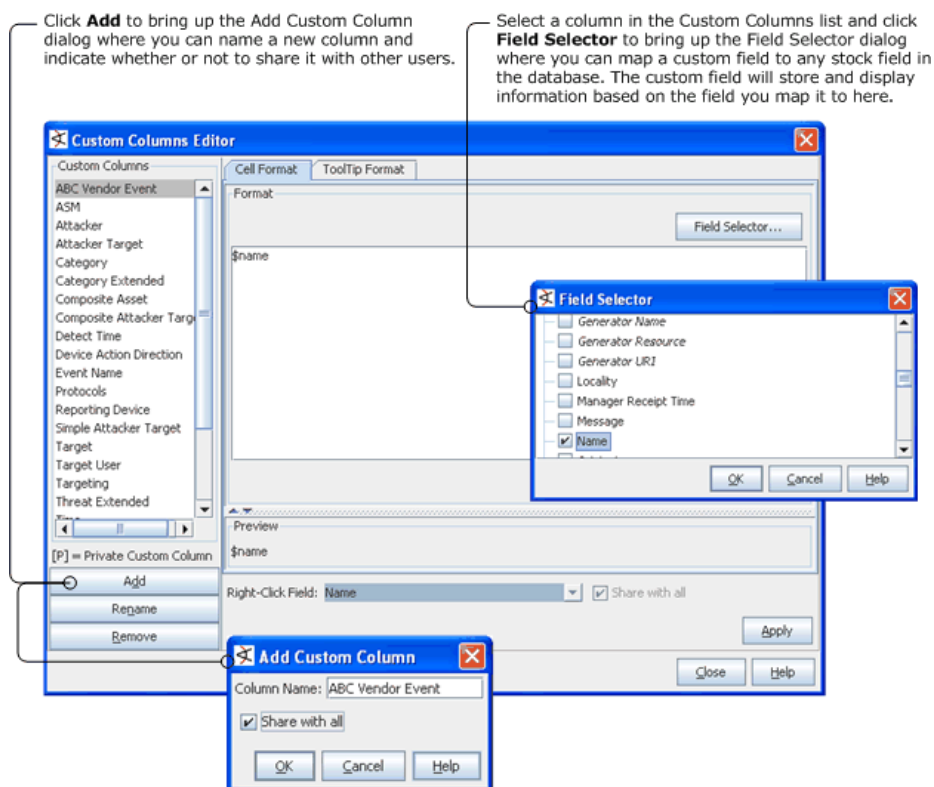
Customizing Grid Columns

You can create Viewer panel grid view columns with customized cell content and presentation formats, tooltip contents, and right-click pop-up values.

You make these changes through the Custom Columns Editor. In the Editor you create new named columns. For each column you select event data fields to display, and if you wish, the HTML formatting to use in its cells. The tooltip option specifies the formatting and content of the tooltips you see when you hover the pointer over cells in that column. The right-click field option sets the event data field to use in columns where there are right-click commands that use field names as arguments such as "Investigate...."

Creating a Custom Column

- 1 Right-click a column header in a Viewer panel grid view and choose **Customize Columns > Edit Custom Columns**. This brings up the Custom Columns Editor.



- 2 Click **Add** to name a new column. If you want everyone to see the new column (not just administrators), select the **Share with all** checkbox. (You can toggle this option on or off later too from the Cell Format tab.) When you click OK on the **Add Custom Column** dialog, the new column name is added to the Custom Columns list on the left side of editor.
- 3 Click **Field Selector** on the **Cell Format** tab to pick the event attribute(s) you want to display in this column and click **OK**.
- 4 In the **Format** text box apply Java-compatible HTML formatting around the field strings, if appropriate. Remember to bracket such formatting with the HTML tag, such as `<HTML>$type</HTML>`.
- 5 Click **Preview** to see how the contents of the **Format** box will look in the grid view.

- 6 Click the **ToolTip Format** tab to define a tooltip.
- 7 Choose a target event attribute in the **Right-Click Field** menu to populate variable right-click commands, when applicable.
- 8 Click **Rename** or **Remove** to change or take away selected items in the **Custom Columns** list.
- 9 Click **Apply** to put your changes into effect and **Close** to close the Custom Columns Editor.

You can edit custom columns after they are created, including toggling on/off the "Share with all" settings for a column, renaming it, changing its Field Selector mappings, and so forth.



- Custom columns are not available as arguments for inline filtering.
- The Java Swing based browser supports basic HTML according to the HTML 3.2 specification. Some more advanced tags may not be supported. For Technical Reports describing HTML 3.2, please refer to the World Wide Web Consortium (W3C) site at <http://www.w3.org/>. For information on HTML support in Java Swing, refer to the Sun Developer Network at <http://java.sun.com/javase/reference/index.jsp>.

Showing a Custom Column

Once a custom column is created, it is available for use in the Console. Right-click the column header in a Viewer panel grid view and choose **Customize Columns > Add Column** to add the new column to a grid view. Custom columns show up in the Available Fields list under **Custom Column**. If a column is configured as **Share with all**, it is available to all administrators. If not, it is available only to the user who created it. For more information, see ["Adding, Replacing, or Removing a Columns" on page 145](#).

Advanced Example: Creating a Custom Column with Velocity

Custom columns can display different contents based on external conditions. Use the Velocity template language to specify these conditions.

To create a custom column that displays a particular image when an event's target is in a specific Zone, create the custom column as described previously, but specify Velocity template-language script in place of the HTML format.

The code in the **Format** text box might look like this:

```
<HTML>
#if (($targetZoneUri.length()>0) &&
    ($targetZoneUri.startsWith("/All Zones/
    System Zones/Public Address Space Zones/
    Ford Motor Company")))
    <IMG src="file:///c:/fordlogo.gif" />
#end
</HTML>
```

Using Dashboards

Dashboards are a graphical display of data gathered from one or more [Data Monitors](#) and [Query Viewers](#). Dashboards can display data in a number of graphical formats, including pie and bar charts, tables, and custom layouts.

Administrators can control visibility of, or access to, dashboards, query viewers, and data monitors by changing access control lists (ACLs) as needed. For more information on general use of ACLs on any resource, see [“Managing Permissions and Resources” on page 646](#).

With ACLs, administrators can also control which users are allowed to *deploy* (enable) or *un-deploy* (disable) a data monitor.

Monitoring Dashboards

You can organize and present events displayed by data monitors and query viewers on the dashboard. Basic tasks include loading and displaying dashboards; inspecting events; using zoom, slide show, or manipulating the views in various ways; working with dashboard layouts; saving dashboards, and so on.

Loading Dashboards

- 1 Choose **Views > Show Dashboard** to open the Load Dashboard dialog box.
- 2 Expand the dashboard groups to locate the dashboard(s) you want to include in your display.
- 3 Select the checkboxes next to the dashboards you want to include.
- 4 When you've finished your selections, click **OK**.

Inspecting Events in Dashboards

You can investigate the events presented on the dashboard by selecting and right-clicking those events and choosing **Show event details** (in LastNEvent) or **Show details**.

If you select events from a Last N Event, the details appear in the Event Inspector.

If you select events from any other data monitor or query viewer, a new **Dashboard Drill-Down View** opens in the Viewer panel for you to investigate.

You can drill down on grid, graph, or chart views.



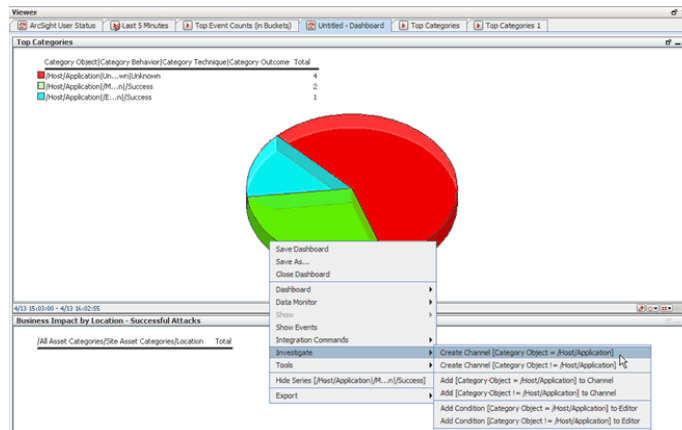
By default on a data monitor, the displayed channel uses the same columns as the default Standard Field Set (as defined in the [console.default.properties](#) file in the ESM Console installation).

If a custom field set is defined for the data monitor [Select Field Set](#) option, the drill-down channel will use that field set. (See [“Data Monitors” on page 905](#) for information on creating data monitors and defining settings for them.)

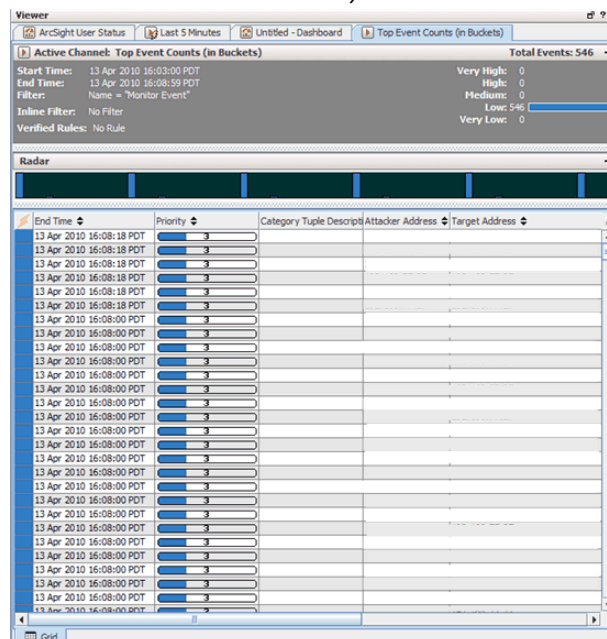
You can add or remove columns in the active channel. To do so, right-click on the active channel column headers to get the **Customize Columns** option.

For example, to drill down on a data monitor pie chart display, either double-click the chart, or right-click and select **Investigate > Create Channel** and choose a [create channel](#)

option (the menu option for a pie chart display of a query viewer may slightly vary with an additional menu level).




An active channel is displayed showing the drill-down information (more detail about the events or resources in the original data monitor or query viewer display). If the channel came from a data monitor, the channel uses the field set columns defined for use in the data monitor [Select Field Set](#) option. (Or if no field set is defined, the data monitor uses standard field set columns.)



Displaying Dashboards

In the Navigator panel's Dashboards resource tree, right-click a dashboard and choose **Show Dashboard**.

Displaying Dashboards in a Slide Show Rotation

To automatically sequentially display all the dashboards present in the Viewer panel, choose **Views > Slideshow > Interval** in the Console's menu. Use **Interval** to set the number of seconds to pause on each dashboard, then choose **Views > Slideshow > Start**, or use the toolbar button , to begin the slide show. Slide shows appear full-window. Also, **Tile Best Fit** is the best display choice in slideshow dashboards so all data

monitors are visible. Use **Views > Slideshow > Stop**, or the toolbar button, to end a slideshow and return to the previous view.

Rearranging Elements in Dashboard Layouts

You can change a dashboard's layout by dragging and dropping the elements on the desired location in the dashboard. You can also click an element's header and drag it to another location.

Using Dashboard Menu Options

Right-click an element in a dashboard to use the **Dashboard** subcommands on its context menu. The nature of the element determines which commands are applicable and enabled.

Zooming In or Out of Dashboards

Right-click an element and choose **Dashboard>Zoom In** or **Dashboard>Zoom Out**.

Fitting all Dashboard Elements

Right-click a dashboard element and choose **Dashboard>Fit in Dashboard**.

Saving Dashboard Layouts

In a dashboard, right-click and select **Save Dashboard**.

Closing a Dashboard

In a dashboard, right-click and select **Close Dashboard**.

Editing Dashboard Elements

Right-click in the element and choose **<Dashboard element>Edit**.

See also:

- [Editing a Data Monitor](#) and [Moving or Copying a Data Monitor](#)
- ["Editing a Query Viewer" on page 323](#)

Changing a Dashboard's Layout

Click the **Layout** button at the lower-right corner of the dashboard in the Viewer panel and choose a tab or tile option.

Managing Dashboards

This topic describes how to create dashboards and adding elements to it. Elements include data monitors and query viewers.

Creating a Dashboard

When you create a dashboard, the ability to add data monitors is automatically available.

- 1 On the Dashboards tab, right-click a dashboard group and choose **New Dashboard**. Alternatively, drag an existing dashboard to a different group, choose **Copy** to copy the dashboard, and then rename it.

If you chose New Dashboard, an untitled dashboard appears in the Viewer panel and the Data Monitors tab automatically comes forward so you can choose monitors to add.

- 2 If you want to add data monitors now:

- a Select the **Data Monitors** tab and navigate through the groups of existing data monitors to find ones you want to add to the dashboard.
 - b Select a data monitor to add, right-click it and choose **Add to Dashboard As**, then choose an applicable display format (see [Display Formats](#)).
 - c Repeat the above step to add other data monitors, as needed. When you've finished, right-click the dashboard in the Viewer panel and choose **Save Dashboard**.
- 3 If you want to add query viewers, see ["Adding a Query Viewer to a Dashboard" on page 157](#).
 - 4 In the Save As dialog box, navigate to a group and type in the **Name** text field.
 - 5 Click **OK**.

Adding a Data Monitor to a Dashboard

- 1 Right-click a dashboard and choose **Show Dashboard**.
- 2 On the Data Monitors tab, navigate through the groups of existing data monitors to find ones you want to add to the dashboard.
- 3 Right-click a data monitor and choose **Add to Dashboard As**, then choose an applicable display format (see [Display Formats](#)).
- 4 To save the dashboard, right-click it and choose **Save Dashboard**. If this is a new dashboard, navigate to the group where you want to save the dashboard, enter a name for the new dashboard, and click **OK**.

Adding a Query Viewer to a Dashboard

You can add a query viewer result to a regular dashboard as follows:

- 1 If you have identified an existing regular dashboard to which you want to add the query viewer, open the dashboard in the viewer and make sure it is the focus. If you want to add the query viewer to a new dashboard, continue to the next step.
- 2 Choose **Query Viewers** in the Navigator.
- 3 Select a query viewer, right-click and choose **Add to Dashboard As >**, then choose an applicable display format (see [Display Formats](#)).

The query viewer result is displayed on the open dashboard. If a dashboard is not displayed, a new untitled dashboard is created for the query viewer result.

- 4 Save the existing dashboard.

Or if this is a new dashboard:

- a Right-click the title bar of the dashboard and choose **Save Dashboard As**.
- b In the popup dialog, navigate to the group where you want to save the dashboard, enter a name for the dashboard, and click **OK**.

By default, this new dashboard is a regular dashboard. You can add multiple query viewer results sets along with other resources to a single dashboard.



Query viewer results on dashboards are accessible from ArcSight Web. For more about ArcSight Web, see ["ArcSight Web" on page 798](#).

Display Formats

The display options available depend on the nature of the dashboard element.

Display Format	Description
Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. Applies to data monitors and query viewers.
Bar Chart Table	A grid of proportional bar elements. Applies to data monitors.
Horizontal Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. This format forces the bars to run left-to-right rather than up-and-down. Applies to data monitors and query viewers.
Pie Chart	Shows data as a circle with proportional wedges for elements. Applies to data monitors and query viewers.
Statistics Chart	Displays Moving Average data monitors, especially those that contain and need to arrange (overlay) multiple graphs in one monitor space. Compare Statistics Chart to Tile, which arranges individual-graph monitors into fixed arrays. Applies to data monitors.
Table	Displays data as a grid. Applies to data monitors and query viewers.
3D Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. The graph also has a third axis (depth) to display more data and can be rotated by dragging. Applies to data monitors.
Stacked Bar Chart	Shows data as a series of proportional bar elements and may include bar segmentation to subdivide the data. Applies to query viewers.
Tile	Arranges individual Moving Average data graphs into separate, fixed positions on a data monitor, when multiple graphs are present. Compare Tile to Statistics Chart, which displays multiple graphs (overlaid) in the same monitor space. Applies to data monitors.

Editing a Dashboard

You edit dashboards by editing the data monitors within them as described in [“Using Custom View Dashboards” on page 167](#).

Deleting a Dashboard

- 1 In the Dashboards tab of the Dashboards resource tree, right-click the dashboard's name and choose **Delete Dashboard**.
- 2 In the dialog box, click **Yes**.

Managing Dashboard Groups

The groups in the Dashboard tab of the Navigator panel's Dashboard resource tree store individual dashboards or other dashboard groups. You use groups within groups to help organize larger numbers of resources.

You can manage groups by drag-and-drop. You can move or copy dashboards or groups within the Dashboards resource tree. And deleting a group also deletes the resources it contained.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **New Group**.
- 2 Type a name in the group's text field.
- 3 Press **Enter**.

Renaming a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Rename**.
- 2 Type a name in the group's text field.
- 3 Press **Enter**.

Editing a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, navigate to a group and drag it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Dashboard Group

- 1 In the Dashboards tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Using Data Monitors

You populate dashboards with *data monitors*, which you most often select from the Data Monitors resource tree in the Navigator panel (under Dashboards). However, when you need to use data monitors that aren't pre-defined, you need to be able to create, edit, and delete them.

Administrators can limit visibility of, or control access to, data monitors by changing access control lists (ACLs) as needed. For more information on general use of ACLs on any resource, see [“Managing Permissions and Resources” on page 646](#).

With ACLs, administrators can also control which users are allowed to *deploy* (enable) or *un-deploy* (disable) a data monitor.

Creating a Data Monitor

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor group and choose **New Data Monitor**.
- 2 In the Data Monitor Editor, select a **Data Monitor Type** from the drop-down menu. See [“Data Monitor Types” on page 164](#) for descriptions of each type. (See also [“Data Monitors” on page 905](#) in the reference section of this guide.)
- 3 Based on the [Data Monitor Types](#) you've selected, specify values and options in the applicable fields to define the data monitor's data collection. Details on fields and appropriate values are given in the information about each data monitor type.



Note

Depending on the permissions associated with the user group to which you belong, you may or may not have an option to **Enable** (*deploy*) or disable (*un-deploy*) the data monitor. For more information, see [“Enabling or Disabling a Data Monitor” on page 161](#).

- 4 If the data monitor uses data fields for evaluation, you can use the Variables tab to create a new specialized field if necessary



Note

The following data monitors support variables:

- Event graph
- Hierarchy Map
- Last N Events
- Last State
- Moving Average
- Statistics
- Top Value Counts (bucketized)

If you select a data monitor that does not support variables, the Variables tab is disabled.

You can also add a global variable anywhere fields can be added. For instructions about how to add a global variable to a data monitor, see [“Adding a Global Variable to a Data Monitor” on page 485](#).

- 5 Click **OK**.

To add the new monitor to the current dashboard, right-click it and choose **Add to Dashboard As**.

Editing a Data Monitor

- 1 Do either of the following to bring up the Data Monitor editor:
 - ◆ In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor and choose **Edit Data Monitor**.
 - ◆ If a Dashboard containing a given Data Monitor is already displayed, hover the cursor over that Data Monitor in the Viewer panel, right-click, and choose **Data Monitor > Edit**.
- 2 In the Data Monitor Editor, edit the applicable fields.
- 3 Click **OK** to save your changes and close the Data Monitor Editor. Or click **Apply** to save the changes and leave the editor open.

See [“Data Monitor Types” on page 164](#) and [“Data Monitors” on page 905](#) for field details on all data monitors.

For customize view options on Last State data monitors, see [Table View \(Color Chooser and Remove Entry\)](#) and [“Tile View \(Customize View\)” on page 926](#) in the [Last State Data Monitor](#) topic.

Moving or Copying a Data Monitor

You can move or copy a data monitor as you would any other resource (as described in [“Moving Copying, Linking, and Deleting Resources” on page 120](#)).



- Users who do not have data monitor deployment permissions can still copy enabled data monitors, but the copies are disabled. Users need both write and deploy permissions to enable or disable a data monitor.
- Users who do not have data monitor deployment permissions can still move data monitors from one group to another if they have write permissions on the data monitor(s) they want to move and the destination group for the move operation.

For more about data monitor deployment permissions, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).

Deleting a Data Monitor

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a data monitor and choose **Delete Data Monitor**.
- 2 In the dialog box, click **Yes**.

Enabling or Disabling a Data Monitor

When a data monitor is enabled (*deployed*) it is actively processing events and updating its display.

When you disable (undeploy) a data monitor, it stops processing events and updating its display. You might choose to disable a data monitor because it is not needed or should not be considered under certain circumstances.

Data monitors can be enabled at time of creation (see [“Creating a Data Monitor” on page 160](#)) or edited later to enable deployment.



Note

Data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions.

Depending on the permissions associated with the user group to which you belong, you may or may not have an option to **Enable** (*deploy*) or disable (*un-deploy*) the data monitor.

- Administrators (all users belonging to the `admin` group) have permissions to deploy/undeploy data monitors.
- To deploy a data monitor, a user needs *both* general data monitor deployment permissions and write permissions to the specific data monitor he or she wants to deploy. Users with permissions to deploy data monitors can deploy only those data monitors for which they have write permissions.
- Administrators can grant permissions to deploy or restrict data monitors to other non-Administrator users through the Access Control Lists (ACLs) editor. For more information, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#) and [“Granting or Removing Resource Permissions” on page 647](#).

Enabling or Disabling a Data Monitor from the Editor



Tip

You can set *operations* permissions on data monitor deployment by editing Access Control Lists (ACLs) on user groups. Administrators can allow or block user groups for data monitor deployment permissions. (This is different than controlling permissions on who has access to the data monitors *resource*.)

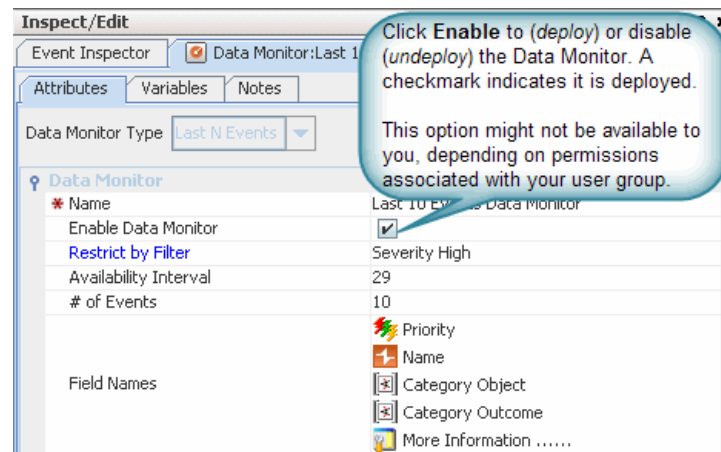
To set permissions for *deploying* data monitors, click the **Operations** tab, then click the **Add** button to get the Permissions Selector dialog for operations, select **Deploy** and click **OK**. For more information, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).

By default, only Administrators have permissions to enable and disable data monitors. Administrators can grant permissions to enable and disable data monitors to other non-Administrator users through the Access Control Lists (ACLs) editor. For more information, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).

If you have appropriate permissions, you can enable and disable data monitors in the Data Monitor Editor. (See [“Editing a Data Monitor” on page 161](#) for information on displaying the editor.)

In the Data Monitor Editor, click the checkbox for **Enable** to toggle the data monitor on or off. (Be sure to click **Apply** or **OK** on the editor to save your changes.)

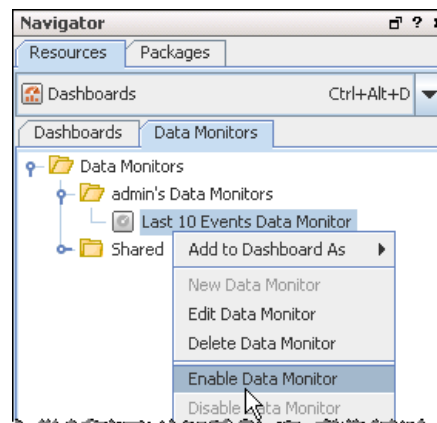
- ◆ A checkmark indicates the data monitor is enabled/deployed.
- ◆ If the box is unchecked, the data monitor is disabled/undeployed.



Enabling or Disabling a Data Monitor in the Navigator

You can also enable and disable data monitors in the Navigator by right-clicking data monitors or a data monitor group.

- 1 In the Data Monitors tab of the Dashboards resource tree, right-click a data monitor or a data monitor group.
- 2 Choose **Enable Data Monitor** to *deploy* or activate the monitor(s) (if disabled) or **Disable Data Monitor** to *undeploy* or deactivate (if enabled).



For information about granting permissions to user groups to enable or disable data monitors, see [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).

Overriding a Data Monitor's Last State

Last State data monitors can sometimes display a status that has served its purpose as soon as you have seen it. Once seen, you may want to directly reset or change the status

so you can watch for a new status change, without waiting for an automatic system update.

When you see a status in a Last State data monitor that you want to reset, de-escalate, or otherwise override, right-click a cell in the monitor and choose **Override Status**. In the Select dialog box, select the new status and click **OK**.

Data Monitor Types

The ESM Console offers these predefined types to choose from when creating a new data monitor. Data monitor types are listed here with a quick-glance description for each. For full detail on each type of data monitor, follow the links or cross-references to the associated topic in [“Data Monitors” on page 905](#) in the reference section of this guide.

Data Monitor Type	Description
“Asset Category Count Data Monitor” on page 906	Enumerate the number of real-time hits (events) that occur per asset category, by priority, within a time interval.
“Event Correlation Data Monitor” on page 907	Provide flow-volume level correlation between two different event streams (based on two different specified filters).
“Event Graph Data Monitor” on page 908	Draw real-time diagrams of selected event activity. Automates the graphing of attacks in real-time. The <i>manual</i> operations are described in “Graphing Attacks” on page 176 .
“Event Reconciliation Data Monitor” on page 909	Correlate events arriving from one sensor with events arriving from another sensor. When qualifying events occur on either or both sensors, this data monitor issues a new event to signal it. Useful in helping to determine the effectiveness of a firewall or IDS deployed in your environment.
“Geographic Event Graph Data Monitor” on page 912	Draw a real-time geographic map of selected events. In effect, it does automatically and in real-time what you can do manually, as described in “Graphing Attacks” on page 176 .
“Hierarchy Map Data Monitor” on page 913	Draw an image made up of proportionally sized panels where each panel represents a group of events selected by group fields selected in the source node identifier. A source-node criteria could be a combination of fields. The Hierarchy Map data monitor includes several enhancements, as described in “Feature Enhancements” on page 913 in Hierarchy Map Data Monitor .
“Hourly Counts Data Monitor” on page 922	Display the total count of events on an hourly basis along with their Priority.
“Last N Events Data Monitor” on page 923	Order events based on a specified configuration. In the Table Viewer, the monitor displays the most recent events by Priority, Event Name, Protocol, and Category. With the BarChartTable configuration, the order is by Priority and Event Name. The PieChart configuration is ordered by Priority.

Data Monitor Type	Description
“Last State Data Monitor” on page 924	Provide an extra level of abstraction that you can use to simplify the information presented to operators. Sometimes called <i>indicator lights</i> or <i>heads-up displays</i> , these monitors show graphics that translate more complex values into simple, rapidly observable results such as green/amber/red signal lights or checkmark/asterisk/exclamation point symbols. Last State data monitors could also be called <i>most recently known state</i> monitors.
“Moving Average Data Monitor” on page 928	Display the moving average of events by a selected data field. The display provides a running count of events within a specified time frame and generates an event when the moving average changes significantly.
“Rules Partial Match Data Monitor” on page 931	Display rules that have partial matches and the total number of partial match events within a specified time frame. For more information on partial matches, see “Creating Rule Actions” on page 451 .
“Session Reconciliation Data Monitor” on page 931	Correlate events on the basis of their occurrence within a relevant time period, as established by a session event.
“Statistics Data Monitor” on page 933	Provide a broader generalization of Moving Average data monitor functionality, except that it allows selection of other statistical methods in addition to Moving Average. Statistical methods include Average, Moving Average, Standard Deviation, Skew and Kurtosis, as well as Moving Average. These added capabilities could be used to detect anomalous behavior that could not be detected using moving average alone.
“System Monitor Data Monitor” on page 936	Provide measurements based on ArcSight Manager internal monitoring system Java classes and attributes. A number of system monitors that might be particularly useful to ArcSight administrators are provided as predefined System Data Monitors that you can include in your dashboard displays to monitor system performance.
“System Monitor Attribute Data Monitor” on page 936	Similar to System Monitor, except that, rather than provide measurements for all attributes of a specified Java class, focus on a single specific attribute of a given ArcSight Java class. Used primarily for measurements on attributes that provide complex data structures.
“Top Value Counts Data Monitor” on page 937	Display top events by selected data field, the total number of events, and the event Severity within the total number of events with the Table and BarChartTable viewer configurations.

Managing Data Monitor Groups

Data monitor groups store similar data monitors in a single location. You can create groups within groups to meet enterprise needs.

You can manage groups by drag-and-drop. You can move or copy dashboards or groups within the Dashboards resource tree. And deleting a group also deletes the resources it contained.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **New Group**.
- 2 Type a name in the text field.
- 3 Press **Enter**.

Renaming a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and select **Rename**.
- 2 Type a new name in the group's text field.
- 3 Press **Enter**.

Editing a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, navigate to a group and drag it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you choose **Link**, you create a copy that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Data Monitor Group

- 1 In the Data Monitors tab of the Navigator panel's Dashboards resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Enabling or Disabling Data Monitor Groups

Data monitors are enabled by default. When you disable data monitors they stop processing events and updating their displays. You might choose to disable a data monitor group because it is not needed or should not be considered under certain circumstances.

You can also enable and disable data monitors individually in the Data Monitor resource tree or Data Monitor Editor.

- 1 In the Data Monitors tab of the Dashboards resource tree, right-click a data monitor group.
- 2 Choose **Enable Data Monitor** to activate all the monitors in the group (if they are disabled) or **Disable Data Monitor** to deactivate them (if they are enabled).

Using Query Viewers

Query viewers are a type of resource used for defining and running SQL queries. Query viewers can be added to the regular dashboard. For more information about defining query viewers and adding them to the dashboard, see [“Query Viewers” on page 287](#).

Using Custom View Dashboards

You can create custom layouts of dashboard data using a browser-based runtime environment embedded in the Console. Also known as *image dashboards*, custom view dashboards enable you to create custom views of dashboard data, and can display data monitors over an imported image, such as a geographical map.

- Viewing custom view dashboards requires the Adobe Flash 10 plugin available with the 32-bit Firefox 3 browser.
- Viewing custom view dashboards using the internal browser is only supported on Windows platforms. You can also use custom view dashboards on Linux, Mac OS, and Windows operating systems using an external browser.
- Custom view dashboards are not officially supported on Solaris.
- ESM may require additional configurations to display content using Adobe Flash depending on the operating system you are running.

For details about what platforms support custom view dashboards, see [“Browser Environments for Custom View Dashboards” on page 168](#).

For details about supported browsers and operating systems and the configurations required to display features that use the internal browser, see [“Web Browsers \(Internal and External\)” on page 1030](#).

Custom view dashboards cannot display data from query viewers, or data from the following types of data monitors:

- Event Graphs
- Geographic Event Graphs
- Hierarchy Maps

To view dashboards with these types of data monitors, use the regular dashboard view.

Custom view dashboards do not support drill-down on events.

To see a change made from another Console, refresh the dashboard manually.

Custom view dashboards provide two modes: *View* mode for monitoring and investigating events, and *Arrange* mode, for customizing the layout and background elements.



Access context menus using Ctrl, Alt, or Shift + left click.

The custom view dashboards internal browser uses Adobe Flash Player. Instead of accessing context menus using right-click, access them using **Alt + left click**.

Custom view dashboards refresh event data at the same rate as regular dashboards.

Browser Environments for Custom View Dashboards

By default, custom view dashboards use the internal browser for display. If your operating environment or settings make it so the custom view dashboard cannot be launched in the internal browser, it opens using the default external browser, if available. (As an option, you can open all features that use the internal browser using the specified external browser. See [“Setting Program Preferences” on page 773](#).)

Follow the guidelines and configuration instructions provided in the section [“Web Browsers \(Internal and External\)” on page 1030](#). The table below describes additional details about the operating environments that support the display of custom view dashboards in both the internal and external browsers.

	Viewing custom view dashboards using the internal browser	Viewing custom view dashboards using the external browser
Operating system	32- or 64-bit Windows	32- or 64-bit Linux, Windows, Mac OS (Solaris not officially supported)
Browser	32-bit Firefox 3 with the Adobe Flash 10 plugin Note: The internal browser requires this particular version of Firefox with the Adobe Flash 10 plugin to be installed in the Console operating environment.	Any 32-bit browser with the Adobe Flash 10 plugin.

Displaying Custom View Dashboards

There are several ways to switch from the regular dashboard view to the custom view dashboard view. Each of these methods loads the custom view dashboard editor in the Viewer Panel in the custom view dashboard's *View* mode with the last configuration you saved.

- **From the regular dashboard view in the Viewer panel.** Open the dashboard in the viewer panel: in the Navigator panel, go to Dashboards; double-click the dashboard you want to open, or right-click it and select **Show Dashboard**.
 - ◆ Click the Layout Selector button at the bottom of the display (🔗) and select **Custom Layout**.
 - ◆ Right-click the dashboard tab and select **Custom Layout**.
 - ◆ Right-click any data monitor in the dashboard and select **Dashboard > Custom Layout**.
- **From the dashboard editor in the Inspect/Edit panel.** Open the dashboard for edit in the Inspect/Edit panel: in the Navigator panel, go to Dashboards; right-click the dashboard you want to edit and select **Edit Dashboard**.
 - ◆ In the Layout field drop-down menu, select **Custom Layout**.

- ◆ Click **Apply** to apply the changes and leave the editor open; click **OK** to apply the changes and close the editor.



- **A new or edited dashboard must be saved before the custom view dashboard is accessible.**

If you are creating a new dashboard or have edited an existing one to use the Custom Layout, you must first save the dashboard to establish the custom layout for this dashboard on the Manager.

- **Custom view dashboards are displayed with the default chart and color settings.**

User customizations to chart settings and color selections applied to dashboards in the regular viewer are not applied to the custom view dashboard view.

- **Custom view dashboard backgrounds scale to fit the available Viewer panel space.**

The background image scales to fit the available space in the Viewer panel. You may need to adjust the shape of your viewer panel or browser window to preserve the proportions of the background image.

For more about selecting and working with background images for custom view dashboards, see ["To Load a Background Image" on page 171](#).

To Launch the Custom View Dashboard in a Separate Browser Window

Click **Launch Browser** in the custom view dashboard top menu bar. The custom view dashboard is accessible from any external browser that supports Flash and Java script at the following URL:

```
https://<hostname>:<port>/www/manager-  
ui/com.arcsight.product.manager.kahuna.dashboard.DashboardLauncher  
/index.html?resourceid=<resourceid>&auth=<auth>
```

To Refresh the Custom View Dashboard Layout

Click the Layout Selector button at the bottom of the display (🔍) and select **Custom Layout**, or use any of the other methods described in ["Displaying Custom View Dashboards" on page 168](#).

Custom View Dashboard Context Menu Options

Both the View and Arrange modes offer the following context menu options (Ctrl, Alt, or Shift + left click):

Option	Description
Save Dashboard	Save the current dashboard layout. This option becomes available when you have selected a different layout using the View As context menu option.
Close Dashboard	Close the dashboard in the Viewer panel.
Data Monitor: Edit	Open the data monitor editor in the Inspect/Edit panel.
Data Monitor: Enable/Disable Data Monitor	Enable or disable the data monitor. For more about enabling and disabling data monitors, see "Enabling or Disabling a Data Monitor" on page 161 .

Option	Description
Data Monitor: Minimize	Hide the data monitor from view. To restore a minimized data monitor in a custom layout view, switch to Arrange mode (“Arranging Custom View Dashboards” on page 171), then select and check the data monitor from the Data Monitors drop down menu.
Data Monitor: Close	Remove the selected data monitor from the dashboard.
View As	Change the data monitor view to a graphical format supported for the data monitor type. For more about data monitor views, see “Display Formats” on page 158 .
Show Events	Show the events displayed in the data monitor in an active channel in a separate Viewer panel tab. This enables you to see the event details and perform all the tasks described in “Monitoring Active Channels” on page 129 .
Export	Export the events shown in the data monitor or dashboard as a JPG, CSV, or HTML file, or export the dashboard or data monitor as a report archive in JPG or CSV format.

To Revert to the Regular Dashboard View

- 1 Close the custom view viewer version of the dashboard in the Viewer panel (right-click the dashboard's tab in the Viewer panel and select **Close**).
- 2 Re-open the dashboard from the Navigator panel (double-click the dashboard in the Navigator panel, or right-click it and select **Show Dashboard**).

Working with Custom View Dashboards

Custom view dashboards open in the *View* mode. In *View* mode, you can interact with the dashboard elements much the same way you do in the normal dashboard mode, such as drill down on the events displayed in a data monitor, and take context-menu actions.


The first time you switch to custom view dashboard mode, if there is no background associated with a dashboard from when it was created using the Dashboard editor, the dashboard will be displayed with a white background; otherwise you will see the last background that was added. The data monitors will be rendered in evenly distributed rows.

To Select View Mode

In the custom view dashboard top menu bar, select **View** from the Mode drop-down menu.

To Show Events in an Active Channel View

As with regular dashboards, you can view the events displayed in many types of event-based data monitors in an active channel, which enables you to see the event details and perform all the tasks described in [“Monitoring Active Channels” on page 129](#). There are two ways to view eligible data monitors displayed in a custom view dashboard in an active channel:

- Double-click the dashboard where the pointing hand cursor () is activated.

- Activate the context menu (Ctrl, Alt, or Shift + left click) and select **Show Events**.



Drill-down in an active channel view is not supported for all data monitor types.

The following types of data monitors do not support drill-down in an active channel view:

- Rules Partial Match
- Asset Category Count
- Event Reconciliation
- Session Reconciliation
- System Monitor
- System Monitor Attribute

Arranging Custom View Dashboards

In *Arrange* mode, you can customize the dashboard layout, toggle data monitors on and off, and upload a background image.

When you switch to Arrange mode, chart-type data monitors appear with a yellow background. You can relocate, resize, and reshape all types of data monitors anywhere in the custom view dashboard view.



Changes saved to a custom view dashboard refreshes the dashboard on all ESM Consoles attached to the Manager.

If the ESM Manager supports more than one ESM Console, any custom view dashboard changes saved on one Console will refresh that dashboard on the other Consoles attached to the Manager.

To Select Arrange Mode

In the custom view dashboard top menu bar, select **View** from the Mode drop-down menu.

To Load a Background Image

You can upload a background image to the custom view dashboard. The image you select will be stretched to fit the available display space in the Viewer panel, so for best results, select an image with adequate size and proportion to fill the space.

- 1 Launch the file upload process. There are several ways to load a background image in a custom view dashboard:

- ◆ **Using the File resource.** In the Navigator panel, go to File.
 - In the Navigator panel, first open the dashboard to which you want to add the background image. It can either be in the regular dashboard view or already in the custom view dashboard view.
In the Navigator panel, go to **Dashboards**. Double-click the dashboard you want to open in the Viewer panel, or right-click it and select **Show Dashboard**.
 - In the Navigator panel, go to **Files**. Create a new file (right-click your personal folder, for example, *Admin's Files*, and select **New File**). In the File editor in the Inspect/Edit panel, give the file a name, and click **Upload**.
 - Right-click the file you uploaded and select **Set as Background**.

- ◆ **From the image viewer Background menu.** In the image viewer Arrange mode, click the **Background** drop-down menu and select **Set Background**.
 - ◆ **From the regular dashboard viewer in the Viewer panel.** You can add a background from the dashboard's Viewer tab context menu (right-click the dashboard's tab in the Viewer panel and select **Set Background**), or from a data monitor (right-click the data monitor and go to **Dashboard > Set Background**).
 - ◆ **In the regular dashboard editor in the Inspect/Edit panel.** Open the dashboard for edit in the Inspect/Edit panel: in the Navigator panel, go to Dashboards; right-click the dashboard you want to edit and select **Edit Dashboard**. In the Background field, select **Set Background**.
- 2 In the Upload File Content dialog, navigate to the location on your system where the background image is stored and click **OK**. This loads the image file as a File resource.

**Tip**

If the background image does not display right away, refresh the custom view dashboard.

To refresh the Custom Layout view, click the Layout Selector button at the bottom of the display (🔍) and select **Custom Layout**.

- 3 To enable others to see the custom view dashboard with the image you uploaded, copy the image from your personal Files folder into one of the Shared folders, such as Public.

To Select a Previously Uploaded Background Image

If you have previously uploaded a background image that you want to load as the custom view dashboard background, or you want to use an image, use the File menu resource.

**Note**

Open the destination dashboard in the Viewer panel first

The File resource **Set as Background** option is only available if the destination dashboard is open in the Viewer panel.

- 1 In the Navigator panel, first open the dashboard to which you want to add the background image. It can either be in the regular dashboard view or already in the custom view dashboard view.
- a** In the Navigator panel, go to Dashboards.
 - b** Double-click the dashboard you want to open in the Viewer panel, or right-click it and select **Show Dashboard**.
- 2 In the Navigator panel, go to Files. Right-click the image file you want to add as the background and select **Set as Background**.

**Note**

Other ways to load previously loaded background images

The File menu is the easiest way to see the available images you have already uploaded, but you can use the methods described in ["To Load a Background Image" on page 171](#) to load a previously uploaded image.

Just go through the process to upload the image from your file system. ESM will notify you that a file of that name already exists and ask if you want to overwrite, use the old file, or cancel to stop.

Using Resource Graphs to Verify that a Background Image is Attached

You can verify that a background image has been attached to a custom view dashboard by viewing a resource graph from Files or Dashboards in the Navigator panel.

- 1 In the Navigator panel, right-click the File or Dashboard resource and select **Graph View**.
- 2 In the Viewer panel, verify that the image file is associated with the dashboard.

Removing a Background Image

To remove a background image from a custom view dashboard using the File resource:

- 1 In the Navigator panel, open the dashboard from which to remove the background image. It can be in the regular dashboard or custom view.
 - a In the Navigator panel, go to Dashboards.
 - b Double-click the dashboard you want to open in the Viewer panel, or right-click it and select **Show Dashboard**.
- 2 In the Navigator panel, go to Files. Right-click the image file you want to remove as the background image on the dashboard and select **Remove as Background**.

To remove a background image from a custom view dashboard using the Dashboard editor:

- 1 In the Navigator panel, go to Dashboards. Open the dashboard from which you want to remove the background image for edit in the Inspect/Edit panel (right-click the dashboard and select **Edit Dashboard**).
- 2 In the Dashboard editor in the Inspect/Edit panel, click the Background field and select **Remove Background**.

To Relocate, Resize, and Reshape Data Monitors

Relocate a data monitor by dragging and dropping it in the desired location. Use the sizing handles at the sides and corners to stretch it to the size and shape you want.

To save the layout, use Ctrl, Alt, or Shift + left click and select **Save Dashboard**.

To Select Which Data Monitors to Display and How

There are two ways to select which data monitors you want to display in this dashboard using what display format. The data monitors available to this dashboard must be set in the regular dashboard view in the Console.

- **In a single operation from the custom view dashboard Data Monitors menu.** The custom view dashboard Data Monitors menu lists all data monitors available for this dashboard.



Custom view dashboards cannot display data from query viewers, or data from the following types of data monitors:

- Event Graphs
- Geographic Event Graphs
- Hierarchy Maps

A dashboard that contains these types of data monitors will only display the supported dashboard types. Data monitor types that are not supported in the custom view dashboard view will appear on the menu of data monitors for this dashboard, but will be unavailable for selection.

- ◆ To add or remove the data monitor from the dashboard, check or uncheck its checkbox.
- ◆ To change the data monitor display format, select a display format from the available formats for this data monitor. For more about display formats, see [“Display Formats” on page 158](#).
- **For each individual data monitor from the custom view dashboard context menu.** Use Ctrl, Alt, or Shift + left click to access the context menu.
 - ◆ To add or remove the data monitor from the dashboard, use Ctrl, Alt, or Shift + left click and select **Data Monitor > Minimize**.
 - ◆ To change the data monitor display format, use Ctrl, Alt, or Shift + left click and select **View As**. For more about display formats, see [“Display Formats” on page 158](#).

You also have the same context menu options described in [“Working with Custom View Dashboards” on page 170](#).

Monitoring Active Lists

You can directly examine and modify the active lists available in the Navigator panel's Active Lists resource tree.

Viewing Active List Contents

- 1 Choose the Active List resource tree in the Navigator panel.
- 2 Right-click an active list and choose **Show Entries**.

Refreshing Active List Views

Active lists show results as of the time they opened for viewing, or the last time they were refreshed.

Click the **Refresh** button in the view header to update the contents.

Adding to or Subtracting from an Active List

You can conveniently add or remove event-attribute-based active list entries using selected events in active channel grid views. This feature automatically offers the name of the active list that is appropriate for the selected event.

- 1 In an active channel grid view, select an event that is relevant to an active list of interest.
- 2 Right-click the event and choose **Active List>Add to><active list>** or **Active List>Remove from><active list>**.



If an active list uses the Old File Size event attribute, note that the value required when adding an entry will be in bytes (not kilobytes or megabytes).

Filtering Active Lists

In addition to the constraints of an active list itself, you can place a temporary filter on an active list view to aid your analysis. Such filters are not saved with the active list.

- 1 Open an active list in the Viewer panel as described above.
- 2 Click the **Filter** status description in the view header to open the Common Condition Editor. For example, the status **No Filter Defined**.
- 3 Use the Common Condition Editor as described in [“Creating Filters” on page 223](#).

Editing Active Lists

You can change an active list's definition or simply add a new entry to its parameters.

- Right-click an active list in the Navigator panel and choose **Edit Active List** to open it in the Active List Editor. See [“Managing Active Lists” on page 571](#) to use the editor.
- Click the **Add Entry (+)** button in the active list view header to open the Add Entry editor.

Clearing Active List Views

While monitoring a particular active list grid view, you may want to see only traffic that happens after a certain point in time. You can accomplish this by clearing the view.

- 1 In the Navigator panel's Active List resource tree, select the active list to clear.
- 2 Right-click and choose **Clear Entries**.

Customizing Active View Grid Columns

You can modify active list grid views just like other grid views, as described in [“Customizing Grid Columns” on page 152](#).

Active List Grid Context Menu Commands

You can also use a set of right-click context commands available in active list grid views.

Menu Command	Description
New	Add an entry to the active list using the Active List Entry Editor.
Edit	Edit the selected entry using the Active List Entry Editor.
Delete	Remove the selected entry from the active list.

Graphing Attacks

You use graphic analytics to quickly identify high-volume attackers or targets at a glance. You can immediately locate and typify cascading attacks (e.g., worms and viruses), and rapidly isolate and analyze events involving interactions between two or more devices (e.g., threat discovery).

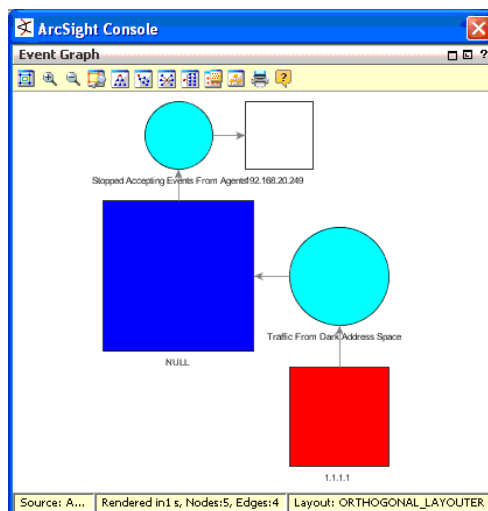
The event data you visualize can be **static** (a snapshot of the selected events) or **live** (continuously updated with specified real-time event data). You create static graphs by selecting certain event data out of a source and casting it as a graph. You create live graphs using a graphic data monitor type.

See [“Changing User Preferences” on page 772](#) to set or change your event graph preferences.

Creating Static Event Graphs

- 1 Select an array of events in a grid, data monitor, or event inspector.
- 2 Right-click the selected set and choose **Event Graph** or **Geographic View**.

The Viewer panel displays the selected events in a new view, using the graphic or geographic styles described below.



Creating Live Event Graphs

- Select an Event Graph or Geographic Event Graph data monitor in the Dashboards tab of the Navigator panel's Dashboards resource tree. Right-click it and choose **Add to Dashboard As>Geographic Graph** or **Graph**.
- Alternatively, right-click your personal Data Monitors folder in the Navigator and choose **New Data Monitor**. In the Data Monitor Editor, in the Data Monitor Type drop-down list, choose **Event Graph** or **Geographic Event Graph**. Define the graphic data monitor in the usual way.

The Data Monitor Editor has certain attributes for these types:

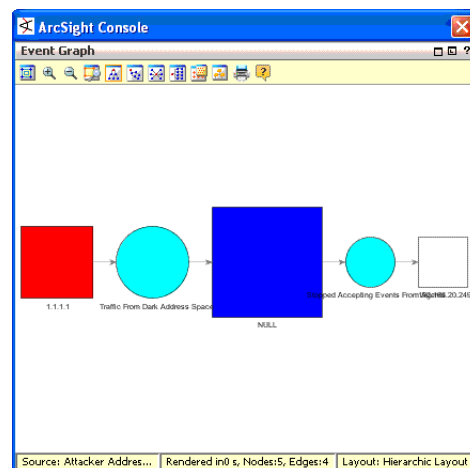
Attribute	Usage
Max Event Count	The number of most-recent events to show. Events older than this are discarded.
Event Node Identifier	The fields that are available to use to uniquely identify the event type in a transaction.
Availability Interval	The number of seconds for the interval between updates to the graphic.
Show Source-Target Nodes as	See "Changing User Preferences" on page 772.
Source Node Identifier	See "Changing User Preferences" on page 772.
Target Node Identifier	See "Changing User Preferences" on page 772.
Show Event Nodes	See "Changing User Preferences" on page 772.

Geographic Event Graph Attributes:

Attribute	Usage
Max Event Count	The number of most-recent events to show. Events older than this are discarded.
Availability Interval	The number of seconds for the interval between updates to the graphic.

Event Graph Notes

Link-analysis visualizations are chart-like or logically oriented. Geo-spatial visualizations are map-based or physically oriented. Node size indicates increasing event volume.



Each event is composed of the event node itself (a turquoise circle) and its connected source node (red square) and target node (white square) device assets. The source and the target may be the same asset.

Blue squares indicate a combined source and target node (a "point event"). Pink nodes indicate IP addresses that are worm or virus infection sources for other nodes.

Point events occur on a single host; for example, a syslog entry for a running process. They graph as IP address nodes that loop to an event node and back.

In geo-spatial displays, source and target location plotting is based on the physical addresses registered for IP addresses. ArcSight includes standard plotting information for this purpose. The addresses are plotted against a world map that you can zoom in or out. All the specific location data that supports this feature also appears as attributes in the Event Inspector.

You can modify the way graphs plot events, choosing to keep the source-event-target visual relationships compact, or to emphasize unique sources, targets, or both in order to more easily clarify the nature of attacks or situations.

Chapter 8

Pattern Discovery

ArcSight Pattern Discovery™ is a separately-licensed product that enables you to discover previously unknown patterns, which might pose a threat, and view them for analysis.

This chapter contains the following sections:

- [Pattern Discovery Overview](#)
- [“Installing Pattern Discovery” on page 181](#)
- [“Pattern Discovery Life Cycle” on page 182](#)
- [“Installing Pattern Discovery” on page 181](#)
- [“Creating or Editing a Profile” on page 182](#)
- [“Taking a Snapshot” on page 188](#)
- [“Investigating Patterns” on page 193](#)
- [“Usage Guidelines” on page 201](#)

Pattern Discovery Overview

When finding threats by matching events against rules, you have to know the threat characteristics and create a rule that matches them. ArcSight Pattern Discovery enables you to search for threat patterns with known characteristics as well, but you can also find unknown patterns, where the only characteristic you specify is that the transactions are related and repeat.

The purpose of ArcSight Pattern Discovery is to:

- Effectively search streams of potentially millions of events for patterns, which are simply repeating sequences of related events.
- Establish a baseline of patterns that represent normal event traffic and filter them out.
- Analyze what remains for threats.

In this way you can discover and investigate patterns that might represent new threats or threats whose characteristics are not known to you.

What Pattern Detection Provides

ArcSight Pattern Discovery can automatically detect subtle, specialized, or long-term patterns that might otherwise go undiscovered in the flow of events. You can use Pattern Discovery to:

- **Detect day-zero attacks:** Pattern Discovery profiles are general enough that they can discover patterns that have never been seen before.

- **Detect low-and-slow attacks:** Low-and-slow attacks involve fewer events over a longer period. Profiles with longer time periods can capture these patterns.
- **Automatically create rules:** You can transform patterns into a rule set that is unique to your environment and more accurate than generic predefined rules.
- **Discover normal patterns:** New patterns discovered from current network traffic are like signatures for a particular subset of network traffic. You can specify which patterns are normal so that matching patterns can be eliminated as a threat.
- **Save a history of threat patterns:** ArcSight Pattern Discovery can use event patterns that originate from or target an asset to categorize those assets. For example, a pattern of events from a machine that has an unauthorized program initiating a connection to an attacker (a back door) can be shown as a cluster. If you see this pattern originating from a new asset, it is a strong indication that the new asset also has a back door installed.

Use Pattern Discovery for preventive maintenance and early detection in your security management operations. Using periodic, scheduled analysis, you can continuously scan for new patterns over varying time intervals to stay ahead of new exploits.

Pattern Components

Events in a pattern share one or more common field values. For example, they could share the same source and target IP addresses, ports, host names, or other data.

The Pattern Discovery algorithm examines event components and identifies groups of related components as transactions. Discovered patterns list the components involved and the transactions containing common components. This data is output as a pattern resource. Components can relate to one another in several ways:

- **Related by session:** Session refers to a unique pair of source and target addresses. The events for which this pair are the same are in the same session.
- **Together in a sub-stream:** The event stream can be divided into sub-streams using a “group by” operation on a subset of event fields. This step can also take time of occurrence into account.
- **Together in time:** All the components occur together in a small time window.

Event components with some kind of relationship are grouped together as transactions, which then become potential candidates for patterns. The Pattern Discovery algorithm processes all the transactions it finds and produces patterns, depending on whether they satisfy one or more conditions that make them discernible as patterns.

Event components are subdivided into transactions in two major ways: time-based division, and event field-based division. These two methods can be combined.

Time-based division is based on timing constraints, and is very similar to the constraints used in defining rules. For example, the system creates a transaction at every division of an event stream. The event stream can be divided depending on the rate of occurrence of events and changes in those rates. This works well for dividing event streams that display events in bursts of activity.

Event field-based division is very similar to doing a “group by” operation on event fields. Every related group of events is a sub-stream of the original stream of events. For example:

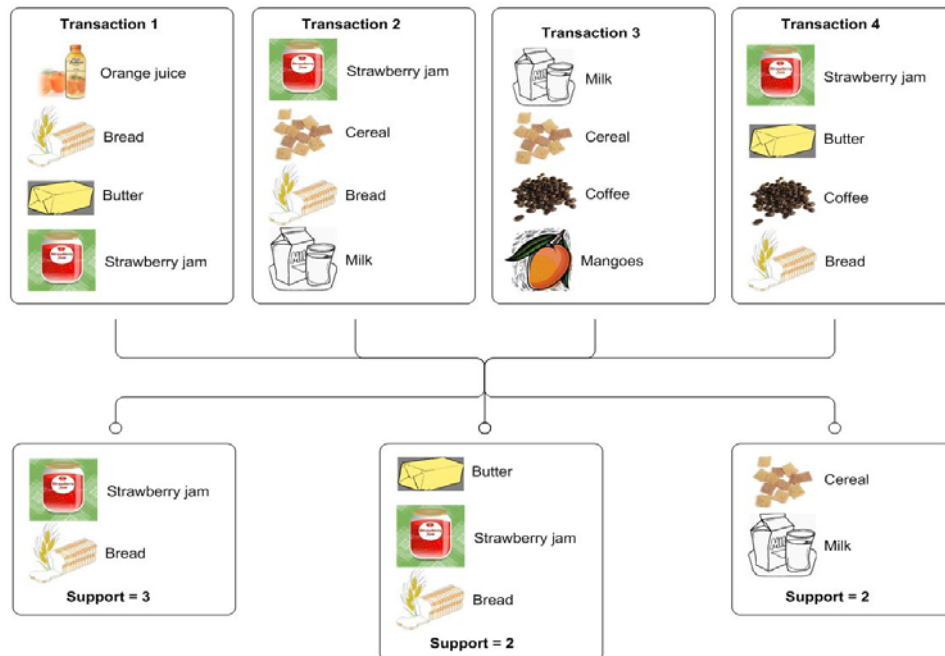
- **Based on source, target address, and port:** Suppose there are three distinct source addresses in the event stream. After doing a “group by,” three sub-streams are generated, each one originating from and corresponding to a unique source address.

- **Based on source and target address:** In this case, all the events that have the same source and target address belong to the same sub-stream.

How Pattern Discovery Works

Once the event stream is divided into transactions, Pattern Discovery identifies and groups events that occur together in multiple transactions. These events are sub-grouped by support level, which is the number of times that event occurred with its related events. A higher support number means that a pattern has occurred more frequently than others.

For example, consider the separate grocery purchase transactions, below. Several patterns emerge: Bread, butter, and jam were purchased together, as were milk and cereal. An analyst can draw conclusions from those patterns: these shoppers intend to make toast, or have cereal. Bread and strawberry jam also appear in two patterns and are a sub-pattern.



You can mask patterns you consider normal traffic so the system recognizes them and does not reevaluate them. For potential threat patterns that you want to watch for, you can build a rule based on the pattern characteristics. When the pattern occurs, the rule triggers an action, such as notifying a group of users or running a command script.

Installing Pattern Discovery

ArcSight Pattern Discovery is a separate feature, installed with ESM, but is enabled by a separate product license. Contact your ArcSight representative to obtain a license key.

The license file is in a ZIP file. Follow the steps below:

- 1 On the system where ArcSight Manager is installed, copy the ZIP file to the ARCSIGHT_HOME directory (the directory that contains the ArcSight installation).
- 2 Run the following command from the \bin directory: `arc sight deploylicense`
- 3 Provide the location for the new license

ArcSight Manager automatically detects the new license.

Pattern Discovery Life Cycle

The creation and use of Pattern Discovery consists of three phases:

- Create a profile (see [“Creating or Editing a Profile” on page 182](#))
- Generate snapshots (see [“Taking a Snapshot” on page 188](#))
- Investigate patterns (see [“Investigating Patterns” on page 193](#)).

Use these options to analyze and respond to the patterns you discover in snapshots.

Option	Usage
Create Rule	Use the Rules Editor to create a rule from a detected pattern of events or a selected event-level in the pattern hierarchy.
Show Related Events	Open a new channel filtered with a <code>matchesPattern</code> operator that uses the whole pattern, or event-levels, as its argument.
Show Event Graph	Graph the complete pattern or a selected event-level in the pattern hierarchy, to analyze using the ESM Console's visualization tools.
Inspect Pattern	The Pattern Inspector shows details, and you can click the Actions button to apply the options described in this table.
Investigate	You can create an active channel, or add a filter to the editor, using (or not using) the name of the selected event item in the pattern.
Tools	Choose one of the network tools ArcSight provides to explore the origin of the selected event item.
Annotate Pattern	You can mark the pattern with a workflow collaboration Stage and Assign it to a user for filtering by Stages and Users resources.

Creating or Editing a Profile

A profile is a set of filters that define what fields to include in your pattern search, and the scope and properties of a pattern. It also specifies the time period to search. Profiles can be general or specific. Typically you would use several different profiles to define the parameters of snapshots, which collect all the events in the specified time frame and evaluates them according to the filters set in the profile.

Pattern Discovery comes with two profiles in the **Shared | All Profiles | ArcSight System** folder:

- **Daily Pattern Discovery** - Searches for patterns over the previous 24 hours from the time of the snapshot. This profile is not scheduled; you can run it on demand.
- **Quarter Hourly Pattern Discovery** - Searches for patterns over the 15 minutes prior to the snapshot. This profile is not scheduled, you can run it on demand.

Use the following procedure to create a new profile:

- 1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
- 2 Expand the Profiles resource tree. Right-click a group in the resource tree and select **New Profile**.
- 3 In the Inspect/Edit panel on the Profile Editor **Attributes** tab, you can modify most of the values.

You cannot rename or delete profiles in the ArcSight System Profiles group. You can edit them, but ArcSight recommends that you edit a copy you have pasted into another profiles folder. To use one of these profiles as is, see [“Taking a Snapshot” on page 188](#).



You cannot delete or modify a profile if it has patterns and snapshots derived from it. This safeguards the relationships with snapshots that share the same profile. To modify or delete a profile, delete associated snapshots or patterns.

To copy and paste a profile to another folder, select the profile to copy. Go to **Edit | Copy (Paste)** or use Ctrl + C (V).

Editing Profile Attributes

Use the following procedure to edit a profile:

- 1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
- 2 Expand the Profiles resource tree and navigate to the profile you want to modify.
- 3 In the Inspect/Edit panel on the **Attributes** tab, you can change most values and click **Apply**. Some values, such as version ID, are set by ArcSight and are not editable.

Property	Usage
Summary	A profile summary appears below the Attributes tab. The underlined items are values entered in the fields below.
Profile	
Name	Enter a descriptive name for your profile
Minimum Pattern Length	Type or use the up/down arrows to select the minimum number of unique associated events necessary to qualify the events as a pattern. The default value is 2 events.
Minimum Pattern Occurrences	Type or use the up/down arrows to select the minimum number of times for an event-association of the specified length to reoccur in order to qualify as a pattern. The default value is 2 occurrences.
Start Time	<p>Select a time stamp expression for the snapshot start time. Expressions are described below.</p> <ul style="list-style-type: none"> • \$Now The current time in the format hh:mm:ss. • \$Now - 1h The current time minus 60 minutes. • \$Now - 1d The current time minus 24 hours. • \$Now - 1w The current time minus 7 days. • \$Today The start of the current day (12:00:00). • \$Today - 1d The start of the current day at midnight (12:00:00) minus 24 hours. In other words, the start of yesterday. • \$CurrentWeek The start of the current week (Sunday 12:00:00). • \$CurrentMonth The start of the current month (the 1st 12:00:00). <p>The format of start time is \$Now-<time>. The time is in increments of hours, days, weeks, or months.</p>

Property	Usage
End Time	Use the \$Now drop-down menu to select a timestamp expression for the snapshot end time. The formats are the same as for Start Time, above.
Events	
Event Fields	<p>You can select one or more of these (event field, source, and target) for the pattern portion snapshot to display. Click in the data entry area and then click drop-down menu to see the field's chooser.</p> <p>In the Available Fields area, click the tab from which you want to choose. you can select one or more:</p> <ul style="list-style-type: none"> Field Sets. If licensed, this includes domain field sets (see "Domain Field Sets" on page 491). Local variables you created for this profile (see "Creating Local Variables" on page 187). Fields and global variables that are relevant to a pattern discovery profile. <p>In the Selected Fields section:</p> <ul style="list-style-type: none"> Use the up and down arrows to specify the order in which they appear. Use the green alias icon to create an alias version. Use the red X icon to remove one from the list.
Source	
Target	
Restrict by Filter	Click the All Events drop-down menu to choose a filter from the Filters resource tree. The filter restricts the pool of events from which the snapshot is constructed.
Advanced	The checkboxes in this section instruct the snapshot to capture elements pertaining to time, which can lend vital insight to a pattern.
Record Time Order	<p>This includes the time sequence of the events contained in patterns. For example, for a three-event pattern, it could record that A-B-C occurred 40 percent of the time, B-A-C 35 percent, and A-C-B 25 percent.</p> <p>Because event sequences can reveal intent, you can detect and act upon certain kinds of activity even sooner.</p>
Split on Inactivity	<p>This detects potentially meaningful decreases in activity between duplicate source/target pairs.</p> <p>It creates a break if there is a pause or significant drop in the number of times a particular pattern occurs. This treats occurrences of the pattern on either side of the break as separate instances.</p> <p>On analysis, a split on occurrences of the same source/target pairs means that there was a slow-down or break in occurrences. This enables you to discover patterns that happen repeatedly for one source/target pair.</p>

Property	Usage
Discovery Results	
Snapshot Retention Time	Click the drop-down menu to select how long you want the system to save a snapshot and its series of events. Snapshots retain all the needed components of the events and make them available during analysis. For example, when you drill down in an event and select "Show related events," the events saved within the time frame set here will be searched for matches. The default retention time is 7 days.
Snapshot Group	Choose a group in the Snapshot resource tree in which to store the resulting snapshots. By default, the system adds the snapshot to the same folder you right clicked to add the profile.
Pattern Group	Choose a group in the Patterns resource tree in which to store the resulting patterns. By default, the system adds the pattern to the same folder you right clicked to add the profile.
Common	
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. Your ArcSight administrator can advise you on the correct values for this field, if applicable.
Alias	An identification string suitable for referencing resources within ArcSight. A given alias appear in place of the resource's name everywhere it may be seen. Your ArcSight administrator can advise you on the correct values for this field, if applicable.
Version ID	If this profile came in a package or if you have exported it to a package, this is the package's version ID.
Description	A text description of the profile.
Assign	
Owner	The user with responsibility for the profile.
Notification Groups	The user group(s) to notify concerning changes to a profile.

- 4 Click **OK** to apply the changes and close the editor.

Specifying Actions

The **Actions** tab enables you to select a trigger, then specify the action to take when that trigger occurs.

To specify an action:

- 1 Open the profile in the profile editor (double click the profile in the Navigator panel).

- 2 In the Inspect/Edit panel, click the **Actions** tab.
- 3 Before you add an action, specify when to take the action (the trigger). Select one of the following trigger options:

Trigger Option	Description
On Pattern Discovered	This specifies that the action be taken the first time a new pattern appears. Choose this option for assigning new patterns to an analyst to investigate.
On Pattern Re-discovered	This specifies that the action will be taken if a new pattern is repeated. Choose this option for ongoing operations.

- 4 Click **Add** and select one of the following options:

Action Option	Description
Annotate Pattern	In the dialog box, enter the following values and click OK : <ul style="list-style-type: none">• Select a Stage from the drop-down menu.• Assign a user from the drop-down menu.
Set Event Field	In the dialog box, enter the following values and click OK : <ul style="list-style-type: none">• Select a Field Set (or domain field set you created) from the drop-down menu.• In the event fields grid, set values for the event fields you are interested in.
Send Notification	Specify a notification group in the Notification Group drop-down menu. <ul style="list-style-type: none">• Click Ack Required if those notified should acknowledge that they received notification.• Write the message to send in the Message field.
Execute Command	In the dialog box, enter the following values and click OK : <ul style="list-style-type: none">• Select an operating system platform from the drop-down menu.• Enter the command string. Use correct syntax; the system does not validate command strings.• Enter required parameters. For example, the archive tool needs the manager name, admin name, and password. Specifying them lets the system execute the command without user intervention.• In the Action Type drop-down menu, select one of the following: Automatically run on manager: Initiates the command with no user intervention. Run on Manager with Console confirmation: Displays a confirmation dialog box in the ESM Console for the designated user before the command is initiated. Run on connector(s): Sends the command to the connector(s) that report the events.

Action Option	Description
Execute Connector Command	<p>Specify a command to be executed at the SmartConnector reporting the events, such as pause or stop/start event flow. Enter the following values and click OK:</p> <ul style="list-style-type: none"> In the Connector drop-down menu, select the SmartConnector to execute the command. When you select an connector, the command field is populated with the commands available for that connector. In the Command field, select the command for the connector to execute. The command may contain required parameters.
Export to External System	You can export the pattern to an external tracking system, such as BMC Remedy, if you configured it to operate with ESM. Click OK .
Active List	<p>You can add (or remove) a pattern to an active list, where its event details are available to other correlation tools for reference.</p> <ul style="list-style-type: none"> To add a pattern to an active list, select Add to Active List. In the dialog box, select an active list from the drop-down menu and click OK. To remove a pattern from an active list, select Remove from Active List. In the dialog box, select an active list from the drop-down menu and click OK.
Session List	<p>You can add a pattern to a session list, or terminate a session list based on a pattern, where its event details are available to other correlation tools for reference.</p> <ul style="list-style-type: none"> To add a pattern to a session list, select Add to Session List. In the dialog box, select a session list from the drop-down menu and click OK. To terminate a session list, select Terminate Session List. In the dialog box, select a session list from the drop-down menu and click OK.

- 5 The action summary will be displayed in the Actions tab. To remove lines that are not used, click **Hide Empty Triggers**.

Creating Local Variables

Click the **Local Variables** tab to manage local variables for this profile. These are available to select from the drop-down menu on the **Attributes** tab for Event Fields, Source, and Target attributes associated with the pattern.

From this tab you can:

- Add a new variable, which enables you to
 - ◆ Name the variable
 - ◆ Specify a function (expression).
 - ◆ Specify the arguments. Available arguments depend on the function.
- Edit an existing variable
- Remove a selected variable
- Make a variable global, which means it is available to resources outside this profile. If you make a local variable global, it moves it from the **Local Variables** tab to the

Fields and Global Variables tab in the chooser for Event Fields, Sources and Targets, on the **Attributes** tab.

For more information on using local and global variables, see [“Variables” on page 1006](#).

Pattern Discovery supports the following variable return data types:

- | | |
|---------------|---------------|
| • Byte | • Long |
| • Double | • Resource ID |
| • Enumeration | • String |
| • Integer | • Address |

Therefore, function variables that return an unsupported data type are not supported. For example, the following functions or function categories are not supported:

- Non-SQL-mode variables.
- Variables that return a list, such as ActorByAccountID.AccountID and variables that operate on multi-mapped active lists or overlapping session lists.
- Variables that return a boolean value, such as the Category Model function *hasRelationship*.

Adding Notes

You can keep track of changes made to a profile using the Notes feature. To add a note:

- 1 In the Profile Editor, click the **Notes** tab.
- 2 In the Notes field, enter a note and click **Save** to log it in the Table/List tabs.
- 3 You can view notes as a table or as a list by toggling between the Table and List tabs. You can re-order the table view by clicking the column header.

Deleting a Profile

- 1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
- 2 Right-click a profile in the resource tree and choose **Delete Profile**.



You cannot delete a profile that has patterns and snapshots derived from it. This safeguards the relationships among snapshots sharing the same profile. To delete a profile, delete all snapshots or patterns associated with it.

- 3 Click **Delete** in the confirmation dialog box.

Taking a Snapshot

A snapshot is a record of qualifying events that occurred over a specified period of time and evaluated according to the snapshot profile. When the Pattern Discovery algorithm runs on the specified data set, it displays the result as a graphic, which you can use for investigation and analysis.

You can generate snapshots manually, or run them on a schedule. You are likely to generate snapshots more frequently during the early stage of implementation, when you are establishing a baseline of normal patterns. Each snapshot is stored in the Navigator panel in Pattern Discovery on the **Snapshots** tab.

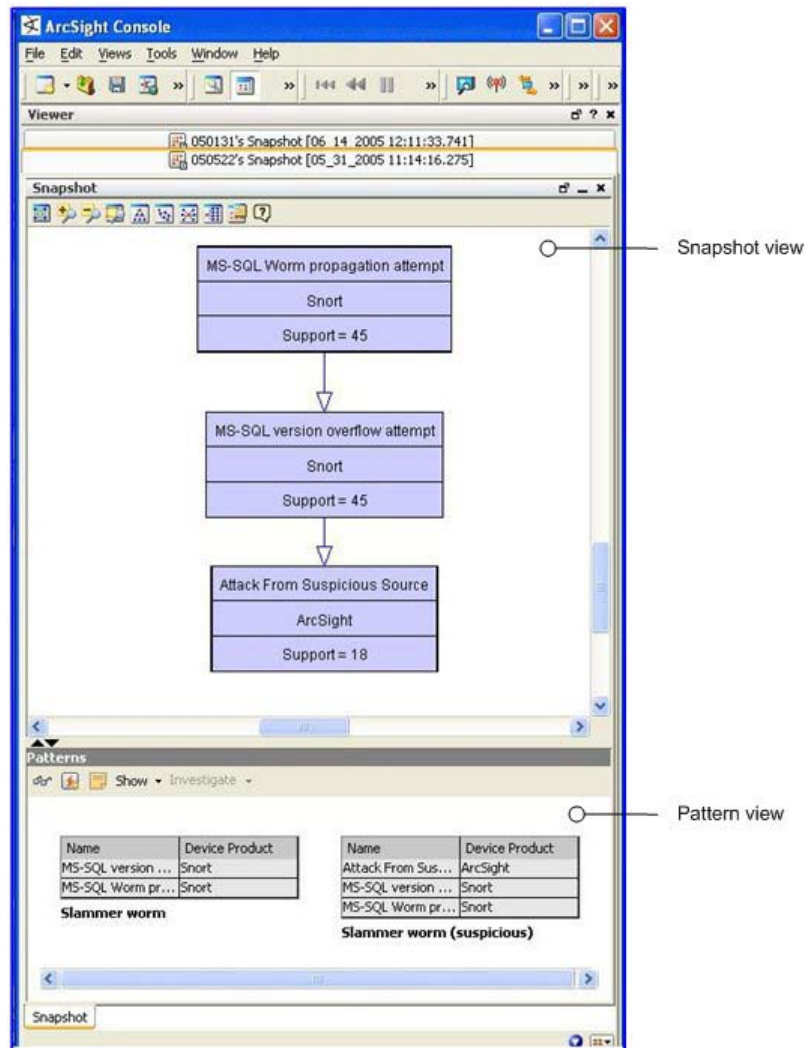
You can also discover patterns directly from active channels. Right-click a channel in the Navigator panel and choose **Discover Patterns**.

To take snapshots:

- 1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
- 2 Right-click a profile in the resource tree and select **Take Snapshot**.
- 3 In the Viewer panel, the system processes the snapshot request and shows each process as the Pattern Discovery engine runs:

	Pattern discovery run scheduled. Done!
	Building snapshot from events. Done!
	Saving snapshot. Done!
	Extracting patterns from snapshot. Extracting patterns from snapshot.

- 4 When the process finishes, the system displays the snapshot in the Viewer panel. The views are linked; click a node in the snapshot view to see its details in the patterns view.



If the pattern is empty, no events passed the profile's filter restrictions during the specified period. Adjust these profile specifications and generate the snapshot again.

Exploring a Snapshot

The upper part of the Viewer panel presents the snapshot view, which shows a hierarchy of related event nodes.

The lower part of the Viewer panel is the patterns view, which shows blocks of events from the hierarchy that are most closely related. Each block of events represents one specific path through the pattern hierarchy.

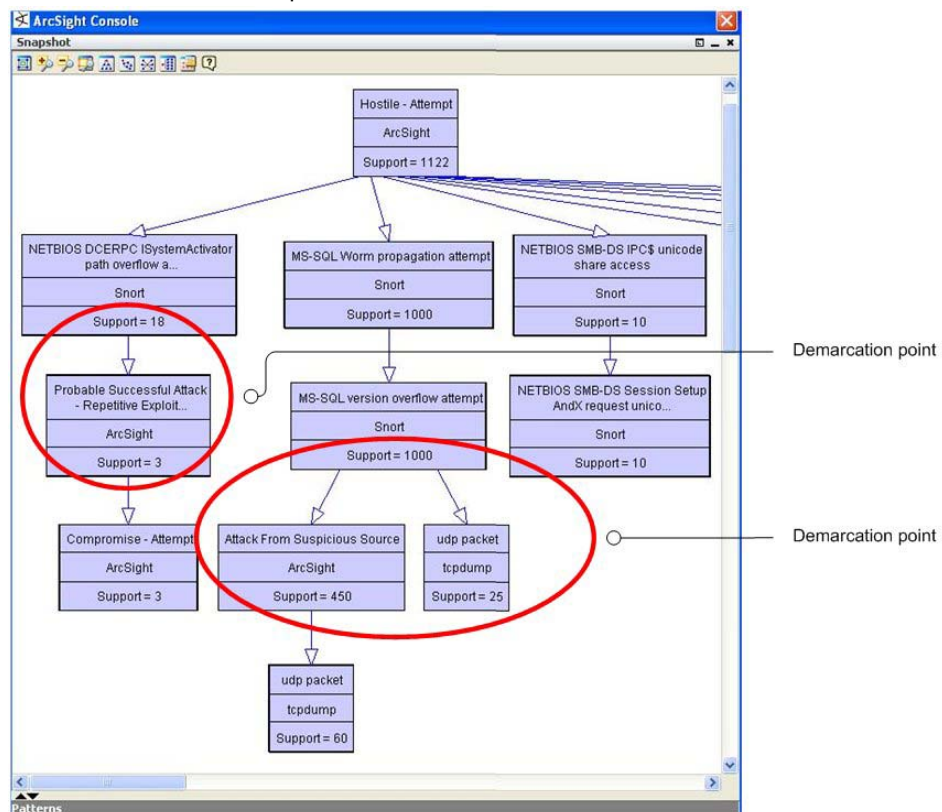
4 on page 190 shows two patterns and a demarcation point (between support = 45 and support = 18). The top two events are the SQL worm. The last event is generated by the system. Pattern Discovery classified 18 of 45 sources as suspicious. There are 27 sources that ran the slammer worm in the network, but they were not added to the suspicious list.

This discovery enables you to investigate why all 27 systems were not caught by the other surveillance mechanisms in place on your network. Determining that will help you to tighten your network security.

The “support” value for each node is the number of times that event occurred with its related events. The higher the number, the higher the item appears in the hierarchy.


For example, in , below, there are two points at which there are sharp differences in support from one item to the next. This shift in support level is called a demarcation point, and indicates a sub-pattern in a longer sequence.








The demarcation points indicate attack stages, and sometimes variations of the same type of attack on different network systems. For example, the SQL worm propagation attempt makes up 1000 of the 1122 hostile attempts. The demarcation point in the center of the graphic shows that there are two variations: attack from suspicious source, and UDP packet tcpdump. This can indicate how different systems process the same type of SQL worm attack. Demarcation points are circled, below:



Arranging Elements in Graphic View

Use the buttons across the top allow you to zoom in, zoom out, and arrange the elements in different formations to give you better visibility of the overall pattern.

Button	Control	Description
	Fit Content	Sizes the graphic to the available display space.

Button	Control	Description
	Zoom in/ Zoom Out	Increases or decreases the size of the displayed graphic.
	Zoom Selected	Zooms in on a selected portion of a graphic.
	Hierarchic Layout	Presents nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing relationships with a common root.
	Organic Layout	Arranges nodes based on minimum edge length, which tends to cluster items with a common relation. Clusters with items in common also tend to group together.
	Circular Layout	Hub-and-spoke arrangements with each node radiating edges to, or receiving edges from, the items with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout.
	Orthogonal Layout	Arranges items on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are useful for clearly tracing connections and identifying node clusters.
	Overview	Opens a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.

In addition to the control buttons, you can drag items around in the Viewer panel while maintaining the connections. This can make the view clearer for overlapped items.

Scheduling a Snapshot

You can schedule a snapshot to be taken at intervals. The schedule frequency can be part of your daily analysis and operations. For example, as a best practice, you can run Pattern Discovery once a day to capture event patterns that happened over the last 24 hours. You can specify a longer period to find patterns with a longer term. To fully automate daily Pattern Discovery, add actions to a schedule, such as sending notifications, opening cases, or adding systems to an active list, if certain conditions are met.

- 1 In the Navigator panel, go to Pattern Discovery and click the **Profiles** tab.
- 2 Right-click a profile in the resource tree and select **Schedule Snapshots**.



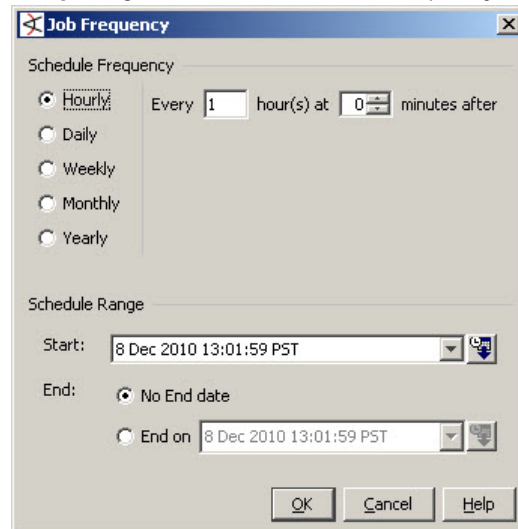
Note

Profiles in the System Profiles group are locked; you cannot add to or modify the schedules for profiles in the System Profiles folder.

To use one of the System Profiles as a template, copy it to another folder.

- 3 On the Jobs tab, click **Add**.

- 4 In the Summary field at the bottom, select **Click here to set up schedule frequency**. This activates the Job Frequency dialog.



- 5 Click **OK** when you have set the frequency and time range.
- 6 Repeat [Step 3](#) to add more schedules for the same snapshot.
- 7 When you have added all the schedules for this snapshot, click **OK** at the bottom of the Jobs tab.
- 8 To add an action to be taken every time the profile is run, specify an action in the Actions tab of the profile editor, as described in [“Specifying Actions” on page 185](#).

Re-opening a Snapshot

If you have closed a snapshot in the Viewer panel, you can re-open it.

- 1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.
- 2 Navigate to the snapshot graph. Right-click the snapshot and select **Show Snapshot**.

When the snapshot's graphic has formed in the Viewer panel, you can click the icons at the top of the view to change its layout as described in [“Visualizing Resources” on page 674](#).

Deleting a Snapshot

- 1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.
- 2 Right-click a snapshot in the resource tree and choose **Delete Snapshot**.
- 3 Click **Yes** to confirm the deletion.

Investigating Patterns

When you take a snapshot, the Pattern view shown in the snapshot is also saved in the Patterns tab of the Pattern Discovery resource tree. You can use the Patterns tab to access more event investigation tools.

Investigating Patterns in the Snapshots View

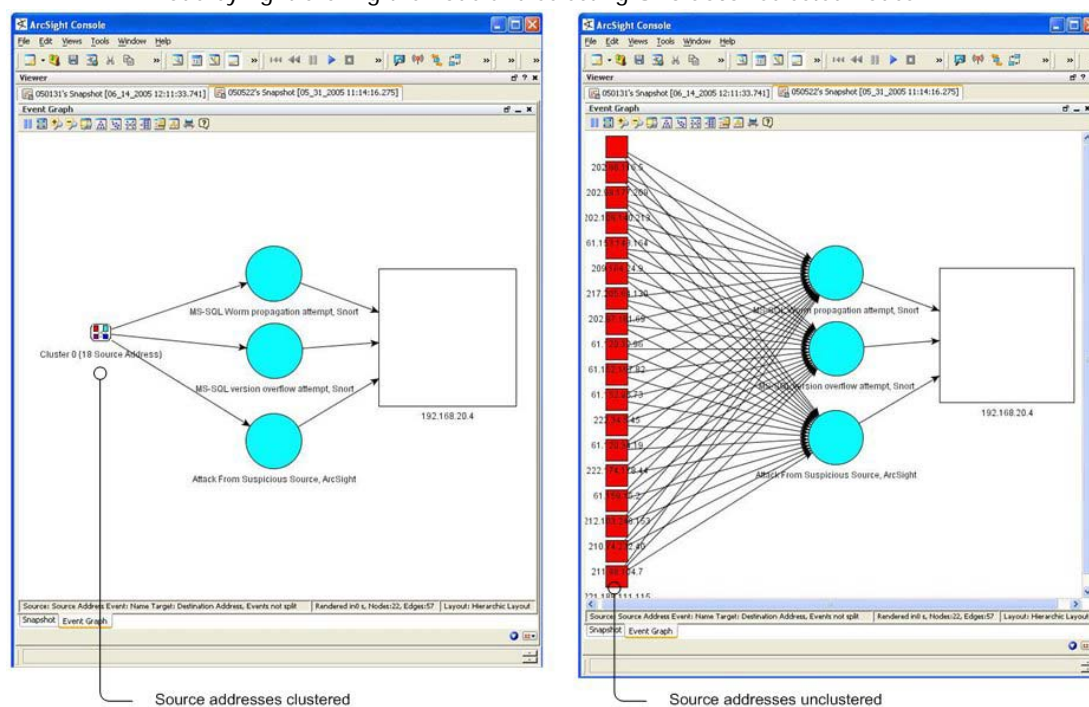
Pattern Discovery gives you access to investigative tools from a series of buttons. These same tools are available from the right-click menu. The snapshot view and the patterns view offer most of the same investigative tools with a few specific differences. Right-click on any item in the graphical Snapshots view to open a new window within the snapshot view that contains details about the related events:

Right-Click Option	Description
Show related events	<p>Opens a new active channel in the Snapshots tab, filtered with a matchesPattern operator. This channel uses the pattern, or selected event-level in the pattern hierarchy, as its argument.</p> <p>To toggle back to the graphic view, click the Snapshot tab at the bottom of the snapshot Viewer panel.</p>
Investigate	Creates a channel in a grid view that contains the associated events sorted according to Attacker Address, Name, and Target Address.
Tools	<p>Configure... includes the following options, and can be accessed directly through the larger Tools menu:</p> <ul style="list-style-type: none"> • Nslookup - Resolves an IP address to a host name (domain name) and vice versa. • Ping - Determines whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response. • PortInfo - Lists standard usage such as WWW or FTP for a specified port number. • Traceroute - Shows the path from the ESM Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between. • WebSearch - Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells. • Whois - Looks up who is behind a given domain name; information might include addresses and telephone numbers. • Results... - provides the results of running a network tool using the attributes of the selected pattern block <p>For more information about network tools, see the online Help.</p>
Create Rule...	<p>Launches a Rules Editor in the Inspect/Edit panel. The rule you create here is stored in the Rules resource tree under the personal rules of the user who created it.</p> <p>For instructions about how to construct a rule, see "Creating Rules from Patterns" on page 198.</p>
Show Event Graph	Displays the pattern as an event graph, which shows pattern components and their relationships in graphic form. For more information about ESM event graphs, see the online Help.

Right-Click Option	Description
Show	Allows you to reset the graphic view with the following options: <ul style="list-style-type: none"> Show all nodes - Displays the entire snapshot graphic. This is helpful if you have drilled down and wish to redisplay the original snapshot. Show all nodes containing selected items - Displays only the event hierarchy that contains the selected item. Hide all nodes containing selected items - Displays all the event hierarchies that do not contain the selected item.

The example in shows our sample pattern displayed as an event graph. To save space, the event graph consolidates items that have many members. In this case, the sample on the left shows the source address nodes consolidated into a single cluster with a single line representing the connections to each of the event name nodes.

To see the details and number of these connections, as shown on the right, uncluster the node by right-clicking the node and selecting **Uncluster** selected nodes.





Toggle between multiple views in the Snapshot window using tabs. Unclustering the source address nodes allows you to see the details of those nodes.

When you use the right-click menu to open a new view, it displays in a new tab within the snapshot pane. Use the tabs at the bottom of the pane to toggle between the views.

To close tabs in the snapshot view, right-click the tab at the bottom and select Close.

To rearrange open tabs in snapshot view:

- 1 Use the down arrow () to tile the open tabs horizontally, vertically, or to fit.








- 2 To select different views on an event graph, use the  button. For details about viewing event graphs, see the online Help.

Investigating Patterns in the Patterns View

You can re-open just the patterns view part of the snapshot in the Viewer panel.

- 1 In the Navigator panel, go to Pattern Discovery and click the Patterns tab.
- 2 Select one or more patterns in the resource tree, right-click the selection(s) and choose View Pattern. This opens the Pattern pane in the Viewer panel.
- 3 You can take the same actions on the Pattern view as described in [“Investigating Patterns in the Patterns View” on page 196](#).

In the Patterns view, you can click the Actions button or right-click a pattern, where you have the following options:

Button	Right-Click Option	Description
	Inspect Pattern	Opens the Pattern Inspector in the Inspect/Edit panel. For more about how to inspect patterns, see “Investigating Patterns” on page 193 .
	Create rule from Pattern	Launches a Rules Editor in the Inspect/Edit panel. The rule you create here is stored in the Rules resource tree under the personal rules of the creating user. For instructions about how to construct a rule, see “Creating Rules from Patterns” on page 198
	Annotate Pattern	Click this to open the Annotations dialog box. This allows you to escalate a pattern to another user for further investigation. For more information about how to annotate a pattern, see “Annotating Patterns” on page 200 .
	Event Graph	Displays the events as an event graph, which shows interactions between two or more devices. For more information about how to use ESM event graphs, see the online Help.
	Related Events	Click this to open a grid view of the events contained in the Pattern Discovery snapshot.
	Create Channel	Creates a channel based on the selected pattern block.
	Add Condition to Editor	Enables you to edit the condition statement(s) associated with this pattern block.

Viewing Patterns with Filter

You can view patterns assigned to a particular user or stage using Annotations.

- 1 In the Navigator panel in Pattern Discovery, click the **Patterns** tab.
- 2 Navigate to the pattern.
- 3 Right click that pattern and select **View Patterns with Filter**.
- 4 To filter for patterns assigned to a user, use the Select a User drop-down menu.

- 5 To filter for patterns assigned to a workflow stage, use the Select a Stage drop-down menu.
- 6 You can use one or both parameters for your search.

Inspecting Patterns

The Pattern Inspector provides you one more level of investigative control. If you decide that a pattern requires more investigation, you can use the Pattern Inspector to edit its details to be more descriptive for other users.

For example, you can rename the pattern from the default date and time of the snapshot to something more specific, such as "Potential worm attack." Then you can add a description of the pattern so that another user can verify your findings.

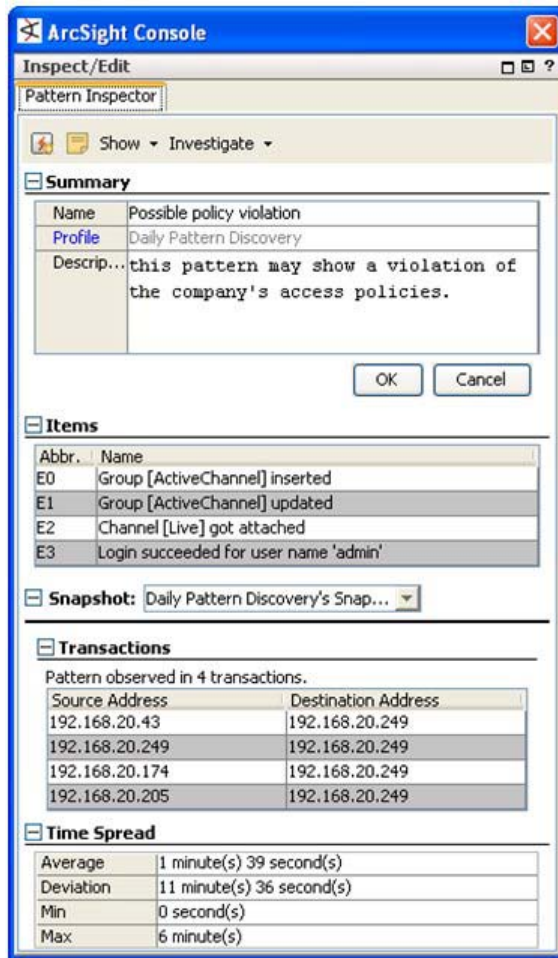
To launch the Pattern Inspector:

- 1 In the Navigator panel, go to Pattern Discovery and click the Patterns tab.
- 2 Right-click a pattern in the resource tree and choose Inspect Pattern....

Details of the pattern are displayed in the Inspect/Edit panel. Use the following sections as described below to tailor the pattern for further investigation:

Section	Description
Summary	Use this section to modify the name of the pattern from the default date-and-time name to a more descriptive name. You can also add a description of the pattern to aid other analysts. The Profile field is not editable.
Items	Use the Investigate drop-down button or right-click an item name to display the associated event details in a channel in the Viewer panel.
Snapshot	Use this drop-down menu to open patterns generated from the same profile definition so you can compare them.
Transactions	This table shows the source and destination data defined in the profile (address, port, host name, and so on) for the events involved in the pattern.
Time Spread	<p>This table is only present if you selected Record Time Order in the profile. This table shows the details about the time spans involved between pattern occurrences.</p> <ul style="list-style-type: none"> • Average - the average time between events in this pattern • Deviation - the difference in time spread between multiple occurrences of this pattern • Min - the minimum time between events in this pattern • Max - the maximum time between events in this pattern

The Pattern Inspector (below) shows item details and source/target transactions. You can rename a pattern to something more specific than the default date and time, and you can include a description.



Creating Rules from Patterns

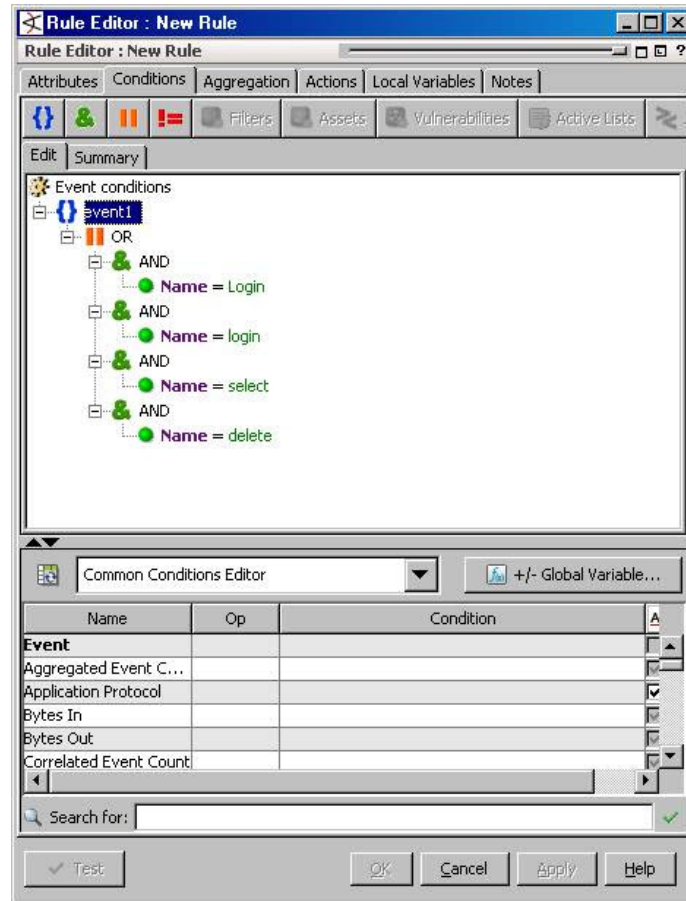
You can create rules based on discovered patterns. Going back to our example, if Pattern Discovery finds a pattern between an MS-SQL worm propagation attempt reported by Snort, an MS SQL version overflow attempt, and an attack from a suspicious source, this indicates dangerous worm activity, and can create a rule to notify users or quarantine a server whenever the system detects traffic that matches this pattern. For additional information on creating and managing rules, see [“Creating Rule Actions” on page 451](#).

You can create rules from patterns in the Snapshot view in the Viewer panel, or in the Pattern Inspector in the Inspect/Edit panel.

- To access the Rules Editor from the Snapshot view:
Right click on any item in the hierarchy graphic and select Create Rule...
- To access the Rules Editor from the Snapshot Patterns view:
Right click on any item in the pattern block and select Create Rule.... You can also click the create rule button (🔥) in the button menu.
- To access the Rules Editor from the Pattern Inspector:
In the button menu, click the create rule button.

The Rules Editor opens in the Inspect/Edit panel showing the Attributes tab. Once the Rules Editor is open, do the following:

- 1 Enter a name for the rule. You can also assign an external ID, alias, description, Version ID, owner, notification groups for the filter, and mark a resource as deprecated. Click **Apply**.
- 2 In the Rules Editor on the **Conditions** tab, the pattern's elements already appear in the common conditions editor. Modify the logic to express additional conditions for the rule to evaluate. For information, see [“Specifying Rule Conditions”](#) on page 442.



Note

The OR conditions are intentional. OR is a more memory-efficient way to process rules than AND because it also applies a threshold value (the number of items involved) and distinct item names to track the components of the rule, rather than a blanket (join) approach.

- 3 At the **Aggregation** tab, set the number of matches and time frame for the rule.
- 4 At the **Actions** tab, set the actions for the rule to trigger when the thresholds are met.
 - a Click **Hide Empty Triggers** in the top row. This reduces the list of available thresholds to those that are active (applicable to the conditions set in the rule).
 - b Select a threshold from the list and click **Add**. Choose an action from the list that appears. See [“Rule Actions Reference”](#) on page 455.
- 5 At the **Variables** tab, enter variables. Variables break down compound data fields into smaller parts so they can be sorted and acted upon. For example, you can break the 7-

part timestamp field or a multi-value URI into component parts, which can be re-assembled in a more human-readable order, or sorted by component. For more about dependent variables, see the online Help and search for Dependent Variables.


- 6 You can keep track of changes made to a profile using the Notes feature:
 - a In the Inspect/Edit panel, click the Notes tab.
 - b In the Notes field, enter a note and click Save. The entry is logged in the Table/List tabs.
 - c You can view notes as a table or as a list by toggling between the Table and List tabs. You can re-order the table view by clicking the column header.

Annotating Patterns

Annotation is a light-weight way to escalate a pattern to other users through your workflow system for analysis or investigation. You can use annotations instead of cases to escalate only one pattern. Use cases to escalate multiple patterns or if you use a third-party incident management system.

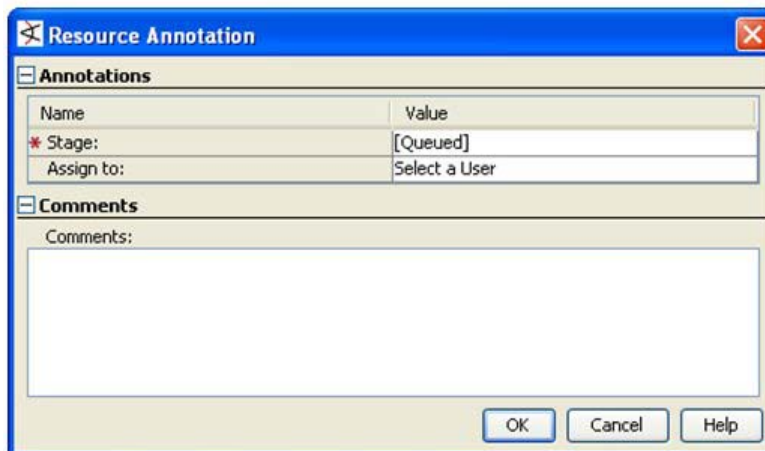
You can annotate patterns from the snapshot and Pattern views in the Viewer panel, or within the Pattern Inspector in the Inspect/Edit panel.

To access the Annotation Editor from the Snapshot Patterns view:

- 1 In the Navigator panel, go to Pattern Discovery and click the **Snapshots** tab.
- 2 Double-click the snapshot to display it in the Viewer panel.
- 3 Expand the pane so you can see the Patterns view at the bottom.
- 4 Right click any item in the pattern block and select **Annotate Pattern....** You can also click the Annotate Pattern button () in the button menu.

To access the Annotation Editor from the Pattern Inspector:

- 1 In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.
- 2 Navigate to the pattern and double-click it.
- 3 In the Inspect/Edit pane on the Pattern Inspector tab button menu, click the Annotate Pattern button.



The Resource Annotation dialog box is titled "Resource Annotation" and contains two main sections: "Annotations" and "Comments".

Annotations: This section contains a table with two columns: "Name" and "Value".

Name	Value
* Stage:	[Queued]
Assign to:	Select a User

Comments: This section contains a large text area for entering comments.

At the bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

Once the Annotation Editor is open, enter the following values and click **OK**.

Field	Value
Stage	Select a stage from the drop-down menu. The default is Queued.
Assign to	Select a user from the drop-down menu.
Comments	Enter any comments to communicate to other ESM users.

Deleting a Pattern

- 1 In the Navigator panel, go to Pattern Discovery and click the **Patterns** tab.
- 2 Select one or more patterns.
- 3 Right-click the selected pattern (s) in the resource tree and choose **Delete Pattern**.
- 4 Click **Yes** to confirm the deletion.

Usage Guidelines

Establishing a Baseline of Normal Patterns

Use broader profiles and more frequent snapshots in order to capture an example of all the patterns that occur as part of normal business practices. Identifying normal patterns takes time and investigation, and requires that you be familiar with traffic in your enterprise.

Once you have identified normal patterns, use annotation for moving them out of the analysis workflow. You can also use filters, but it is more reliable to move patterns by annotating them to a stage, such as Closed, because it assures that the pattern has been inspected and classified. For instructions about how to use event annotation to manage Pattern Discovery workflow, see [“Annotating Patterns” on page 200](#).

Using Pattern Discovery in Routine Operations

Once normal patterns are identified and annotated so they are removed from the routine traffic flow, you can focus on the new patterns that are not yet classified. Routine operations consist of the following tasks:

- **Workflow.** As Pattern Discovery turns up new or unclassified patterns, a designated user needs to review them and start them through the workflow using the ESM annotations feature. You can also schedule Pattern Discovery to run at intervals.
- **Investigation and analysis.** Once assigned to an analyst, the analyst can use the full array of ESM's investigation and analysis tools, including snapshot and pattern graphics, event graphs, filters, and rules, to determine the level of threat represented by the pattern.

During this investigation, it may be useful to drill down to the native device information to help identify the significance of a pattern. For example, if an event in a pattern was generated by Snort, you can retrieve the Snort rule number and look for its detailed explanation to obtain important event details.

- **Take action.** When a threat level is determined, the analyst can take a number of actions, such as use the ESM rule builder to take a prescribed action on this pattern and others that match it that may occur in the future; assign it to another user for follow-up; or close the pattern if it is deemed benign.

Adjusting Pattern Discovery Memory

By default, Pattern Discovery limits its memory usage to about 4 GB of memory. However, if the search for patterns involves too many transactions and events, the task can run out of memory and abort. If the pattern discovery task aborts, a message to that effect appears in the ESM Console. Run the pattern discovery task again after increasing the pattern discovery memory usage limit. You can control the memory usage limit indirectly by changing the maximum number of transactions and events that can be held in memory.

For information, see [“Adjusting Pattern Discovery Memory” on page 23](#).

Chapter 9

Field Sets

The field sets panel provides access to resources that are used to group and extend the fields of the event and resource schema. The Field Sets tree presents tools for the following tasks:

	Who	License Required?	Permissions Required?	Configuration Required?	What	Why	When	Where	How
Creating Field Sets	SOC operators, authors, and analysts concerned with traditional security-related use cases.	N	N	N	A named subset of available data fields in the standard schema and the user-defined dynamic schema.	To narrow the fields available in the standard 400+ field event schema and the user-defined dynamic schema to make it easier to select and view fields.	Anytime	Active channels, CCE	See "Field Sets" on page 204 .
Creating Domain Field Sets	Admins, analysts, and authors with domain authoring privileges concerned with use cases involving different user-defined business verticals.	Y	Y	Y	A named subset of available data fields in the user-defined dynamic schema used to identify incoming events as a particular type.	To define the list of fields that identifies events that belong to a specific type of business activity.	When setting up system to monitor specific business scenarios.	Active channels, CCE	See "Domain Field Sets" on page 491 .

	Who	License Required? Permissions Required? Configuration Required?			What	Why	When	Where	How
Creating Global Variables	SOC operators, authors, and analysts concerned with any type of use case.	N	N	N	A method for deriving a unique value from existing values in a data field, and the derived value itself, stored in a global variable field.	To make correlation, monitoring, and investigation more precise.	Anytime	Active channels, CCE, regular field sets, other global variables	See “Global Variables” on page 477 .

Field Sets

[“Navigating to Field Sets” on page 204](#)
[“Creating and Using Field Sets” on page 204](#)
[“Where Field Sets can be Selected” on page 212](#)
[“About Global Variables” on page 212](#)
[“About Domains” on page 212](#)

Navigating to Field Sets

In the Navigator panel, select **Field Sets** from the drop-down menu.

Creating and Using Field Sets

Field sets are named subsets of available *data fields*. Field sets can help you quickly focus a grid view, Event Inspector, or other field array on a particular context, such as customer accounts or vulnerability.

Field sets are a shareable resource that you can manage and apply through the Field Sets resource tree in the Field Sets section of the Navigator panel. (In the Navigator, choose **Field Sets**, and click the **Field Sets** tab.) Field sets also support local and global variable data fields.

In addition to field sets based on the Security Event schema, you can create field sets based on certain resources. ArcSight supports the following types of field sets:



- **Actor field set.** An actor field set contains fields that make up the Actors resource. Actor fields are attributes to identify users and track their activity. ArcSight provides a base set of Actors fields from which you can make user-defined subsets.

- **Asset field set.** An asset field set contains fields that make up the Assets resource. Asset fields are attributes used to identify monitored assets. ArcSight provides a base set of Asset fields from which you can make user-defined subsets.
- **Case field set.** A case field set contains fields that make up the Cases resource. Case fields are attributes used to track events that have been added to cases. ArcSight provides a base set of Case fields from which you can make user-defined subsets.
- **Domain field set.** A domain field set is a field set that contains custom domain fields that define a specific range of application. When selecting a domain field, you first select the Domain field set, so domain fields must be part of a field set to be used. For more about domain fields, see [“Domain Field Sets” on page 491](#).
- **Event field set.** An event field set is a named subset of available data fields from the ESM security event schema.

A base or root field set is provided for each schema type (Event, Actor, Asset, and so on) from which you can create user-defined subsets. A derived field set may inherit all or a subset of its parent's base fields, and additionally may include local or global variables not present in the parent. All field sets will have a parent (field sets created in previous versions of ESM will by default use the Event base field set as its parent).

Creating a Field Set

To create a field set:

- 1 Choose **File>New** on the Console's menu, or the **New Resource** button () and the **Field Set** () command. You can also right-click a folder in the **Field Sets** resource tree and choose **New Field Set**.



Creating a domain field set?

For instructions about how to create domain field sets, see [“Creating Domain Field Sets” on page 498](#).

Domain fields can only be added to the [All Fields/ArcSight System/Domain Field Sets](#) group by the Admin user, or a user with Domain Authoring and Read/Write permissions for domain fields and domain field sets.

- 2 In the Field Set Editor in the Inspect/Edit panel, enter attributes for the field set and assign it one or more existing fields.
- 3 Click **Apply** to save the field set in the resource tree and continue editing. Click **OK** to save the set in the resource tree and close the editor.

For details about what to enter in each field of the Field Set Editor, see [“Field Set Editor: Attributes Tab” on page 205](#).

Field Set Editor: Attributes Tab

The attributes tab is where you name the field set and specify what type of field set it is.

Field	Description
Name	Enter a name for the field set that identifies what it represents.

Field	Description
Type	<p>From the drop-down menu, select what type of field set it is:</p> <ul style="list-style-type: none">• Actor Field Set. Select this if the field set will contain only actor fields for use cases relating to tracking actors.• Asset Field Set. Select this if the field set will contain only asset fields for use cases relating to tracking assets.• Case Field Set. Select this if the field set will contain only case fields for use cases relating to tracking cases.• Event Field Set. Select this if the field set will contain fields from the ESM security event schema for event-based use cases.

For a description of what to enter in the Common fields, see [“Common Resource Attribute Fields” on page 684](#).

Field Set Editor: Fields Tab

The Fields tab is where you add the data fields to the field set.



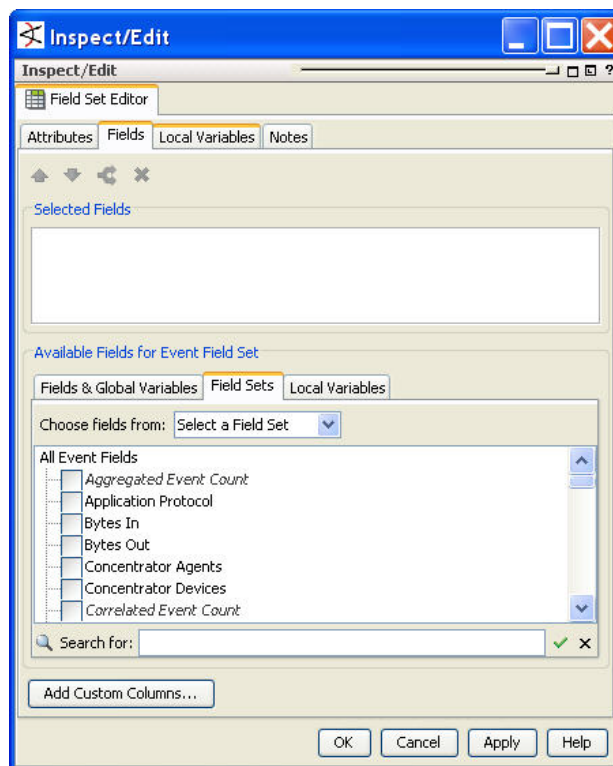
Creating a domain field set?

If you are creating a domain field set, see [“Creating Domain Field Sets” on page 498](#).

The Field Set editor provides several ways to add different types of fields:

- **Fields & Global Variables tab.** Use this tab to add existing user-defined domain fields and global variables.
- **Field Sets tab.** Use this tab to add standard event and resource schema fields. This field selector is similar to those available in the CCE and active channel editors.

- **Local Variables tab.** Use this tab to add one or more local variables defined on this field set's top level Local Variables tab.



Once fields are added to the field set, you can re-order and delete them, and create aliases for event-based fields. For instructions, see [“Editing a Field Set” on page 211](#).



Note

Fields shown in italics

Fields shown in italics are *derived* from data in other fields. Derived fields appear in various places on the Console UI including on the Field Set editor, and the Common Conditions Editor (CCE) aggregation tabs (for example, Rules, Filters, and so forth). See also [“Using Field Sets” on page 855](#) in the [“Common Conditions Editor \(CCE\)” on page 846](#) reference topic.



Tip

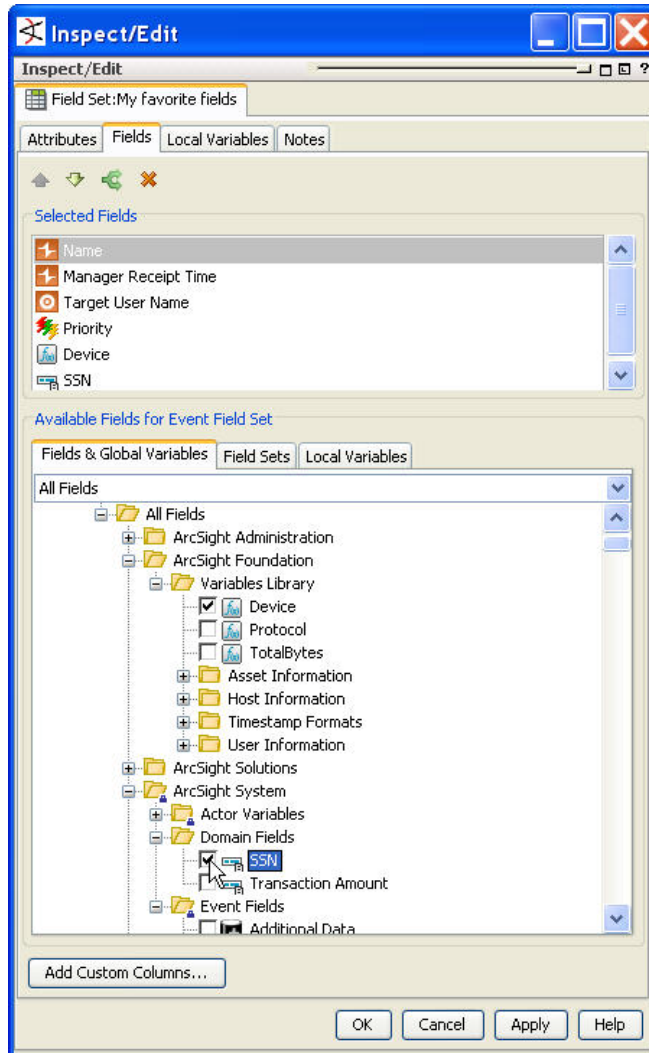
Looking for information about custom columns?

If you want to add a custom column, you need to create or define it first. For information about creating custom columns, see [“Customizing Grid Columns” on page 152](#). For information about working with grid views, see [“Using Grids” on page 145](#).

Once a custom column is created, you can add it to your field set using the **Add Custom Columns** button at the bottom of the Fields tab editor. For details, see [“Adding Custom Columns” on page 210](#).

Adding Fields from the Fields & Global Variables Tab

The Fields & Global Variables tab enables you to select fields from a resource tree like the one presented in the Fields & Global Variables Navigator panel. Use this tab to add user-defined domain fields (if applicable) and global variables to your regular field set.



Note

Fields & Global Variables tab also presents regular event fields

The Fields & Global Variables selector also provides a tree-level view of the standard event and resource schema fields. You can use this view to add event fields, or add them from the Field Sets tab described in [“Adding Fields from the Field Sets Tab” on page 209](#).

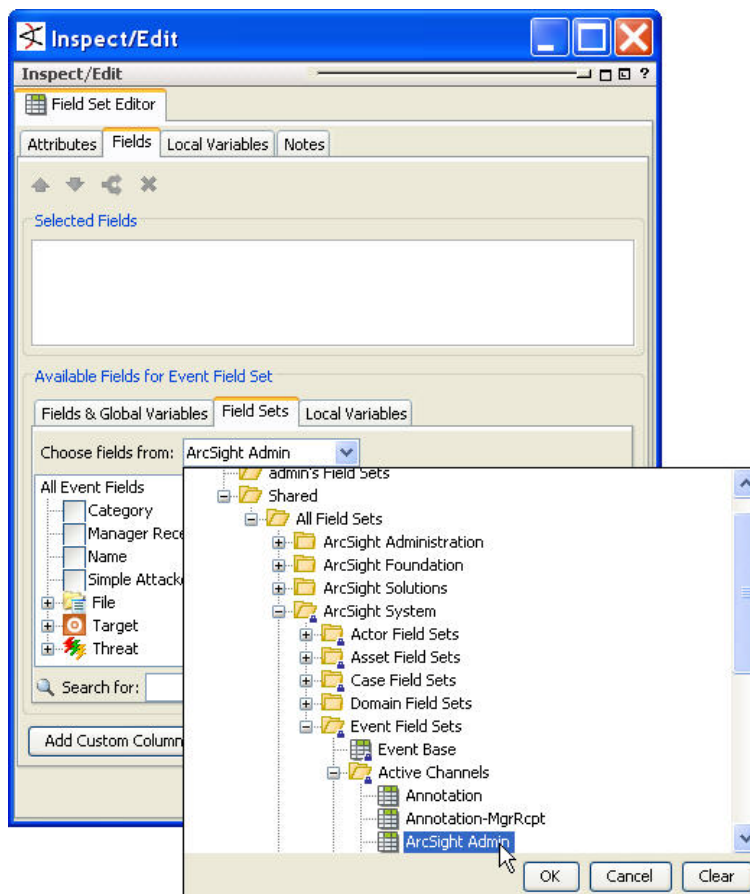
In the *Fields and Global Variables* tab, select any existing domain fields or global variables you want to add to the field set. The selected field will appear in the *Selected Fields* panel.

For more about domain fields, see [“Domain Field Sets” on page 491](#).

For more about global variables, see [“Global Variables” on page 477](#).

Adding Fields from the Field Sets Tab

The Field Sets tab enables you to select regular event fields and domain fields that are part of a domain field set using a functionally organized field selector similar to that in the CCE and active channel editor. You can also use field sets in the Field Sets tab to narrow the list of fields down to those you are interested in.



You can navigate the entire event and resource schema for the fields you are interested in, or select a field set from which you want to select fields in the *Choose fields from* drop-down menu.

Adding Local Variables from the Local Variables Tab




In the *Available Fields for <type of> Field Set* section at the *Local Variables* tab, select a local variable that you define in [“Field Set Editor: Local Variables Tab” on page 210](#).



Create a local variable in the Local Variable tab first

If you want to add a local variable to this field set, but the local variables tab in the Field tab contains no items to select, first define the local variable in [“Field Set Editor: Local Variables Tab” on page 210](#).

In the *Available Fields for <Type of> Field Set* panel in the *Local Variables* tab, select the checkbox for the local variable you want to add to the field set.

- To re-order the local variables in the list, select a field and use the up /down  arrows to place it in the desired order. The variables will be evaluated in the order shown here.
- To remove the local variable from the list, select the field and click the delete button .
- For instructions about how to construct a local variable using the Field Set editor's Local Variables editor, see [“Field Set Editor: Local Variables Tab” on page 210](#).

Adding Custom Columns

The bottom of the Fields tab provides a button that enables you to add an existing custom column to the field set. To add a custom column:


- 1 Click **Add Custom Columns**.
- 2 In the Add Custom Columns dialog, select an existing custom column and click **OK**.



For more about custom columns and how to create them, see [“Customizing Grid Columns” on page 152](#).


Field Set Editor: Local Variables Tab

Use this top-level local variables tab to define one or more local variables that you can then add to this field set in the Local Variables tab of the Fields tab. You can create multiple chained variables and add one or more of them to the field set itself.

- 1 In the *Local Variables* tab, click add  to launch the *Add Local Variable* editor.
- 2 In the *Name* field, give the local variable a name. In the *Function* drop-down, select a function category, then select a function and click **OK**.
- 3 In the *Arguments* section, enter appropriate arguments for the function you selected in the previous step.
- 4 In the *Preview* section, select or enter parameters and click **Calculate** to test the results of the function.
- 5 When you are finished editing the field set, click **OK** to close the editor.

For complete instructions about constructing a variable, see [“Variables” on page 1006](#).

Editing a Field Set

- 1 In the Field Sets tab of the Active Channels resource tree, right-click a field set and select **Edit Field Set**.
 - 2 In the Field Set Editor, use the **Attributes** tab to change the field set's name.
 - 3 Click the **Fields** tab and use its Available Fields list to select fields to add to the list.
 - ◆ **To Reorder Fields:** To re-order the fields in the list, select a field and use the up/down arrows to place it in the desired order. Fields and variables will be displayed and evaluated in the order specified in this list.
 - ◆ **To Create an Alias for Event-Based Fields:** To create an alias for a field, select the field, then click the alias button (🔗). In the Create Alias dialog box, enter an alternate name for the field. This alias will be used to identify this field in this field set anywhere this field set is used to select or display fields, such as an active channel column heading or a CCE field selector.
-
- 

You can create an alias for event-based fields only

You cannot create an alias for resource-based fields, such as assets or cases. You also cannot create an alias for a field set or a global variable.
-
- ◆ **To Delete a Field from the Field Set:** To remove the field from the list, select the field and click the delete button (✕).
 - 4 Use the **Local Variables** tab to define variables you can add to the field set using the Local Variables tab in the Fields tab. See [“Adding Local Variables from the Local Variables Tab” on page 209](#)
 - 5 Rearrange or remove fields in the Fields to Show list.
 - 6 Click **Apply** to save the set in the resource tree and continue editing. Click **OK** to save the set in the resource tree and close the editor.

Sharing a Field Set

When you create a field set in the Shared folder in the Field Sets resource tree, it is available to other users who have permission for those folders. If you create one in your own folder, it is not available to other users unless you move, copy, or link it into a Shared folder.

- 1 Click the field set in your folder and drag it to the appropriate Shared folder.
- 2 In the Drag and Drop dialog box, choose to **Move**, **Copy**, or **Link** the resource in its new location.
 - ◆ **Moving** relocates the resource, leaving a single instance of it in the tree.
 - ◆ **Copying** makes a duplicate, leaving two independent instances of the resource.
 - ◆ **Linking** leaves the original in place, and creates a connected copy in the new location that will change whenever the master instance changes.

You create sortable field sets in the same way, but without the option to add variables to the sets.

You control access to field set folders like any other resource.

See also [“Applying a Field Set to an Active Channel” on page 132](#) and Sorting Events in a Channel.

Deleting a Field Set

- 1 In the Navigator panel at the Field Sets tab, right-click the field set you want to delete and select **Delete Field Set**.
- 2 In the confirmation dialog box, click **Delete** to delete the field set.

Where Field Sets can be Selected

Field sets can be applied in the following resources:

- **To sort active channels.** For more about how to use field sets in active channels, see [“Applying a Field Set to an Active Channel” on page 132](#).
- **To narrow the list of fields available for selecting in the CCE.** For more about how to use field sets when authoring resources in the CCE, see [“Common Conditions Editor \(CCE\)” on page 846](#).

About Global Variables

Global variables are created from the Fields & Global Variables tab in the Field Sets Navigator panel.

For more information about global variables, see [“Global Variables” on page 477](#).

About Domains

Domain fields and domain field sets are created from the Fields & Global Variables and Field Sets tabs in the Field Sets Navigator panel.

For more information about domains, see [“Domain Field Sets” on page 491](#).

Selecting and Investigating Events

This chapter describes how you use ArcSight to monitor enterprise security.

[“Handling Events in Grid Views” on page 213](#)
[“Showing Event Details and Rule Chains” on page 214](#)
[“Investigating Session Events” on page 215](#)
[“Collaborating on Events” on page 216](#)
[“Showing Event Payloads” on page 219](#)
[“Getting Knowledge Base Articles” on page 221](#)

Handling Events in Grid Views

In active channel or active list grid views you can select events to investigate. After selecting one or more events in a grid, you can handle them in several basic ways. This handling is in support of other analysis and authoring tasks.

Selecting Events to Investigate in a Grid View

Within a Viewer panel grid view, click an event or **Ctrl+click** a set of events. To select a range of events, click one event and **Shift+click** the event at the end of the range.

Inverting Event Selections in a Grid View

Select one or more events in a grid view, right-click and choose **Invert selection**.

Selecting Events with Matching Cells in a Grid View

Select a cell in a grid view, right-click and choose **Select events with matching cell** to see if other events in the grid view have matching cell values.

Exporting Data Fields to a CSV File

You can export a set of channel events into a comma separated values (CSV) file. The procedure for doing this is described here and also in [“Exporting Events to a File” on page 147](#).

- 1 In a grid view, select one or more events.
- 2 Right-click and choose **Export > Events in Channel**.

- 3 On the Export Events file browser, navigate to the location where you want to save the CSV file, then enter or select options for these fields:

File Name	Type a file name for the CSV file. (Note: No need to include the file name extension; the <code>csv</code> extension is added automatically when the file is created.)
Files of Type	Select Comma separated values (*.csv).
Export Data Options	<p>For "Rows", you have two options:</p> <ul style="list-style-type: none"> If you choose "All in channel", all events in the channel will be exported to the CSV file. If you choose "Selected rows only", only those rows highlighted for the right-click operation will be exported to the CSV file. <p>The default for "Columns" is the Export field set. You can keep the default, or select other field sets from a list of All Field Sets.</p> <p>The exported CSV file will include the fields in the selected field set. If you want to limit the exported columns (field sets) to only those showing in the current channel, see "How to Limit Export to Fields Visible in Channel" on page 148.</p> <p>(For more information on creating, editing, and applying field sets, see "Creating and Using Field Sets" on page 204.)</p> <p>For "Destination", choose "Local CSV File"</p>

- 4 Click **OK** to save the file.

Showing Event Details and Rule Chains

Displaying Event Details

In a grid view, select an event. Right-click and choose **Show event details**. The event's details appear in the Event Inspector.



Note

If you encounter an "unable to retrieve event" message while viewing events in the Events tab of the Case Editor, be advised that those events are unavailable because they are archived in an offline partition.



Note


Load Time Expected When Applying an Actor Field Set in the Event Inspector

When you apply an actor field set to an event being displayed in the event inspector, you may experience an extended load time.

Displaying Simple Event Rule Chains

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Simple chain**.

Displaying Detailed Event Rule Chains

Rule-based Correlation events are those generated by a triggered ArcSight rule as a reaction to an original sensor-generated event. In other words, an event concerning an event. You recognize correlation events in grid views by their red **Flash** icon . To mask grid views so they show **only** correlation events, select the checkbox at the top of the grid's left-most column.

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Detailed chain**.

The events leading up to the correlation event appear in the Description panel at the top of the Inspector. Click any event in the chain to see its details below.

Displaying Correlation-Event Rules

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Show triggering resource**.

The rule or resource that triggered the correlation event is selected in the Navigator panel's Rules resource tree and that rule appears in the Rules Editor.

Executing or Clearing Rule Actions in a Grid View

In a grid view, select a correlation event. Right-click and choose **Rule options**, then **Clear Rule Actions** to clear all actions associated with this rule. For more information, see ["Creating Rule Actions" on page 451](#).

Launching Event Details in a Browser

- 1 In a grid view, right-click an event and choose **Show event details**.
- 2 In the condition table of the Event Inspector, right-click and choose **Launch Event Details in Browser**.

A Web browser opens with the selected event's details.

Hiding Empty Rows in the Event Inspector

- 1 In a grid view, right-click an event and choose **Show event details**.
- 2 In the condition table of the Event Inspector, right-click and choose **Hide Empty Rows**.

Investigating Session Events

This topic explains how to use the ESM Console's **Investigate > Session Events** command to easily refine and explore channels contextually, using attributes of the events already being displayed in grid views.

Session List entries can be investigated two ways: you can filter the set of entries based on the attributes of a particular entry, or you can create an Investigation Channel that contains only the entries that match one or more attributes of the initial Session List entry.

Investigating a Session Event

- 1 Right-click a Session List in the Navigator and choose **Show Entries**.

- 2 In the Viewer panel, select an entry that bears investigation by clicking it.
- 3 Right-click the selected entry. The menu includes commands to **Create Channel** and **Add Condition to Channel Editor**. The details of each command will vary based on which column you right-click.

For example, if you right-click a Source IP column containing the value `192.168.10.0`, the choices will be:

- ◆ Create Channel (Source IP = 192.168.10.0)
- ◆ Create Channel (Source IP != 192.168.10.0)
- ◆ Create Channel >
- ◆ Add Condition to Channel Editor (Source IP = 192.168.10.0)
- ◆ Add Condition to Channel Editor (Source IP != 192.168.10.0)
- ◆ Add Condition to Channel Editor >

The sub-menus (indicated by the >) will offer similar choices for all the other columns of the Session List entry.

If you Create Channel, a new grid is added to the Viewer panel. If you Add Condition to Channel Editor, a channel editor will open in the Inspect/Edit panel.

For more information about creating and using views for investigation, see [“Investigating Views” on page 140](#).

Collaborating on Events

You can use workflow-style annotation to collaborate with other users in analyzing or reviewing selected events. (See also [“Case Management and Queries” on page 585](#).)

When you are annotating, you can make collaboration-stage changes to just the event you originally selected, or have that change also affect a larger set of similar events that should also be carried forward in the review process.

The central tasks in annotating events for collaborative analysis are assigning them to yourself or another user, then assigning them to one of the available sequential workflow stages (dispositions). While ArcSight comes with a default set of stages, your enterprise will very likely have edited these stages and created new ones.

Compare collaborative annotation to cases, which are a more formal way to track sets of events that are under investigation.

Viewing Annotations for an Event

Annotations on an event are displayed in the **Annotations** tab of the Event Inspector when that event is selected.

To view the annotations for an event:

- 1 Right-click an event in a grid view (such as an active channel or active list) and choose Show Event Details to bring up the Event Inspector.
- 2 In the Event Inspector, click the **Annotations** tab.

Annotating an Event

- 1 Select one or more events in any grid view. If not already annotated, you can start a collaboration cycle.
- 2 Right-click the events and choose **Annotate Events** (or **Ctrl+T** keyboard command).
- 3 In the Annotate Events dialog box, set or change the events' Annotations fields, as described below.
- 4 To have this change also affect related events, use the **Mark Similar Events** fields, as described below.
- 5 Click **OK** to update the event.

Event Annotation Fields

Event Annotation Field	Usage
Stage	Click this field to choose a different disposition state for the events' collaboration cycle. The default stages run from Initial to Closed ; other stages may be available.
Assign to	Click this field to choose an ArcSight user to take the next step.
Is Reviewed	This read-only field tells you whether this event has been reviewed.
In Case	This read-only field tells you whether these events are already part of an ArcSight case. If they are, you have more ways to track their disposition.
Correlated	This read-only field tells you whether these events are part of a correlated event chain. If so, you can learn more through the rules authored to control that chain of correlation.
Hidden	This read-only field tells you whether these events are hidden from all but the assigned user(s) of this stage.
Closed	This read-only field tells you whether the investigation of these events has been marked as closed. Closed events may no longer be visible to interested parties through active channels, etc.

Comments Field

The **Comments** field is for text comments you can add as needed to clarify the collaborative process.

Mark Similar Events Fields

Event "similarity," for collaboration purposes, is defined as a combination of time constraints and having certain key event attributes in common. For example, you could apply a collaboration change to additional events received in the future on the basis of those events having the same Attacker value and having occurred within the last two days.

Similarity Field	Usage
Time Constraints	Choose a bracketing combination of Start Time and End Time or Duration.

Similarity Field	Usage
Start Time	Date and time values to set the beginning of a time-constraint window. Choose from the drop-down menu of expressions or click the ellipsis button to set exact times.
End Time	Date and time values to set the end of a time-constraint window. Choose from the drop-down menu of expressions or click the ellipsis button to set exact times.
Duration	The length of the time window, relative to a Start Time or End Time, when using Duration as a time constraint.
Criteria	A menu of key event-attribute characteristics you can use to define similarity. The text box below specifies the criteria being set.

Creating New Stages

- 1 Choose the **Stages** resource tree in the Navigator panel.
- 2 Right-click the **All Stages** group and choose **New Stage**.
- 3 In the Stage Editor, enter a name for the stage.
- 4 Make other appropriate choices, as described in the following table showing [Stage Editor Fields](#).
- 5 Click **Apply** to save your changes and keep the editor open, or click **OK** to save and close.




Please keep stages provided as standard content in the given folders and do not move them into another folder. (See [“What is Standard Content?”](#) on [page 47](#).) Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.

Stage Editor Fields

Stage Editor Field	Usage
Subsequent stages	Select one or more stages to set as follow-on stages to this one. Events in this stage will show these other stages as options in the Stage field of the Annotate Fields dialog box.
User required	Select whether you want to prompt for a user assignment when assigning this stage. If you don't prompt for a different user, or no change is made, the current user remains in effect.
Comment required	Select whether you want to require users to add a comment when assigning this stage.
Can be skipped	Select whether this stage can be bypassed when assigning from one stage to the next.

Stage Editor Field	Usage
Mark similar required	Choose whether you want events that are similar to the selected events to be automatically assigned to this stage. Similarity is scoped at assignment time through the Mark Similar Events fields of the Annotate Events dialog box you see when you choose Annotate in a grid view. Note that similarity marking applies only to subsequent events received in the future. Events already processed are not affected.
Mark similar stage	Select whether you want to use this stage as a routing mechanism for other stages in a workflow. When selected, assigning one or more events to this stage causes all following (subsequent) similar events to be automatically redirected to the chosen stage. Events already processed are not affected. Similarity is scoped at assignment time through the Mark Similar Events fields of the Annotate Events dialog box you see when you choose Annotate in a grid view.
Hidden	Select whether you want events assigned to this stage to be hidden from all but the assigned users (True), left visible to everyone (False), or to leave the current visibility unchanged (Ignore).
Closed	Select whether you want events assigned to this stage to be marked as closed to investigation (True), not marked as closed (False), or left in their previous state (Ignore).



With the assistance of ArcSight Professional Services, you can customize the similarity criteria selector for Mark Similar events. In this way you can have conditions that are different from the defaults. This is done with the Velocity scripting language, by modifying certain Velocity templates present on the ESM Console, in the [config/similarity](#) directory. Ask your ArcSight administrator for more information or to make a request of ArcSight Professional Services.

Editing Stages

- 1 Choose the **Stages** resource tree in the Navigator panel.
- 2 Right-click a stage under the **All Stages** group and choose **Edit Stage**.
- 3 In the Stage Editor, make any necessary changes to the fields as previously described in [Stage Editor Fields](#).
- 4 Click **Apply** to save your changes and keep the editor open, or click **OK** to save and close.




Please keep stages provided as standard content in the given folders and do not move them into another folder. (See [“What is Standard Content?” on page 47](#).) Standard content stages are Closed, Final, Flagged as Similar, Follow-up, Initial, Monitoring, Queued, and Rule Created.

Showing Event Payloads

An event “payload” is the information carried in the body of the event's network packet, as distinct from the packet's header data. From the ESM Console, you can search, retrieve, view, save to a file, or discard event payloads.

Finding Payloads

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view.

- 1 In a grid view, right-click a column header and choose **Add Column>Device>Payload ID**.
- 2 Look for events showing a Payload ID  in that column.

Retrieving Payloads

- 1 In a Viewer panel grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Retrieve Payload**.

Preserving Payloads

You can select to preserve the payload for an event in either of two ways:

- In a grid view, right-click an event with an associated payload, choose **Payload**, then **Preserve**.
- Or
- In the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discarding Payloads

In a grid view, right-click an event with an associated payload and choose **Payload**, then **Discard Preserved**.

You can also use the Event Inspector.

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Discard Preserved Payload**.

Saving Payloads to Files

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Save Payload**.
- 4 In the Save dialog box, navigate to a directory and enter a name in the **File name** text field.
- 5 Click **Save**.

Viewing Payloads in Other Viewers

- 1 In a grid view, double-click an event with an associated payload.
- 2 In the Event Inspector, click the **Payload** tab.
- 3 Click **Launch External Payload Viewer**.

- 4 View the payload using the **Preferred Payload Viewer** and **Text to PCAP Converter**, specified in the ESM Console's **Edit>Preferences>Programs** panel.

Getting Knowledge Base Articles

Knowledge Base articles can be associated with events, rules, or any ArcSight resource. Knowledge Base articles can have links or notes to help you respond to events.

Displaying Articles from the Knowledge Base Window

In the Navigator panel drop-down menu, select **Knowledge Base**. Navigate to and right-click an article, and choose **Show Article**.

You can also choose **Knowledge Base** from the **Help** menu.

Displaying Articles from a Grid View

In a grid view, right-click an event and choose **Knowledge Base**, then **Show**. Choose **KB entry for cell**, **KB entry for row**, or **KB entry for column**, then the article name.

The Knowledge Base article opens in an [ArcSight Web](#) client. For more information about grid views, see ["Using Grids" on page 145](#).

Displaying Articles from the Event Inspector

In the Event Inspector, right-click an event and choose **Knowledge Base**, then **Show Article**.

The Knowledge Base article opens in an ArcSight Web client.

Chapter 11

Filtering Events

The Filters resource tree in the Navigator panel is pre-populated with some typical event filters you can use directly, or as templates for more specific purposes. You can create and edit your own filters and inline filters for use in active channels.

["Creating Filters" on page 223](#)
["Moving or Copying Filters" on page 226](#)
["Deleting Filters" on page 227](#)
["Debugging Filters to Match Events" on page 227](#)
["Applying Filters" on page 231](#)
["Importing and Exporting filters" on page 232](#)
["Using Filter Groups" on page 232](#)
["Investigating Views" on page 233](#)
["Modifying Views" on page 236](#)

Creating Filters

This topic discusses creating and editing filter resources through the Filter Editor. As a matter of efficient authoring and enterprise-wide analysis consistency you should always seek to use the established filter resources you find in the Navigator panel's Filters resource tree. These filters should have been designed and tested to appropriately accomplish your organization's analytical goals.

As of v4.0, Inline filters offers you a user-friendly visual representation of Boolean logic, typically found in the [Common Conditions Editor \(CCE\)](#). The inline filters feature allows you to preview matching events through highlighting, thereby verifying the accuracy of your filter prior to applying it, and the ability to create AND/OR conditions effortlessly.

Creating a New Filter

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a group and choose **New Filter**.
- 3 In the Filters Editor, type in the **Name** text field.
- 4 In the table, scroll to a relevant event field and choose a logical operator (**Op**), enter a conditional statement (**Condition**), select case-sensitivity (**Aa**), and select inequality or negate (**Not**), if appropriate.

- 5 Customize the filter, if appropriate, using the features described in [“Common Conditions Editor \(CCE\)” on page 846](#).
- 6 Repeat the above step for each condition you want to add to the filter.
- 7 Click **Apply** below the Inspect/Edit panel to update the filter or click **OK** to add the filter to the resource tree.

**Caution**

Filter definitions (meaning the total text used in a filter's condition statements) cannot exceed 10,000 characters. If your filter uses more than 10,000 characters, create a second filter by splitting the definition, and use the **matchesFilter** operator to combine the two.

**Tip**

Because you can reference filters in other filters you can create hierarchies similar to style sheets. It is wise to plan your filtering needs in advance so you can create filters, filter groups, and filter hierarchies that will promote the most efficient and consistent analysis results.

Changing or Editing a Filter

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a filter and choose **Edit Filter**.
- 3 In the Filters Editor, you can edit the filter name, if needed.
- 4 You can make changes to the filter conditions as described in [“Common Conditions Editor \(CCE\)” on page 846](#). You can edit logical operators and condition statements in the filter using the CCE as follows:
 - ◆ To edit a logical operator, right-click the logical operator and choose **Edit**, then choose a logical operator and click **OK**. (For more information, see [“Logical Operators” on page 947](#).)
 - ◆ To edit a condition statement, right-click the condition statement and choose an operator, condition editor, or selection operation. For more information, see [“Creating Filters” on page 223](#) and [“Common Conditions Editor \(CCE\)” on page 846](#) (CCE). (Search fields and undo/redo features are now available, as described in [“Editor Features” on page 846](#) in the CCE topic.)
 - ◆ To delete a logical operator, right-click the operator and choose **Delete**. In the confirmation dialog box, click **Yes**. The logical operator and all its condition statements are removed.
 - ◆ To delete a condition statement, right-click it and choose **Delete**. In the confirmation dialog box, click **Yes**.
 - ◆ To edit or delete a filter, right-click the filter and choose **Edit** or **Delete**.
- 5 Click **Apply** in the Inspect/Edit panel to put the modified filter into effect or **OK** to save the filter as a resource.

**Tip**

- Be cautious when making changes to filters used in hierarchies.
- Understanding how to use the Common Conditions Editor (CCE) is integral to creating and editing filters. Please refer to [“Common Conditions Editor \(CCE\)” on page 846](#), [“Conditional Statements” on page 859](#), and [“Conditions” on page 860](#) for more information.

Creating an Inline Filter



Steps to create an inline filter are summarized here. For more details and examples, see also [“Filtering Grid Views with Inline Filters” on page 150](#).

In any active channel grid view you can use the fields of the grid's top line to select filtering event-attribute values for certain columns, which will be used with implied AND operators to impose *ad hoc* filters and use the grid's bottom line to select filtering event-attributes values which will use OR operators.

These filters are **not** retained with the prior active channel, but you can give the revised channel a name and save it through the Active Channel Editor.



You cannot select a grayed-out column to include in your filter. Grayed-out columns have either variables or they are a custom column.

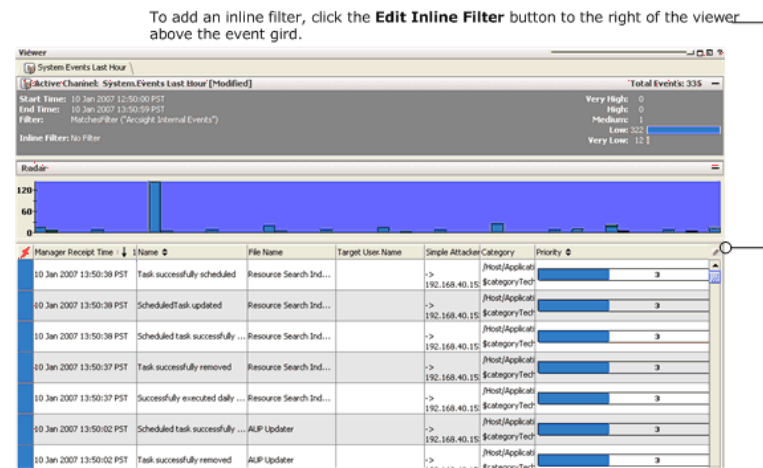
- 1 In the Navigator panel, choose **Active Channels**.
- 2 In the Active Channels resource tree, select a channel you want to add an inline filter.
- 3 In the Viewer panel, go to **Inline Filter** and click **No Filter**. This opens the inline filter pane.
- 4 Select the parameters for your inline filter: Manager Receipt, Name, Attacker, Target Address, Target Port, Priority, Device Vendor, and Device Product. Click **Apply**.
- 5 To highlight all matching events for your filter, select the **Highlight** checkbox. Highlighting allows you to preview the events that match your filter prior to saving the filter. Click **Apply** to activate the inline filter.

You can specify the highlight color by clicking the drop-down picker and select your color.

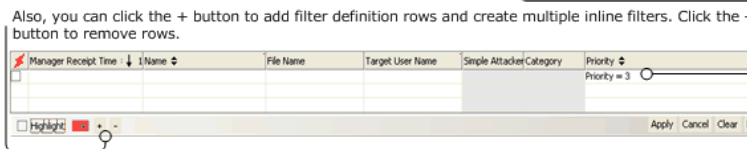
- 6 To add or delete rows to the inline filter table, click + (plus) or click - (minus).

To create and manage multiple inline filters, click the + button next to the Highlight options under the inline filters to add filter definition rows. (Click the - button to remove filter rows.) The potential uses of multiple inline filters are extensive, but essentially this provides a means of creating a filter with complex conditions, inline in an active channel. For example, in the Name column for an event, you could specify that the event name contains "ActiveList" on the first filter row and that the name does not contain "Successful". You could extend this filter by specifying what you are

looking for in some of the other fields or even add more qualifiers on the Name field. All fields can be narrowed down in this way, using multiple filter definition rows.

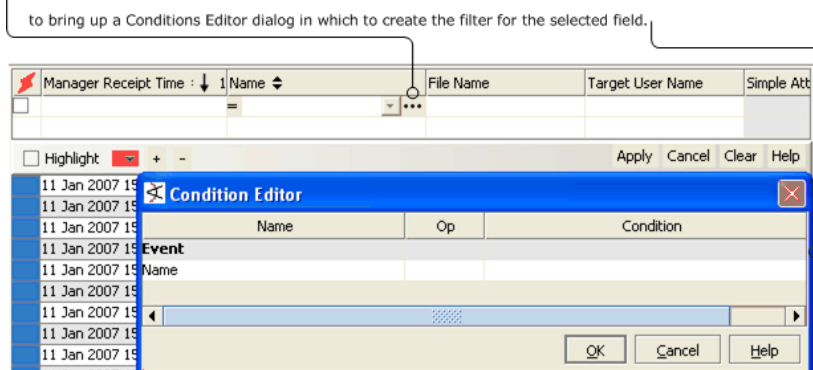


Clicking the **Edit Inline Filter** button opens an inline filtering window. Type a value in one or more fields to further filter the event stream. In this example, we add an inline filter on the Priority field to specify showing only events of Priority 3. Click **Apply** to apply the inline filter.



When you click into a field, you get an equals operator, a drop-down list of available values for that field based on the events currently displayed, and an ellipses (...) indicating another dialog is available.

If these inline options are not enough to create the filter, click the ellipses (...) to bring up a Conditions Editor dialog in which to create the filter for the selected field.



Moving or Copying Filters

- 1 In the Filters resource tree, navigate to a filter and drag and drop it into another group.
- 2 Choose **Move** to move the filter, **Copy** to make a separate copy of the filter, or **Link** to create a copy of the filter that is linked to the original filter.

If you choose **Copy**, you create a separate copy of the filter that will not be affected when the original filter is edited. If you choose **Link**, you create a copy of the filter that is linked to the original filter. Therefore, if you edit a linked filter, whether it be the original or the copy, all links are edited as well. When deleting linked filters, you can either delete the selected filter or all linked filter copies.

Deleting Filters

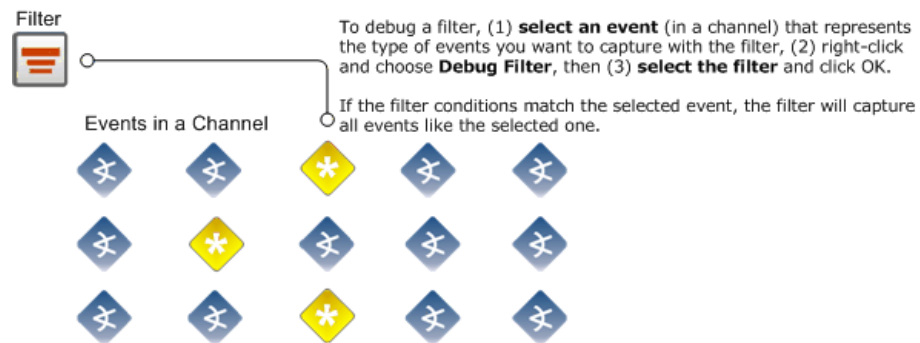
To delete a filter resource:

- 1 In the Filters resource tree, right-click a filter and choose **Delete filter**.
- 2 In the dialog box, click **Yes**.

For information on how to delete inline filters, see [“Creating an Inline Filter” on page 225](#).

Debugging Filters to Match Events

Starting with ESM v4.5, you can use a filter debugger to test whether a selected filter matches a certain type of event and, if there are mis-matches, to determine which filter conditions are not matching the event details.



On an Active Channel, select the kind of event you want to capture and test (debug) your filter against it.

The new debug filter utility is available as a right-click option on an event in an active channel. The filter debugger compares the conditions in a selected filter with the metadata that describes the selected event to determine whether the filter would capture such events. The filter definition is displayed to show the results of this comparison.

- If the selected filter matches the event, the filter definition shows no errors or mis-matches.
- If the filter does not match the event, the filter definition highlights the mis-matches between the filter conditions and the selected event with red-highlighted **X**'s.

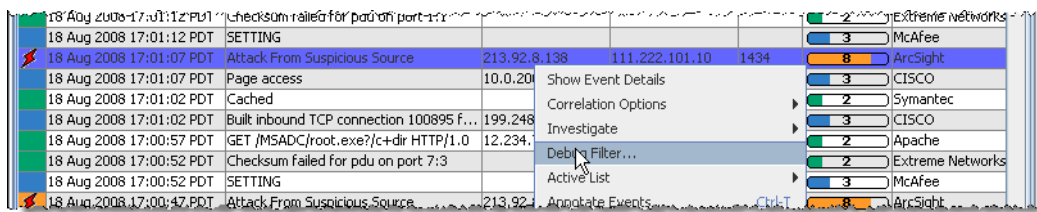


The display of red highlighted **X**'s in a filter as a result of filter debugging on an event *do not necessarily indicate* that the filter is *invalid*. Red highlights are shown here only to highlight where the selected filter does not match the selected event.

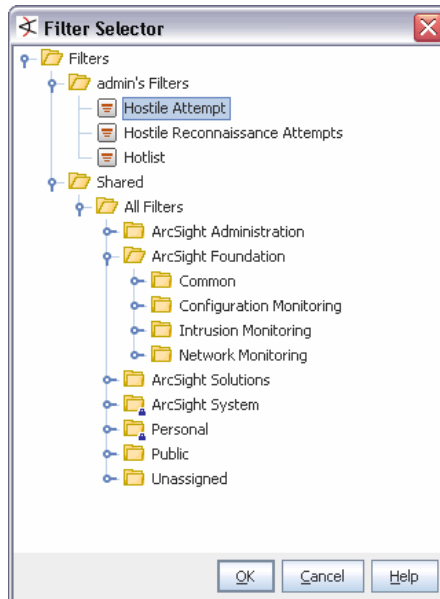
To debug a filter against an event:

- 1 Select an event in the viewer in an active channel against which you want to test a filter.

- 2 Right-click and choose **Debug Filter** from the context menu.

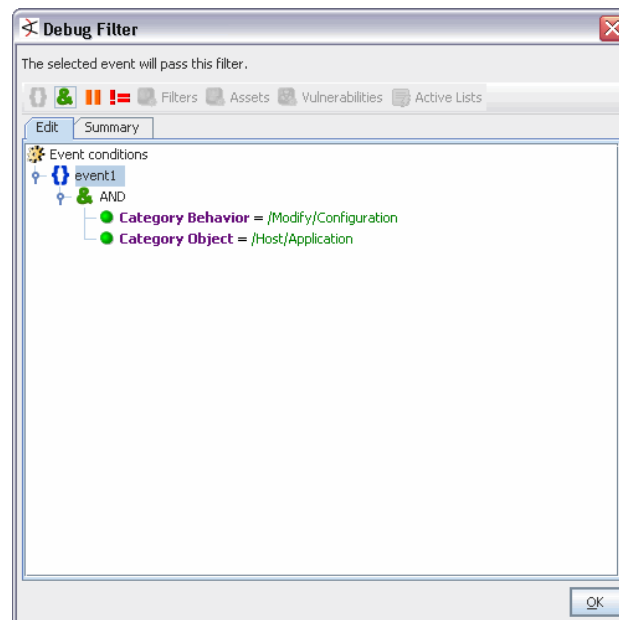


- 3 In the filter selector dialog, navigate to and select the filter you want to test.



The filter definition is displayed in its editor.

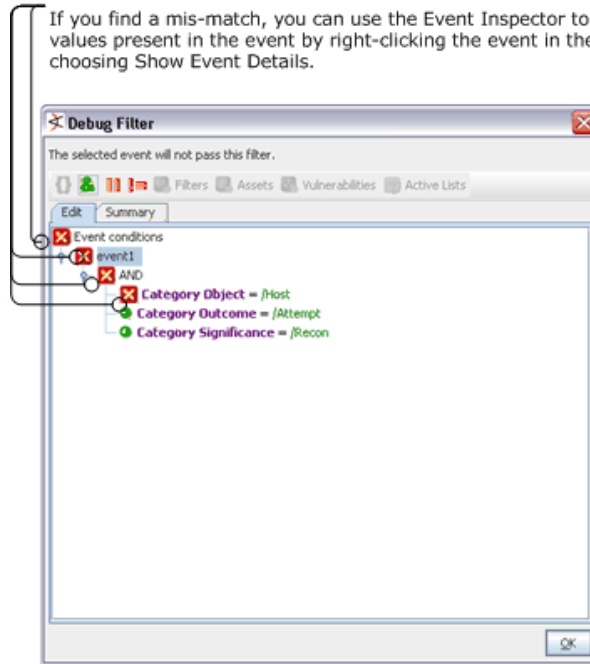
- ◆ If the selected filter matches the event, the Debug Filter dialog shows no errors or mis-matches in the definition.



- ◆ If the filter does not match the event, the Debug Filter dialog highlights the mismatches between the filter conditions and the selected event with red X's.

The filter definition highlights the mis-matches between the filter conditions and the selected event with red highlighted X's.

If you find a mis-match, you can use the Event Inspector to check the field values present in the event by right-clicking the event in the channel and choosing Show Event Details.

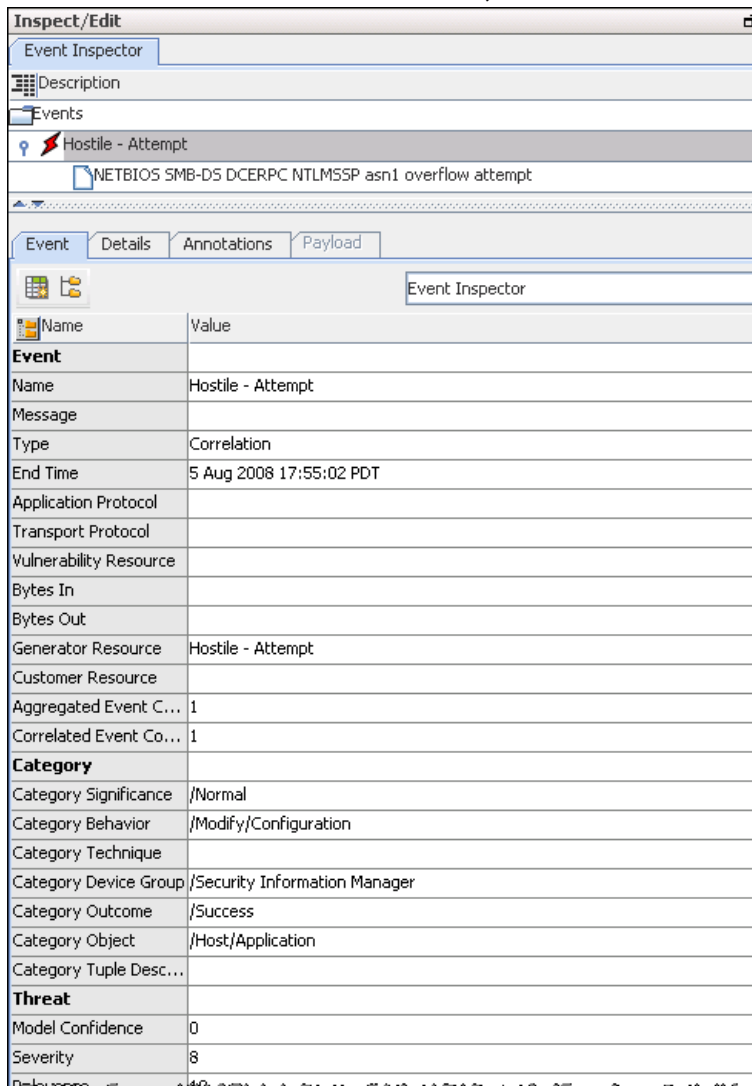


The display of red highlighted X's in a filter as a result of filter debugging on an event *do not necessarily indicate* that the filter is *invalid*. Red highlighted X's are shown here only to highlight where the selected filter does not match the selected event.

- 4 If you find mis-matches between filter conditions and an event type that you want to capture with the given filter, use the debug highlights in the filter definition along with the Event Inspector to adjust the filter to match the event.

In the example shown above, we are comparing a Hostile Attempt event to two different filters; a filter called "Hostile Attempt" and another filter called "Hostile Reconnaissance".

Here is a snapshot of the Event Inspector for this event. (To get this view, right-click the event and choose **Show Event Details**.)



- ◆ The first filter (our “Hostile Attempt” filter) matches the selected because both conditions on the filter match field values present in the event:

`Category Behavior = /Modify/Configuration`

and

`Category Object = /Host/Application`

Our “Hostile Attempt” filter would capture these types of events.

- ◆ The second filter (our “Hostile Reconnaissance” filter) has a condition that does not match field values present in the event.

The filter is looking for an event where `Category Object = /Host`, but ESM categorizes this event as `Category Object = /Host/Application`

To capture this type of event with our “Hostile Reconnaissance” filter, we would have to modify the filter.

The filter editor provides a *common conditions editor* (CCE) you can use to define, edit, and debug filters. For more information on using the CCE, see [“Common Conditions Editor \(CCE\)” on page 846](#).

For more information about using the Event Inspector to investigate events, see [“Inspecting and Editing” on page 102](#) and [“Event Inspector” on page 940](#).

See also [“Creating Filters” on page 223](#) and [“Applying Filters” on page 231](#).

Applying Filters

This topic discusses how to apply the filtering resources in the Navigator panel to other filterable analysis resources: active channels, SmartConnectors, filters, reports, and rules.

Adding Filters to Resources

You apply existing filters to other resources by referencing them in those resource editors.

- 1 Right-click a resource in the Navigator panel such as a filter or rule and choose **Edit <resource>**.
- 2 Click the editor's **Conditions** tab if it isn't already at the front.
- 3 In the Inspect/Edit panel, click the **Filters** button and select a filter in the Filter Selector dialog box. The selected filter becomes a new condition line in this resource's filter.
- 4 Click **OK** or **Apply** to save the resource's definition including its new filter reference.



You can use hierarchies of filter references (including filters within filters) to better manage them, similar to style sheets.

Applying Resources as Filters to Active Channels

You can quickly apply or test the effects of using particular SmartConnectors, assets, categories, zones, vulnerabilities, customers, stages, or filter resources as conditions to filter active channels. These filters make the referenced resource a condition for the channel in use. You can choose to make the condition exclusive or additive.

- 1 Open the channel to filter in the Viewer panel or select it to bring it forward.
- 2 In an applicable resource tree in the Navigator panel, right-click an item and choose **Set as current filter** or **Add to current filter**. The filter change takes effect automatically and the channel's header immediately shows the new filter condition exclusively (set as) or as an addition (add to).
- 3 You can click the filter description in the channel's header to open the filter in the Active Channel Editor.

Removing a Filter Condition or Resource

You use the Filters tab of a resource's editor to change or remove any filters that affect it.

- 1 In the Navigator panel, right-click the filtered resource and choose **Edit <resource>**.
- 2 In the Inspect/Edit panel, click the **Filter** tab of the resource's editor.

- 3 In the Conditions editor, right-click the statement that imposes the condition you want to remove and choose **Delete**.
- 4 Confirm the deletion and click **Apply** to restart the channel.

Importing and Exporting filters



To import and export filters, use the packages feature. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. For more information on packages, see [“Managing Packages” on page 686](#).

For information on how to import and export filters on SmartConnectors, see [“Importing and Exporting SmartConnector Configurations” on page 724](#) (especially the topics on [“Creating SmartConnector Filters” on page 712](#) and [“Adding SmartConnector Filter Conditions” on page 712](#)).

Using Filter Groups

Filter groups are created to store similar groups or filters in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's access control list (ACL).

Groups and filters can be managed with drag and drop functionality. You can move or copy groups and filters into other groups. If a group is deleted, the filters within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating Filter Groups

- 1 In the Navigator panel, choose **Filters**.
- 2 In the Filters resource tree, right-click a group and choose **New Group**.
- 3 In the Name text field, type in a name.
- 4 Press **Enter**.

Renaming Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.
- 2 In the Name text field, rename the group.
- 3 Press **Enter** and click **OK**.

Editing Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields, and press **Enter** after each.

- 3 Click **OK**.

Moving or Copying Filter Groups

- 1 In the Filters resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that will not be affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting Filter Groups

- 1 In the Filters resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

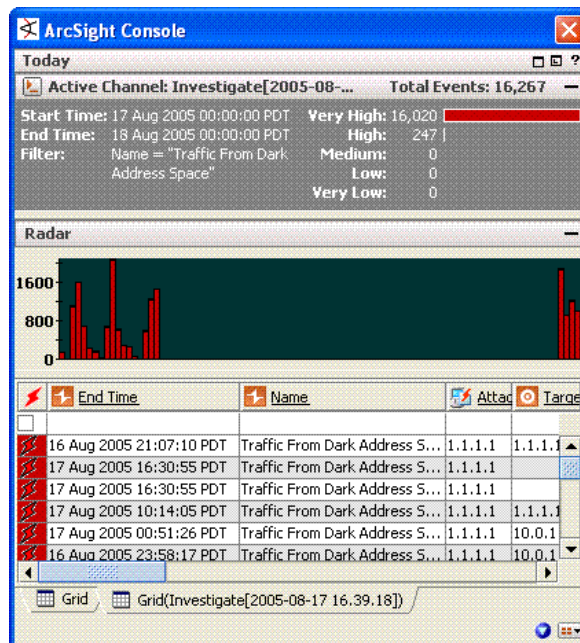
Investigating Views

This topic explains how to use the Console's Investigate command to refine and explore channels contextually, using attributes of the events already being displayed in grid views.

The Investigate command uses these attributes, and the values found in their events, to automatically formulate simple filters or conditions.

When you create or refine a filter through Investigate, the Viewer panel automatically opens a new view of the channel with the filter applied. You explore the filter's effect in this view. You can keep the view by saving the channel under a new name, or discarding it by right-clicking in the grid and choosing **Close**.

Below is a temporary view created with the Investigate command



When you use Investigate to add a condition to a resource editor such as Rules or Filters, the condition appears in the editor panel where you can modify it or click **Apply** to put it into effect.

The new or modified views you generate with the Investigate command can be grids, or you can choose to display them in applicable chart formats using the **Viewer Selector** icon in the lower-right corner of the Viewer panel.

To learn more about the event attributes these options use, please see [“Data Fields” on page 867](#).

Using an Event Attribute to Show a New Filtered View

These options completely control the new view created, ignoring the filter in the original view. You most often use them to test and explore.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Create Filter [Attribute=Value]	Show only those events in which the selected attribute matches the value in the selected event.
Create Filter [Attribute!=Value]	Show only those events in which the selected attribute does not match the value in the selected event.
Create Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. Generally, attributes are considered related if they share a common focus such as IP addresses.

Refining a Filter with an Event Attribute

These options open a new view that uses a version of the prior filter modified to include the new filter component just selected. You usually apply these as part of a filter-refinement process.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add [Attribute=Value] to Filter	Show only those events that match both the prior and new filter elements.
Add [Attribute!=Value] to Filter	Show only those events that do not match both the prior and new filter elements.

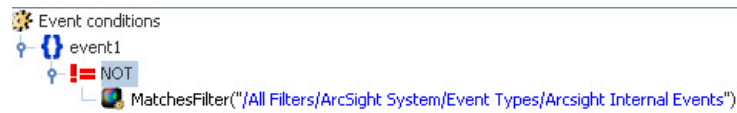
Option	Use
Add to Filter [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, choose to show only those events that do (or do not) match one of the related attributes on the additional menu. This filtering element is applied in addition to any other already present. Generally, attributes are considered related if they share a common focus such as IP addresses.

Filtering Out ArcSight Events or Other Customizations

You can modify existing filters to refine your view to show only the events you want to see. Suppose you have an active channel that includes both system events and non-system events, but you want to see only the non-system events. You can modify the filter on the channel (or copy it and modify the copy) as follows:

- 1 Double-click the filter in the channel header to get the channel editor.
- 2 Click the **Filter** tab in the channel editor.
- 3 Add this condition to the filter (with an AND):

```
!=NOT MatchesFilter("/All Filters/ArcSight System/Event Types/ArcSight Internal Events")
```



To create or customize active channels in other ways, follow this same approach. Find a filter that does what you want and add condition statements to filters for a channel. Or, as in the example above, find a filter that does the opposite of what you want, add it to a channel, and negate the condition statement as shown above. Since we wanted to limit the channel to show only non-ArcSight events, we found the ArcSight Events filter, added the ArcSight Events condition to a channel, and negated it to get the effect of filtering out all ArcSight events.

Adding an Event Attribute to a Filtering Condition

The **Add condition to editor** options apply to the editor in the Inspect/Edit panel that currently has focus. If no editor is open, the default target is the Filters Editor.

In a grid view, right-click an attribute (column) in an event listing and choose **Investigate**, followed by one of these options:

Option	Use
Add Condition [Attribute=Value] to Editor	In the current editor, insert a new condition in which the selected attribute matches the value in the selected event.
Add Condition [Attribute!=Value] to Editor	In the current editor, insert a new condition in which the selected attribute does not match the value in the selected event.

Option	Use
Add Condition to Editor [List of Related Attributes=Value, !=Value]	When the selected attribute is of a type that has related attributes, add a condition to the current editor using the available list of attribute-value pairs that do (or do not) equate. Generally, attributes are considered related if they share a common focus such as IP addresses.

To remove a condition from the editor, right-click it and choose **Delete**.

When you are using these options to affect a view that is subject to the editor in use, click **Apply** or **OK** in the editor to put the condition into effect.

Contextual filters (in contrast to conditions) are temporary unless you save the modified view as a named active channel. Condition statements are saved with their relevant editors.

Permanently Modifying an Active Channel

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

Showing an Exploited Vulnerability

The Investigate options include the ability to look for potentially exploitable vulnerabilities associated with an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Exploited Vulnerabilities**. Available information appears in the Vulnerabilities tab of the relevant Asset Editor.

Showing a Targeted Asset

You can also find out more about an asset targeted by an event.

- 1 Select an event in a grid view.
- 2 Right-click the event and choose **Investigate>Show Targeted Asset**. Available information appears in the Asset Editor.

Modifying Views

This topic covers the use of "inline" (in the grid itself) grid view filtering options. The inline filter is the row of blank event values you see at the top of any grid in the Viewer panel.

Inline filtering directly affects the current view. Changes you make to a grid view by inline filtering also apply to any other versions of the view you open such as its applicable chart types.

Modifying a View Inline

Use inline filters by clicking the inline fields at the top of view columns and choosing an event-attribute value to use as a constraint. When you choose multiple fields they automatically form AND conditions. Click the **Checkmark** icon to apply your filter selections.

Inline filters are temporary unless you save the modified view as part of a named active channel.

Undoing an Inline Filter

- 1 Click any of the filter fields in the top line of the grid view to show the inline filter control buttons.
- 2 Click the **X** (clear) button to remove the current filter elements and restart the view.

For details on working with filters and inline filters, see [“Creating Filters” on page 223](#) and [“Filtering Grid Views with Inline Filters” on page 150](#).

Permanently Modifying a View

- 1 Use the Navigator panel's Active Channel resource tree to open the view's channel in the Active Channel Editor.
- 2 Modify a view as described above.
- 3 In the editor, give the channel a new name and click **OK**.

The actors feature creates a real-time user model that maps humans or agents to activity in applications and on the network, making it possible to identify the actors behind events.

Once the actor model is in place, you can construct category models to visualize relationships among actors and use those relationships for correlation. Actors is a separately licensed feature that is available with an ArcSight Identity View license.

This topic describes how to use the *actors* resources to model users and associate them with events. It also describes how to construct *category models* to depict relationships among actors.

[“About Actors” on page 239](#)

[“Navigating to Actors” on page 245](#)

[“Configuring Actors \(for Administrators\)” on page 245](#)

[“Viewing Actors in the ESM Console” on page 249](#)

[“Investigating Actors” on page 258](#)

[“Creating and Editing Actors for Testing Purposes” on page 262](#)

[“Creating and Using Category Models” on page 266](#)

[“Actor-Related Resources Provided in Standard Content” on page 278](#)

About Actors

A critical factor in having situational awareness is knowing who is doing what with resources on your network, when they're doing it, and how. This awareness is critical for maintaining network security and demonstrating compliance with the increasing requirements of regulatory standards.

Identity management systems (IDMs) enable IT security professionals to protect their assets while granting different levels of access to a range of users, such as full-time employees, part-time employees, employees with certain security clearances, partners, contractors and customers.

However, following exactly what a specific person is doing across all the resources on your network can be difficult, because each user will have different account IDs and roles on different systems and applications. Examples of different information used to identify a given user include badge IDs (physical access devices), MAC addresses (for devices assigned to a specific person), email addresses, user names, Distinguished Names (particularly for Active Directory-related events), and so on.

The Actors feature maps humans and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems and correlating them with user account information from the user authentication systems on your network. Correlating user identifiers from the event traffic that reflects their activity throughout the day makes it possible to ensure that users are doing role-appropriate activity across the assets in your organization, and to detect and track inappropriate access and suspicious activity.

The actors feature works in conjunction with ArcSight's new *Actor Model Import connectors*, which regularly poll your Identity Management System (such as the SmartConnector for Active Directory Actor Model Import). This system automatically maintains an up-to-date actor model you can use to correlate users and their roles with their activity on the network.



ArcSight Supports Actor Models with up to 50,000 Actors

ArcSight supports actor models with up to 50,000 members. Supporting a large actor model can require special configuration. For details, see ["Tuning Guide for Supporting Large Actor Models" on page 247](#).

Once the actor model is in place, use the modeling and visualization tools (*category models*) to show direct and indirect relationships among actors in the Actor model. You can use this model to group and visualize users in your organization in numerous ways, such as reporting structures, organizational units, or role-based functions, then use these relationships as parameters in user-defined monitoring, analysis, and correlation.

For testing purposes, you can also manually add actors. You can also import or redefine views of user groups and relationships with category models.

Actor Channels and Navigating Thousands of Actors

Actor channels present all the actors in your actor model in a single, scrollable view. Like active channels, apply local filters to actor channels to find actors with certain attributes.

Actor channels are the only way to see actor models that contain 1,000 or more members because display space in the Navigator panel is limited. You can also use actor channels for viewing actor models with fewer than 1,000 members.

For more about viewing actors in actor channels, see ["Viewing Actors in an Actor Channel" on page 253](#).

Viewing Relationships Among Actors Using Category Models

Once you have actor information created, you can make logical groupings to represent relationships among actors and actor attributes using category models.

Category models can reflect direct actor relationships, such as reporting hierarchies, or relationships between actors who share common attributes, such as actors in a particular location. Category models can also reflect relationships between actors using custom attributes defined by the user.

You can use category models to visualize these relationships, then leverage the data gathered in them using the `HasRelationship` function in local and global variables.

For more about category models, see ["Creating and Using Category Models" on page 266](#).

For more about how to view actors using resource graphs, see ["Viewing Category Models in Graphs" on page 275](#).

For more about using category model relationship data in monitoring, investigation, and correlation, see [“Leveraging Category Model Data Using Variables” on page 277](#).

Using Actor Global Variables to Identify Actors from Events

The actor data stored in the Actor Resource Framework coupled with actor global variables make it possible to identify an actor from any given event, then correlate that activity with other activity or attributes of that actor. The ability to identify an actor from a given event and correlate that activity with other events involving that actor and attributes of that actor, such as location and role, make it possible to verify that an actor's activity across the network is appropriate.

Standard content provides a series of actor global variables that are part of the Actor Resource Framework, which identifies and stores actor-related data from events in the look-up tables of the Actor Resource Framework. You can also use these global variables in your own correlation content. For more about using the Actor Resource Framework global variables, see [“Actor Resource Framework Global Variables” on page 278](#).

You can construct your own actor global variables. For an outline of this process, see [“Leveraging Actor Data Using Variables” on page 265](#).

Using Standard Content to Track Actor Configuration Changes

Standard content also provides a set of coordinated resources that track actor configuration changes, such as when actors are created, updated, and deleted.

For more about this standard content, see [“Tracking Actor Configuration Changes Using Standard Content” on page 281](#).

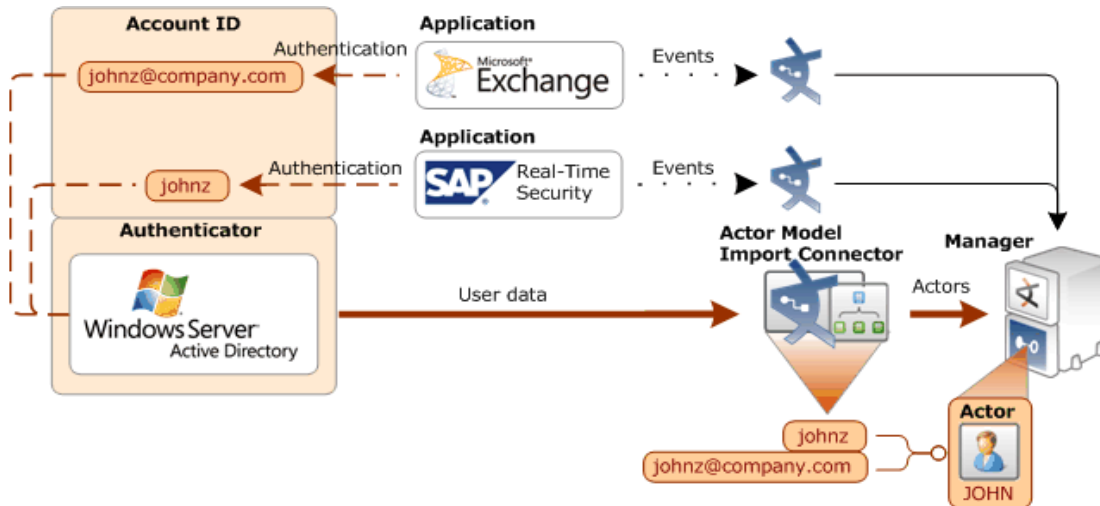
How the Actors Feature Works

ArcSight SmartConnectors normalize event data from hundreds of different devices on a network into a common data schema. The Actors feature normalizes user identity information stored in different formats in different authentication data stores to create a complete profile of data used to identify each user on your network in various contexts.

As shown in [on page 242](#), a model import connector imports data from an identity management system, such as Microsoft Active Directory. For a complete list of supported identity management systems, contact ArcSight Customer Support.

In the following example, the actor data comes in from the Microsoft Active Directory system using a model import connector. Events arrive from applications that all use different data stores to authenticate user activity, which all use different account IDs to

identify the user John Zed. The activity is identified as belonging to the same actor. That actor is represented as JOHN.



The actors feature works in conjunction with an Actor Model Import connector to import user data from an identity management system and to normalize user data in event traffic.

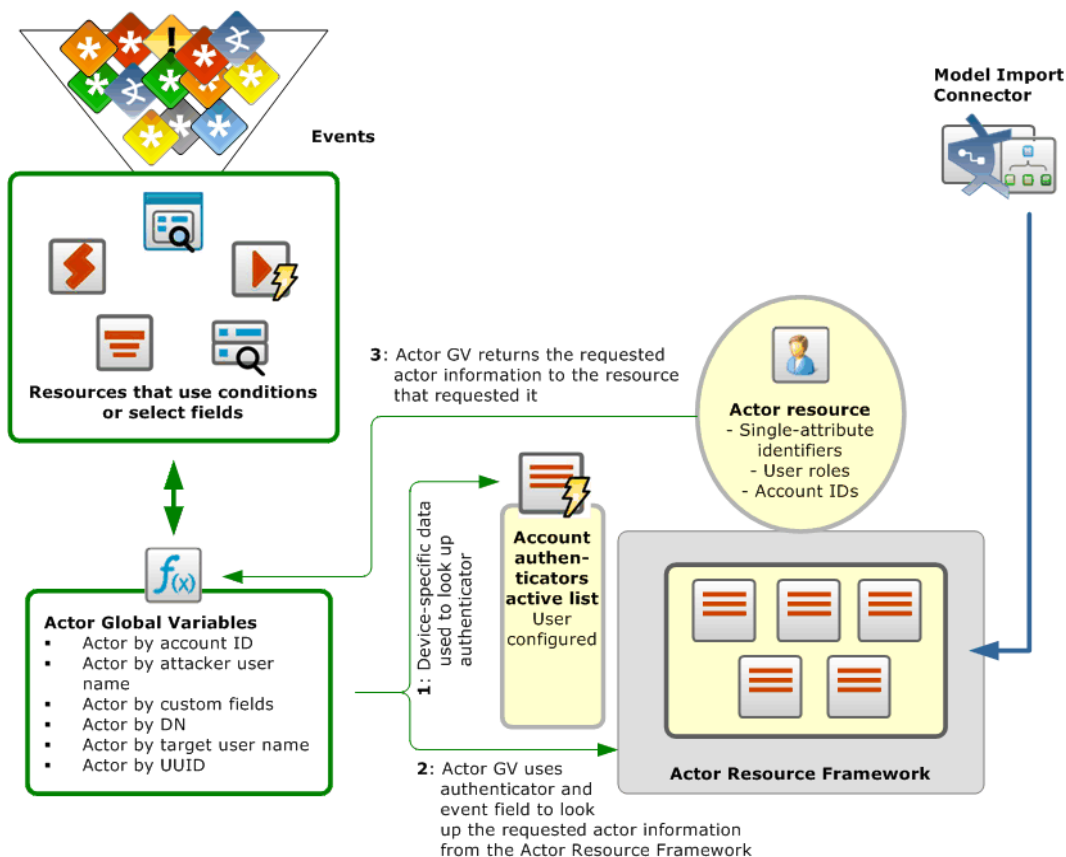
The actors feature is supported internally using the Actor Resource Framework, a series of internal look-up tables maintained by regular updates from the Actor Model Import connector.

As part of setting up the actors feature, you also configure an applications and *authenticators active list* to identify the mapping between the applications in your network environment and the data stores they use to authenticate users. In the example shown above, Windows Server Active Directory is the authentication data source for Microsoft Exchange and SAP Real-Time Security.

The diagram below shows a detailed look at how the Actors feature works. When events arrive at the Manager, resources that use conditions or select fields invoke one or more of the actor global variables provided in standard content. These global variables and the actor data maintained in the Actor Resource Framework provide several ways to identify actors using whatever user identity attributes are available in events arriving from different applications from across the network.

The global variables first look up the authenticator using the device-specific data, such as vendor and product information in the event, then look up the relevant user information from the Actor Resource Framework tables to positively identify the actor. For details about

the Actor Global Variables in standard content, see [“Actor Resource Framework Global Variables”](#) on page 278.



Resources leverage system-provided actor global variables to look up actor identity attributes maintained in the Account Authenticators table and the Actor Resource Framework.

About the Actor Model Import Connectors

The ArcSight *Actor Model Import connectors* support bulk import of user accounts from multiple identity management systems, such as Microsoft Active Directory. (For a complete list of supported identity management systems, see the ArcSight connector documentation.)

The Actor Model Import connector supports the Identity View solution. The Actor Model Import connector imports the user data into the actors resource, where it is leveraged by the infrastructure that identifies and tracks user activity. Correlated and normalized data about user activity is then available for monitoring and investigation, further correlation, and reporting.

The actor model used to describe users is automatically populated with the attributes configured for it by the Actor Model Import connector when connecting to the connector.


Caution

Actor Model Import connector should be configured with all attributes you are interested in tracking before initial connection.

During Actor Model Import connector configuration, make sure that all the attributes you are interested in tracking are configured. Once actor information is imported, the list of attributes the Actor Model Import connector sends for existing actors is not updated.

If you add or remove attributes to be sent from the Actor Model Import connector after an actor model has already been imported, you must first delete the actor group, then re-import the actor data.

For details about how to delete an existing actor group, see [“Deleting Actors” on page 265](#).

The following table lists the attributes that the actor model supports. The Actor Model Import connector administrator configures the Actor Model Import connector with the attributes from this list that it will send to populate the actor model. Not all IDM systems support all these attributes. An actor resource is only populated with the attributes configured by the Actor Model Import connector administrator.

Single-value attributes		Multi-value attributes
UUID	Business PhoneMobile	Account
First Name	Phone	• Account ID
Middle Initial	Fax	• Authenticator
Last Name	Pager	
Full Name	Address	Role
IDM Identifier	City	• Role Name
DN	State	• Resource Name
Employee Type	Zip Code	• Role Type
Status	Country Or Region	
Title		
Company		
Organization		
Department		
Manager		
Assistant		
Email Address		
Location		
Office		

In addition to the basic single-value attributes, each actor will likely have multi-value attributes, specifically multiple account IDs, and multiple roles, which are tracked using your IDM system. These multi-value attributes can appear differently in events coming from different devices. In some cases, such as a non-IT-related role, the information is not included in event data at all, but is still valuable information to help identify users and correlate their activity to help ensure appropriate behavior and access to resources hosted on the network.

Troubleshooting Errors with Actor Model Imports

It is possible that during the actor import process from the Actor Model Import connector, one or more actor import files containing data for multiple actors may not have imported successfully into the Manager. This might happen because of network connection

problems, an out-of-memory error, or some other problem that caused the import of that file to fail.

In such cases, there is an archive file in `$ARCSIGHT_HOME/archive/webservices` for each actor import file that failed to import successfully. Each such archive file is created with the file extension `.bad`.

If an actor file did not import as expected, or during routine maintenance, check the `$ARCSIGHT_HOME/archive/webservices` directory for actor files that failed to import.

The `.bad` archive file contains all the missing actor information, and you can use the ArcSight Archive utility to import that file individually from a command line on the Manager system. For instructions about how to run the ArcSight Archive utility to import an archive file, see the topic “The Archive Command Tool” in the *Administrator's Guide*.



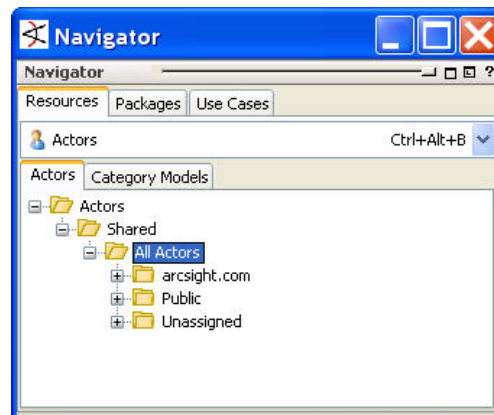
Tips for using the ArcSight Archive utility:

- To see a list of commands available with the ArcSight Archive utility, include `-h` (for “help”) in the archive utility command script.
- If the archive file name starts with a dash (`-`), rename the file before running the ArcSight Archive utility to ensure that the command works.
- If the archive file name starts with a dash (`-`), rename the file before running the ArcSight Archive utility to ensure that the command works.

For details about the Actor Model Import connector and how to configure it, see the Actor Model Import connector documentation for your IDM system, for example, the *SmartConnector™ Configuration Guide for Microsoft Active Directory Actor Model*.

Navigating to Actors

In the Navigator panel, select **Actors**. Here you will find the actors resource and the category models you can use to organize and visualize them.



Configuring Actors (for Administrators)

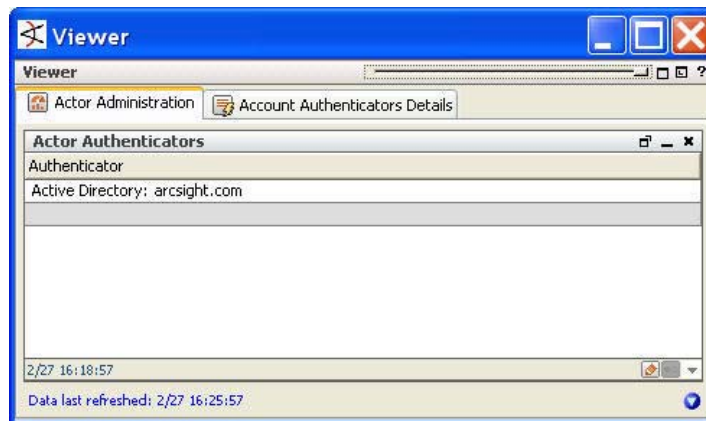
Configuring the Actors feature requires a one-time setup procedure and minimal maintenance if authentication systems are added, modified, or removed from your network. This setup procedure maps the user authentication systems you use in your network environment and the account IDs for each user on those systems.

- 1 **Install the Actor Model Import connector appropriate for your IDM.** For complete instructions about how to install the connector, see the relevant SmartConnector installation and configuration guide, such as the *SmartConnector™ Configuration Guide for Microsoft Active Directory Actor Model*. Once installed, the connector polls the IDM and imports the user data into the Actor model.
- 2 **Identify the authenticators in your environment.** In preparation for configuring the authenticator mapping table, open the dashboard for automatically identifying the user authentication data stores running in your environment and their type:

[/All Dashboards/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Administration](#)

This dashboard is populated by the following query viewer, which looks for events with a value in the Authenticator field: [/All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actor/Actor Authenticators](#)

The example below shows the value of the Attributes field for an active directory system configured as [Active Directory:<domain>.com](#). Use this exact value, including punctuation, spaces, and capitalization, to populate the account authenticators mapping table described in the next step.



- 3 **Configure the Authenticators mapping table.** Using the information gathered in step 2, fill out the account authenticators mapping table provided at [/All Active Lists/ArcSight System/Actor Data Support/Account Authenticators](#). The data you enter here must exactly match the values displayed in the Actor Administration dashboard.
 - a In the Navigator panel, go to **Lists > Active Lists**. Right-click the active list [/All Active Lists/ArcSight System/Actor Data Support/Account Authenticators](#) and select **Show Entries**.
 - b In the Account Authenticator Details tab in the Viewer screen, click the add icon (+).
 - c For each account authenticator data store, enter the following data:

Column	Description
Device Vendor	The vendor that supplies the authentication data store, such as Microsoft.
Device Product	Provide the application name of the authentication system, such as Active Directory.

Column	Description
Agent Address	The IP address of the reporting SmartConnector.
Agent Zone Resource	The zone in which the reporting SmartConnector resides.
Authenticator	Enter the exact value(s) returned for Authenticator in the Actor Administration dashboard from the previous step, including punctuation, capitalization, and spaces. Using the example shown in the previous step, the value you would enter in this column would be: Active Directory: arcsight.com

When you are finished, the Account Authenticators table should look something like this:

Device Vendor	Device Product	Agent Address	Agent Zone Resource	Authenticator	Creation Time	Last Modified Time	Count
Microsoft	Microsoft Windows	10.10.10.10	<Resource URI="/All Zon...	Active Directory: company.com	14 Apr 2010 17:27:36 PDT	28 Apr 2010 14:27:14 PDT	1
Microsoft	Exchange Server	10.10.10.12	<Resource URI="/All Zon...	Active Directory: company.com	28 Apr 2010 10:42:18 PDT	28 Apr 2010 14:27:23 PDT	1
SAP	Security Audit Log	10.10.10.11	<Resource URI="/All Zon...	Active Directory: company.com	28 Apr 2010 10:41:28 PDT	28 Apr 2010 14:27:29 PDT	1

Tuning Guide for Supporting Large Actor Models

If your actor model contains tens of thousands of members, follow the guidelines in this section to allow adequate processing capacity for best results.

- 1 Shut down the Manager
- 2 **Increase settings in `server.properties`.** Increase the following default values to support managing large blocks of actors by setting following properties in the `config/server.properties` file:

Server Property Name	Default Setting [units]	Comments
<code>dbconmanager.provider.oracle.pool.maxcheckout</code>	600 [seconds]	The maximum time for a database connection before the process is terminated. This setting comes into play when you want to delete a large block of actors from the ESM Console. The default value should be increased by a factor of 3-6x, for example, 1800 to 3600 .

- 3 **Adjust Java Heap Memory Size in the `arcsight managersetup` utility.** Supporting 50,000 actors will require an additional 2 GB of Java heap memory in the Manager. An additional 300 MB is needed for each category model you construct that uses 50,000 actors. This additional memory will not be in use all the time, but will be needed for certain operations.

For instructions about how to run the `managersetup` utility, see the *Administrator's Guide*.

- 4 Re-start the Manager.
- 5 Proceed with importing the actor model.

For details about starting and stopping the Manager, see “Basic Administration Tasks” in the *Administrator's Guide*

For details about working with the `server.properties` file, see “Managing and Changing Properties File Settings” in the *Administrator's Guide*.

Permissions Required to Use Actors and Actor-Related Data

By default, Admin users have full read/write access to the actors feature and the other resources that actors depend on. The Admin can grant permissions for actors and the other resources upon which the actors feature depends to other users.

To create actors, actor channels, and category models:

- Read and write on `/All Actors`
- Read and write on `/All Session Lists/ArcSight System/Actor Data` and `/All Session Lists/ArcSight System/Actor Data Support`
- Read on `/All Field Sets/ArcSight System/Actor Field Sets/Actor Base`
- Read on the filters used to define the event ACLS for that user group, for example, `All Filters/ArcSight System/Core`
- Read and write on the group in which the new resource is being created

To view actors and category models, and monitor actor channels:

- Read on `/All actors`
- Read on `/All Session Lists/ArcSight System/Actor Data` and `/All Session Lists/ArcSight System/Actor Data Support`
- Read on `/All Field Sets/ArcSight System/Actor Field Sets/Actor Base`

To use actor global variables provided in standard content rules, active channels, and reports that leverage actor data:

Read access on the following resources and groups:

- `/All Fields/ArcSight System/Actor Variables` (either directly, or inherited from `/All Fields/ArcSight System`)
- `/All Actors`
- `/All Session Lists/ArcSight System`
- `/All Active Lists/ArcSight System/Actor Data Support` (for the authenticator active list)
- `/All Filters/ArcSight Foundation`
- The appropriate group that gives all the queries used by a query viewer that leverages actor data
- The appropriate group that contains a query viewer that leverages actor data
- The appropriate group(s) for the filters used by any queries and query viewers that leverage actor data

In addition to these permissions on the actor-related resources themselves, read permissions are needed for any resources (such as filters, user-created actor global variables, and so on) upon which these actor-related resources rely.



Best practice: Log out and log back in again for permission changes to take effect

As a best practice whenever an admin changes another user's permissions, the other user should log out and log back in again. This ensures that the new permissions are registered with the Manager, and the user can see the changes.

For details about how to assign permissions to user groups, see [“Granting or Removing Resource Permissions” on page 647](#).

About Exporting Actors

If you need to export your entire actor model to image another Manager, you can do it using the `export_system_tables` command-line utility using the `-s` parameter, the parameter used to specify export of session list data. The `-s` parameter captures the special session list infrastructure that is part of the Actor Resource Framework in addition to the actor resources themselves.

For instructions about how to use the `export_system_tables` command-line utility, see the *Administrator's Guide*.

Viewing Actors in the ESM Console

In a typical workflow, actors are created automatically by installing the ArcSight Actor Model Import connector and configuring it to your IDM system. New actors added to the IDM are automatically created and existing ones updated with changes made on the IDM with every connection made between the Manager and the Actor Model Import connector as described in [“About the Actor Model Import Connectors” on page 243](#).

For testing purposes, you can also create an actor individually using ESM Console resources, or edit an existing one. For more about creating actors individually for testing purposes, see [“Creating and Editing Actors for Testing Purposes” on page 262](#).



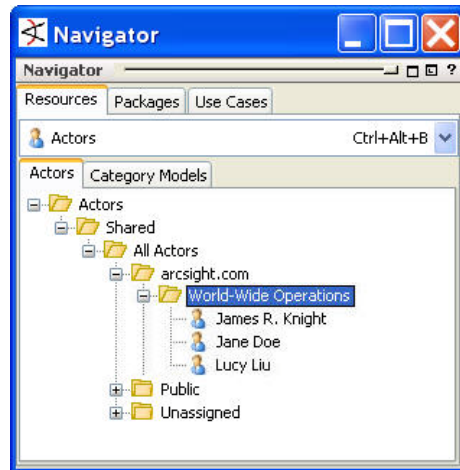
ESM Console-created actors or those edited individually using ESM Console resources do not update the user information stored in the IDM.

Communication from your IDM to the Manager is one way. Any actors that you add from scratch or existing ones that you update using ESM Console tools are not added to the IDM system. Any changes you want to persist to the IDM should be made at the IDM, and the new actor information will be automatically imported into the actor model at the next Actor Model Import connector connection.

Viewing Actors in the Navigator Panel

Actor models with fewer than 1,000 members can be viewed from the Navigator panel. Upon connection, the Actor Model Import connector creates the destination group in which

the actors are placed based on the value set at the Actor Model Import connector. The example below shows three actors in a group called World-Wide Operations.



Viewing Actors in the Actor Editor

To view the details of a particular actor in the Actor editor, double-click the actor, or right-click the actor and select **Edit**. Use the scroll bar to see all the actor attributes.

Inspect/Edit

Actor: 00082A1B-ABCD-8BD6-F1886...

Attributes | Notes

Actor

* UUID	00082A1B-ABCD-8BD6-F18864D6B703
* Full Name	John Doe
First Name	John
Last Name	Doe
Middle Initial	
IDM Identifier	Active Directory
D N	CN=John Doe, OU=Sales, DC=companyname...
Employee Type	full time exempt
Status	active
Title	Manager
Company	My Company
Org	SSD
Department	Sales
Manager	Jane Lane
Assistant	
Email Address	jdoe@companyname.com
Location	Dallas Fort Worth
Office	US/CA/Bldg 5
Business Phone	888-555-1212
Mobile Phone	888-555-1234

(Name)
(Description)

Account_Attributes + x

Authenticator	Account ID
Active Directory: companyname.com	CN=John Doe, OU=Sales, DC=companyname...
Active Directory: companyname.com	john_doe
Active Directory: companyname.com	jdoe@companyname.com

Role_Attributes + x

Role Name	Resource Name	Role Type
Manager	companyname.com	Business
Administrator	Security Software	

OK Cancel Apply Help

Viewing Actor Base Attributes

The attributes in the Actor section of the Actor editor is also referred to as the Actor Base attributes. These are the basic standard attributes that describe an actor. These base attributes are part of the Actor Base field set. (For more about actor field sets and usage, see [“Creating and Using Field Sets” on page 204.](#))

Attribute	Description
UUID	The Universally Unique Identifier for the actor
Full Name	The actor's full name
First Name	The actor's first name
Last Name	The actor's last name
Middle Initial	The actor's middle initial

Attribute	Description
IDM Identifier	The friendly name for the IDM selected by the Actor Model Import connector administrator at Actor Model Import connector setup time.
DN	The distinguished name for the actor, for example, <code>CN=JohnDoe, OU=Sales, DC=companyname, DC=com</code>
Employee Type	The type of employee this actor is in your company, for example, <code>full-time</code> , <code>exempt</code> , or <code>contractor</code> .
Status	<p>The employment status of the actor's account, for example, <code>Active</code>, <code>Deleted in IDM</code>, or <code>Disabled</code>.</p> <p>Notes:</p> <ul style="list-style-type: none"> When an actor is deleted from the IDM, the actor will remain in the actor model with the status <code>Deleted in IDM</code>. The license tracking feature includes actors that are still in the actor model with the status <code>Disabled</code> or <code>Deleted in IDM</code>. The identity management feature preserves disabled and deleted actors in the actor model to track any unauthorized activity related to disabled or deleted actors. If you do not want the license tracking feature to evaluate actors with the status <code>Disabled</code> or <code>Deleted in IDM</code>, you can manually remove them from the ESM actor model. Manually removing disabled or deleted actors also removes the ability to track unauthorized activity related to these accounts. <p>For more about the license tracking feature, see "License Tracking" on page 112.</p>
Title	The actor's job title
Company	The company by whom the actor is employed.
Org	The organization within your company of which the actor is a member
Department	The department within your company of which the actor is a member
Manager	The distinguished name of the actor's manager
Assistant	The name of the actor's assistant as it appears in the IDM
Email Address	The actor's company email address
Location	The actor's location name
Office	The actor's office name
Business Phone	The actor's business phone
Mobile Phone	The actor's mobile phone
Fax	The actor's fax number
Pager	The actor's pager number
Address	The actor's business address
City	The city of the actor's business address
State	The state of the actor's business address
Zip Code	The zip code of the actor's business address

Attribute	Description
Country Or Region	The country of the actor's business address

Viewing Actor Account Attributes

The Account_Attributes table displays the unique account IDs attributed to this user by the various user authentication data stores relevant to this user. Like the base actor attributes, the values in this table are populated by values from the Actor Model Import connector for your IDM system.

Field	Description
Authenticator	The friendly name for the user authentication data store containing the actor's account ID
Account ID	The account ID for the actor

Viewing Actor Role Attributes

The Role_Attributes table displays role name, resource type, and role type for each role represented by the actor. The values in this table are also populated by values from the Actor Model Import connector for your IDM system.

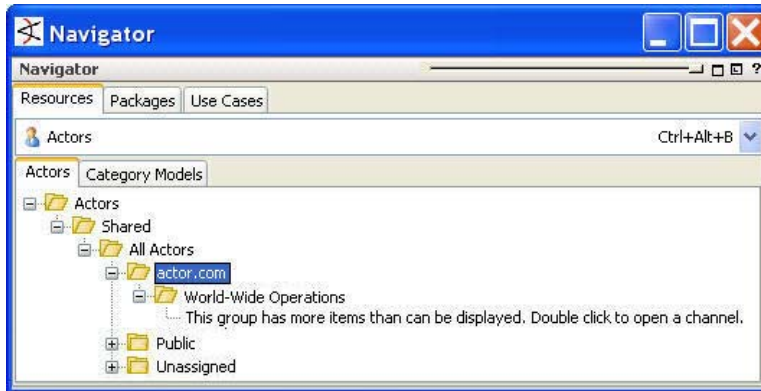
Field	Description
Role Name	The name of the role or group, such as Administrators or Software Developer
Resource Name	The name of the resource in which the role is assigned, such as the active directory domain, identity management system, or application
Role Type	The role's category, such as Global Security Group , Business Role , or IT Role

Viewing Actors in an Actor Channel

For actor models that contain thousands of members, actor channels present all the actors in your actor model in a single, scrollable view. You can apply local filters to actor channels to find actors with certain attributes.

If a group in your actor model contains more than 1,000 members, the actor tree in Navigator panel displays the message:

“This group has more items than can be displayed. Double click to open a channel.”



You can also view actor models with fewer than 1,000 members in an actors channel.

To view an actor model in an actors channel:

- 1 In the Actors navigation panel, right-click an actors group and select **Show Actors**. If your actor model contains more than 1,000 members, you can also double-click the message **“This group has more items than can be displayed. Double click to open a channel.”**



Note

‘Show Actors’ on a Group Shows Actors Only for that Group

When you select **Show Actors** on a group of actors, the actor channel will only display the members of that immediate group. If the group has a sub-group, the actors in that sub-group will not be displayed in the actor channel.

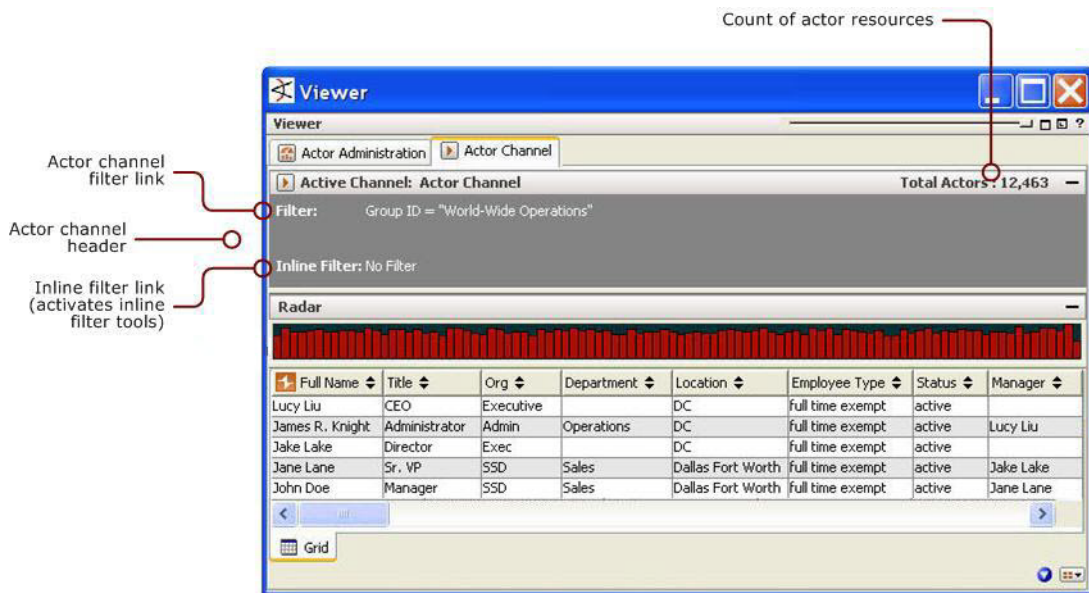
To view the actors in a sub-group, right-click that group and select **Show Actors**.

- 2 In the Viewer panel, navigate to the actor channel.

The following sections describe the attributes of an actor channel, and how to interact with them.

About the Actor Channel UI

The actor channel is an active channel with a simplified header that displays the actor resources in your actor model.



Sorting Fields in Actor Channels

The fields shown are from the Actor Information Field Set ([/All Field Sets/ArcSight System/Actor Field Sets/Actor Information](#)).



Sort fields in actor channels the same way you sort fields for event-based channels.



Multi-value columns cannot be sorted.

Columns that contain multi-value attributes, such as Account ID, cannot be sorted.

The names of sortable fields in column headers are indicated with a double-arrow icon .

If a field is already sorted, an up  or down  arrow indicates the direction of the sort.

- To sort the list by a column, right-click over the column and select **Sort Column**.
- To reverse the sort order, select **Sort Column** again on an already-sorted column.
- To remove a sort, right-click over a sorted column and select **Remove Sort**.

For more about sorting columns in channels, see ["Sorting Events in an Active Channel" on page 131](#).

Actor Channel Options

There are several options available to take on actors from the tree view in the Navigator panel and from the grid view in the Viewer panel.

Right-Click Options from the Grid View

Option	Description
Export	Save the actor data in this actor channel as a CSV list.
Edit Actor	Open the selected actor to view its details in the event inspector.
Delete Actor	Delete the selected actor from the actor model. Caution: Make sure the actor is also deleted from the source IDM. Subsequent updates from the IDM that still contains this actor data can result in an unstable actor data set for this actor.
Add Actors to Category Model	Add the selected actors to an existing category model.
Add to Package	Add the selected actor(s) to a new or existing package.
Report	Run a custom actor context report, or one using default values. For more about actor context reports, see
Find Actor in Navigator	Expand the containing group and highlights the selected actor in the Navigator panel.
Graph View	Display the actor in a resource graph in the Viewer panel.
Lock Actor	Locking is a common feature for all resources.

Filtering Actor Channels

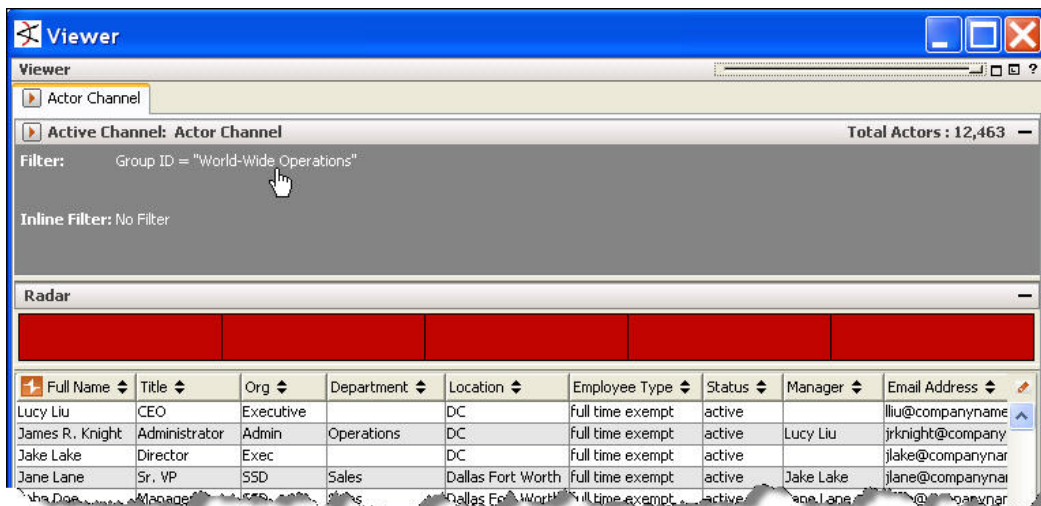
There are two ways to filter the contents of an actor channel: adding a local filter to the resource itself, or applying an inline filter to one or more columns.

Adding a Local Filter to the Actor Channel Resource

You can add a local filter to the actor channel using the Active Channel: Actor Channel editor. This enables you to use the CCE to apply a filter locally to the selected actor channel. You cannot save a local filter added to an actor channel.

To add a local filter to the resource:

- 1 click the **Filter** link in the channel header:



This opens the Active Channel: Actor Channel editor in the Inspect/Edit panel.

- 2 In the **Attributes** tab, set the name and select the Actor field set you want to use.
 - a **Name.** Replace the default name Actor Channel with a name that describes the channel, and maybe the filter you want to apply to it, such as *Managers in World-Wide Operations*.
 - b **Default Field Set.** By default, no field set is used. You can select a field set if you want to select a specific actor field in a particular field set. If you choose to specify a field set, only the actor field sets are displayed, such as the Actor Base field set ([Field Sets/Shared/All Field Sets/ArcSight System/Actor Field Sets/Actor Base](#)). You can select this field set, or another actor field set created in your environment.
 - c **Common Attributes.** Set any other common attributes you want for the actor channel. For a description of the data that goes in the Common section, see ["Common Resource Attribute Fields" on page 684](#).
- 3 In the **Filter** tab, construct the filter you want to apply. You can select any existing Actor field set, or apply a global variable.

For instructions about constructing a condition using the Common Conditions Editor (CCE), see ["Common Conditions Editor \(CCE\)" on page 846](#).
- 4 In the **Sort Fields** tab, select the columns by which you want the actor channel to sort. Fields that contain lists and multi-values cannot be sorted. For instructions about using the Sort Fields tab, see [Step 4 on page 136](#).
- 5 On the **Local Variables** tab, define any local variables you want to use to extract a particular value from a particular field. For instructions about how to use the Local Variables editor, see ["Variables" on page 1006](#).
- 6 Click **Apply** to apply changes to the actor channel displayed in the Viewer panel. Click **OK** to save the filtered actor channel.



Where to Find Saved Actor Channels

Once you have modified and saved an actor channel, you can find it in the Active Channel area of the Navigator panel. Actor channels are saved with the suffix [Actor] behind the active channel name, for example, *Managers in World-Wide Operations [Actor]*.

Creating an Inline Filter

Like event-based active channels, you can create an inline filter to operate on one or more columns to find actors with particular attributes in common.

For instructions about how to construct inline filters, see ["Filtering Grid Views with Inline Filters" on page 150](#).

In an actor channel, if you apply an inline filter to a specific column, the inline filter automatically becomes part of the actor channel's filter condition, as if you manually edited the actor channel and entered settings on the Filter tab. You have the option to save the actor channel with the new filter, or close the channel without saving the filter.

To save the filtered version of the channel, see ["Saving Actor Channels" on page 257](#).

Saving Actor Channels

To save an actor channel from the Viewer panel:

- 1 Right-click the active channel header and select **Save Active Channel As**.
- 2 In the Active Channels Selector, navigate to where in the Active Channels branch you want to save the actor channel and click **OK**.

You can also save an actor channel by opening the actor channel editor in the Inspect/Edit panel as described in [“Filtering Actor Channels” on page 256](#).



Where to Find Saved Actor Channels

Once you have modified and saved an actor channel, you can find it in the Active Channel area of the Navigator panel. Actor channels are saved with the suffix [Actor] behind the active channel name, for example, *Managers in World-Wide Operations [Actor]*.

Editing Saved Actor Channels

You can find saved actor channels in the Active Channel area of the Navigator panel. Actor channels are saved with the suffix [Actor] behind the active channel name.

To edit a saved actor channel:

- 1 In the Navigator panel, go to Active Channels.
- 2 Right-click the actor channel you want to edit and select **Edit Active Channel**.
- 3 Make modifications to the actor channel in the Active Channel: Actor Channel editor in the Inspect/Edit panel and click **OK**. For details about what to enter in the active channel editor, see [“Filtering Actor Channels” on page 256](#).

Viewing Saved Actor Channels

To view a saved actor channel:

- 1 In the Navigator panel, go to Active Channels.
- 2 Double-click the actor channel you want to view, or right-click it and select **View Active Channel**.

For details about viewing actors and navigating actor channels, see [“Viewing Actors in the ESM Console” on page 249](#).

Investigating Actors

You can investigate events to identify the actor behind the activity represented in an event by running a context report from an event or actor channel. The actor context report looks at which actor is bound to the event you are investigating, and then run a report that will show activity for that actor.

Running Context Reports from an Actor Channel

From an actor channel, you can choose to run the report based on the following actor global variables:

- ActorByAccountID
- ActorByAttackerUsername
- ActorByCustomFields
- ActorByTargetUsername

The report will be populated if the actor global variable finds the values for the supported attributes, for example, account ID, custom field, attacker user name, and so forth. When the report is launched, it will use the actor global variable specified in the field set. If there is more than one actor global variable in the field set, the report will default to ActorByAccountID.



Actor context reports will not show data if you are looking up actors using the ActorByUUID or ActorByDN global variable. These global variables are used for internal actor lookups.

For context reports out of the actor channel, you have the following choices for running actor context reports:

- With default parameters:
 - ◆ Default time range: last hour
 - ◆ Default filter: correlation events only
- With custom parameters (you set these explicitly)
 - ◆ Start time
 - ◆ End time
 - ◆ Filter by

The following example shows the available options for running actor context reports from an actor channel.

To run an actor context report from an actor channel:

- 1 Display an actor channel and right-click an actor.
- 2 Select **Report** and then select one of the displayed report types.

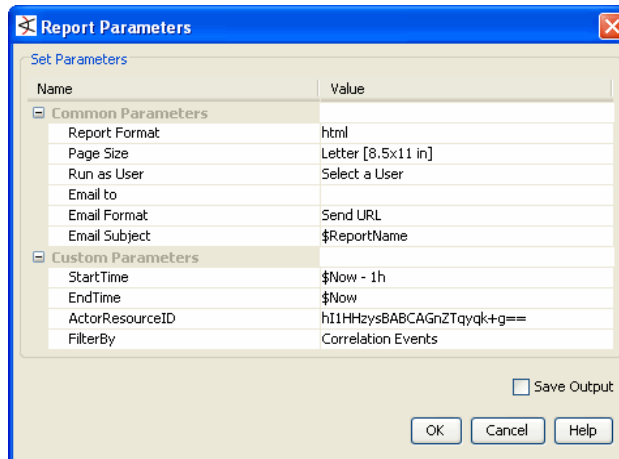


If you have the ArcSight IdentityView solution, you can also run context reports on global variables that come with the IdentityView. Refer to the *ArcSight Solution Guide IdentityView* for a list of actor global variables provided by the solution.

If you choose a report type that ends in *with defaults*, for example, **Actor Context Report by Attacker Username with defaults**, the report is displayed with the following parameters:

- ◆ Default time range: last hour
- ◆ Default filter: correlation events only

If you choose a report type that does not end in *with defaults*, for example, **Actor Context Report by Attacker Username**, the following screen appears:



- 3 Set your custom parameters. For example, set StartTime, EndTime, and FilterBy. Keep the ActorResourceID parameter value; this is the value used to identify the actor of interest.
- 4 Click **OK**.

Investigating an Actor from an Event Channel

You can investigate an actor from an event channel in one of the following ways:

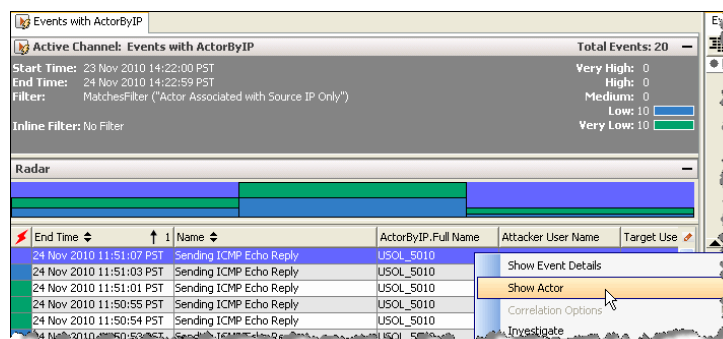
- By using the Show Actor option on an event that is related to an actor. This option is enabled if the channel contains ActorResourceID values, for example, ActorByAccountID.ID. Actor data is displayed on the Inspect/Edit panel.
- By running an actor context report on any active channel that has ActorResourceID values, for example, ActorByAccountID.ID.

Running an actor context report provides additional options:

- ◆ Report with default parameters (see [related information on page 259](#))
- ◆ Report with custom parameters which you set explicitly (see [related information on page 259](#))

To show an actor related to an event:

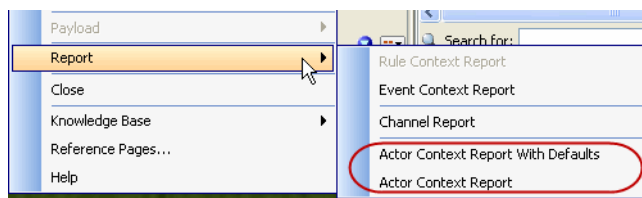
- 1 Display an event channel.
- 2 Right-click an event and select **Show Actor**. If the channel does not use a field set containing an actor global variable, then the Show Actor option is disabled.



The edit panel displays details about the actor. See [“Viewing Actors in the Actor Editor” on page 251](#) for an example of an actor edit panel.

To run an actor context report from an event channel:

- 1 Display an event channel.
- 2 Right-click an event and select **Report**.



- 3 Select the report with defaults or the report that provides options to set report parameters.

The report is displayed on the ESM Console's Viewer panel.

Actor Context Reports in Standard Content

If needed, you can modify the resources upon which these context reports are based.

Reports

[/All Reports/ArcSight System/Core/](#)

Report	Description
Actor Context Report by Account ID	This report is used by the system to show activity related to an actor based on the ActorByAccountID global variable.
Actor Context Report by Attacker Username	This report is used by the system to show activity related to an actor based on the ActorByAttackerUserName global variable.
Actor Context Report by Custom Fields	This report is used by the system to show activity related to an actor based on the ActorByCustomFields global variable.
Actor Context Report by Target Username	This report is used by the system to show activity related to an actor based on the ActorByTargetUserName global variable.

For details about modifying reports, see [“Defining Report Settings” on page 387](#).

Queries

[/All Queries/ArcSight System/Core/Actor Context Report/](#)

Query	Description
Actor Event Count by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.
Actor Event Count by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.
Actor Event Count by Custom Fields	This query shows activity related to an actor based on the AccountByCustomFields global variable.

Query	Description
Actor Event Count by Target Username	This query shows activity related to an actor based on the AccountByTargetUserName global variable.
Actor Events by Account ID	This query shows activity related to an actor based on the ActorByAccountID global variable.
Actor Events by Attacker Username	This query shows activity related to an actor based on the ActorByAttackerUserName global variable.
Actor Events by Custom Fields	This query shows activity related to an actor based on the ActorByCustomFields global variable.
Actor Events by Target Username	This query shows activity related to an actor based on the ActorByTargetUserName global variable.
Actor Information	This query shows activity related to an actor.

For details about working with queries, see [“Defining Query Settings” on page 357](#).

Report Template

[/All Report Templates/ArcSight System/](#)

Report	Description
Actor Context Report	This report template is used by the "Actor Context Report".

For details about working with report templates, see [“Designing Custom Templates” on page 338](#).

Creating and Editing Actors for Testing Purposes

For testing purposes, you can create an actor from scratch using ESM Console resources, or edit an existing one. If you are manually creating actors, manually enter data in the fields you are interested in tracking.

In a production situation, the Actor Model Import connector automatically populates the actor attributes it has been configured to send based on values set at the source IDM. The IDM may not use or store data for every field. To learn more about the values the Actor Model Import connector can be configured to send, see the Actor Model Import connector documentation for your IDM system, for example, the SmartConnector™ Configuration Guide for Microsoft Active Directory Actor Model.

Important points to consider about making manual changes to actors

If you are creating, editing, or deleting an existing actor that IDM sent through the Actor Model Import Connector, you should first consider the following points:

- Actors you create using the ESM Console are not sent back to the IDM. The flow of data is one way from the IDM through the connector.
- Any changes you want to persist to the IDM should be made at the IDM. Any new actor information will be automatically imported at the next scheduled Actor Model Import connector connection.
- If you made manual changes in the ESM Console to actors imported from the IDM, these changes will be overwritten the next time the Actor Model Import connector sends updated data for the same actors.


- If you manually deleted an actor attribute, that attribute will not be updated by a subsequent update from the Actor Model Import connector, unless the connector report includes an updated value for the very attribute that was deleted.
- You should be careful about using the ESM Console to delete actors sent by the IDM, especially if the actors still exist in the IDM, because it is possible that the actor will not be updated during a subsequent import.

Creating Actors for Testing Purposes

Before proceeding, review the information in [“Important points to consider about making manual changes to actors” on page 262](#).

To test the process of creating an actor using ESM Console tools:

- 1 In the Navigator panel, go to **Actors**. Right-click the **All Actors** group (or any group under **All Actors**) and select **New Actor** to launch the Actors editor.

You can also launch the Actors editor by going to **File > New > Actor**, or by clicking the New Resource icon () and selecting **Actor**. If you used the File > New > Actor menu option, the actor will appear in the Unassigned folder. Later, you can move the unassigned actor to an existing group.
- 2 In the Actor Editor in the Inspect/Edit panel, enter the following values and click **OK** to save the actor and close the editor (click **Apply** to save the actor and keep the editor open).
 - a In the Actor section of the Attributes tab, enter values for the required fields, UUID and Full Name. Enter any other relevant attributes. All attributes are treated as data type **string**. Use the scroll bar to see all the Actor attributes.
 - b In the *Account_Attributes* table, add all the unique account IDs attributed to this user by the various user authentication data stores relevant to this user.



Completing the Account_Attributes Table

- In a production environment where the IDM sends data through an Actor Model Import connector, this table will be automatically populated with the user account ID and authenticator values the Actor Model Import connector is configured to send.
- For tips about tools to use to find user account IDs and authenticator information, see [“Configuring Actors \(for Administrators\)” on page 245](#).
- In a test situation, or any situation where an actor has been added manually using ESM Console tools, you must populate the account attributes you are interested in tracking.

- Click the Add icon () to make the fields editable.

In the *Authenticator* column, enter an identifier for the user authentication data store, for example, **Active Directory: mycompany.com**. This is a friendly name that will help admins and other users identify which data store is the authentication source.

In the *Account ID* column, enter the user's account ID used in that authentication data store, for example, **john_doe**, **jdoe**, or **john.d**.


With each entry, the next set of fields becomes editable. Add as many data store authenticators and account IDs as are relevant. For example, an entry for an Active Directory authenticator could be **Active Directory:**

[companyname.com](#). Following is an example of a completed Account_Attributes table:

(Description)

Account Attributes + x

Authenticator	Account ID
Oracle	meerkat
MS Windows	jmeerkat
MS Exchange Server	jmeerkat@jaygroup.com

- To remove an entry, click anywhere on the row you want to delete and click the Delete icon ().
- c** In the *Role_Attributes* table, add all the unique roles attributed to this user and their type.



Completing the Role_Attributes Table

- In a production environment where the IDM sends data through an Actor Model Import connector, this table is automatically populated with the user role values the Actor Model Import connector is configured to send.
- In a test situation, or any situation where an actor has been added manually using ESM Console tools, you must populate the role attributes you are interested in tracking.

- Click the Add icon () to make the fields editable.

In the *Role Name* column, enter a role name, such as [Administrator](#), [User](#), [Approver](#), or [Manager](#).


In the *Resource Name* column, enter the application to which this role applies, for example, [SAP](#), or [Microsoft Exchange](#).

In the *Role Type* column, enter what type of role it is, such as whether it's an IT role or a business role.

With each entry, the next set of fields becomes editable. Add as many user roles as are relevant. Following is an example of a completed Role_Attributes table:

Role Attributes + x

Role Name	Resource Name	Role Type
DBA	Oracle database	IT
Administrator	MS Exchange Server	IT

- To remove an entry, click anywhere on the row you want to delete and click the Delete icon ().

Editing Actors for Testing Purposes

This section contains instructions for how to edit the actors you've created manually for testing purposes. In a production environment, actor changes should be managed automatically through the Actor Model Import connector.

- 1 In the Navigator panel, go to Actors.

- 2 Double-click an actor (or right-click an actor and select **Edit Actor**) to open the Actor Editor in the Inspect/Edit panel.



How to find an actor among thousands of actors

If a group in your actor model contains more than 1,000 members, view the actors using an actors channel. In the Actors navigation panel, right-click the group and select **Show Actors**.

For more about creating and viewing actors in an actors channel, see [“Viewing Actors in an Actor Channel” on page 253](#).

- 3 Refer to the topic [“Viewing Actors in the Actor Editor” on page 251](#) for details about what to enter in the editor’s fields.

Deleting Actors

The actors feature is designed to reflect the latest state of your IDM data as sent through regular updates from the Actor Model Import connector. As such, changes made to actor data in your environment should be made first at the IDM, which is then sent through an update from the Actor Model Import connector.

If you delete a user at the IDM, the actor remains in the actor model, and its status is updated to “Deleted in IDM.”

- To delete an actor from the actor model permanently, right-click the actor and select **Delete**.
- To delete a group of actors permanently, right-click the actor group and select **Delete**.

Leveraging Actor Data Using Variables

You can create a local or global variable that focuses just on actor base and list fields. This enables you to make a specific value derived from actor data available for use in actor-related resources: actor field sets, actor queries (used both in reports, query viewers, and trends), and actor channels.



ESM v5.0 does not support velocity expressions for actor fields

ESM v5.0 does not support using velocity expressions for actor fields in local or global variables.

Creating an Actor Global Variable

Variables derive particular values from existing data fields. The global variables feature enables you to define your variables only once, and then re-use it in multiple places wherever conditions can be expressed. Global variables work with the actors feature so you can build user correlations.

To create an actor global variable:

- 1 Launch the global variable editor: in the Navigator panel, go to Field Sets. On the Fields & Global Variables tab, right-click a group and select **New Global Variable**.
- 2 In the Attributes tab, give the global variable a name, and specify **Actor Global Variable** as the variable type.

For details about the fields in the Global Variable Editor Attributes tab, see [“Global Variable Editor: Attributes Tab” on page 479](#).

- 3 In the Parameters tab, specify the parameters you want to set for the actor global variable.
 - a In the Function field, select a category, then a function appropriate for the data you want to extract from the actor fields.
 - b In the Arguments section, select the field(s) or resource(s) to which you want to apply the function. Enter the other relevant arguments for that function.
 - c To test the result returned by the parameters you selected, enter test value(s) and click **Calculate** to test the results of the actor global variable.
- 4 In the Local Variables tab, you can optionally add a local variable to the actor global variable, which will extract a value from a field that you want to use in the overall actor global variable.

For details about how to create a global variable using the global variable editor, see [“Creating a Global Variable” on page 478](#).

For details about the functions available to local and global variables, see [“Variables” on page 1006](#).

Creating an Actor-Based Variable in Another Resource

Actor-based variables are only applicable to Actor-based resources. You can add a local variable based on an actor field to the following resources:

- Active channels
- Field sets
- Global variables
- Queries (available to reports, trends, and query viewers)

To create actor-based local variables:

- 1 In the resource editor Local Variables tab, click **Add**.
- 2 In the Add Local Variable dialog:
 - a Enter a name for the local variable
 - b Select a function that is compatible with the actor field whose values you want to leverage in the variable
 - c In the Arguments section, select fields and add values relevant to the actor data you want to leverage
 - d In the Preview section, enter test value(s) and click **Calculate** to test the results of the actor global variable.
 - e Click **OK**.

Creating and Using Category Models

Once you have actor information created, you can make logical groupings to represent relationships among actors and actor attributes using category models.

Category models can reflect direct actor relationships, such as reporting hierarchies, or relationships between actors who share common attributes, such as actors in a particular location. For reporting hierarchies, your model can consist of a top-to-bottom structure (by

Manager), or its reverse (by Assistant). Category models can also reflect relationships between actors using custom attributes defined by the user.

You can use category models to visualize these relationships, then leverage the data gathered in them using the [HasRelationship](#) function in local and global variables.

Memory Recommendations for Using Category Models

Category models can be resource intensive on run-time processing memory, depending on the size of your actor model and the nature of the relationships you are modeling. For best results, adjust Java Heap Memory Size in the ESM Console setup script to at least 1 GB.

To adjust the Java Heap Memory Size on the ESM Console:

- 1 If running, close the ESM Console.
- 2 In the directory `<ARCSIGHT_HOME>/bin/scripts/`, make a backup of the ESM Console startup script file:
 - ◆ Windows: `console.bat`
 - ◆ Unix: `console.sh`
- 3 Open the Console startup file (`console.bat` or `console.sh`) in a text editor, and change the default maximum heap size value from `-Xmx512m` to `-Xms1024m`.

For example (value to change is highlighted):

Windows: Change the line

```
set ARCSIGHT_JVM_OPTIONS=-Xms64m -Xmx512m -XX:MaxPermSize=84m -
to
```

```
set ARCSIGHT_JVM_OPTIONS=-Xms64m -Xmx1024m -XX:MaxPermSize=84m -
```

Unix: Change the line

```
ARCSIGHT_JVM_OPTIONS="-Xms32m -Xmx512m -XX:MaxPermSize=84m "
to
```

```
ARCSIGHT_JVM_OPTIONS="-Xms32m -Xmx1024m -XX:MaxPermSize=84m "
```

- 4 Save the updated Console startup file.
- 5 Restart the ESM Console.

Creating Category Models

You can create three types of category models depending on the type of relationships you want to represent:

- **Actor-to-actor.** Actor-to actor category models establish direct or indirect relationships between actors themselves, such as reporting hierarchies. This category model is also called a dual-field category model.
- **Model by actor attributes.** Actor attribute category models are a way to group actors who share one base actor attribute in common, such as location, department, or country. This category model is also called a single-field category model.
- **Model by user-defined attributes.** User-defined category models are a way to group actors who share one or more attributes that are outside of the schema, for example, users who come in on Saturdays, users who play racquetball, or users who

take public transportation. This category model is also called a manually-created category model.



Manually-created category models will not be included in an export of the actor resource. For more information about exporting resources, see [“Creating Packages” on page 687](#).

To create a category model:

- 1 In the Navigator panel, go to Actors and click the **Category Models** tab.
- 2 Right-click an existing group, such as Public, and select **New Category Model**.
- 3 In the Category Model Editor in the Inspect/Edit panel, name the category model, select its type, and select the field(s) by which you want it to model. For details about what fields to populate for which type of category model, see the following topics:
 - ◆ [“Creating Actor-to-Actor Category Models” on page 268](#)
 - ◆ [“Creating Actor Attribute Category Models” on page 270](#)
 - ◆ [“Creating User-Defined Category Models” on page 272](#)
- 4 Depending on the type of category model you create, use the Data tab to view the members of the category model, or use the Attributes tab to define the attributes by which you want to model users.
- 5 Click **OK** to save the category model and close the editor, or click **Apply** to save the category model and leave the editor open.

Creating Actor-to-Actor Category Models

Actor-to-actor category models establish direct or indirect relationships between actors themselves, such as reporting hierarchies. The categorization is based on what data you want to track using the Parent Field, and how to look up the actors for populating the model through the Child Field.

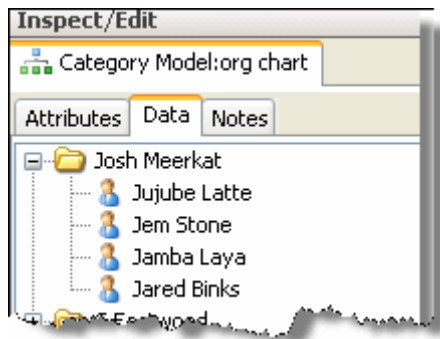
When creating actor-to-actor category models, enter the following values in the Attributes tab of the Category Model editor:

Attribute Field	Description
Name	Enter a name for the category model. This name will appear in pick lists and wherever category models can be referenced in conditions. Spaces, underscores, and hyphens are allowed.
Create From	Use the Create From field to select the type of category model. For an actor-to-actor category model, select Actor Fields . After the category model is saved, this field becomes read-only.
Field Set	By default, the system uses the Actor Base field set, because only actor-based fields are relevant for category models. You can also select a user-defined actor field set. The field set selected here defines the fields available for the parent and child field choices and defines the columns available for the table below the graph view (for more about the graph view, see “Viewing Category Models in Graphs” on page 275). After the category model is saved, this field becomes read-only.

Attribute Field	Description
Relationship Name	<p>Use this optional field to describe the relationship you want the category model to show.</p> <p>For example, if you want the category model to show managers and their direct reports, you could enter Direct Report to identify the relationship between the manager and the direct report.</p> <p>The value you enter here appears as a mouse-over tool tip on the relationship lines that connect the parent and child fields in the category model graph view.</p>
Parent Field	<p>This field enables you to establish which Actor data field to use to build a hierarchy of relationships.</p> <p>From the drop-down menu, select Manager or Assistant as the parent field.</p> <p>For example, if you are building an actor-to-actor category model that shows top-down reporting relationships, select Manager to produce a category model of every manager identified in your IDM data. The resulting model will display managers at the top.</p> <p>A Parent Field of Assistant will display an inverted hierarchy with lower-level actors appearing at the top.</p> <p>Note: Only the Manager and Assistant fields are supported for the Parent Field when building actor-to-actor category models.</p>
Child Field	<p>In Child Field, the UUID (or DN, if used) is the unique identifier the system uses to look up the actors and populate members who are related to Parent Field.</p> <p>From the drop-down menu, select UUID or DN as the unique identifier to correctly determine who the members are in a particular structure. (DN is specific to the Active Directory IDM.)</p> <p>Note: Only the UUID and DN fields are supported in the Child Field when building actor-to-actor category models.</p> <p>For example, if you selected Manager in the Parent field, and the actor's Manager field is populated by a UUID value, then select UUID as the Child Field here. Likewise, if the actor's Manager field is populated by the DN value, then select DN here. The following example scenario explains how the category model is created based on the Parent Field and Child Field values.</p> <p>Example scenario:</p> <p>Let's say you are building an organizational chart with managers at the top node.</p> <ul style="list-style-type: none"> • Actor A has a UUID = 1234. Actor A is the manager of Actor B and Actor C. • Actor B and Actor C's values for Manager = 1234, which corresponds to Actor A's UUID. • In building this category model, use Parent Field = Manager and Child Field = UUID. The Manager looks up Actor B and Actor C's Manager field, which has Actor A's UUID. It then creates Actor B and Actor C under Actor A in the resulting category model.
Delimiter	<p>The delimiter field does not apply to the actor-to-actor category model.</p>

For a description of the data that goes in the Common section, see [“Common Resource Attribute Fields” on page 684](#).

Use the Data tab to view the members of the group in tree form.



You can also view the group hierarchy in a resource graph. Right-click the category model and select **View Category Model**. For details, see [“Viewing Category Models in Graphs” on page 275](#).

Creating Actor Attribute Category Models

Actor attribute category models are a way to group actors who share one base actor attribute in common, such as location, country, or any actor attribute that can possibly have a hierarchical groupings.

When creating actor attribute category models, enter the following values in the Attributes tab of the Category Model editor:

Attribute Field	Description
Name	Enter a name for the category model. This name appears in pick lists and wherever category models can be referenced in conditions. Spaces, underscores, and hyphens are allowed.
Create From	Use the Create From field to select the type of category model. For an actor attribute category model, select Single Actor Field . After the category model is saved, this field becomes read-only.
Field Set	By default, the system uses the Actor Base field set, since only actor-based fields are relevant for category models. You can also select a user-defined actor field set. The field set selected here defines the fields available for the parent and child field choices, and also defines the columns available for the table below the graph view (for more about the graph view, see “Viewing Category Models in Graphs” on page 275). After the category model is saved, this field becomes read-only.

Attribute Field	Description
Relationship Name	<p>Use this optional field to describe the relationship you want the category model to show.</p> <p>For example, if you want the category model to show employees by location, you could enter Location to identify the relationship between the actor and the group he is associated with.</p> <p>The value you enter here appears as a mouse-over tool tip on the relationship lines that connect the actor and the attribute they're being modeled by in the category model graph view.</p>
Parent Field	<p>From the drop-down menu, select the attribute that you want to model the users by.</p> <p>For example, if you are building an actor attribute category model that categorizes all the actors by their location, select Location.</p>
Child Field	<p>The child field does not apply to single-actor field category models.</p>
Delimiter	<p>Enter the delimiter you used in the actors' Delimiter attribute. The default is the forward slash (/).</p> <p>The Delimiter is used to denote the hierarchy of values, from top to bottom, in the attribute you are tracking in Parent Field.</p> <p>Example scenario:</p> <ul style="list-style-type: none"> Actor A has Location = /USA Actor B has Location = /USA/California/Mountain View Actor C has Location = /USA/California/Mountain View <p>The delimiter used to denote a hierarchy is /, therefore, in the category model editor, set Delimiter = /.</p> <p>The resulting resource graph produced by these values has three levels: USA, California, and Mountain View.</p>



A combination of delimiters builds a hierarchy if one is found

If the attribute from which you are creating the category model contains multiple values with more than one type of delimiter, for example, a URL, such as

`http://www.arcsight.com,`

include all the delimiter characters in the Delimiter field. For example:

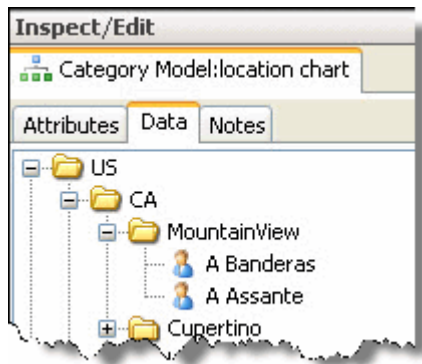
`://.`

This indicates that the dot (.) is the delimiter used to separate all the elements of the URL into the following hierarchy:

`http`
`www`
`arcsight`
`com`

For a description of the data that goes in the Common section, see ["Common Resource Attribute Fields" on page 684](#).

Use the Data tab to view the members of the group in tree form.



In the example above, the value for the two actors' Location field are entered as /US/CA/MountainView.

You can also view the group hierarchy in a resource graph. Right-click the category model and select **View Category Model**. For details, see ["Viewing Category Models in Graphs" on page 275](#).

Creating User-Defined Category Models

User-defined (or manually-created) category models are a way to group actors who share one or more attributes that are outside of the actor schema, for example, users who come in on Saturdays, users who play racquetball, or users who take public transportation.

The user-defined groupings can be created in hierarchical fashion. For example, users to who take public transportation can be further classified into those who take the train, those who take the bus, and those who take a ferry. For user-defined category models, the hierarchy evaluation is based on the actor's UUID value.

- 1 When creating category models based on user-defined attributes, enter the following values in the Attributes tab of the Category Model editor:

Attribute Field	Description
Name	Enter a name for the category model. This name will appear in pick lists and wherever category models can be referenced in conditions. Spaces, underscores, and hyphens are OK.
Create From	Use the Create From field to select the type of category model. For a user-defined attribute category model, select Manually . After the category model is saved, this field becomes read-only.
Field Set	By default, the system uses the Actor Base field set, since only actor-based fields are relevant for category models. You can also select a user-defined actor field set. The field set selected here defines the columns available for the table below the graph view (for more about the graph view, see "Viewing Category Models in Graphs" on page 275). After the category model is saved, this field becomes read-only.

Attribute Field	Description
Relationship Name	<p>Use this optional field to describe the relationship you want the category model to show.</p> <p>For example, if you want the category model to show actors who take different types of public transportation, you could enter Commutes By to identify the relationship between the actor and the group he is associated with.</p> <p>The value you enter here appears as a mouse-over tool tip on the relationship lines that connect the actor and the attribute they're being modeled by in the category model graph view.</p>

Parent Field, Child Field, and Delimiter don't apply to this category model.

For a description of what to enter in the Common fields, see ["Common Resource Attribute Fields" on page 684](#).

- 2 Use the Data tab to define the attributes by which you want to group users, and to add actors to the category model.

For example, if you want to create a hierarchy of users that take different types of public transportation, do the following:

- a In the Category Model editor at the Data tab, click **New Group**.

The name of the new group is automatically highlighted so you can give it a relevant name, for example, **Public Transportation Commuters**. Press the Enter key to save the new name.

To rename a group at any time, right-click the group and select **Rename**; or click the **Rename** button. After entering the new name, press Enter.

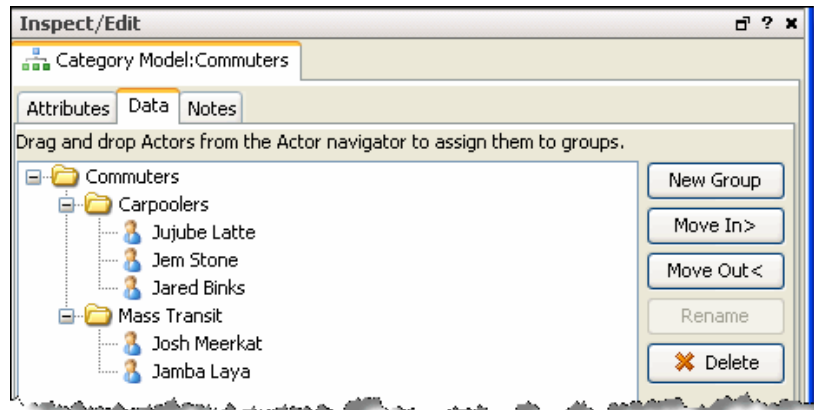
- b Add actors to the category model group. You can add actors from the Navigator panel and from an actors channel in the Viewer panel.

From the Navigator panel: Drag and drop actors from the navigator panel into the category model group. You can drag and drop multiple actors at a time.

From an Actors channel in the Viewer panel: You can view any group of actors in an actors channel in the Viewer panel. An actors channel is the only way to view groups with 1,000 or more members. Select the actors you want to add to the category model group, right-click, and select **Add to Category Model**.

- To select multiple actors in a row, use **shift + click**.
 - To select multiple actors out of sequence, use **ctrl + click**.
- c To create a sub-group of the first group, such as Train Commuters and Bus Commuters, click **New Group** again. You can also right-click the existing group (or right-click anywhere in the editor panel and select **New Group**).
 - By default, the new group is made a child of the first group.
 - You can make the new group a parent group by dragging and dropping it to the desired location, or click **Move Out** (or right-click the group and select **Move Out**).

- You can make a parent group the child of another by dragging and dropping the group to the desired location, or click **Move In** (or right-click the group and select **Move In**).



- There is no limit to the number of parent nodes you can have, nor a limit on the number of child nodes
- 3 View the category model in a resource graph. Right-click the category model and select **View Category Model**. For more about viewing category models as graphs, see [“Viewing Category Models in Graphs” on page 275](#).

Editing a Category Model

To edit an existing category model:

- 1 In the Navigator panel, double-click the category model to open the Category Model editor. Or right-click the category model and select **Edit Category Model**.
- 2 Make edits to the category model attributes, click **OK** to save, and close the editor. Click **Apply** to save the category model and leave the editor open.

For details about the category model fields for the different types of category models, see [“Creating and Using Category Models” on page 266](#).

Moving or Copying a Category Model

You can move or copy a category model the same way you move or copy any resource.

To move or copy a category model:

- 1 In the category model resource tree, navigate to an asset and drag and drop it into another group.
- 2 Choose **Move** to move the category model, **Copy** to make a separate copy of the category model, or **Link** to create a copy of the category model that is linked to the original category model.

If you choose **Copy**, you create a separate copy of the category model that will not be affected when the original category model is edited. If you choose **Link**, you create a copy of the category model that is linked to the original asset. Therefore, if you edit a linked category model, whether the original or the copy, all links are edited as well. When deleting linked category models, you can either delete the selected category model or all linked category model copies.

Deleting a Category Model

To delete a category model:

- 1 In the Navigator panel, right-click the category model and select **Delete Category Model**.
- 2 At the confirmation dialog box, click **Delete**.

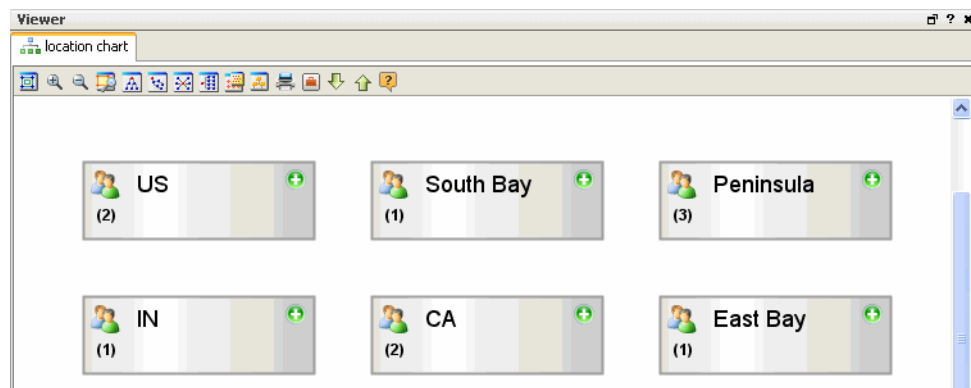
Viewing Category Models in Graphs

To fully visualize a category model, view it as a graph. Category model graphs are very similar to resource graphs, only instead of modeling relationships among all resources, category model graphs render relationships among attributes of actor resources.

To view category model graph:

In the Navigator panel, right-click a category model and select **View Category Model**.



The Viewer panel displays the graph. By default, all top-level nodes are displayed in collapsed form.

















Working with Category Model Graphs

The category model graphs are displayed on the Viewer panel. As with all resource graphs, There is a set of command buttons at the top of the view and a parallel set of commands available by right-clicking the graph itself.

The table below shows the Category Model Toolbar Buttons and Right-click Commands

Command	Button	Description
Fit Content		Size the model to the available display space.
Zoom In / Zoom Out		<p>Increase or decrease the size of the displayed model.</p> <p>The system is optimized to show the entire category model graph in the available space of the viewer panel. If a category model has many nodes and members, its elements can appear very small. To zoom in, click the zoom in icon (+ magnifying glass). To zoom out, click the zoom out icon (- magnifying glass).</p>

Command	Button	Description
Zoom Selected		Zoom in on a selected portion of the model.
Hierarchic Layout		Present nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing event relationships that have a common root.
Organic Layout		Display nodes in an arrangement based on minimum edge length, which tends to cluster nodes that relate to a common node. Likewise, node clusters with nodes in common will also tend to group together.
Circular Layout		Position nodes in hub-and-spoke arrangements with each node radiating edges to, or receiving edges from, the nodes with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout instead.
Orthogonal Layout		Arrange nodes on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are very useful for clearly tracing connections and identifying node clusters.
Overview		Open a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.
Hierarchy Tree		Open a complete list of the nodes as seen on the category model editor's Data tab. Click a node in the list to scroll to that node in the main view.
Print		Print the displayed model.
Export to JPEG		Create and save a JPEG-format copy of the current image.
Add Graph View to Case		Add the current graph view to a case you select. Choosing this option opens the Case Selector dialog, where you can browse cases. Select a case to which to add the current graph view and click OK on the Case Selector dialog. The graph view is added to the selected case as an attachment, accessible on the Attachments tab in the case editor for that case.
Help		Display the relevant ESM Console online Help topic.
Expand One Level/ Collapse One level		Expand <i>all</i> collapsed nodes to display nodes one level below. Collapse one level of all expanded nodes. This feature works only if any node was not manually expanded or collapsed previously.

Command	Button	Description
Plus (+)/Minus (-)		Expand or collapse a single node on the graph.
Increase/ Decrease Node to Node Distance		Increase or decrease distances between nodes by small increments. This feature works on expanded nodes.
Single-person icon		Denotes an individual actor.
Two-person icon		Denotes a group of actors.

Every time a node is expanded or collapsed, the entire category model graph re-sizes to fit into the available space of the viewer panel



Actors with no value for the field used to define the category model do not appear in the model

If an actor does not have a value for the field that was used to build the category model, that actor will not appear in the model.

For example, if you build the category model on the Office attribute, and if an actor does not have a value in the Office field, that actor is not represented in the category model view.

For more about resource graphs, see [“Visualizing Resources” on page 674](#).

Leveraging Category Model Data Using Variables

You can use the [HasRelationship](#) function in local and global variables to leverage data represented in a category model.

Local and global variables are available in resources that use conditions: active channels, filters, rules, data monitors, and queries. Local variables are available for use only in the resource for which the variables are defined; global variables can be re-used in multiple condition-based resources.

To leverage data represented by a category model in a variable:

1 Launch the variable editor.

- ◆ **Local variable:** From the channel, filter, rule, query, or data monitor editor, click the Local Variable tab. Click **Add** to launch the *Add Local Variable* dialog box.
- ◆ **Global variable:** In the Navigator panel, go to Field Sets. On the Fields & Global Variables tab, right-click a group and select **New Global Variable**.

In the Attributes tab, specify **Event** as the variable type.

For details about the fields in the Global Variable Editor Attributes tab, see [“Global Variable Editor: Attributes Tab” on page 479](#).

- 2 Select the function category **Category Model** and the [HasRelationship](#) function. In the Arguments section, select the category model whose data you want to leverage and specify the parent and child field or group.

Field	Description
Name	When creating local variable based on category model data, provide a friendly name for the variable. This name is used anywhere the variable is applied (CCE, resource field selectors).
Function	From the Function drop-down menu: <ol style="list-style-type: none"> 1 Select the category Category Model. 2 Select the function HasRelationship. 3 Click OK.
Category Model	Browse to and select the category model from which you want to leverage data.
Parent Field or Group	Navigate to the field or single-value variable you want to use as the parent. Use the Field/Group drop-down to indicate whether the parent is a field (single attribute) or a group.
Child Field or Group	Navigate to the field or single-value variable you want to use as the child.
Inherit All Related Actors	Select true for the variable to consider all the actors in a related hierarchy. For example, VP > Director > Manager > direct report . Select false for the variable to consider only direct relationships between actors. For example, Manager > direct report .

For details about working with the Global Variable editor, see [“Creating a Global Variable” on page 478](#).

For details about local variables and the functions available to both local and global variables, see [“Variables” on page 1006](#).

Actor-Related Resources Provided in Standard Content

Standard content includes basic resources that provide infrastructure support for the Actor Resource Framework, global variables for extracting specific data from actor fields, and basic resources that track statistics when actors are added, updated, and deleted.

For an overview of the infrastructure that supports the actors feature, see [“How the Actors Feature Works” on page 241](#).

For a list of the audit events generated by actor change events, see [Table 31-14, “Audit Events on Actor Category,” on page 814](#).

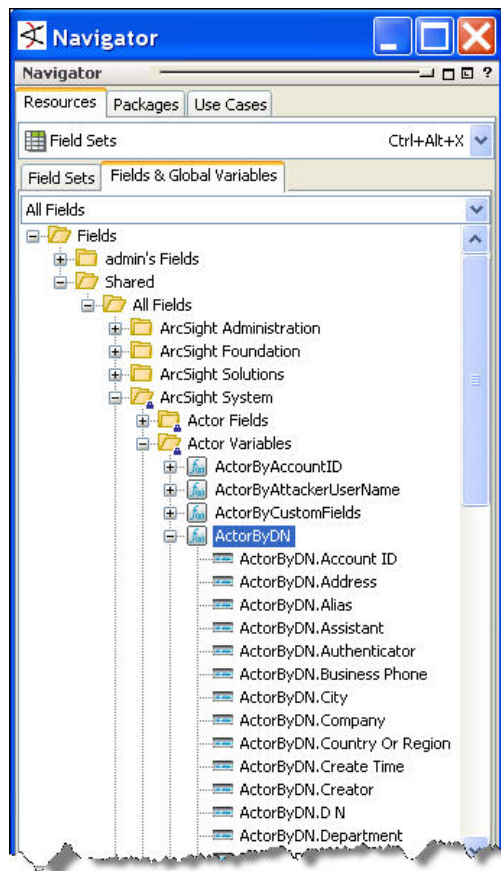
Actor Resource Framework Global Variables

The Actor Resource Framework provides a series of actor global variables and uses the following variables to identify an actor from data contained in the base actor fields and in

elements of the Actor Resource Framework. These global variables are located in **Field Sets > Fields & Global Variables** [All Fields/ArcSight System/Actor Variables](#).

Actor Variable	Description
ActorByAccountID	This variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker or target user name, with preference to the attacker user name.
ActorByAttackerUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the attacker user name.
ActorByCustomFields	This variable attempts to retrieve actor information from events where the authenticator information is maintained in device custom strings. It works similarly to the ActorByAccountID variable, but maps Device Custom String 1 to the vendor field, Device Custom String 2 to the product field, and Device Custom String 3 should hold the Account ID.
ActorByDN	This Actor global variable looks for a DN (Distinguished Name) in Device Custom String1, and retrieves the Actor with that DN.
ActorByTargetUserName	This variable maps the account information in an event with an actor. The account information consists of the device vendor and product, and information derived from the target user name.
ActorByUUID	This Actor global variable looks for a UUID in Device Custom String1, and retrieves the Actor with that UUID.

When expanded in the Navigator panel, the global variable lists all the fields produced as a result of the global variable conditions.



Although these global variables are leveraged by the Actor Resource Framework, you can also select any of these global variables wherever global variables can be selected: active channels, filters, report queries, rules, field sets, and data monitors.

The Actor Resource Framework uses these variables to identify actors, and you can also use these global variables in a condition, or as a field selection. For example, a query could use one of the Actor Resource Framework global variables to get the full name of an actor related to the selected events, or the actor field **Full Name** could be used as a display field in a data monitor.

The Actor Resource Framework global variables rely on an the actor's account and identity information available in the actor resource and in the look-up tables provided the ArcSight Actor Framework. To establish an actor's identity, the Actor Resource Framework global variables perform the following steps:

- 1 Selects a field from an event that contains information that can be tied to a specific actor.
- 2 Determines the Authenticator using the event's agent address and zone, and device vendor and product information.
- 3 Combines the Authenticator with the data from the event field (from step 1) to look up the actor data:
 - a Uses the Authenticator and event field data as keys to get the value representing the actor from the Actor Resource Framework.

- b** Returns the information as the returned value of the global variable based on information stored in the Actor Resource Framework.

As a user, you can use an Actor Resource Framework global variable in a condition (for example, `ActorByAccountID.Manager = John Doe`), or as a display value in a query, data monitor, or to set an event field action in a rule (for example, select `getActorByEmail.fullName, targetAssetZoneName, targetAssetName, name, count`).

For instructions about how to add global variables to a resource, see [“Adding a Global Variable to a Resource” on page 484](#), and [“Adding or Removing Global Variables Using the CCE” on page 857](#) in the reference topic [“Common Conditions Editor \(CCE\)” on page 846](#).

Tracking Actor Configuration Changes Using Standard Content

The actor configuration changes resources show different configuration changes made to the actor resources using an active channel, dashboards and data monitors, query viewers, and reports. The changes can be initiated either by edits made directly to an actor resource, or updates received from an Actor Model Import connector.

Actor Configuration Changes: Monitoring

You can use these resources to monitor actor configuration changes.

Resource	Name	Description, Location
Active Channel	Actor Audit Events	This active channel displays events related to changes to data in the actor resources. All Active Channels/ArcSight Administration/ESM/Configuration Changes/Actors
Dashboard	Actor Administration	This dashboard shows the "Actor Authenticators" query viewer. All Dashboards/ArcSight Administration/ ESM/Configuration Changes/Actors
Dashboard	Actor Change Log	This dashboard shows an overview of Actor resource changes based on the Actor Change Overview and Actor Change Log query viewers. All Dashboards/ ArcSight Administration/ ESM/ Configuration Changes/Actors

Resource	Name	Description, Location
Data monitor	Actor Change Log	<p>This data monitor displays the most recent events related to changes in actors. These changes include creation, deletion, and modification of single-valued and multi-valued parameters of actor resources.</p> <p>Note: This Data Monitor will not populate all values when running in Turbo Mode Fastest!</p> <p>All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Log</p>
Data monitor	Actor Change Overview	<p>This data monitor shows an overview of the ArcSight Actor resource changes. The data monitor shows the total number of changes by type for the last hour.</p> <p>All Data Monitors/ArcSight Administration/ESM/Configuration Changes/Actors/Actor Change Overview</p>

Actor Configuration Changes: Query Viewers

You can use these query viewers directly to monitor actor configuration changes, and they are also used by the actor configuration dashboards and reports. These query viewers are all located in [All Query Viewers/ArcSight Administration/ESM/Configuration Changes/Actors](#).

The queries upon which these query viewers are based can be found in **Reports > Queries** [All Queries/ArcSight Administration/ESM/Configuration Changes/Actors](#).

Query Viewer Name	Description, Location
Actor Authenticators	This query viewer shows the list of all the authenticators for actors.
Actor Configuration Changes	<p>This query viewer displays all audit events resulting from changes to Actor resources.</p> <p>Note: This will not populate all values when running in Turbo Mode Fastest!</p>
Actor Full Name and Email Changes	This query viewer shows information from Actor audit events resulting from changes to an actor's Full Name or Email attribute, showing the old and new information.
Actor Manager and Department Changes	This query viewer shows information from Actor audit events resulting from changes to an actor's Department or Manager attribute, showing the old and new information.
Actor Title and Status Changes	This query viewer shows information from Actor audit events resulting from changes to an actor's Title or Status attribute, showing the old and new information.

Query Viewer Name	Description, Location
Actors Created	This query viewer displays all the audit events for actors that have been created. Note: This will not populate all values when running in Turbo Mode Fastest!
Actors Deleted	This query viewer displays audit events for actors that have been deleted. Note: This will not populate all values when running in Turbo Mode Fastest!
Actor Updated	This query viewer displays audit events for actors that have been updated. Note: This Report will not populate all values when running in Turbo Mode Fastest!
IDM Deletions of Actors	This query viewer shows a list of actors that have been deleted by the IDM. The query will not show actors that you deleted.

Actor Configuration Changes: Reports

These reports leverage queries to report about specific types of changes made to actor resources, and by whom the changes were made. These reports are all located in [All Reports/ArcSight Administration/ESM/Configuration Changes/Actors](#).

The queries upon which these query viewers are based can be found in **Reports > Queries** [All Queries/ArcSight Administration/ESM/Configuration Changes/Actors](#).

Name	Description, Location
Actor Full Name and Email Changes	This report shows information from Actor audit events resulting from changes to an actor's Full Name or Email attribute, showing the old and new information.
Actor Manager and Department Changes	This report shows information from Actor audit events resulting from changes to an actor's Department or Manager attribute, showing the old and new information.
Actor Title and Status Changes	This report shows information from Actor audit events resulting from changes to an actor's Title or Status attribute, showing the old and new information.
Configuration Changes by Type	This report shows recent ArcSight Actor configuration changes in a table. The table lists all the changes, grouped by type and user, and sorts them chronologically.
Configuration Changes by User	This report shows recent ArcSight Actor configuration changes in a table. The table lists all the changes, grouped by user and type, and sorts them chronologically.
Created	This report shows the list of all the actors created on the previous day. Note: This Report will not populate all values when running in Turbo Mode Fastest!

Name	Description, Location
Deleted	This report displays audit event information for actors that have been deleted. Note: This does not populate all values when running in Turbo Mode Fastest!
IDM Deletions of Actors	This report shows a list of actors that have been deleted by the IDM. The report does not show actors that you deleted.
Updated	This report shows the list of all the actors updated on the previous day. Note: This Report does not populate all values when running in Turbo Mode Fastest!

Actor Configuration Changes: Global Variables

The actor configuration changes content leverages a series of global variables that extract particular values out of actor fields that enable the resource to focus on the actor change the resource monitors. These global variables are located in **Field Sets > Fields & Global Variables** [All Fields/ArcSight Administration/ESM/Actor](#).

Name	Description, Location
Department New Value	This global variable extracts the new value for the Department in actor update audit events (single-value parameters).
Department Old Value	This global variable extracts the old value for the Department in actor update audit events (single-value parameters).
DN New Value	This global variable extracts the new value for the DN (Distinguished Name) in actor update audit events (single-value parameters).
DN Old Value	This global variable extracts the old value for the DN (Distinguished Name) in actor update audit events (single-value parameters).
Email Address New Value	This global variable extracts the new value for the Email Address in actor update audit events (single-value parameters).
Email Address Old Value	This global variable extracts the old value for the Email Address in actor update audit events (single-value parameters).
Employee Type New Value	This global variable extracts the new value for the Employee Type in actor update audit events (single-value parameters).
Employee Type Old Value	This global variable extracts the old value for the Employee Type in actor update audit events (single-value parameters).
Full Name New Value	This global variable extracts the new value for the Full Name in actor update audit events (single-value parameters).
Full Name Old Value	This global variable extracts the old value for the Full Name in actor update audit events (single-value parameters).

Name	Description, Location
Location New Value	This global variable extracts the new value for the Location in actor update audit events (single-value parameters).
Location Old Value	This global variable extracts the old value for the Location in actor update audit events (single-value parameters).
Manager New Value	This global variable extracts the new value for the Manager in actor update audit events (single-value parameters).
Manager Old Value	This global variable extracts the old value for the Manager in actor update audit events (single-value parameters).
Org New Value	This global variable extracts the new value for the Org in actor update audit events (single-value parameters).
Org Old Value	This global variable extracts the old value for the Org in actor update audit events (single-value parameters).
Status New Value	This global variable extracts the new value for the Status in actor update audit events (single-value parameters).
Status Old Value	This global variable extracts the old value for the Status in actor update audit events (single-value parameters).
Title New Value	This global variable extracts the new value for the Title in actor update audit events (single-value parameters).
Title Old Value	This global variable extracts the old value for the Title in actor update audit events (single-value parameters).

4

Chapter 13

Query Viewers

This topic describes how to define and use query viewers to get high-level summaries about trends, events, other resources, and system health along with drill-down capability in a dynamic viewer.

[“What are Query Viewers?” on page 287](#)
[“Navigating to Query Viewers” on page 289](#)
[“Pre-Built and Custom Query Viewers” on page 289](#)
[“Running Queries and Viewing Results” on page 291](#)
[“Adding Query Viewers to Dashboards” on page 302](#)
[“Making Query Viewer Results Available to ArcSight Web” on page 302](#)
[“Adding Query Viewers as Startup Views” on page 302](#)
[“Generating Reports from Query Viewers” on page 303](#)
[“Defining and Using Baselines” on page 304](#)
[“Customizing Query Viewers” on page 311](#)
[“Editing a Query Viewer” on page 323](#)
[“Deleting a Query Viewer” on page 323](#)
[“Example Queries for Common Scenarios” on page 323](#)

What are Query Viewers?

Query viewers are a type of resource for defining and running SQL queries on other resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results. The query viewer you create displays all the fields and domain fields specified in the query you select (or create) for the query viewer.

You can use query viewers to run the same SQL queries used for reports, and get results quickly. Then, if desired, you can generate a simple report directly from the query viewer results. Full-featured reporting (with queries, trends, and templates) is still offered for more robust reporting requirements (see [“Building Reports” on page 331](#)), but query viewers provide a shortcut to running those same SQL queries apart from reporting. (See also, [“Active Channels or Query Viewers?” on page 138](#).)

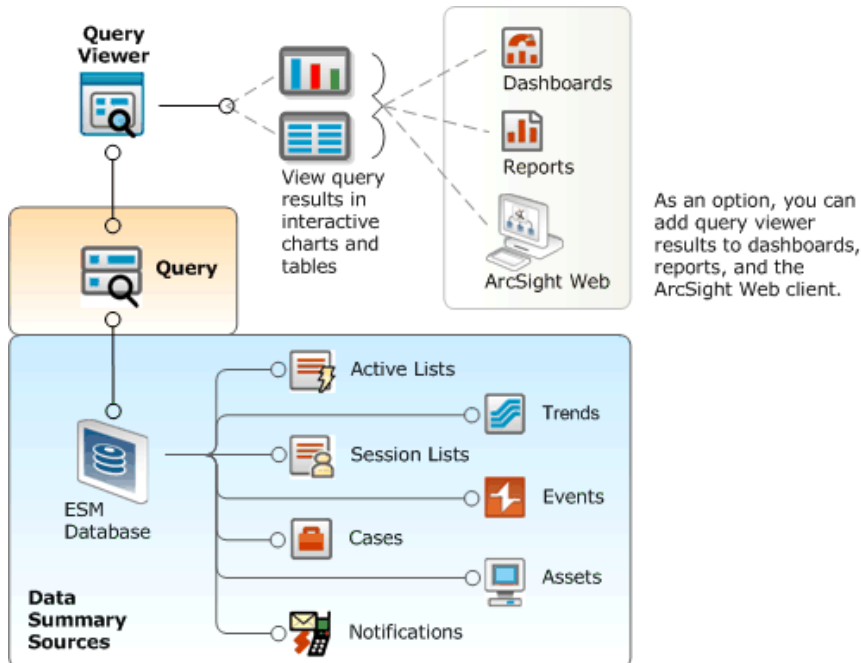
Query viewers provide high-level summaries to monitor system health, reveal trends, and allow for drill-down investigation of all types of resources. Query viewers can work with

trend tables rather than event tables, and so can return results much faster than [Active Channels](#).

The SQL-based summary views and trend analysis in query viewers use aggregation to provide a higher-level perspective than data gleaned from exclusively event-focused active channels and snapshot, limited-range data monitors.

Query viewers offer a way to run queries outside of a full reporting paradigm (where queries and trends are always tied to a particular report). They offer a quick way to run SQL queries on the data sources available to report queries.

Also, you can generate simple reports directly from query viewer results.



Query Viewers leverage an existing report query to run SQL queries on data sources, such as trends, active lists, session lists, assets, cases, events, and notifications. Each query viewer contains a base SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find trends, and performing drill-down investigation on a particular aspect of the result. The results are displayed in interactive charts and tables, which can be added to dashboards and published as reports.

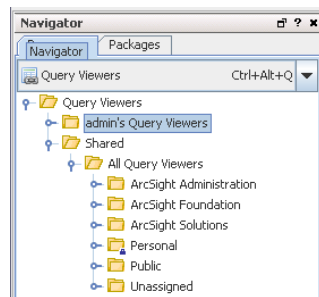
Query viewers provide:

- **A quick way to run SQL queries and trends apart from full-scale reporting.** If you want to run a pre-built SQL query and view results quickly, or build and test several iterations of a custom query, query viewers are an easy way to do it. (You can also generate a simple report directly from a query viewer.)
- **High-level summaries.** For example, using the aggregation provided by queries and trends allows summaries of "interesting things" over the last month, day, or hour.
- **Non-event-based summaries.** Queries can be used to analyze resources other than events (such as assets and cases).
- **Event-based summaries.** Queries can be used to analyze events, and eventually lead to active channels (with drill-down investigation).

- **Baselines.** Analysts can apply a baseline to the information resulting from a particular run of a query viewer. A baseline acts as a reference point against which to compare results of other runs of the same query and highlights the *deltas* (differences) to help identify areas that vary significantly from normal.
- **Drilldown.** Query viewers can provide drilldown investigation into the same or another query viewer for good performance on the next level of results as well. Ultimately, the drilldown can lead to an event channel, where the performance costs are the trade-off for the power of event-based analysis in an active channel. The query viewer author defines the appropriate drilldown paths and levels.
- **Performance.** Query viewers can use trend tables which are typically much smaller than event tables, and can be pre-built with summary views in mind. So, in most cases query viewers can return and display results faster than [Active Channels](#).
- **History.** When based on trends, query viewer result data can be kept for as long as desired and be independent of the event archival process.
- **Flexibility.** ArcSight provides both pre-built query viewers and a resource editor for adding custom query viewers to suit the needs and environment of your organization.
- **Presentation Options.** Query viewer results can be displayed as tables (with baselines, if desired), pie charts, and bar charts, and added to [Dashboards](#) for quick display and monitoring.

Navigating to Query Viewers

In the Navigator panel, select **Query Viewers** resource from the drop-down menu.



Pre-Built and Custom Query Viewers

The Manager to which your Console is connected has pre-built query viewers available for use. At a minimum, you have access to standard content query viewers that ship with ArcSight. You might also have access to custom query viewers provided by content developers for your organization.

Standard Content

ArcSight comes with a set of pre-built query viewers that address common network monitoring and trend analysis scenarios. To access the standard content query viewers, in the Navigator panel select **Query Viewers**, then click to expand the list to **Query Viewers/Shared/All Query Viewers**.

Folders for ArcSight Foundation and ArcSight Administration include the standard content query viewers.

If you have purchased ArcSight Solutions packages, query viewers for those are displayed under ArcSight Solutions.

For information on how to run and use any pre-built query viewer, see [“Running Queries and Viewing Results” on page 291](#), [“Generating Reports from Query Viewers” on page 303](#), and [“Defining and Using Baselines” on page 304](#).

Custom Query Viewers

When administrators or content developers at your organization create custom query viewers, they have the option of sharing these with other administrators and users. So, depending on your role and user permissions, you might have access to:

- query viewers that ship with ArcSight
- custom-built query viewers that other administrators have shared
- your own custom-built query viewers

For information on how to create your own custom query viewers, see [“Customizing Query Viewers” on page 311](#).

Customizing Query Viewers as Needed

You can modify the provided query viewers as needed to get the data you want. Customizing an existing query viewer can range from hiding or showing data fields, changing the sort order inherited from the base query, to adding variables and modifying key fields. These kinds of changes do not affect the base query, only the query viewer.

Once a query viewer is defined to reference a particular base query, that query viewer cannot be changed. If you want to reference a different base query, you need to create a new query viewer. Which brings us to an important point. *Where do you get the base queries you need?* See [“Query Viewers Need Base Queries” on page 290](#) to find out.

inActiveList Conditions for Queries

In a query, you can define an inActiveList condition and map multi-valued attributes to single-valued active list fields. For example, you have an active list that keeps track of roles, where one of the role values can be Normal, Restricted, and Privileged. You can test if an actor has one of these roles through the inActiveList condition. In this scenario, your list has a field called RoleName. You map the actor's role name attribute to this field. Keep in mind that an actor's RoleName attribute is multi-valued because an actor can have multiple roles. Through the inActiveList condition, your query will check if one of the actor's roles is, for example, Privileged.

Query Viewers Need Base Queries

A primary attribute of any query viewer is the SQL query it references and uses. This is the core of the query viewer. If you create the query viewer yourself, you define this as part of the initial query viewer attributes by browsing to and choosing a query from the [Reports/Queries](#) tree. If you are using a pre-defined query viewer, it already references a base query.

Reports, trends, and query viewers are all consumers of SQL queries, which still must be created first in the **Reports** resource **Queries** tab. So, if you don't find a query viewer or query that gives the data view you want, you first need to create a new query in **Reports > Queries**. Then go to the Query Viewers resource to create a new query viewer that references the base query you just created. (For information on creating queries, see [“Building Queries” on page 354](#).)

Running Queries and Viewing Results

To run a query defined in a query viewer, do either of the following:

- Select a query viewer and choose **View Data as...** > *<Display Format>*
Or
- Double-click a query viewer
Double-clicking provides the default view, as defined in the query viewer. For information on how to set the default view, see [related information on page 313](#) in “Query Viewer Attributes” on page 312.

The query runs, and returns results in the Viewer on the current state of the network and event flow.



Chart-style views (Pie and Bar charts) are limited to showing a maximum of 99 rows. This is a hard limit for charts to guarantee readability; it is not user-configurable. Therefore, results in chart views and table views for the same query viewer might not match since table views can accommodate up to 10,000 rows of data in a query result.

Alternatively, you can add the result of a query viewer directly to a dashboard. For information on this, see [“Adding Query Viewers to Dashboards” on page 302](#).

To run queries and view results:

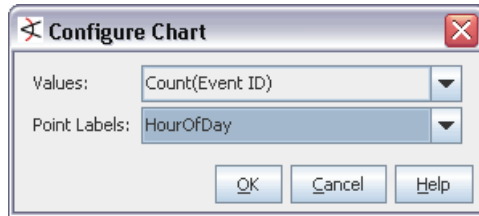
- 1 In the Navigator panel, choose the **Query Viewers** resource.
- 2 Navigate the tree, and select the query viewer you want to run.
- 3 Right-click the selected query viewer and select **View Data as** > *<Display Format>* and choose one of these options:

Results Display Format	Description
Bar Chart	Display query results as a bar chart.
Horizontal Bar Chart	Display query results as a horizontal bar chart.
Pie Chart	Display query results as a pie chart.
Table	Display query results in table format. Note: Baselines can only be applied to or viewed for query results shown in table format. (For more about establishing and using baselines, see “Defining and Using Baselines” on page 304 .)

Details on how to read and manipulate query results for each of these formats is provided.

- 4 If you choose a Table display format, the results are displayed instantly.

If you choose a bar chart or pie chart, you are asked to configure the chart display in the Configure Chart dialog.



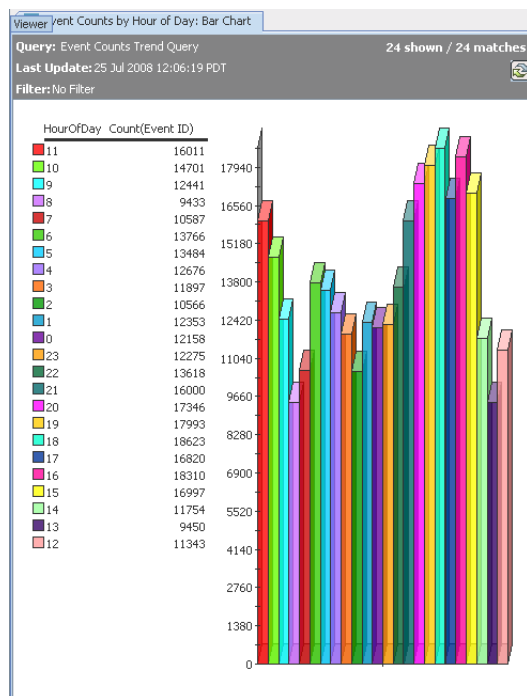
Select fields for **Values** and **Point Labels**.

Field	Description
Values	<p>The Values drop-down menu provides fields in the query result that contain data types. The value chosen is used as the numbers by which to plot the vertical y axis points on a bar chart or the slice sizes on a pie chart.</p> <p>Values typically represent an unknown set of values, like a count. A common example of numeric data appropriate for values is a time like HourOfDay or a count like Count(Event ID).</p>
Point Labels	<p>The Point Labels drop-down menu provides fields in the query result that contain non-numeric data types. The point labels are used to plot the horizontal x axis labels on a bar chart or the slice labels on a pie chart</p> <p>Examples of non-numeric data types appropriate for point labels are timestamps, strings such as are used for event names, and different types of addresses such as IP or MAC addresses. Point labels are typically a known set of limited values (like hours in a day denoted by timestamps).</p>

Example View Settings

For example, for the Event Counts by Hour of Day query viewer, selecting [Count\(Event ID\)](#) for **Values** (the y axis) and [Hour of Day](#) (or Timestamp) for **Point Labels** (the x axis) results in the following display showing the event count for each hour of the day. The event count is depicted on the vertical y axis, with higher bars representing a higher event count for that hour. The hour of day (time) is

represented on the horizontal x axis. The event count is shown for the last 24 hours starting at 11 am.

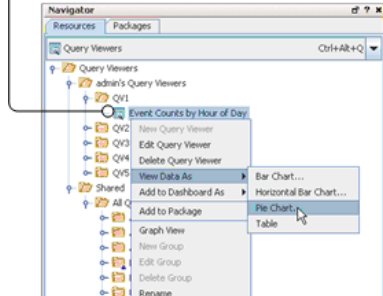


Understanding the Results View

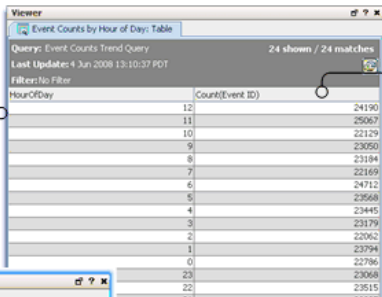
The results are displayed in the Viewer, as shown below.

Below is the “Event Counts By Hour of Day” query result as table, bar chart, pie chart.

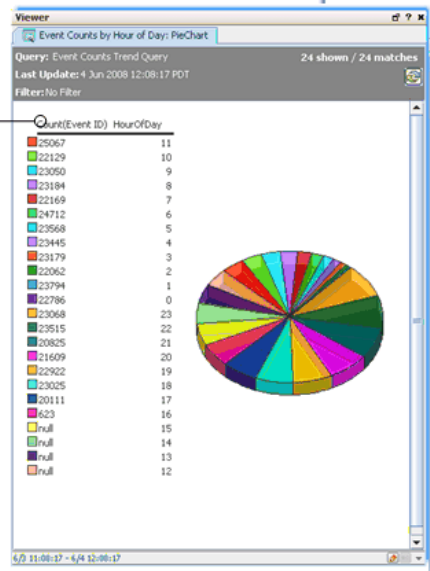
To run a query viewer, right-click one and choose **View Data as > <Display Format>**.



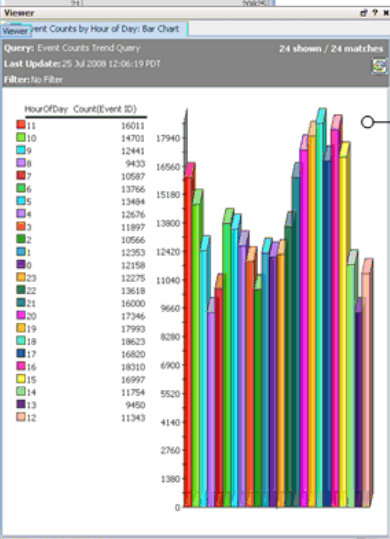
Depending on the display format you select, the query viewer results is shown as a bar chart, pie chart or table. (Right click query results in the viewer to generate a report.)



Query Viewer result for View Data as > Table



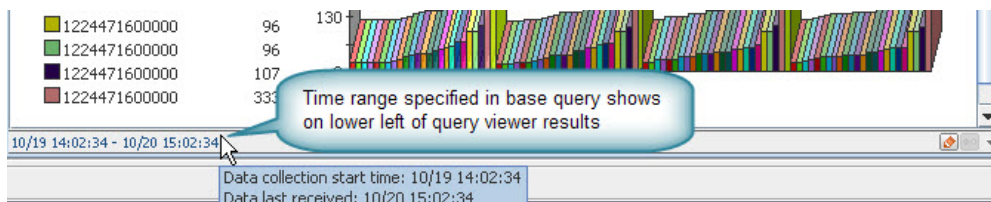
Query Viewer result for View Data as > Pie Chart



Query Viewer result for View Data as > Bar Chart

Notice that the time range for the base query is shown on the lower left of the query viewer results. Hover the cursor over the time range to see an annotated view of start and end times (**data collection start time** and **data last received**). This time range comes from the base query. (Another way to see the query time range is to open the query viewer in the editor and double-click ***Query** in the Attributes display to drill down to the base query editor, which shows query start and end times.)

Below is the Time Range of Base Query



Working with Query Viewer Results

Various options are available to you with the different query result display formats (Bar Chart, Horizontal Bar Chart, Pie Chart, or Table).

Viewing query results in table format give you the ability to establish baselines and make comparisons, as well as manipulate the table data.



Note

Query viewers and channels display results from variable calculations differently. For example, a value may be displayed as -0.1 in a query viewer, and -0.099999999999... in a channel.

Such variations are due to differences in the way floating point operations are carried out in Oracle and in Java.

Bar charts and pie charts provide at-a-glance, graphical overviews of the results but with fewer options for manipulating the data after the fact.

Other options, such as filtering a query viewer results or running reports, are available on all result views.

Details of working with each view format are provided in the following topics.

Results in Table Format

To get results in Table format, right-click a query viewer and choose **View Data as > Table**. You can sort, re-order, and create/compare baselines for data in a table view.

Right-click a table column header to get a list of sort and edit options for the column.

The arrow next to a column header indicates the column is determining the current sort order for the table and shows the current sort order. (For example, this column is sorted showing highest count first.)

Left-click a table column header to sort or reverse-sort it. This affects the entire table.

Timestamp	Name	Count(Event ID)	Count(Event ID) - (Reference Baseline)
16 Apr 2008 13:00 PDT	Sort Column	5990	5375
16 Apr 2008 13:00 PDT	Monitor Event	5460	5896
16 Apr 2008 13:00 PDT	ip value count data monitor value...	773	772
16 Apr 2008 13:00 PDT	Timestamp	5811	42
16 Apr 2008 13:00 PDT	Name	5704	42
16 Apr 2008 13:00 PDT	Count(Event ID)	5685	33
16 Apr 2008 13:00 PDT	Count(Event ID) - (Typical Weekday Baseline)	5630	3
16 Apr 2008 13:00:00 PDT	Count(Event ID) - (Reference Baseline)	5460	0
16 Apr 2008 13:00:00 PDT	Starting Trend Query	96	0
16 Apr 2008 13:00:00 PDT	SideTable Sizes (Rows)	30	0

You can add a baseline to a **table** view of query result data, then run **baseline** comparisons to identify deltas in network behavior.

Only **table views** of query result data can be baselined and compared.

Investigate View Options

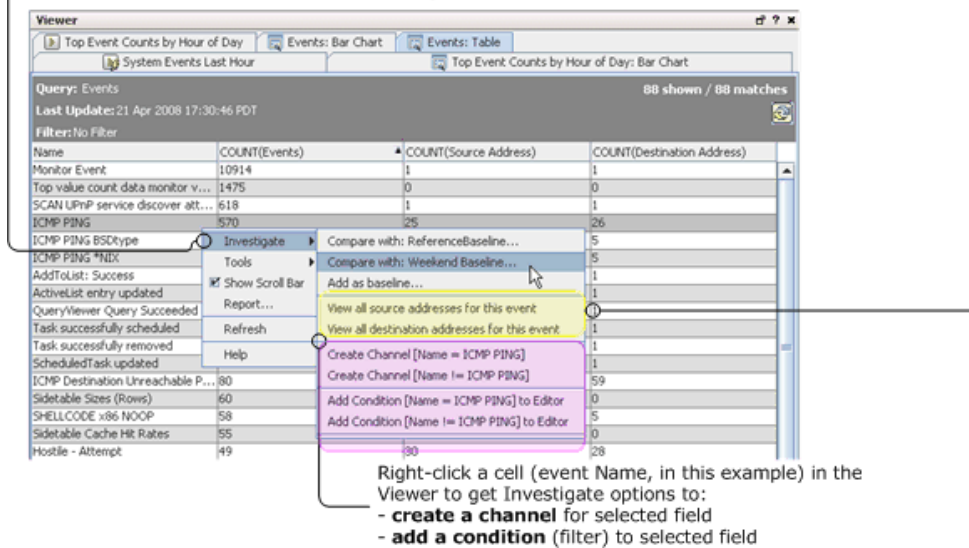
The following right-click **Investigate** options are available on query viewer results in **table** format (obtained by choosing **View Data as > Table**):

- **Baselines.** Right-click *anywhere on the table of results* in the Viewer to add a baseline or compare the current results to an existing baseline.
- **Drilldowns.** Right-click a *row* in the table result to launch a given drilldown on that row item (if drilldowns are provided in the query viewer).
- **Channels.** Right-click a *cell* in the table result to create an active channel with a filter based on the value of the selected table cell.
- **Conditions.** Right-click a *cell* in the table result to add a filter condition based on the value of the cell.

These options are described in detail in the table below.

Right-click a table in the Viewer over a table result to get **Investigate** options. (By default, add baselines and view available baselines here.)

If a query viewer includes drill-downs, these are shown as **Investigate** options (e.g., this one has drill-downs to source and destination addresses). Drill-downs are "row-specific". Right-click a row in a table view to get drill-down options for that row.



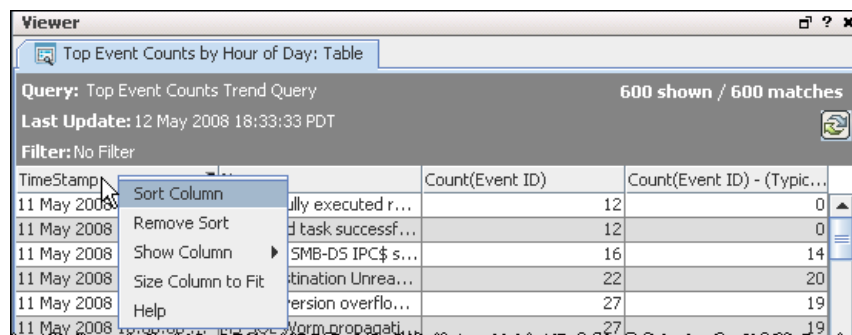
Investigate Options for Results are shown in the following table.

Option	Description
Add as baseline	<p>Add the current results as a baseline for the query viewer.</p> <p>Right-click <i>anywhere on the table result</i> in the Viewer to add a baseline to the query viewer or compare the current results to an existing baseline.</p> <p>(See "Defining and Using Baselines" on page 304 and "Adding a Baseline" on page 306.)</p>
Compare with: < Baseline >	<p>Compare the current results with the selected baseline.</p> <p>Right-click <i>anywhere on the table result</i> in the Viewer to compare the current results to an existing baseline.</p> <p>This menu option is available if there is one or more baselines established for the query viewer. All baselines associated with the query viewer are available from this menu for comparison.</p> <p>(See "Comparing Displayed Results to a Baseline" on page 308.)</p>

Option	Description
Drilldowns	<p>Query viewers enable you to drill down to Active Channels. If the query includes an event ID or resource ID, you can also drill down to that resource. See “Viewing an Event or Resource Directly from the Query Viewer” on page 301 for details.</p> <p>If there are drilldowns associated with the query viewer, these are listed after the baseline options on the right-click Investigate menu for a selected row in the query viewer result.</p> <p>Right-click a <i>row</i> in the table result, and choose Investigate > <Drilldown Option>.</p> <p>For example, an Events query viewer could provide drilldowns to view all source addresses for a selected event. Assuming each row in the result table represents an event, choosing this drilldown from the Investigate menu would lead to a table showing source addresses for the selected event.</p> <p>(See “Query Viewer Drilldowns” on page 319 and “Drilldown Example” on page 326.)</p>
Create Channel	<p>Creates an active channel with a filter based on the selected cell in the table result.</p> <p>For example, right-clicking a table cell with an event name and choosing Investigate > Create Channel [EventName] creates an active channel that monitors and filters for occurrences of that event name. The filter is always set to the value of the cell (which in this example would be the event name).</p> <p>For more information about using active channels, see “Viewing and Using Channels” on page 130.</p>
Add Condition	<p>Brings up the Conditions Editor for the selected item, where you can add or modify conditions (filters) on the selected item.</p> <p>Right-click a <i>cell</i> in the query viewer table result to add a filter condition based on the value of the cell.</p> <p>For more information on working with Conditions, see “Common Conditions Editor (CCE)” on page 846.</p>

Column Sort, Display, and Edit Options

Right-click a column header in a query viewer table result to get various options on that column.



Option	Description
Sort Column	<p>Sort items in the column in ascending or descending order.</p> <p>Columns that have been sorted after the query viewer run show an up or down arrow next to them to indicate the direction of the sort.</p> <p>You can also sort the column by left-clicking the column header. Clicking multiple times toggles the sort between:</p> <ul style="list-style-type: none"> • ascending order (indicated by a up arrow next to the header) • descending order (indicated by a down arrow next to the header) <p>Notes:</p> <ul style="list-style-type: none"> • Sorting on the contents of a column after a query viewer displays its results changes the view of the data provided by the original query. A query sorts during a query run, and then displays the data based on the sorting it did. If you click columns to re-sort, you are changing the sort order the query gave you. In the cases where the original query used a "single-column" sort, you can "get back" to it in the viewer, but you can't get back to a multi-column sort because this is offered only in the query sort options, not on the Console UI. • Keep in mind that this option sorts on the data result returned by the query. This in combination with query row limits (applied when the query is run) can sometimes yield unexpected results. Example: If the query is defined to run on 2 days' worth of data but hits the 10,000 row limit after processing only 1 day of data, then only 1 day's worth of data is returned in the result. An "after-query" sort, in this example, is a sort on only 1 day's worth of data. • Sorting at the query viewer level sorts only the data returned by the query to Viewer. Initial sorting is done by the base query, which is responsible for running against the database. If the query level sort is yielding unexpected results, keep in mind that the original base query sort determines how much you can modify the view of the result. <p>See also "Sort Baseline Data" on page 309.</p>
Remove Sort	<p>Remove a sort on the selected column. You can remove sorting imposed when the query viewer was run or when a UI column-click sort was done on the displayed result.</p>
Show Column	<p>Right-click anywhere on any column header in a table to get a context menu of columns included in the display result.</p> <p>Select columns to hide or show in the result. Columns with no checkmark beside them are hidden.</p> <p>This is the equivalent of hiding or showing a column before the query viewer runs. (However, only columns configured to be included in the original query are available to hide/show after the query is run.)</p> <p>To show a column in the results view that is currently hidden (whether before or after the query ran), right-click again and choose it (checkmark it).</p> <p>See also "Show or Hide Baseline Columns" on page 309.</p>
Size to Fit	<p>Expand the column, if needed, to accommodate the full width for text in each row of the selected column.</p>

Option	Description																																				
Drag-and-Drop options	<p>Left-click-and-drag on a column header to reposition it in a different horizontal order in the table. For example, if the original query viewer result shows columns in this order:</p> <table><tr><th>TimeStamp</th><th>Name</th><th>Count(Event ID)</th></tr><tr><td>12 May 2008 18:00...</td><td>Monitor Event</td><td>5460</td></tr><tr><td>12 May 2008 18:00...</td><td>Top value count data monitor value current</td><td>807</td></tr><tr><td>12 May 2008 18:00...</td><td>NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...</td><td>661</td></tr><tr><td>12 May 2008 18:00...</td><td>NETBIOS SMB-DS Session Setup AndX req...</td><td>658</td></tr><tr><td>12 May 2008 18:00...</td><td>Task successfully scheduled</td><td>40</td></tr></table> <p>You can click-and-drag TimeStamp to the right so that the columns display in this order:</p> <table><tr><th>Name</th><th>TimeStamp</th><th>Count(Event ID)</th></tr><tr><td>Monitor Event</td><td>12 May 2008 18:00...</td><td>5460</td></tr><tr><td>Top value count data monitor value current</td><td>12 May 2008 18:00...</td><td>807</td></tr><tr><td>NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...</td><td>12 May 2008 18:00...</td><td>661</td></tr><tr><td>NETBIOS SMB-DS Session Setup AndX req...</td><td>12 May 2008 18:00...</td><td>658</td></tr><tr><td>Task successfully scheduled</td><td>12 May 2008 18:00...</td><td>40</td></tr></table>	TimeStamp	Name	Count(Event ID)	12 May 2008 18:00...	Monitor Event	5460	12 May 2008 18:00...	Top value count data monitor value current	807	12 May 2008 18:00...	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	661	12 May 2008 18:00...	NETBIOS SMB-DS Session Setup AndX req...	658	12 May 2008 18:00...	Task successfully scheduled	40	Name	TimeStamp	Count(Event ID)	Monitor Event	12 May 2008 18:00...	5460	Top value count data monitor value current	12 May 2008 18:00...	807	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	12 May 2008 18:00...	661	NETBIOS SMB-DS Session Setup AndX req...	12 May 2008 18:00...	658	Task successfully scheduled	12 May 2008 18:00...	40
TimeStamp	Name	Count(Event ID)																																			
12 May 2008 18:00...	Monitor Event	5460																																			
12 May 2008 18:00...	Top value count data monitor value current	807																																			
12 May 2008 18:00...	NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	661																																			
12 May 2008 18:00...	NETBIOS SMB-DS Session Setup AndX req...	658																																			
12 May 2008 18:00...	Task successfully scheduled	40																																			
Name	TimeStamp	Count(Event ID)																																			
Monitor Event	12 May 2008 18:00...	5460																																			
Top value count data monitor value current	12 May 2008 18:00...	807																																			
NETBIOS SMB-DS DCERPC NTLMSSP asn1 ...	12 May 2008 18:00...	661																																			
NETBIOS SMB-DS Session Setup AndX req...	12 May 2008 18:00...	658																																			
Task successfully scheduled	12 May 2008 18:00...	40																																			

Results in Chart Formats

To get results in Chart format, right-click a query viewer and choose either:

- View Data as > Bar Chart or Horizontal Bar Chart
- View Data as > Pie Chart.

Right-click an item in a chart view to get **Investigate** options for that item (e.g., event)

Investigate menu includes options to:

- create a channel for selected item
- add a condition (filter) to selected item

Chart Option	Description
Drilldowns	<p>Query viewers can provide <i>drilldowns</i> to Active Channels. If the query includes an event ID or resource ID, you can also drill down to that resource. See “Viewing an Event or Resource Directly from the Query Viewer” on page 301 for details.</p> <p>If there are drilldowns associated with the query viewer, select an item in the first or key column, then right-click to get drilldown options in the Investigate menu.</p> <p>For example, an Events query viewer could provide drill-downs to view all source addresses for a selected event. Choosing this drilldown from the Investigate menu on a query result would lead to a table showing source addresses for the selected event.</p> <p>(See “Query Viewer Drilldowns” on page 319 and “Drilldown Example” on page 326.)</p>
Create Channel	<p>Creates a channel on the selected item. (For example, right-clicking an event and choosing Investigate > Create Channel [EventName] creates an active channel that monitors and filters for occurrences of that event.</p> <p>For more information about using active channels, see “Viewing and Using Channels” on page 130.</p>
Add Condition	<p>Brings up the Conditions Editor for the selected item, where you can add or modify conditions (filters) on the selected item.</p> <p>For more information on working with Conditions, see “Common Conditions Editor (CCE)” on page 846.</p>

Filtering Query Viewer Results

You can filter query viewer results shown in table and chart formats.

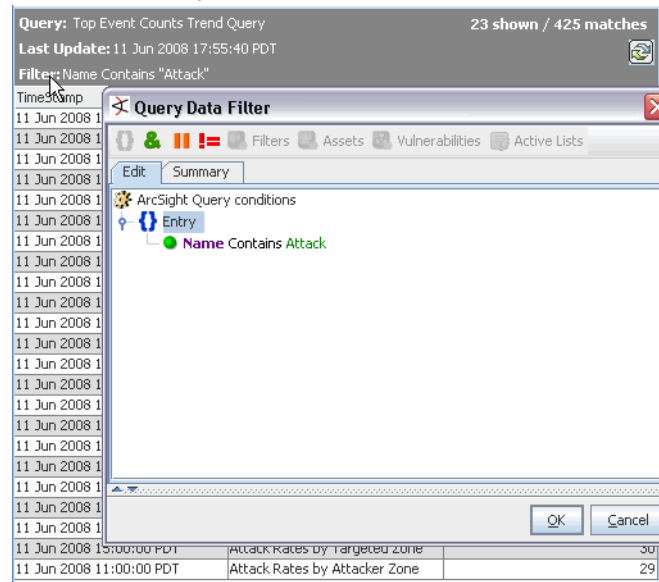
Adding a Filter

To filter query viewer results:

- 1 Click **Filter: No Filter** in the header of a query result view. (You can also right-click the filter name and choose **Edit Filter** from the context menu.)

The Common Conditions Editor (CCE) dialog opens.

- 2 Use the CCE dialog to add a filter. (For details on how to use the CCE dialog to create filters, see the topic on the [“Common Conditions Editor \(CCE\)”](#) on page 846.)



- 3 Click **OK** to save the filter, and filter the current result view.



Filters on query viewer results are locally saved and available only while the current result set is displayed. These filters are not saved as a part of the query viewer. When you close the query viewer result, the filter is no longer available; recreate it on a new result set.



Filters can also be applied to baseline *delta* columns. (See [“Defining and Using Baselines”](#) on page 304.)

Removing a Filter

To remove a filter from a displayed query viewer result, right-click the filter name in the header of the result view and select **Remove Filter** from the context menu.

Viewing an Event or Resource Directly from the Query Viewer

If your query viewer is for events or resources and the query viewer results include an event ID or resource ID field, you can go directly to a specific event or resource from the query viewer.

Right-click the event or resource and select **View > [Event Name] Details** or **View [Resource Name] Details**. For example, drill down to

- An event if the query includes the event ID field
- An actor if the query includes the actor ID field
- An asset if the query includes the asset ID field
- A case if the query includes the case ID field

Adding Query Viewers to Dashboards

You can add a query viewer result to a regular dashboard. Refer to [“Adding a Query Viewer to a Dashboard” on page 157](#).

For more information about working with dashboards, see [“Using Dashboards” on page 153](#).

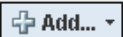
Making Query Viewer Results Available to ArcSight Web

Query viewer results on dashboards are accessible from ArcSight Web. For more about ArcSight Web, see [“ArcSight Web” on page 798](#).

For more information about working with dashboards, see [“Using Dashboards” on page 153](#).

Adding Query Viewers as Startup Views

Query Viewers can be set as the startup view for a group as follows:

- 1 Select **Users** in the Navigator
- 2 Right-click a group and choose **Edit Groups** from the context menu.
- 3 In the editor for the selected group, click **Startup Views** tab, then click **Query Viewers** subtab.
- 4 Click **Add** () to bring up the Query Viewer Selector.
- 5 In the Query Viewer Selector dialog, navigate to and select (checkmark) the query viewer you want as the startup query viewer for this group and click **OK**.

The full path to the query viewer you selected is shown on the Query Viewers tab in Startup Views.
- 6 Click **Apply** to save your changes and leave the group editor open, or click **OK** to save and close the group editor.

For more information on editing groups and startup views, see [“Editing User Groups” on page 645](#) and [“Setting Startup Views” on page 646](#).



Regardless of startup view settings for groups, the Query Viewers you have showing when you close the Console are reloaded when you restart the Console.

Generating Reports from Query Viewers

After you run a query viewer, you can generate a simple report containing the results.



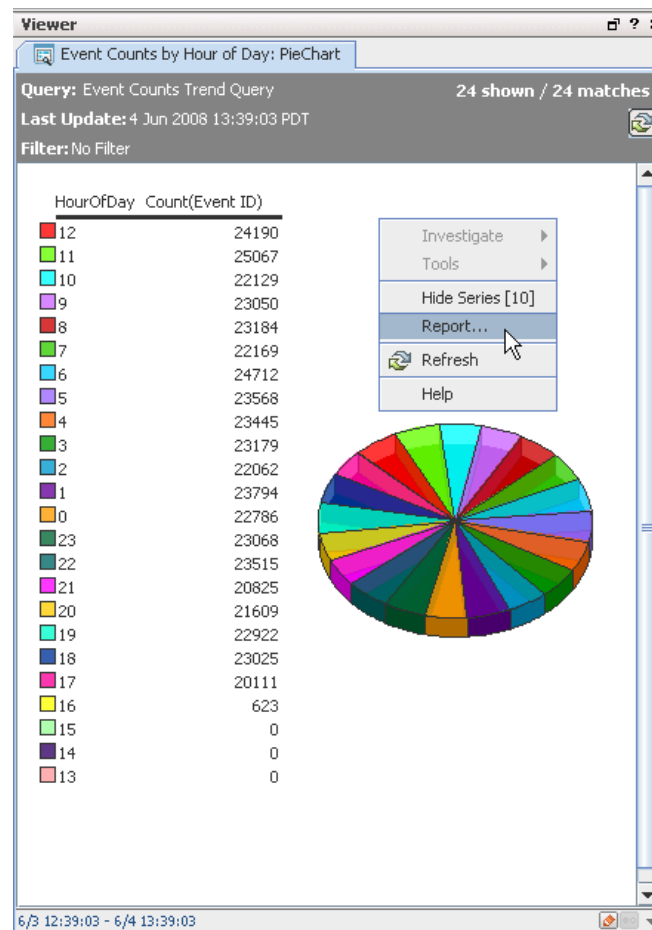
The report display format is based on the query viewer result display. For example, if you chose to view query data as a *pie chart*, the generated report shows the same pie chart view. To generate a report showing results for the same query as a *bar chart* or *table*, you would need to re-run the query viewer (<Query Viewer> > View Data as) in one of those formats, and then generate the report from that view.

The report contents might not include as much data as the query viewer result shown in the Console for these reasons:

- Reports on pie charts and bar charts have a default row limit of 25. This is user-configurable. You can set a higher or lower row limit on the Report Parameters dialog you get when you run the report. (See [Step 2 on page 304.](#))
- Reports on *tables* have no hard limit on number of rows in the table.
- Data viewed in *chart* format has a hard limit of no more than 99 rows, therefore reports on charts have the same hard limit of no more than 99 rows displayed on the Console and Web user interface.

To generate a report on a query viewer:

- 1 Right-click the query viewer results table or chart (anywhere in the Viewer panel) and click **Report**.



- 2 Specify the options on the Report Parameters dialog or take the defaults and click **OK**.

Name	Value
Common Parameters	
Report Format	pdf
Page Size	Letter [8.5x11 in]
Email to	
Email Format	Send URL
Email Subject	\${ReportName}
Row Limit	25

Name	Value
Output Parameters	
Archive Report Folder	Select a Archived Report Group
Archive Report Name	\${Today}/\${ReportName}_\${Now}
Archive Report Expiration Time	\${Now}+6M

☒ Save Output

OK Cancel Help



Tip

- For more about Report row limits, see these Tips and [related information on page 303](#).
- If you click **Save Output** on the Report Parameters dialog, you get additional options for setting archived report "Save Output Parameters".

For more help on setting report parameters, see "[Report Parameters](#)" on page 425.

- 3 When the report is ready, a dialog gives you the option of opening it to view it now or saving it to a location you specify through a file browser.

Choose **Open** to view the report or **Save** to save it in a specified location.



Tip

Reports initiated from query viewers are provided for convenience as a quick way to share the result data. Query viewer reports are limited to displaying data from the single query covered by the query viewer and retain the format of the chart or table in which the query viewer results are displayed. For information on creating and publishing richer, highly formatted reports on multiple data sources see [Chapter 14, Building Reports, on page 331](#) and [Chapter 15, Running and Managing Reports, on page 423](#).

Defining and Using Baselines

You can establish a particular set of query results as a **baseline** snapshot against which to compare the results of other runs of the same query. Comparing the results of the same query run at different times and in different contexts highlights the *deltas* (differences) and helps identify areas that vary significantly from normal.

You can define baselines and run comparisons with any query viewer that:

- Lends itself well to a table format display
- Includes one or more key fields by which to locate matching entries between the baseline and currently displayed information.

For example, suppose you have a query that returns the top 10 event counts by name and you want to compare it against some baseline. A reasonable comparison would be between

similarly named events in both sets of data. In this case, the event name would be used as the key field.



Note

- **Baselines are applicable only to table views of result data.** Baselines do not apply to graphical views such as pie charts, bar charts, and so on. You always have the option to view query data from any query viewer as a graphical chart or a table, but the baseline data is only accessible from the table view of the data.
- **Baselines require one or more key fields** by which to locate matches between the baseline and the displayed data. The key fields must be built into the query viewer to which you want to add a baseline.
- **Values for Key fields must be unique.** When adding baselines, make sure key field(s) in the query viewer have unique values. (See the **Fields** tab in the query viewer editor.) Also, check the query viewer start and end times (on the **Attributes** tab in the query viewer editor) to make sure the time frame over which the query runs makes sense.

You can add one or more baselines to a single query viewer, and delete them as needed.

Why Baselines are Useful

In addition to providing a way to compare result data from different query runs, baselines provide an efficient way to save, annotate, and retrieve data that might otherwise be too difficult to access in any meaningful way.

Once a baseline is defined, it is preserved as a File resource that is associated with the query viewer. In the Navigator, choose **Files** and expand the **Query Viewer Baselines** folder to view the new baseline files.

In **Query Viewers**, you can create, save, and use **Baselines** to compare result data from the same query viewer run at different times and dates.

The screenshot displays the ArcSight Console interface. The main window shows a query viewer titled 'Top Event Counts by Hour of Day: Pie Chart' with a table view of event counts. The table has columns for 'Timestamp', 'Name', 'Count(Event ID)', and 'Count(Event ID) - (Typical Weekday Baseline)'. The 'Add as baseline' button is highlighted in the context menu. The Navigator on the left shows the 'Query Viewer Baselines' folder expanded under 'Files'.

Baselines created in Query Viewers also show up under the Files resource in the Navigator.

With Query Viewer baselines, you can:

- Retrieve the snapshot baseline data by running comparisons against it.
- Compare current result data against one or multiple baselines.
- Get meta-information about the baseline (such as when it was saved, by whom, and comments).
- Sort, show, or hide the baseline comparison columns.
- Maintain the baseline data as a Files resource baseline even if the original data is lost or is too performance-intensive to re-generate (for example, an aggregation query). (All baselines are automatically added as Files resources when they are created.)
- Add and remove baselines as needed, and edit some meta-information on baselines (for example, description comments).
- Use filters on the baseline (*delta*) columns. For example, you could filter on a baseline column to find where the current results differ from the baseline by more than some specified value.

Planning for Baseline Comparisons

Query viewer baselines might prove most useful if you take a little time to identify some goals for their use or questions you want answered, and then plan how to implement the baselines for those purposes. Here are some suggestions to start off with.

- 1 Establish questions or goals for baseline comparison monitoring and identify the type of data you want to evaluate.

For example, you might want to determine what type of event traffic is at its highest at different times of day or when network attacks tend to increase. Or, you might notice a spike in certain query viewer results (such as more logins from a particular user) and decide to compare the behavior against a sampling of results from subsequent or previous query runs.

- 2 Identify the query viewer (and associated query) appropriate to use. If the query viewer you need is not provided, you can develop it. See [“Customizing Query Viewers” on page 311](#) for more information on this.

For example, if you want to monitor what type of event traffic is at its highest, you could establish a baseline for a query viewer that returns “Top Event Counts by Hour of Day.” You could also use a query viewer *baseline* to take snapshots of event counts throughout the day, either for record-keeping or to explore and compare later.

- 3 Monitor results for your chosen query (by running the query viewer) to identify a “typical” or “normal” result set to use as a baseline.
- 4 Add (capture) the baseline from the typical/normal result set.
- 5 Monitor subsequent results for variation (spikes, dips) or time periods against which you want to compare with the baseline, and run baseline comparisons on these.

Adding a Baseline

A baseline is a snapshot of the current results that can be used later as a reference point to compare other query result views. Baselines are often added to capture “normal” network behavior, so that when spikes, dips, or other anomalies surface, these can be compared against the baseline.

Baselines can only be defined on numeric data (because they are designed to show *deltas*, the difference or change between two values).

To add a baseline to a query viewer:

- 1 In the Navigator panel, choose the **Query Viewers** resource.
- 2 Select and run the query viewer (containing the query) for which you want to define a baseline.

To do this, right-click the query viewer and choose **View Data As > Table**.



Baselines are applicable only to table views of result data.

The query viewer result is displayed in the Viewer.

- 3 Right-click anywhere in the results table in the Viewer, and select **Investigate > Add as baseline...** to get the Add a baseline... dialog.

- 4 Enter a name for the baseline, optional description, and click **OK** to add it.

This saves the current query result data as a named baseline for the selected query viewer, and makes it available for use (through **Investigate > Compare with...** against results from other runs of the same query viewer).

The baseline is shown on the Fields tab of the query viewer to which you added it.



If the query viewer editor is not currently displayed, double-click the same query viewer in the Navigator panel to open it in the editor. Click the query viewer editor **Fields** tab.

Comparing Displayed Results to a Baseline

Once you establish a baseline for a query, you can compare subsequent results for the same query against the baseline.



Note

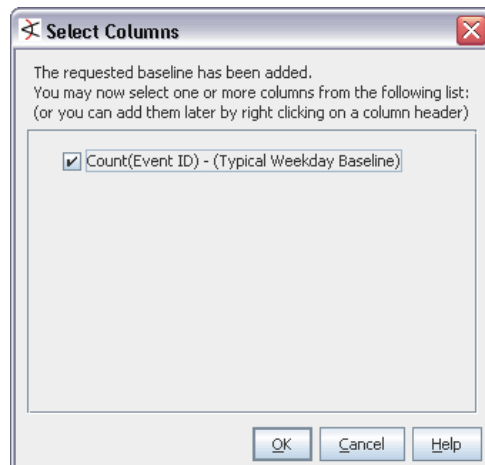
- Baseline comparisons, like baselines, can only be derived from *table* views of the query viewer results. (Select a query and choose View Data as > Table. See ["Results in Table Format" on page 295.](#))
- The query viewer you select for baseline comparison needs to have at least one baseline already added to it. Baselines are shown on the **Fields** tab of the Query Viewer editor.

To run a comparison:

- 1 If you do not already have a table view of the data you want to compare, right-click the query viewer you want to evaluate against a baseline, and choose **View Data as > Table** from the Navigator menu.
- 2 In the Viewer, right-click anywhere on the table view results and select **Investigate > Compare with: <SomeBaseline>**.

The comparison data is collected and added as a new column. You have the option of hiding or showing it in the table as needed.

- 3 Make your selections on the Select columns table and click **OK**.



If you selected the comparison column, it is displayed on the table next to the original results for that column.

Events: Table		
Query: Events		
Last Update: 1 Aug 2008 16:40:14 PDT		
Filter: No Filter		
10 shown / 10 matches		
Name	COUNT(Events)	COUNT(Events) - (Typical Weekday Baseline)
Monitor Event	14071	-929
Top value count data monitor val...	10209	1209
ICMP PING	976	
ICMP PING *NIX	852	-57
ICMP PING BSDtype	852	-56

Note that differences between the current values and the baseline can be positive or negative, as shown in the example comparison above. A positive value in the baseline comparison indicates more events in your current sample, compared to the baseline. A

negative value in the baseline comparison indicates fewer events in your current sample, compared to the baseline. If the baseline field for a row is null, this indicates that no baseline value was available for that key.



- By the time the Select Columns dialog is displayed, the Baseline comparison is already available. If you select columns, those are displayed in the viewer on the Table result.
- After running a baseline comparison, the right-click over Table **Investigate > Compare with <Baseline>** option for the baseline you just ran is grayed out (even if you chose not to immediately select any columns or clicked Cancel on the Select Columns dialog). This is because the baseline is already added.
- To show or hide more columns (including baseline columns), right-click the column header, choose **Show Column**, and check (enable) or uncheck (disable) columns. See also [“Show or Hide Baseline Columns” on page 309](#)

Show or Hide Baseline Columns

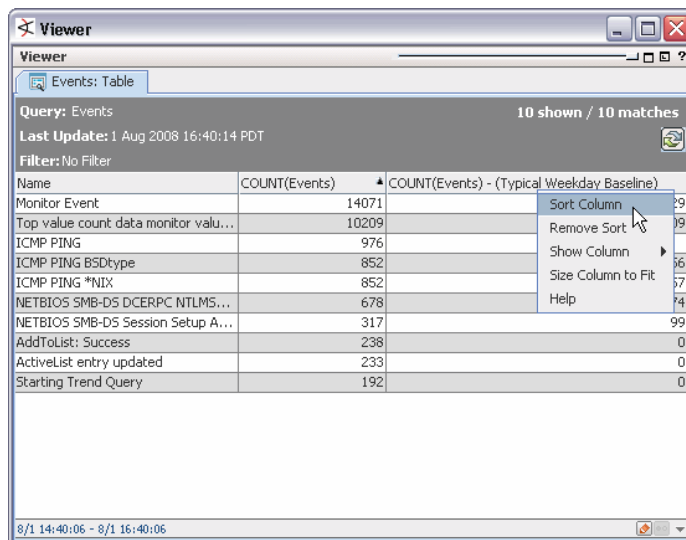
You can always show or hide columns, including baseline columns. To do this right-click anywhere in the table header (on any of the column titles), choose **Show Column > <SomeField>**.

Name	Count(Event ID)	Count(Event ID) - (Typical Weekday Baseline)
Sort Column	6990	6905
Remove Sort	5896	5811
Show Column		5734
Size Column to Fit		5726
Help		5619
		5600
Monitor Event		5545
Monitor Event		5375
Monitor Event	5460	5375

See also [“Column Sort, Display, and Edit Options” on page 297](#).

Sort Baseline Data

You can perform an after-query sort on baseline comparison data by clicking the column headers. A pre-query sort for baseline data is not available. (That is, there is no option to add a sort as a part of the baseline in the query viewer definition.)

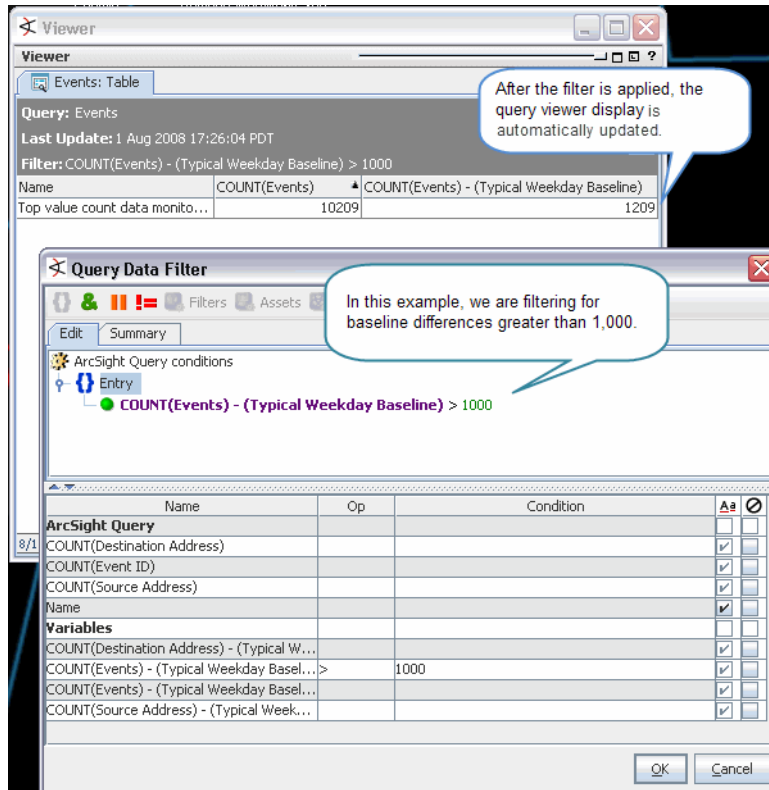


See also [“Column Sort, Display, and Edit Options” on page 297](#).

Filter Baseline Data

You can filter on the baseline comparison column the same way you would filter on any other column. Click the **Filter** in the query viewer header to bring up the Query Data Filter dialog. Enter your filter conditions and click **OK**. After the filter is applied, the query viewer automatically updates.

The Query Data Filter is based on the Common Conditions Editor (CCE). For information about using the CCE to define filters, see [“Common Conditions Editor \(CCE\)” on page 846](#).



Removing a Baseline

Baselines, like the queries themselves, are associated with and contained in query viewers. To remove a baseline, you remove it from the list of baselines in the query viewer editor.



Tip

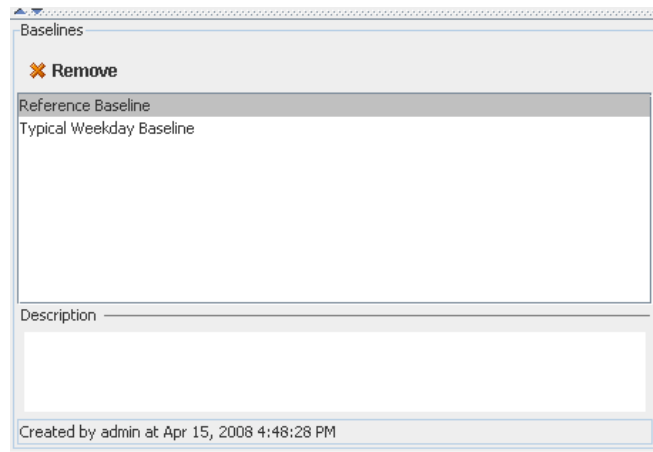
Removing a baseline from a query viewer is different from hiding or showing a baseline column in a query result. If all you want to do is temporarily hide a baseline column in a results table, use the right-click “Show Column” option in the Viewer on the results table as described in [“Column Sort, Display, and Edit Options” on page 297](#) in [“Results in Table Format” on page 295](#).

To remove a baseline from a query viewer:

- 1 In the Navigator panel, right-click the query viewer containing the baseline you want to remove and select **Edit Query Viewer**.

This opens the editor for the query viewer in the Inspect/Edit panel.

- 2 In the editor, click the **Fields** tab.
- 3 Under Baselines, select the baseline you want to remove and click **Remove**.



- 4 Click **Apply** to save your changes to the query viewer, or click **OK** to save changes and close the editor.

Note that there is no confirm dialog for this Remove baseline action, but if you do not want to save your changes, click **Cancel** and the baseline is not removed.

Customizing Query Viewers

Query viewers provide a shortcut alternative to running SQL queries as a part of reporting. Keep in mind that query viewers use base queries, so a first step in creating a query viewer is deciding what SQL query you want to use. If you can't find one that does what you want, you'll need to create one first, before defining your query viewer.

Creating a New Query Viewer

The high-level steps for creating a query viewer are as follows:

- 1 Identify your question(s) and what information you are looking for. (For example, "What types of actions represent the highest volume of events on my network during various times of day?")
- 2 Based on the question you want answered, decide what kind of query you need and determine whether it is available or you have to create it.

If you do not find a suitable query when you browse the choices under Reports/Queries (or on the Query Viewer "Query" field "Select a Query" drop-down menu), you can create one. To get started creating a new query, navigate to **Reports**, and click the **Queries** tab. For more information see ["Building Queries" on page 354](#).

When you know which query you want to use and have either found a pre-built one or created a new one, you are ready to create a query viewer that uses that query.

- 3 Select **Query Viewers** in the Navigator.

- 4 Right-click a group (folder) and select **New Query Viewer**. This launches the Query Viewer Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 5 Define general attributes for the query viewer as described in [“Query Viewer Attributes” on page 312](#). At a minimum, fill in the required values (red asterisks) on the **Attributes** tab (query viewer name and “base query” to use).
- 6 Choose the **Fields** to display for the query viewer as described in [“Query Viewer Fields” on page 316](#). (Fields are inherited from those available in the base query.)
- 7 Define **Variables** for use in the query viewer as described in [“Query Viewer Variables” on page 318](#) (optional).
- 8 Specify any **Drilldowns** you want to make available as described in [“Query Viewer Drilldowns” on page 319](#) (optional).
- 9 Click **Apply** or **OK** to create the new query.



Be sure to click **Apply** or **OK** frequently to save settings periodically as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings using these buttons, your settings are not saved.

The following sections provide details on defining attributes, fields, variables, and drilldowns for a query viewer.

Defining Query Viewer Settings

Use the Query Viewer Editor to build a new query viewer or edit an existing one. Query viewer settings are defined on multiple sub-tabs.



- To get to the editor for a query viewer, follow the first steps in either [“Creating a New Query Viewer” on page 311](#) or [“Editing a Query Viewer” on page 323](#).)
- If you want to edit more than one query viewer at a time, choose **Edit > Preferences** from the Console menu, then click **Global Options**. On the Global Options panel, check **Allow multiple editors of the same type**, then click **OK** to save the change and close the Preferences dialog. For more on setting Console preferences, see [“Changing User Preferences” on page 772](#), especially the subtopic [“Changing Global Options Like Panel and Editor Characteristics” on page 774](#).

Query Viewer Attributes

The following fields in the **Query Viewer** section are attributes to specify when creating a new query viewer.

Query Fields	Description
Name	Name for the query viewer. Spaces and special characters are okay. This is a required attribute.

Query Fields	Description
Query	<p>Specifies the base query used in this query viewer. This is a required attribute.</p> <p>If you are creating a new query viewer:</p> <ol style="list-style-type: none"> 1 Click this field to get a drop-down menu showing all available queries on this Manager. You can choose from queries created for reports, for other query viewers, or a new query you created specifically for this query viewer. <p>If you want to create a new query, you need to do this first before creating the query viewer. (See also “Building Queries” on page 354.)</p> <ol style="list-style-type: none"> 2 From the drop-down menu, select the query you want to use. <p>Note: If you are editing an existing query viewer, the Query field is not editable since the base query is set at the time the query viewer is created. If you want to use a different query, create a new query viewer.</p>
Refresh Data After	<p>Sets an amount of time (in minutes or hours) after which the query viewer automatically runs again and shows new data based on that most recent run. The query viewer is regularly refreshed based on the specified refresh time period.</p> <p>The default for this setting is after every 15 minutes. To change this default:</p> <ol style="list-style-type: none"> 1 Click the field to activate the settings. 2 In the left-hand field, enter a numeral, and in the right-hand drop-down menu, select minute(s) or hour(s).
Query Time Out	<p>Defines a time out limit in which the query must return results. If the query does not complete and send results within the specified time out period, the Manager stops the query run.</p> <p>By default, a time-out of 300 seconds (5 minutes) is configured on the Manager in server.defaults.properties. If you do not specify a Query Time Out in the Attributes tab, this time-out of 5 minutes applies (even if the Query Time Out field shows “None”). If you specify a time out here, then that one is used instead of the default.</p> <p>Setting a a time out limit is good practice especially if the event rate (events per second or <i>EPS</i>) is unusually high, start/end time range is large, or the query is complex. Time outs can help guard against infinite or long running queries that impact system performance. Although this is less of an issue with query viewers since they are designed to minimize impact on system performance, this can still be an issue in some scenarios.</p> <p>Setting time outs can be a useful troubleshooting technique for new queries, or existing queries in new scenarios, for example where event counts spike higher.</p>
Default View	<p>The Default View attribute determines how the result data are displayed when you double-click the query viewer to open the results in the Viewer panel.</p> <p>Define the default (double-click) view format for this query viewer. The choices are to show data as:</p> <ul style="list-style-type: none"> • Table (this is the default) • Pie chart • Bar chart <p>Double-clicking a query viewer in the Navigator displays result data in the format set here.</p> <p>If you choose Pie Chart or Bar Chart as the default view format, choose fields to use for the Values Column (to plot the y axis points on a bar chart or slice sizes on a pie chart) and Points Labels column (to plot the x axis labels on a bar chart or slice labels on a pie chart). The Values Column and Points Labels are also described in , “Select fields for Values and Point Labels.” on page 292.</p>

Query Fields	Description
Values Column	<p>The Values field applies to bar charts and pie charts. This setting provides fields in the query result that contain data types. The value chosen is used as the numbers by which to plot the vertical y axis points on a bar chart or the slice sizes on a pie chart.</p> <p>Values typically represent an unknown set of values, like a count. A common example of numeric data appropriate for values is a time like <code>HourOfDay</code> or a count like <code>Count(Event ID)</code>.</p>
Point Labels Column	<p>The Point Labels field applies to bar charts and pie charts. This setting provides fields in the query result that contain non-numeric data types. The point labels are used to plot the horizontal x axis labels on a bar chart or the slice labels on a pie chart.</p> <p>Examples of non-numeric data types appropriate for point labels are timestamps, strings such as are used for event names, and different types of addresses such as IP or MAC addresses. Point labels are typically a known set of limited values (like hours in a day denoted by timestamps).</p>
<p>Setting the following attributes (start time, end time, or row limit) in the Query Viewer overrides these settings in the base query. (See related information on page 313 about defining the base query in the <i>Query</i> attribute.)</p>	
Start Time	<p>Specifies the starting point for the data gathering.</p> <p>A drop-down menu provides values to select based on Velocity Templates (such as <code>\$Now</code>, <code>\$Now - 1d</code>, and so on). You can also provide a timestamp such as: <code>27 Jul 2008 16:00:00 PDT</code>.</p> <p>For more on timestamps and timestamp variables, see "Timestamps" on page 1002, "Timestamp Variables" on page 1003, and "Variables" on page 1006.</p>
End Time	<p>Specifies an end point for the data gathering.</p> <p>A drop-down menu provides values to select based on Velocity Templates (such as <code>\$Now</code>, <code>\$Now - 1d</code>, and so on). You can also provide a timestamp such as: <code>28 Jul 2008 16:00:00 PDT</code>.</p> <p>For more on timestamps and velocity references, see "Timestamps" on page 1002, "Timestamp Variables" on page 1003, and "Variables" on page 1006.</p>
Row Limit	<p>Set the row limit for the data table.</p> <p>The default for all new base queries is the maximum allowable, which is 10,000 rows.</p> <p>If the default is not changed in the base query, and no limit is specified here in the query viewer, the result shows up 10,000 rows of data.</p>

Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes

sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

Inspect/Edit

Event Inspector | Query Viewer: Event Counts by H...

Attributes | Fields | Variables | Drilldowns | Notes

Query Viewer

Name	Event Counts by Hour of Day
Query	Event Counts Trend Query
Refresh Data After	None
Query Time Out	None
Default View	Table
Values Column	
Point Labels Column	

Common

Resource ID	cFm5wlh8BABCAD-IXW8gdhA==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>

Assign

Owner	
Notification Groups	

Creation Information

Created By	admin
Creation Time	20 Feb 2009 17:27:51 PST
Time Since Creation	1 sec(s)

Last Update Information

Last Updated By	admin
Last Update Time	20 Feb 2009 17:27:51 PST
Time Since Last Update	1 sec(s)

Parent Groups

admin's Query Viewers	/All Query Viewers/Personal/admin's Qu...
-----------------------	---

(Name)
(Description)

Name	Value	Use Default
Query Parameters		
Start Time	\$Now - 25h	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Row Limit	10000	<input checked="" type="checkbox"/>

OK Cancel Apply Help

Query Viewer Fields

To define the data display, click the query viewer **Fields** tab.

Inspect/Edit

Event Inspector | Query Viewer: Event Counts by H...

Attributes | **Fields** | Variables | Drilldowns | Notes

Data Fields

Name	Alias	Use	Key
HourOfDay	HourOfDay	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Count(Event ID)	Count(Event ID)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TimeStamp	TimeStamp	<input type="checkbox"/>	<input type="checkbox"/>

Sort Options

+ Add... - Remove

Column	Sort Order
TimeStamp	Z-A ↑

Baselines

- Remove

Newest Weekday baseline
WeekDay

Description

OK Cancel Apply Help

Data Fields

The data fields shown on this tab are inherited from the base query. When a query viewer is first created, the data fields are shown here with the same settings they inherited from the base query for **Use** and **Key** fields. So, initially all fields are enabled for **Use** and fields that are grouped by columns in the base query show as **Key** fields here.

You have the option of overriding the base query settings for **Use** and **Key** settings on inherited data fields in the query viewer. (Settings here do not affect the base query.) You can override these settings when you first create the query viewer, or when you edit it later.

Select (check) **Use** for fields to display in the query viewer results. Fields not selected to Use do not show up in the query results.

Optionally, you can select one or more fields to use as **Key** fields. Key fields are columns that can be used to uniquely identify a role in the query. Only the fields selected as keys are used when doing baseline comparisons.

Data Fields

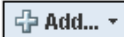
Name	Alias	Use	Key
TimeStamp	TimeStamp	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Name	Name	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Count(Event ID)	Count(Event ID)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The query viewer displays results from these columns, showing them from left to right in the order specified. The above settings would result in a query viewer that shows Timestamp as the left-most column, followed by Name, and so forth. You can re-order the columns by selecting a row and clicking the up or down arrow to move it.

Sort Options

The query viewer inherits the sort options from the base query, but you can override those sort options here, without affecting the base query.

You can add data fields from the base query to sort the query results in the query viewer display.

Click **Add** () to get the list of available fields and select those you want to sort on.

Column	Sort Order
TimeStamp	Z-A ↑
Count(Event ID)	A-Z ↓

In the example above, the Timestamp is sorted from newest to oldest. Data with the newest Timestamp is at the top of the list. Data with the oldest Timestamp is at the bottom of the list. (This is indicated by the Z-A sort order and up arrow.) In a case where multiple rows have the same Timestamp, these are sorted by the Count(Event ID) from smallest to largest (as indicated by the A-Z sort order and down arrow).

You can change the priority of a column by selecting a column and clicking the up or down arrow to move it.

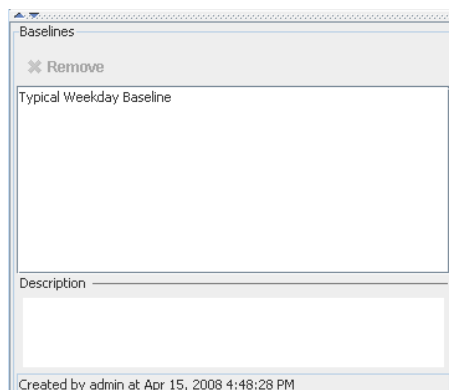
Note: It is possible to sort on fields that you choose not to display in the query result.

Suppose you decide to hide the timestamp and count (event ID) columns. In the query viewer Sort Options, you can still sort by Count (Event ID) and Timestamp.

The list of event names and results for this query viewer display in this multi-column sort order by timestamp and count (event ID), but those *columns* do not show up in the display.


BaseLines

If any baselines have been set on results returned on this query viewer, those are listed in the Baselines area of the Fields tab.



Baselines are created on query results tables using the right-click popup option **Investigate > Add as baseline...** after a query runs. (See [“Defining and Using Baselines” on page 304.](#))

When a query has one or more baselines available, you can compare the current results of a table view with the baseline.

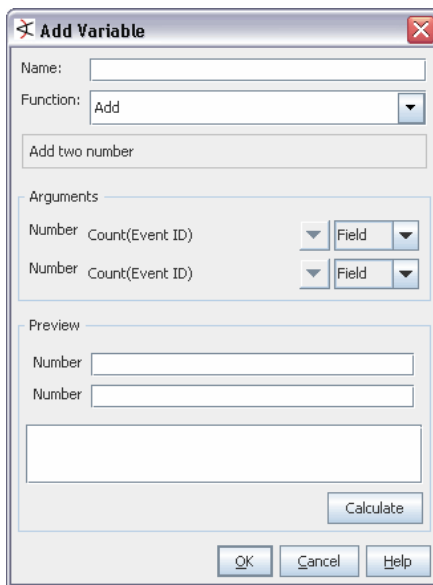
To remove baselines from the query viewer, click the **Fields** tab, select the baseline name, and click **Remove** ( **Remove**). Be sure to click **OK** or **Apply** on the Query Viewer Editor to save your changes.

If you remove the baselines from the query viewer definition, they are not available on the next run of the query viewer.

Query Viewer Variables

To add a local variable, click the **Variables** tab.

- Provide a name for the local variable.
- Choose a function from the drop-down Function menu.
- Fill in other details as needed and click **OK** to add the variable to the query viewer.



The **Add Variable** dialog box is shown. It contains the following fields and controls:

- Name:** A text input field.
- Function:** A dropdown menu currently showing **Add**.
- Add two number:** A text input field.
- Arguments:** A section containing two rows. Each row has a **Number** label, a text input field containing **Count(Event ID)**, and a dropdown menu currently showing **Field**.
- Preview:** A section containing two **Number** labels, each followed by a text input field.
- Calculate:** A button located below the preview fields.
- OK, Cancel, Help:** Three buttons at the bottom of the dialog.

The variable you add here shows up in the following views:

- As a field in the Fields tab in the query viewer editor definition (including the options to **Use** and use as a **Key** field)
- As a column in the query viewer result (If the query viewer result is displayed in the viewer when you add the variable, the variable shows up immediately as a column in the result.)

For example, you can add a Timestamp Function (such as GetHour, GetDayOfWeek, GetDayOfMonth, and so forth).



A query viewer local variable cannot be promoted to a global variable

Local variables defined for data from events, actors, cases, and assets can be promoted to a global variable.

Local variables defined for a query viewer cannot be promoted to a global variable. Query viewers operate on queries, which have their own distinct schema for each instance. A local variable defined for a query viewer is likely only applicable to the specific query viewer it applies to.

For more on using variables in resources, see [“Variables” on page 1006](#).

For more information on global variables (which can be used in queries), see [“Global Variables” on page 477](#).

Query Viewer Drilldowns

Adding **drilldown** capability to a query viewer provides the user the option of getting more focused views (by means of additional query viewers) on particular aspects of a single item (asset, case, event, and so on) in the query result.

On the Drilldowns tab, you can define one or more drilldowns for a query viewer, along with options for each drilldown.

A drilldown always leads to (is based on) another query viewer. Therefore, the first step in creating drilldown(s) is to define the query viewer(s) that provide drilldown results. Once the drilldown query viewers are defined, you can add these to the “starting point” query viewer using its Drilldowns tab.

Drilldowns are presented to users on the right-click **Investigate** menu on results displays in the Viewer.

Create Query Viewers for Drilldowns

As a first step in adding drilldown capability to a query viewer, decide what kind of information you want the user to be able to focus in on and then create query viewers that get that information.

For example, suppose you have a query viewer that returns the top 10 most frequent events by name. The query viewer might also show timestamps for the events and other information, depending on the base query it leverages and what fields are hidden or shown in the query viewer.



Adding a Drilldown to a Query Viewer

To add a drilldown to a query viewer, click the **Drilldowns** tab.

- 1 Click **Add** (+ Add...) to add a new drilldown definition, mappings, and data fields as described in 2.

- 2 Fill in the fields as described in the following table.

Option	Description
Drill down to	<p>Select the query viewer to use for the drilldown.</p> <p>This option provides a drop-down menu for navigating the query viewer tree and selecting a query viewer for the drilldown.</p>
Menu prompt	<p>Provide a description of the drilldown for the Investigate menu prompt.</p> <p>The user will see the text you provide here as a drilldown option on the right-click Investigate menu for this query viewer.</p> <p>Note: Drilldowns are available to users only when they view a query viewer result in table format (View Data As > Table).</p>

Option	Description
Column Mappings	<p>The left side of the Column Mappings shows the columns from the source query viewer (the one you are drilling down <i>from</i>).</p> <p>The right side of the Column Mappings shows the columns from the target query viewer (the one you are drilling down <i>to</i>).</p> <p>For example, the Drilldown definition shown in the figure in Step 1 on page 320 maps the source query viewer "Name" column to the target query viewer "Name" column. This constructs the following drilldown filter:</p> <pre><target>.Name = <source>.Name</pre> <p>where <code><source>.Name</code> is replaced by the actual value from the source query viewer row.</p> <p>You can add or remove column mappings, but your choices are limited to the columns already provided in the query viewer, and field mappings need to be consistent.</p> <p>A field mismatch triggers an error. For example, mapping a name to an IP address is not allowed.</p> <p>For a summary of usage notes, see "Tips on Drilldown Definitions" on page 321.</p>
Data Fields	<p>Data fields are inherited from the query viewer selected for the drilldown. By setting options here you can choose a subset of columns and/or show them in a different order.</p> <p>Settings on data fields here override other query viewer settings.</p> <ul style="list-style-type: none"> You can choose to show (check Use) or hide (uncheck Use) the data fields in the drilldown query viewer result. You can reorder the data fields. To do this, select a data field, then click the up  or down  arrow buttons. (The buttons are on the right, below the Data Fields list). <p>For a summary of usage notes, see "Tips on Drilldown Definitions" on page 321.</p>
Sort Options	<p>Sort options on a drilldown override other query viewer sort settings, and provide an different way of sorting.</p> <p>Click Add to add a field in the query viewer as a column to sort on before displaying.</p> <ul style="list-style-type: none"> Column Sort Order <p>Only fields available in the query viewer being drilled down to are provided as sort options here.</p> <p>To remove a sort on a field, select a column in the Sort Options list and click Remove.</p>

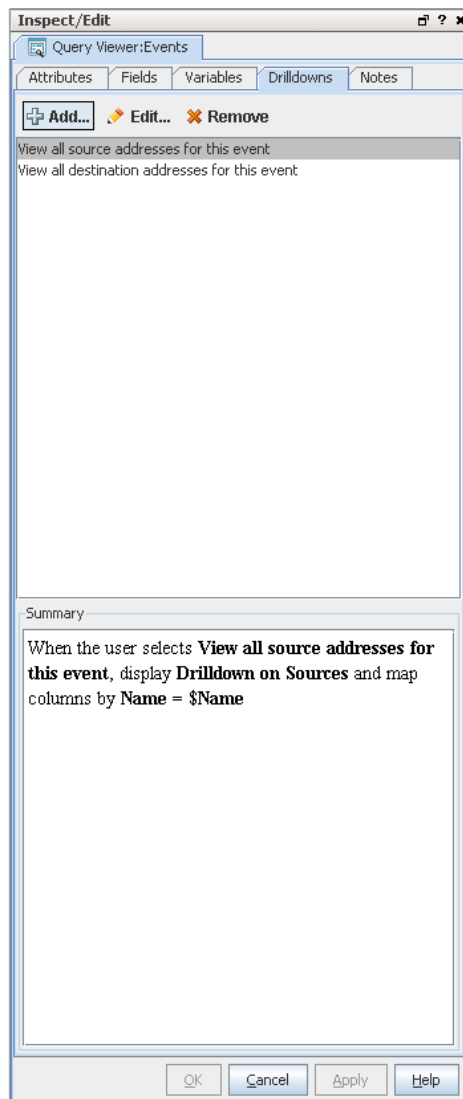
Tips on Drilldown Definitions

- ◆ Drilldowns can be defined for multiple fields of different data types. For example, you could define a drilldown to return a combination of event name and IP

address. The first step would be to define a base query viewer to return these fields in a result (see [“Create Query Viewers for Drilldowns” on page 319](#)), and then, as a next step, add a drilldown and select that query viewer to use as the “Drill down to” query viewer.

- ◆ Drilldowns cannot be defined to go to fields that are SQL functions.
 - ◆ Column and Data Field mappings need to be consistent; a field mismatch triggers an error. For example, mapping a name to an IP address is not allowed.
- 3 Click **Apply** to save the drilldown and keep the query viewer editor open (or click **OK** to save the drilldown and close the query viewer editor).


The “Drilldown to” description is listed on the Drilldowns tab after you click Apply. You can add multiple drilldowns to the same query viewer. All drilldowns are shown on this tab.



Editing a Drilldown

To edit a drilldown:


- 1 If you have not done so already, open the editor for the query viewer you want to edit. (See [“Editing a Query Viewer” on page 323](#).)
- 2 Click the **Drilldowns** tab.

- 3 Select the drilldown you want to edit and click **Edit**  Edit...

The drilldown dialog for this drilldown is displayed. Make changes to the fields and options as described in [“Adding a Drilldown to a Query Viewer” on page 320](#).

Removing a Drilldown


To remove a drilldown from a query viewer:

- 1 If you have not done so already, open the editor for the query viewer you want to edit. (See [“Editing a Query Viewer” on page 323](#).)
- 2 Click the **Drilldowns** tab.
- 3 Select the drilldown you want to remove and click **Remove**  Remove.

Editing a Query Viewer

- 1 Navigate to **Query Viewers** in the Navigator panel and select the query viewer you want to modify.
- 2 Right-click the query viewer and select **Edit Query Viewer** from the context menu. This launches the Query Viewer Editor in the Inspect/Edit panel, and shows the definition for the selected query viewer.
- 3 Edit the query viewer definition as needed. (See [“Customizing Query Viewers” on page 311](#) for details.)
- 4 Click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query Viewer editor without saving changes.)



To edit a query viewer for which results are currently displayed in the Viewer, click the Edit Query Viewer button  on the lower right of the Viewer.

The results display for the query viewer you want to edit must have focus (i.e., be on top) in the Viewer.

Deleting a Query Viewer

- 1 Navigate to **Query Viewers** in the Navigator panel, right-click the query viewer you want to delete, and select Delete Query Viewer.

A confirmation dialog is displayed.
- 2 Click **Delete** to confirm your choice and delete the query viewer. (Or click **Cancel** if you decide you do not want to delete it.)

Example Queries for Common Scenarios

Query viewers can be used to monitor daily network traffic and get high level summaries of typical activity. Query viewers can also be used to drill down on anomalies or other interesting events.

Following is a brief, conceptual scenario of how an *analyst* might use query viewers to *monitor and investigate* certain types of activity.

Also included here is a description of how the *query content developer* might **build and configure** the base query and query viewers that the analyst uses.



In practice, ArcSight ships with pre-built queries and query viewers as standard content. It is likely that the types of resources described here are provided with ArcSight.

Even so, the configuration of the base query and query viewers is described to illustrate and support this example, and show how a content developer might fine tune these resources to gather the information needed.

Basic Analysis High Level Summaries

A security analyst wants to check if anything unusual is happening on their system. He or she brings up a query viewer called “Events” that shows all events by event name for the last 2 hours. The columns include:

- Event name
- Total count of all events
- Count by unique source address
- Count by unique destination address

Analyst’s First View of Events

The analyst can easily glance at the data and see if anything looks out of the ordinary. Columns can be sorted and filters can be changed to refine the details. The data should come up almost immediately.

The screenshot shows the ArcSight Query Viewer window. At the top, there are tabs for 'Live' and 'Events: Table'. Below the tabs, it says 'Query: Events' and '114 shown / 114 matches'. The 'Last Update' is '18 Jun 2008 10:08:20 PDT' and the 'Filter' is 'No Filter'. The table has four columns: 'Name', 'COUNT(Events)', 'COUNT(Source ...)', and 'COUNT(Destina...'. The table lists various events such as 'ActiveList entry expired', 'ActiveList entry updated', 'AddToList: Success', etc., with their respective counts.

Name	COUNT(Events)	COUNT(Source ...)	COUNT(Destina...)
ActiveList entry expired	338	0	1
ActiveList entry updated	2979	0	1
AddToList: Success	3213	0	1
Agent [Nifty Event Player] reconnected	1	1	1
Agent Login	2	1	1
Agent [Nifty Event Player] heartbeat time...	1	0	1
Agent [Nifty Event Player] type [testalert...	1	0	0
Agent updated	2	1	1
Application Event Counts	8	0	0
ArcSight Event Flow Statistics	9	0	0
ArcSight Manager Started	1	0	1
ArcSight User Login	1	1	0
Asset updated	40	0	1
AttachmentOnlyGroup [Package] inserted	1	1	1
Attack From Suspicious Source	2	1	1
Attack Rates by Attacker Zone	2	0	0
Attack Rates by Service	2	0	0
Attack Rates by Targeted Zone	2	0	0
Attacker Zones by Service	2	0	0
Case inserted	2	0	1
Case updated	2	0	1
Channel [Last Hour] got attached	1	1	1
Channel [Last Hour] query completed	2	0	1
Channel [Live] got attached	1	1	1
Channel [Live] query completed	2	0	1
Compromise - Success	2	1	1
Connector Down	1	0	0
Connector Still Down	2	0	0
Connector Up	1	0	0
CreateNewCase: Success	2	0	1
Data_Monitor_Entry_Timeout	1	0	1

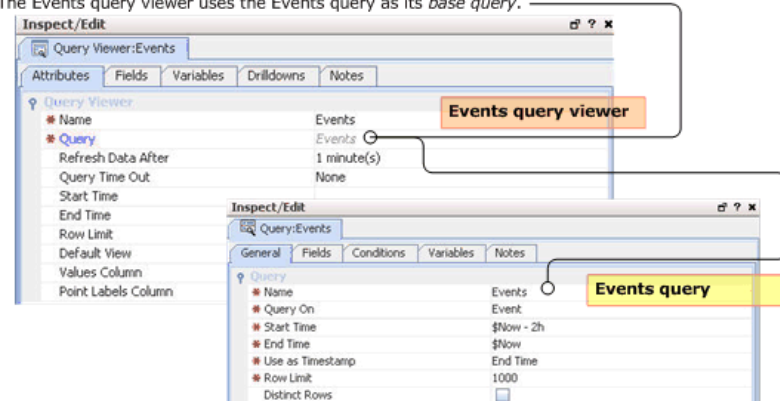
How the Events Query Viewer is Built

The **Events query viewer** described in this example leverages the Events query

Attributes

Bringing up the *query viewer editor* for the **Events query viewer** shows that the Events query is used as the base query. Bringing up the **Events query** (base query) in the *query editor* shows that the base query searches on events for the last 2 hours. (Queries are under Reports > Queries in the Navigator.)

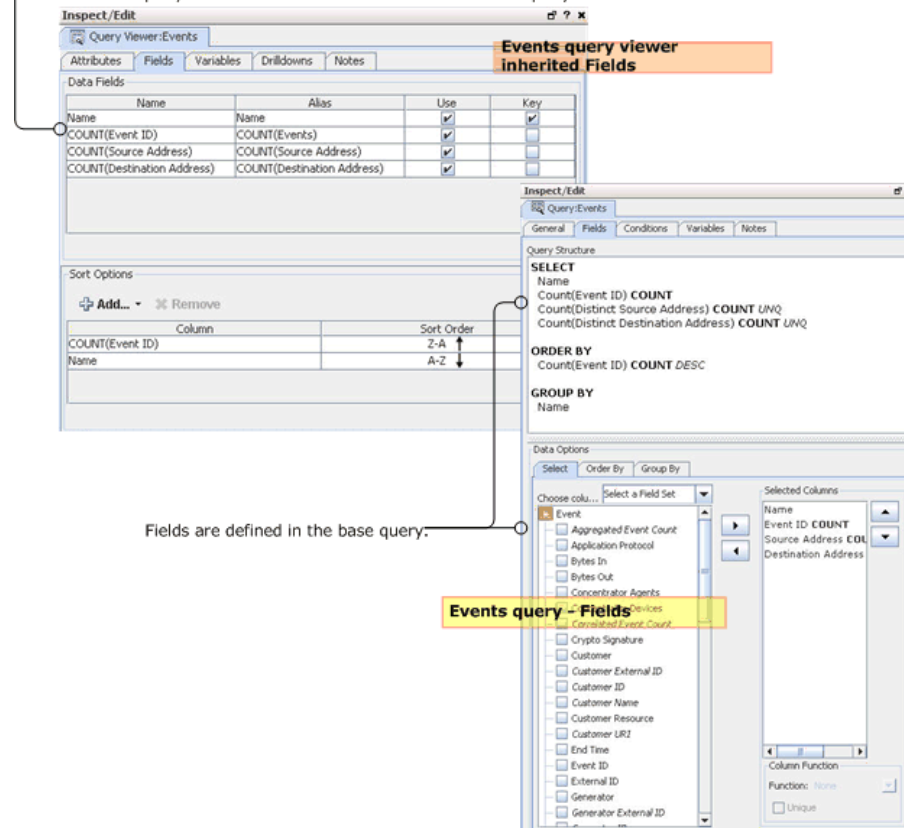
The Events query viewer uses the Events query as its *base query*.



Fields

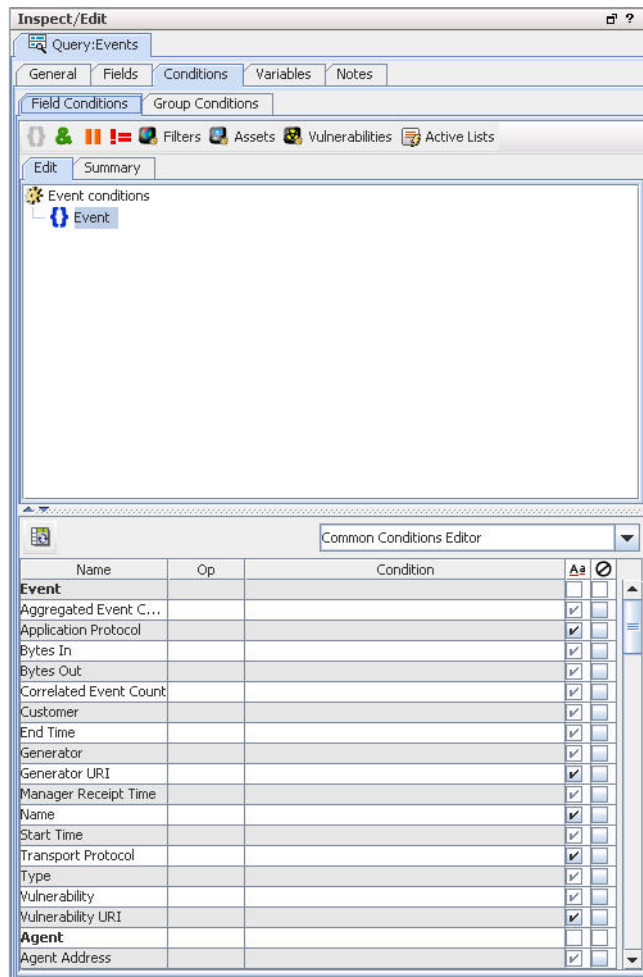
The fields selection, order by, and group by logic are all defined in the Fields tab for the base query. The Events query viewer inherits the fields from the base query. These show up on the query viewer Fields tab.

The Events query viewer inherits fields from the Events base query.



Events Base Query Conditions Tab

The condition logic to search on Events is defined in the Conditions tab for the base query.



Note

If the event value in your query is the @ symbol by itself, enclose it in double quotes. For example:

Name Contains "@"

You are not required to use the double quotes if the @ symbol is used with other text, for example, **Name Contains @mycompany**.

Drilldown Example

Continuing with the previous example, the security analyst notes that one of the counts seems troublesome. For example, "Attack from Suspicious Source" is high and showing a lot of unique destination addresses. The analyst would right-click this row and choose **Show Source Addresses**.

The resulting query viewer would show, for this event and time range, the source addresses, as well as other columns of interest (for example, destination address). Then by sorting by source address, the analyst could decide if a single source address (probably with the highest count) was the initiator of most of the attacks. This information could also be provided from an appropriate back end trend table (the same one or a different one), and, as a result, the display should come up almost immediately.

The screenshot shows the ArcSight Viewer window with the title bar 'Viewer'. The main content area displays a table titled 'Drilldown on Sources: Table'. The query is 'Drilldown-src' with 13 matches shown. The last update is '1 Aug 2008 18:24:12 PDT'. The filter is 'Name = "ICMP PING"'. The table has two columns: 'Source Address' and 'COUNT(Source Address)'. The data is as follows:

Source Address	COUNT(Source Address)
4.158.210.103	1
63.193.245.15	482
64.185.36.108	1
81.43.59.4	1
165.247.165.115	2
203.87.70.177	1
203.203.198.49	1
209.179.130.133	1
209.209.220.94	1
209.214.97.116	1
209.240.160.175	1
218.15.205.24	1
218.52.201.132	1

The status bar at the bottom shows the time range '8/1 16:22:58 - 8/1 18:22:58'.

The analyst could also show **destination** addresses for the same event row, if that drilldown is defined as a part of the query viewer.

The screenshot shows the ArcSight Viewer window with the title bar 'Viewer'. The main content area displays a table titled 'Drilldown on Destinations: Table'. The query is 'Drilldown-dst' with 7 matches shown. The last update is '1 Aug 2008 18:31:53 PDT'. The filter is 'Name = "ICMP PING"'. The table has two columns: 'Destination Address' and 'COUNT(Destination Address)'. The data is as follows:

Destination Address	COUNT(Destination Address)
111.222.101.10	1
111.222.101.20	4
111.222.101.21	3
111.222.101.30	2
111.222.101.140	2
111.222.101.174	1
111.222.121.206	577

The status bar at the bottom shows the time range '8/1 16:31:43 - 8/1 18:31:43'.

How the Drilldowns are Built

The source and destination drilldowns are added to the Events query viewer on the Drilldowns tab at content development time.

Here is the drilldown on sources defined in the Events query viewer example.

The screenshot shows the 'Edit DrillDown Definition' dialog box. The 'Drill down to:' dropdown is set to 'Drilldown on Sources'. The 'Menu prompt:' text box contains 'View all source addresses for this event'. The 'Column Mappings' section shows a table with columns 'Events' and 'Drilldown on Sources', with 'Name' mapped to 'Name'. The 'Data Fields' section shows a table with columns 'Name', 'Alias', and 'Use'. The 'Use' column has checkboxes for 'Source Address', 'COUNT(Source Address)', and 'Name'. The 'Sort Options' section shows a table with columns 'Column' and 'Sort Order'.

Events		Drilldown on Sources
Name	=	Name

Name	Alias	Use
Source Address	Source Address	<input checked="" type="checkbox"/>
COUNT(Source Address)	COUNT(Source Address)	<input checked="" type="checkbox"/>
Name	Name	<input type="checkbox"/>

Column	Sort Order
--------	------------

Here is the drilldown on destinations defined in Events query viewer example.

The screenshot shows the 'Edit DrillDown Definition' dialog box. The 'Drill down to:' dropdown is set to 'Drilldown on Destinations'. The 'Menu prompt:' text box contains 'View all destination addresses for this event'. The 'Column Mappings' section shows a table with columns 'Events' and 'Drilldown on Destinations', with 'Name' mapped to 'Name'. The 'Data Fields' section shows a table with columns 'Name', 'Alias', and 'Use'. The 'Use' column has checkboxes for 'Destination Address', 'COUNT(Destination Address)', and 'Name'. The 'Sort Options' section shows a table with columns 'Column' and 'Sort Order'.

Events		Drilldown on Destinations
Name	=	Name

Name	Alias	Use
Destination Address	Destination Address	<input checked="" type="checkbox"/>
COUNT(Destination Address)	COUNT(Destination Address)	<input checked="" type="checkbox"/>
Name	Name	<input type="checkbox"/>

Column	Sort Order
--------	------------

Non-Event Analysis Example

A security analyst wants to examine "Asset Counts by Vulnerability." The analyst selects this viewer and gets the most recent result (from a trend run) and can examine a table containing columns: Vulnerability and Asset Count. Right-clicking a particular vulnerability row would allow drilldown into the assets with that vulnerability.

Baseline Analysis for Data Comparison

Continuing with the previous example, the security analyst notes that one of the counts seems significantly higher than last recalled. The analyst right-clicks the query viewer and selects "Compare with Baseline", from which there are zero or more baselines to choose.

This makes additional columns available to the currently displayed viewer that can be added by the user. For example, a new column could be added next to the current "Count" column showing "Count - <Selected Baseline>". This is a comparison number showing the difference between the current value of the count and the baseline value for the count. This is positive, negative, or empty (if a baseline doesn't exist for this vulnerability). The analyst can right-click the new column to sort this column in ascending or descending order.

Other options available to the analyst would be:

- **Add as Baseline...** to save the current values in the display as the new named baseline.
- **Compare with...** to compare to any other set of data available in the trend table.

History Analysis Example

As hinted in the previous example, any previous trend runs can be used for baseline comparison. Similarly, the analyst can change the query viewer to go back into the past to look at previous data. The analyst could use the default baseline and go back in history to see when some count began to significantly differ from the baseline.

Chapter 14

Building Reports

These topics describe how you use ArcSight to monitor enterprise security.

[“Understanding Reporting Workflow” on page 331](#)

[“Using Report Templates” on page 335](#)

[“Building Queries” on page 354](#)

[“Building Trends” on page 369](#)

[“Creating Reports” on page 385](#)

[“End-to-End Reporting Examples” on page 407](#)

Reports are captured views or summaries of data that can be viewed in the ESM Console or exported for sharing in a variety of file formats. Reporting is an essential tool for communicating the state of your enterprise security to internal and external stakeholders.

Reporting is a broad subject in ArcSight. Because it can use all the scheduling, conditional logic, resource- and rules-based filtering capabilities of the system, the possibilities can take some time to explore. Creating a report is a multi-step process that can involve steps using several different resources.

See also [Chapter 15, Running and Managing Reports, on page 423](#) and [“Archiving and Scheduling Reports” on page 431](#).

For other options for filtering the database, see [“Query Viewers” on page 287](#), [“Viewing and Using Channels” on page 130](#), and [“Active Channels or Reports?” on page 138](#) under [“Best Practices to Optimize Active Channel Performance” on page 137](#).

Understanding Reporting Workflow

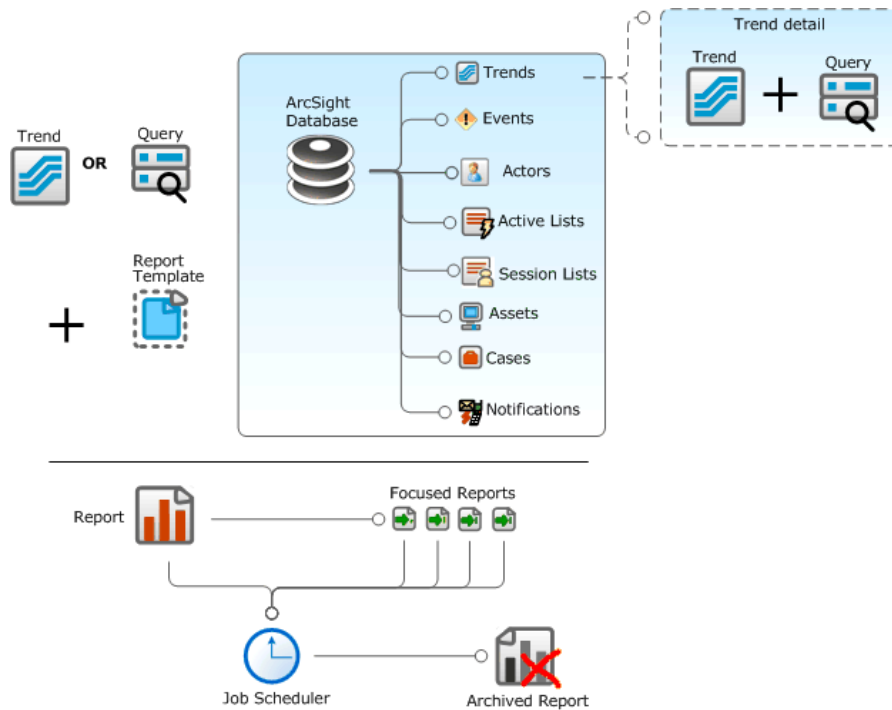
Building Reports is a multi-step process that involves use of a few different data gathering and reporting tools. ArcSight can gather report data using standard queries or trends.



Reports can be relatively simple (you can create a report with the Report Wizard based on the results of a single query) or complex (you can create a report based on the results of layers of queries and trends that feed data results up the chain as the basis for new queries). See [“End-to-End Reporting Examples” on page 407](#) for examples of both basic and complex reports.

Following is a quick overview of reporting workflow tasks and tools, along with a reminder about dependencies among reporting resources.

For a more in-depth description of how these elements build on each other to create various views of the data, see also [“Query-Trend Relationships in Reporting” on page 370](#).



1. Build a Query

A query is an ArcSight resource that defines the parameters of data you want to gather from an ArcSight data source. The results of the query then become the basis for one or more ArcSight report(s) and/or trend(s). As a data source, queries can use the ArcSight database of events, assets, cases, notifications, active lists, session lists, or data gathered from a trend.

Queries are described in [“Building Queries” on page 354](#).



Note

If all you want to do is build a report based on a single query, at this point you can skip to step 4 and select a template. (See [“4. Select or Design a Report Template” on page 333](#).)



Tip

Queries built for reports can be used in query viewers also.

And if you want to run quick SQL queries for monitoring and analysis outside of the reporting resource, you can use query viewers. You can add query viewers to dashboards and generate simple reports on query viewer results.

For information on query viewers, see [Chapter 13, Query Viewers, on page 287](#).

2. Build a Trend (Based on a Query)

A trend is an ArcSight resource that defines how and over what time period data is evaluated for trends. A trend is always based on a query. The trend results are stored in a trend table in the ArcSight database, and are themselves queryable. Trends can also be used as the primary data source for a report.

Trends are described in [“Building Trends” on page 369](#).





If you want a report based on a single trend-query, at this point you can skip to step 4 and select a template. (See [“4. Select or Design a Report Template” on page 333](#).)

3. Build a Query (Based on a Trend)

At this point you have the option of using a simple query or trend in a report, or you can further refine query results by using a trend in another query.


See the [“Building Queries” on page 354](#) and [“Building Trends” on page 369](#) for more information on how to do this.

Data Gathering: Query Building	Data Gathering: Trend Defining
 <p>Query source data</p> <ul style="list-style-type: none"> Specify the data you want to work with Narrow the results by setting conditions and variables 	 <p>Is data a trend?</p> <ul style="list-style-type: none"> Design interval trend to operate on events Design snapshot trend to operate on assets, network model, cases, and notifications

4. Select or Design a Report Template

Use an existing report template layout or create your own using the new Report Designer tool. For information on working with templates, see [“Using Report Templates” on page 335](#).

Layout Designing



Design report template

- Using a stock template?
- Design your own: chart, table, combination

5. Create a Report


A report is an ArcSight resource that binds data from a query or trend to an existing report template. Once run, the results of a report can be viewed in the ESM Console Viewer panel, saved (archived), and/or exported in a variety of formats. Reports can be scheduled to run at regular intervals, and also can be run on demand as needed.

Reports are described in [“Creating Reports” on page 385](#), and an overview of the whole topic is provided in [“Understanding Reporting Workflow” on page 331](#).

Focused reports enable you to run the same report definition on different subdivisions of the data without having to copy and modify the master report every time. For example, you can run an individual Top 10 Infected Systems report for each of your business divisions.

The job scheduler enables you to schedule reports and focused reports to run automatically at specific time intervals. (The job scheduler is also used as a part of building trends which, by nature, involve scheduling.)


Report Building



Bind the query data to the report template

- Refine or customize the query by choosing specific elements of the data
- Add functions
- Format, organize, and re-order results
- Format fonts, text color, and background color

Report Refining



Create focused reports

- Optional
- Narrow the focus of a report using focused reports
- Run the same report with different parameters for each division



Note

Queries and trends are intended to capture data. Reports are used to display the data from queries and trends. For example, if you wanted to run monthly or quarterly reports on VPN login statistics, you would first create one or more queries to capture the data, then create trends (based on the queries) to define a schedule for running the queries and storing the results, and finally create and run reports on the trends. For a full walk-through of this process, see [“End-to-End Reporting Examples” on page 407](#).

6. Run a Report

ArcSight ships with a set of ready-made reports available under the Reports resource. (For example, on the Navigator panel under the Reports resource look in /Reports/Shared/All Reports/ ArcSight Solutions/. Open the sub-groups (folders) to see provided reports.)

For information on how to run an existing report, see [“Running Reports” on page 423](#) and [Running a New or Archived Report](#).

7. Archive and Maintain Reports

After running a report, you can elect to save (archive) the report results. This enables you to retrieve a particular report for immediate viewing without having to regenerate the report. Reports that are run on demand are saved on the Archives tab just like scheduled reports. If the Save Output option is chosen for an on-demand report, the archived report has an expiration date of 6 months from the time it was run (by default). If the Save Output option is not chosen for an on-demand report, the report is maintained in the archive for one day only.

Archived reports can also be sent to a notification group after the scheduled report is run.

For information on how to archive and maintain reports, see [“Archiving and Scheduling Reports” on page 431](#) and [“Managing Reports” on page 428](#).

Report Sharing and Maintenance



Share and maintain report output

- Save report output to share with others using archived reports
- Create and maintain trend partitions

Managing Dependencies for Reports Resources

As you work with these resources, keep in mind that queries, trends, and reports generally have multiple dependencies upon each other. Modifying some elements within one resource can affect another. If modifications to a resource impact another to the extent that the dependent resource is rendered unusable, errors are reflected in the ESM Console. ArcSight manages and updates most of these resources and dependencies automatically, but not all.

For example, a trend built on a query relies on a set of fields (columns) contained in the base query. If you modify fields in the base query that are used in the trend, the trend is disabled. (The proper approach for modifying a query used in a trend is to create a new trend.) Similarly removing a resource (like a query) that another resource (like a report) depends on generates error messages on the ESM Console.

Using Report Templates

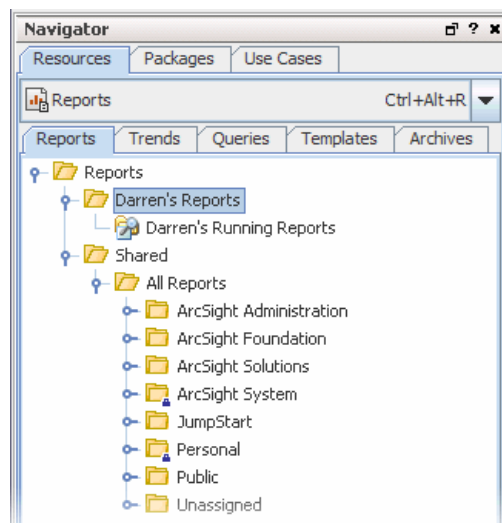
To provide more flexibility in reporting, ArcSight now offers powerful report template tools including a rich offering of ready-made templates and a template design wizard for more customized reports. Template definitions determine how query and trend data are displayed in a report. You can create and adjust templates to specify which data is displayed, what visual elements are used (variations on tables, charts, graphs, and so on), the layout of those elements, the report output file format, and much more. A template consists of report design elements, such as headers, footers, title bars, charts, and tables, arranged on a page according to a layout specification.

Templates can accommodate input from multiple queries and show multiple visual elements, such as three charts and a table each pulling from a different data source, in a single report.

You can use the templates provided or create custom templates with the report template designer.

Navigating to Templates

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Templates** tab.



Report templates are a component of ArcSight Reporting resource tools. Be sure to see ["Building Reports" on page 331](#) for an overview of all reporting tasks and tools.

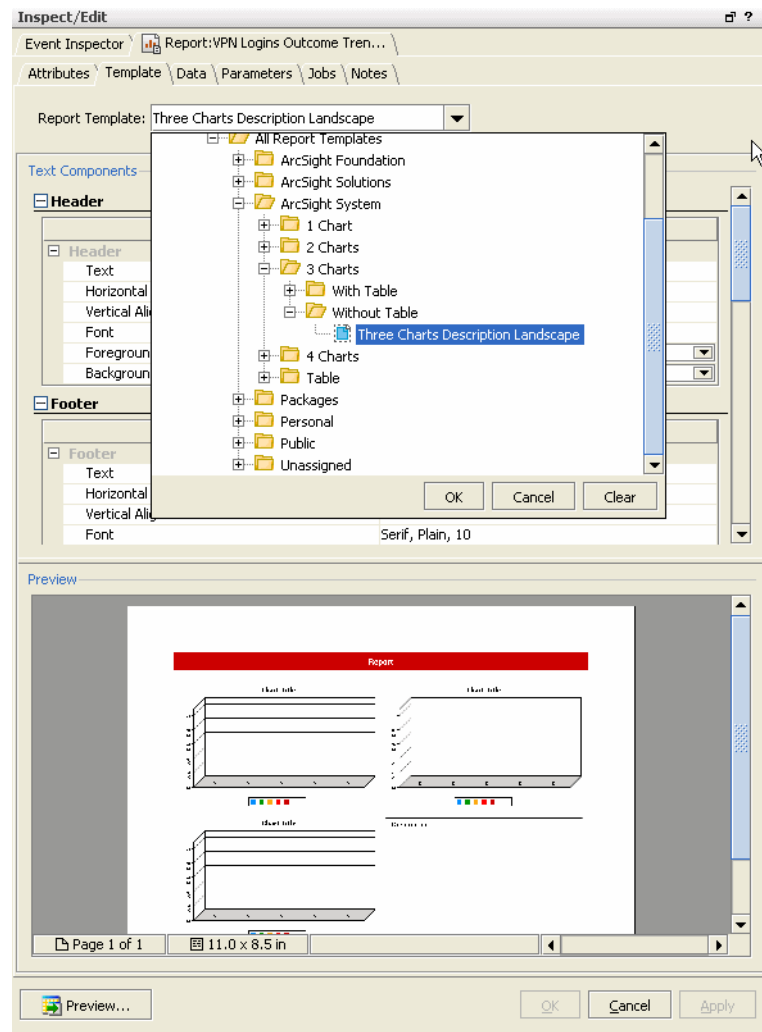
Using Standard Templates

To get you started, ArcSight provides a rich set of templates you can use as-is or copy to use as a starting point for your own template layouts. There are two ways to use standard templates for reports. You can apply a template to an existing report, or you can create a new report based on a template.

Applying a Template to an Existing Report

- 1 With the **Reports** resource selected in the Navigator panel, click the **Reports** tab.
- 2 If Reports groups (folders) are collapsed, click **+** to expand user and Shared folders and view reports.
- 3 Double-click the report to which you want to apply a template. (Alternatively, you can select the report, right-click and select **Edit Report** from the context menu.) This brings up the Report editor in the Inspect/Edit panel.
- 4 In the Report editor, click the **Templates** tab for the selected report.
- 5 In the **Report Template** field drop-down menu, select a template.
- 6 Click **OK** to apply the template and close the file browser.

- 7 Click **Apply** or **OK** to verify and save the template choice for the selected report.



Creating a New Report Based on a Template

- 1 With the **Reports** resource selected in the Navigator panel, click the **Templates** tab.
- 2 Right-click your user folder (group) and select **New Report from Template**. This launches the Reports Editor in the Inspect/Edit panel with the chosen template.
- 3 See [“Creating Reports” on page 385](#) for details on how to define data for your report and fine-tune the template by means of the Template tab in the Report editor for this report.

Copying a Template

An easy way to get started customizing a template is to copy an existing template and modify it to suit your needs. To copy a template:

- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Open the All Report Templates folder, navigate to a template you want to copy, and select it.
- 4 Left-click, and drag and drop the selected template into your user folder.

- 5 Select **Copy** from the Drag & Drop Options dialog. A copy of the template is dropped into your user folder.

Alternatively, you can select the template you want to copy in the Navigator and choose **Edit > Copy** from the menus. Then select your user folder and click paste to drop the template into the folder.

Opening the Designer to Edit a Template

- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Right-click a template and choose **Open in Designer**, or choose **Edit Template** and click the **Open in Designer** button on the Attributes tab for the template editor.

For more about using the template Designer, see [“Designing Custom Templates” on page 338](#).



Note

The Report Designer is powered by InetSoft, who provide the Report Designer's online help.

- There are additional InetSoft documents available online for the report designer. They are attached to an ArcSight Knowledge Base article entitled “InetSoft's Online Help Guides.”
 - For support, contact ArcSight support. Do not use the InetSoft support information mentioned in their documentation.
-

Designing Custom Templates

You can use the report template designer to create report templates specific to the needs of your organization. This can be useful, for example, if you need to customize reports per corporate branding, policy requirements, or standards compliance. This can be useful, for example, if you need to customize reports per corporate branding, policy requirements, or standards compliance. (You can also copy the stock templates and use the Designer to modify these templates to suit your needs.)

Opening the Template Designer to Edit Existing Templates

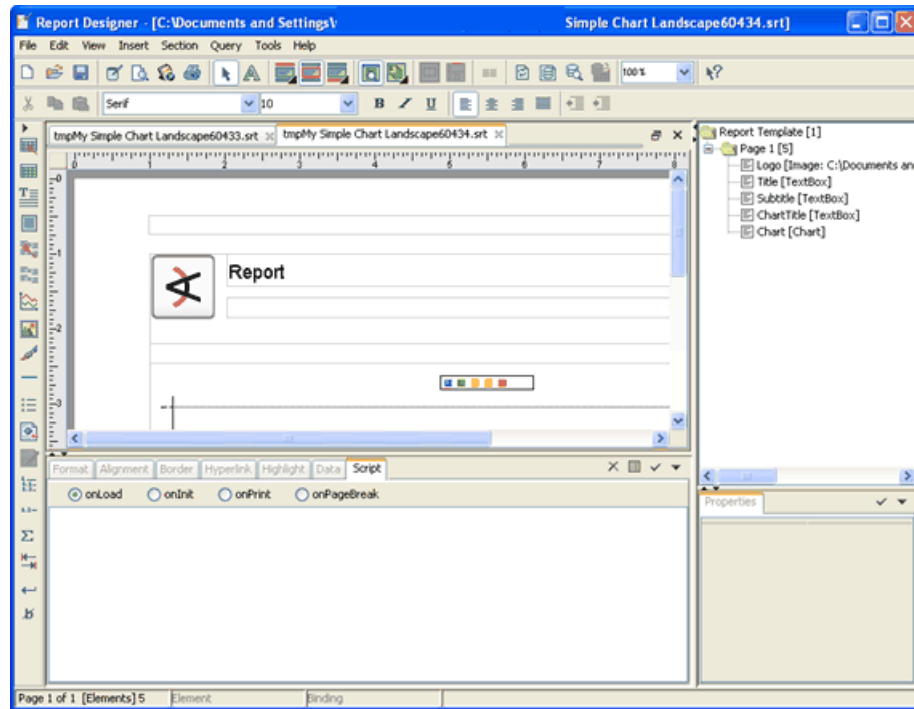
- 1 Select the **Reports** resource in the Navigator.
- 2 Click the **Templates** tab.
- 3 Right-click a template and choose **Open in Designer**, or choose **Edit Template** and click the **Open in Designer** button on the Attributes tab for the template editor.

Creating a New Template

To design a custom template, you need to first create a new template then launch the report designer wizard:

- 1 With the Reports resource selected in the Navigator panel, click the **Templates** tab.
- 2 Select the template group (folder) where you want to store your new template. (We suggest that you create new content in your user folder. The name of this folder depends on the user name with which you logged into the ESM Console.)
- 3 Right-click and select **New Template** from the context menu. This brings up the Template editor in the Inspect/Edit panel.
- 4 Provide a **Name** for the new template in the Template Editor and click **OK**. (Your new template is now displayed in the group you selected in the Navigator.)

- 5 In the Navigator panel, select the template you just created, right-click, and select Launch Designer from the context menu. This starts the Report Designer, as shown below. Use the Report Designer to create custom templates.



From the Report Designer menus, you can launch wizards for building common report elements such as **Section > Section Wizard** and **Query > Table Wizard**.

Template Designer User Interface

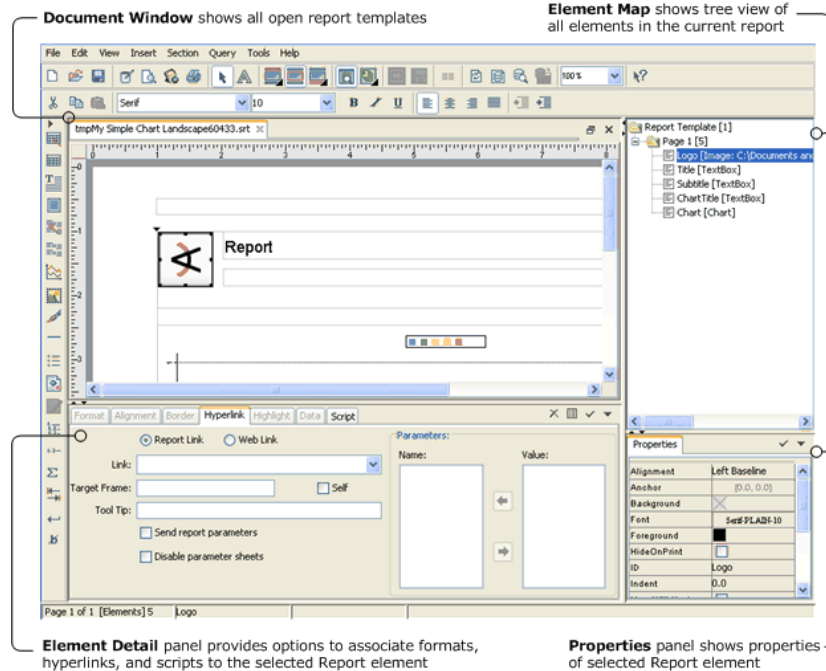
The Report Template Designer provides options for creating fully customized report templates. These topics introduce the Designer features and functions, and provide a quick tour of the user interface (UI).

Tour of Designer UI

The Report Template Designer user interface (UI) consists of the following panels and tools. See also ["Menus" on page 341](#) and ["Toolbars" on page 344](#) for detailed descriptions of those options.

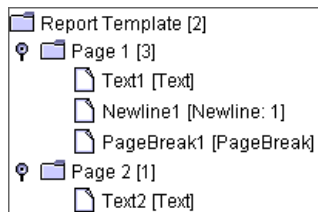
Overview Diagram

Report Template Designer: You can use the Report Designer to create custom templates. To launch the Report Template Designer, right-click a template in the Navigator and choose Open in Designer, or choose Edit Template and click the Open in Designer button on the Attributes tab for the template editor.



Element Map

The element map displays a hierarchical tree view of all elements in the current report. The element map appears in a frame between the report element toolbar and the document window, and looks like this:



Selecting an element on the element map causes that element to be selected in the report.

To display the element map, click **Element Map** on the **View** menu.

Document Window

The document window is the largest window on the Report Designer screen and contains all the currently opened report templates. Reports can be minimized, maximized, resized and moved within the document window.

- To arrange open report templates, click **Cascade** on the **Window** menu.
- To change the active report template, click the template's file name on the **Window** menu.

Status Bar

The status bar appears at the very bottom of the Report Designer application window and looks like this:



The information displayed on the status bar, from left to right, is as follows:

- Current page number
- The number of elements in the current page
- The ID of the currently selected report element
- Information about the currently selected report element: ID and element type

Change the Report View

Normal View

Click the **View** menu
Check the checkbox button to
the left of **Layout View**

or

Click the **Layout**  toolbar button
when the report is in page layout view



Page Layout View

Click the View menu
Uncheck the checkbox button to
the left of **Layout View Change
the Editing Mode**

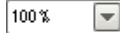
or

Click the **Layout**  toolbar button
when the report is in normal view.

Change the Editing Mode

- To switch to Element Selection Mode, click the **Selection Mode (Pick Tool)**  toolbar button.
- To switch to Text Mode, click the **Text Mode (Text Tool)**  toolbar button.

Change the Report Magnification

To increase or decrease the display size of the report (zoom in or zoom out), select the magnification percentage from the drop-down list  on the toolbar.

Menus

The Report Template Designer menus are described in the following tables.


















File Menu item	Description
New	Creates a new Style Report template.
Save	Saves the current report template.
Export	Exports the current report in one of the following formats: PDF, HTML, Excel, RTF, SVG, CSV, or text.
Preview	Displays a preview of the generated report in a new window.
Print	Prints the current report.



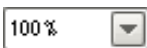

















File Menu item	Description
Page Setup	Sets the current report's page format properties.
Most recently used file list	These menu items display the most recently opened reports. Clicking one of these items opens the corresponding report template in a new window.
Exit	Exits the Report Designer.
Edit Menu item	Description
Undo	Reverses, one at a time, a series of editor actions.
Copy	Copies the current selection to the clipboard.
Cut	Deletes the selection from the report and copies it to the clipboard.
Paste >> Into Page	Inserts the contents of the clipboard into the current document.
Paste >> Into Section	Inserts the contents of the clipboard into selected Section element.
View Menu item	Description
Layout View	Sets the report view to either Normal view or Layout view.
Element Map	Displays a tree mapping all report elements on the page in a frame to the left.
Ruler	Sets the visibility of the ruler.
Grid	Sets the visibility of the grid.
Snap To Grid	Sets whether inserted report elements should be placed at the nearest grid vertex or not.
Properties	Displays the properties dialog for the selected report element.
Console	Displays the error console.
Insert Menu item	Description
Header	Elements are inserted into the page header.
Body	Elements are inserted into the page body.
Footer	Elements are inserted into the page footer.
Basic Element >> Table	Inserts a table.
Basic Element >> Text	Inserts a text element.
Basic Element >> Textbox	Inserts a text box.
Basic Element >> Image	Inserts an image.
Basic Element >> Chart	Inserts a chart.



Insert Menu item	Description
Basic Element >> Tab	Moves the insertion point to the next tab stop.
Basic Element >> Bullet	Inserts a bulleted item.
Basic Element >> Separator	Inserts a horizontal line across the page.
Spacing Element >> Newline	Inserts a newline.
Spacing Element >> Break	Inserts a line break.
Spacing Element >> Space	Inserts a non-breaking space.
Spacing Element >> Page Break	Inserts a page break.
Spacing Element >> Conditional Page Break	Inserts a page break that only occurs when one or more specified conditions are met.
Spacing Element >> Area Break	Inserts an area break.
Special Field >> Table of Contents	Inserts a table of contents.
Special Field >> Page Number	Inserts a text element displaying the current page number into the header or footer.
Special Field >> Page Count	Inserts a text element displaying the page count into the header or footer.
Special Field >> Date	Inserts a text element displaying the current date into the header or footer.
Format Menu item	Description
Preference	Displays the formatting preferences dialog.
Draw Area	Inserts a new page area into the report template.
Order Area	Changes the flow order of the page areas in the report template.
Window Menu item	Description
Cascade	Places all document windows in a cascading arrangement.
Close All	Closes all document windows.
Window list	This list contains a menu item for each open document window. Clicking one of these items brings the corresponding window to the foreground.

Toolbars

The Report Template Designer toolbars are described in following tables.

Standard Toolbar	Description
 Save	Saves the current report template.
 Preview Report	Displays a preview of the generated report in a new window.
 Print	Displays the print dialog, allowing the user to print the active document.
 Selection Mode (Pick Tool)	Switches to element selection mode.
 Text Mode (Text Tool)	Switches to text editing mode.
 Cut	Copies the current selection to the clipboard and deletes the selection from the report.
 Copy	Copies the current selection to the clipboard.
 Paste	Inserts the contents of the clipboard into the current document.
 What's This	Clicking this item and then a menu item, toolbar button or window region displays help information on what was clicked.
Layout Toolbar	Description
 Header	Elements are inserted into the page header.
 Body	Elements are inserted into the page body.
 Footer	Elements are inserted into the page footer.
 Element Map	Sets the report view to Normal Layout view, with a tree mapping all report elements on the page in a frame to the left (in Report Designer).
 Layout View	Switches between Normal and Layout views, and displays the page layout properties dialog.
 Draw Area	Inserts a new page area into the report template.
 Order Area	Changes the flow order of the page areas in the report template.
 Columns	Places two page areas side-by-side on the page to split the report into columns. The areas flow from left to right.

Format Toolbar button		Description
	Font	Sets the current font. To use Japanese characters in reports, install the Arial Unicode MS True Type font (ARIALUNI.TTF) or an equivalent Unicode font in your system font directory. Use that font for any component (such as a textbox or a table) for which you want Japanese/Unicode characters.
	Font Size	Sets the current font size.
	Zoom	Zooms in and out according to the percentage selected.
	Bold	Makes text boldface.
	Italic	Renders the current text in italics.
	Underline	Underlines the current text.
	Left Justify	Changes the alignment to left justification.
	Center	Changes the alignment to center justification.
	Right Justify	Changes the alignment to right justification.
	Fill	Changes the alignment to fill justification.
	Decrease Indent	Decreases the current indentation.
	Increase Indent	Increases the current indentation.
Report Element Toolbar button		Description
	Table	Inserts a table.
	Text	Inserts a text element.
	Text Box	Inserts a text box.
	Chart	Inserts a chart.
	Image	Inserts an image.
	Separator	Draws a horizontal line across the page.
	Table of Contents	Inserts a table of contents.
	Tab	Moves the insertion point to the next tab stop.

Report Element Toolbar button	Description
 Newline	Inserts a newline.
 Space	Inserts a non-breaking space.

Setting Report Page Options

As a part of your report template designs, you can set page options such as page size, orientation, margins, and so forth. The page settings you define at template design time are built into the “deployed” template as defaults.

Setting the Page Size

- 1 Select the **File > Page Setup** from the menus.
- 2 Select a page size from the drop-down list, or enter the size and units of measurement for non-standard page sizes.
- 3 Click the **OK** button.

Setting the Page Orientation

- 1 Select the **File > Page Setup** from the menus.
- 2 Select either **Portrait** or **Landscape**.
- 3 Click the **OK** button.

Setting the Page Margins

- 1 Select the **File > Page Setup** from the menus.
- 2 Set the distance, in inches, from the edge of the page for the **Left**, **Top**, **Right**, and **Bottom** fields
- 3 Set the distance, in inches, from the edge of the page to the top of the page header and footer in the **Header** and **Footer** fields.
- 4 Click the **OK** button.

Setting the Page Background

Select the **File > Page Setup** from the menus, and click the **Background** tab.

Setting a Background Color


- 1 Select the **Color** option.
- 2 Select a color from the drop-down list.
- 3 Click the **OK** button.

Setting a Background Image


- 1 Select the **Image** option.
- 2 Enter the path to the image.
- 3 Select the loading method.
- 4 To embed the image in the template file, check the **Embed** option.
- 5 Select either **Tile** or **Center** positioning option.
- 6 Enter preferred size of image or leave unspecified for actual image size.

- 7 Click the **OK** button.

Editing the Page Header

- 1 Click the Header  toolbar button or select the **Header** item from the **Insert** menu.
- 2 Insert and edit report elements as you would normally.


Editing the Page Footer

- 1 Click the Header  toolbar button or select the **Header** item from the **Insert** menu.
- 2 Insert and edit report elements as you would normally.


Designing Report Flow Layout

With the Report Template Designer, you can design the flow layout for a report template that specifies layout of the report content on the page.

Drawing a Page Area

- 1 Change the report view to **Layout**
- 2 Click the **Draw Area**  toolbar button.
- 3 Click and hold the left mouse button where you want the upper-left corner of the page area to be placed.
- 4 Continue holding the left mouse button and drag the cursor to the location you want for the lower-right-hand corner of the page area.
- 5 Release the mouse button.


Changing the Order of Page Areas

- 1 Set the report view to **Page Layout**.
- 2 Click the **Order Areas**  toolbar button.
- 3 Move the mouse over the area you want to receive the flow first. The cursor should turn into a hand.
- 4 Click the left mouse button. The number in the corner of the page area should now be "1".
- 5 Repeat steps 3 and 4 for each page area, in the order you want to flow.

Inserting an Area Break

- 1 Click the cursor on the location where you want the break.
- 2 Select the **Area Break** from the **Insert»Spacing Element** menu.

Creating a Non-flow Area


- 1 Set the report view to **Page Layout**.
- 2 Click the **Draw Area**  toolbar button.
- 3 Click and hold the left mouse button where you want the upper-left corner of the page area to be placed.
- 4 Continue holding the left mouse button and drag the cursor to the location you want for the lower-right corner of the page area.

- 5 Release the mouse button.
- 6 Right-click the page area you just created.
- 7 Click **Properties** on the popup menu.
- 8 Disable (uncheck) the **Flow Area** property.
- 9 Click the **OK** button.

Creating a Fixed Position Element

- 1 Set the report view to **Page Layout**.
- 2 Click a non-flow area.
- 3 Set the report view to **Normal**.
- 4 Insert the element into the non-flow area as you would a normal page area.

Creating an Element Associated Area

- 1 Set the report view to **Page Layout**.
- 2 Click the small arrow in the corner of the **Layout**  toolbar button.
- 3 Click the **Edit** item on the drop-down menu.
- 4 From the drop-down list on the dialog, select the report element you want to associate with the page layout.
- 5 Click the **New** button.
- 6 Click the **OK** button.

Creating Parallel Report Flows

- 1 Set the report view to **Page Layout**.
- 2 Create a non-flow area to one side of the report.
- 3 Create normal report areas in the remaining page area however you want.
- 4 Right-click the non-flow area.
- 5 Click the **Properties** item on the popup menu.
- 6 Deselect (uncheck) the **Repeat Contents** property.
- 7 Set the report view to **Normal**.
- 8 Place report elements in the non-flow area for one part of the parallel report flow.
- 9 Place report elements in the other page areas for the other part of the parallel report flow.

Designing Report Tabular Layout

Using the Report Template Designer, you can define the default layout for tables in a report template.

Inserting a Row

- 1 Set the report view to **Page Layout**.
- 2 Click the row you want to insert the new row before.
- 3 Right-click the row.

- 4 Click **Insert Row** on the popup menu.

Inserting a Column

- 1 Set the report view to **Page Layout**.
- 2 Click the column you want to insert the new column before.
- 3 Right-click the column.
- 4 Click **Insert Column** on the popup menu.

Deleting a Row

- 1 Set the report view to **Page Layout**.
- 2 Click the row you want to delete.
- 3 Right-click the row.
- 4 Click the **Delete Row** item from the popup menu.


Deleting a Column

- 1 Set the report view to **Page Layout**.
- 2 Click the column you want to delete.
- 3 Right-click the column.
- 4 Click the **Delete Column** item from the popup menu.

Splitting a Cell

- 1 Set the report view to **Page Layout**.
- 2 Click the cell you want to split.
- 3 Right-click the cell.
- 4 Select the **Split Cell** item on the popup menu.
- 5 To split the cell horizontally select **Rows**; to split the cell vertically select **Columns**.
- 6 Enter the number of cells to split the current cell into.
- 7 Click the **OK** button.

Resizing a Cell

- 1 Set the report view to **Page Layout**.
- 2 Move your mouse over the cell's edge until the cursor changes to the resize cursor. 
- 3 Press and hold the left mouse button.
- 4 Drag the mouse until the cell is the desired size.
- 5 Release the mouse button.


Building Report Elements into a Template

The following topics describe how to use the Report Template Designer to include different types of report elements into a template.

Inline Elements

Inline elements include options for inserting text, text formatting, working with tabs, and spaces.

Inserting Text

- 1 Click the report at the location you want to insert the text.
- 2 Click the Text  toolbar button or select the **Text** item from the **Insert>>Basic Element** menu.
- 3 Type the text to display.


Formatting text

- 1 Right-click the text or textbox element.
- 2 Select the format to apply from the **Format** submenu on the popup menu.

These formats are available in the Report Designer:

Format Type	Description
Date format	Specifies conversion for date/time values.
Decimal format	Specifies conversion for numeric values.
Currency format	Specifies formatting of numbers as currency (with a currency symbol).
Percent format	Specifies formatting of numbers as percentages.

Inserting a Tab

To insert a tab, press the **Tab** key or click the Tab  toolbar button.

Setting the Tab Stops

Select the **Format > Preferences** item from the menus, and click the **Tab Stops** tab.

Adding a Tab Stop


- 1 Enter the distance, in inches, from the left margin to position the tab stop in the text field.
- 2 Click the **Set** button.

Removing a Tab Stop

- 1 Select the tab stop from the list.
- 2 Click the **Clear** button.

To apply the changes, click the **OK** button.

Inserting a Space

To insert a space, press the **Space** key or click the Space  toolbar button.

Setting a Space's Width

- 1 Click the space element to format.
- 2 Right-click the element.

- 3 Select the **Properties** item from the popup menu.
- 4 Enter the width, in points, of the space in the **Number of Points** field.
- 5 Click the **OK** button.

Float Elements

Float elements include options for setting anchors, working with text wrap, setting margins, working with charts and text boxes, and inserting images.

Setting the Anchor

- 1 Move the mouse over the float element.
- 2 Click and hold the left mouse button.
- 3 Drag the element to the desired position.
- 4 Release the mouse button.

If a float element's anchor is not set, it is laid out as an inline element.

Setting the Text Wrapping

When one or more anchored elements exist on a line, other flow elements could wrap around the anchored elements. To set the wrapping:

- 1 Click the element to edit.
- 2 Right-click the element.
- 3 Select the **Properties** item from the popup menu.
- 4 Click the **Layout** tab.
- 5 Select the wrapping style to apply to this element.

The Report Designer offers these wrapping styles:



No wrapping; the flow overlaps the float element.



Wraps around the left side of the float element.



Wraps around the right side of the float element.



Wraps around both sides of the float element.




No contents allowed on either side of the float element.

Setting the Margins


- 1 Click the element to edit.
- 2 Right-click the element.
- 3 Select the **Properties** item from the popup menu.
- 4 Click the **Layout** tab.

- 5 Enter the size, in points, in the **Left**, **Top**, **Right**, and **Bottom** fields.
- 6 Click the **OK** button.


Inserting a Chart

- 1 Click the report at the location you want to insert the report.
- 2 Click the Chart  toolbar button or select the **Chart** item from the **Insert** >> **Basic Element** menu.
- 3 Select the chart type from the drop-down list that appears.

Inserting a Text Box

- 1 Click the report at the location to insert the element.
- 2 Click the Text Box  toolbar button or select the **Text Box** item from the **Insert** >> **Basic Element** menu.
- 3 Type the text to display.
- 4 Right-click the text box and select the **Properties** item from the popup menu to apply formatting.

Inserting an Image


- 1 Click the report at the location you want to insert the image.
- 2 Click the Image  toolbar button or select the **Image** item from the **Insert** >> **Basic Element** menu.
- 3 Enter the path to the image in the text field.
- 4 Check the **Embed** option if you want to embed the image data in the report template.
- 5 Select the loading option (see below) to use.
- 6 Click the **OK** button.

The loading options supported by the report designer are:

Loading Option	Description
Resource	Loads the image as a resource. The path to the image must be relative to the class path.
URL	Loads the image from the specified URL.
Relative path	The path to the image is relative to the location of the report template in the local file system.
Full path	The path to the image is the full path on the local file system.

Block Elements


Inserting a Table

- 1 Click the report at the location you want to insert the table.
- 2 Click the Table  toolbar button.
- 3 Select the number of rows and columns for the table.


Or

- 1 Click the report at the location you want to insert the table.
- 2 Select the **Table** item from the **Insert>>Basic Element** menu.
- 3 Edit the number of rows and columns for the table by selecting the table element.
- 4 Right-click and select **Properties**.
- 5 Select **Headers and Data** tab and modify rows and columns fields and click **OK**.


Inserting a Bullet

- 1 Click the report at the location you want to insert the bullet.
- 2 Click the Bullet  toolbar button or select the **Bullet** item from the **Insert>>Basic Element** menu.
- 3 Type the text to appear next to the bullet. The bullet and the text are separate elements.

Inserting a Separator Change a Separator's Line Style

- 1 Click the report at the location you want to insert the separator.
- 2 Click the Separator  toolbar button or select the **Separator** item from the **Insert>>Basic Element** menu.

Inserting a Newline

- 1 Click the report at the location to insert the newline.
- 2 Click the Newline toolbar  button or press the **Enter** key.

Changing a Newline's Height

- 1 Click the newline element to edit.
- 2 Right-click the element and select the **Properties** item from the popup menu.
- 3 Enter the number of lines in the **Number of Newlines** field.
- 4 Enter the height, in points, of each newline in the **Newline Size** field.
- 5 Click the **OK** button.

Inserting a Page Break

- 1 Click the report at the location to insert the page break.
- 2 Select the **Page Break** item from the **Insert>>Spacing** Element menu.

Inserting an Area Break




- 1 Click the location in a page area to insert the break.
- 2 Select the **Area Break** item from the **Insert>>Spacing Elements** menu.

Drawing a Freehand Shape


- 1 Change the report view to **Page Layout**
- 2 Click one of the shape buttons on the report element toolbar.
- 3 Press and hold the left mouse button at the location of the upper-left corner of the shape.

- 4 To constrain a rectangle to a square, or an oval to a circle, hold down the **Shift** key.
- 5 Drag the mouse to the location of the lower-right corner of the shape.
- 6 Release the mouse button.


You can draw these freehand shapes:

	A rectangle or square
	An oval or circle
	A line

Inserting a Numbered Heading


- 1 Click the report at the location to insert the heading.
- 2 Click the Heading  toolbar button.
- 3 Select the heading level from the drop-down list.
- 4 Type the text for the heading.

Inserting a Table of Contents

- 1 Click the report at the location to insert the table of contents.
- 2 Click the Table of Contents  toolbar button or select the **Table of Contents** item from the **Insert>>Special Field** menu.
- 3 Select the style for the table of contents from the drop-down list.
- 4 Click the **OK** button.

The table of contents is generated automatically, based on the numbered headings in the report.

Changing an Element's Font

- 1 Click the element whose font you want to modify.
- 2 Select the font's name from the drop-down list on toolbar.
- 3 Select the font size from the drop-down list on the toolbar.
- 4 To make the font bold, click the Bold **B** toolbar button.
- 5 For an italic font, click the Italic  toolbar button.
- 6 To underline the font, click the Underline U toolbar button.

Building Queries

A query is an ArcSight resource that defines the parameters of the data you want to report on derived from an ArcSight data source. The result of the query then becomes the basis

for one or more ArcSight report and/or trend. The Query Editor is a component of ArcSight Reporting resource tools.



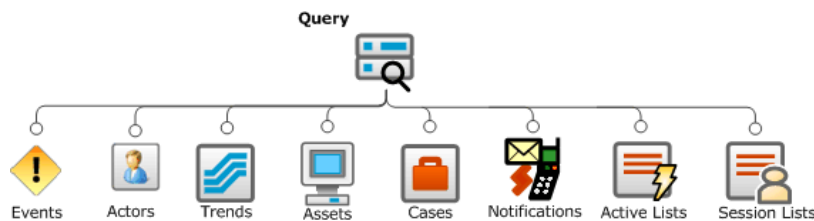
Queries built for reports can also be used in query viewers

And if you want to run quick SQL queries for monitoring and analysis outside of the reporting resource, you can use query viewers. You can add query viewers to dashboards and generate simple reports on query viewer results.

For information on query viewers, see [Chapter 13, Query Viewers, on page 287](#).

How Queries Work

As a data source, queries can use the ArcSight database of events, actors, modeled network objects (assets), cases, notifications, session lists, or active lists, or data gathered from a trend.



In a query, you select the data fields you want to report on, specify any additional functions you want run on them (such as sum, average, and so on), and any sort or group-by conditions you want to add, such as grouping results by source address, zone, or priority.

Using Queries and Trends Together for Reports

A query can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.

For a more detailed description of the relationships you can build between queries and trends for reporting, see the [“Query-Trend Relationships in Reporting” on page 370](#).

Using Queries in Query Viewers

You can use queries built for reports in *query viewers*, outside of the reporting paradigm. Query viewers provide a “channel-style” view of SQL query results but are not limited to events in terms of scope. They provide high-level summaries to monitor system health, reveal trends, and allow for drill-down and investigation of all types of resources across time. Query viewers are performance-tuned to work with trend tables rather than event tables, and so can return results much faster than active channels.

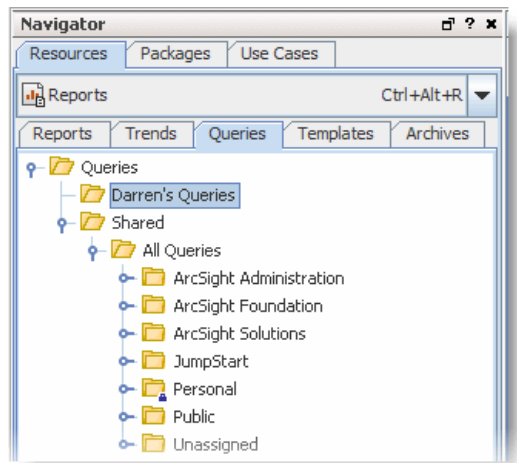
Query viewers include their own simple reporting option by which you can initiate a report on the query results from the query viewer.

For more about using query viewers, see [Chapter 13, Query Viewers, on page 287](#).

Building a Query

Navigating to Queries

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Queries** tab.



Creating a New Query

The high-level steps for creating a query are as follows:

- 1 Right-click a group (folder) and select **New Query**. This launches the Query Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 2 Define General Attributes. At a minimum, fill in the required values (red asterisks) on the General tab.
- 3 Define a schema for Query Fields.
- 4 Create Query Conditions.
- 5 Define Query Variables (optional).
- 6 Click **Apply** or **OK** to create the new query.



Be sure to click **Apply** or **OK** frequently to save settings intermittently as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings using these buttons, your settings are not saved.

The following sections provide details on how to use the Query editor to define query attributes, fields, conditions, and variables.

Defining Query Settings

Use the Query Editor to build a new trend or edit an existing one. Query settings are defined on multiple sub-tabs.

General Attributes

The following fields in the **Query** section are required attributes that must be specified when creating a new query.

Query Fields	Description
Name	Name for the query. Spaces and special characters are OK. This is an alias for the query that appears in pick lists in other editors.
Query on	<p>From the drop-down menu, select one of the following data sources:</p> <ul style="list-style-type: none"> • Event - Select Event if you want to create a report or view trends on event activity • Active List - Select Active List to query or view trends on list entries. (For more about active lists, see "Managing Active Lists" on page 571.) • Actor - Select Actor to query or view trends on actor information. (For more information on actors, see "Actors" on page 239.) • Asset - Select Asset if you want to report or view trends on statistics about the assets on your network, such as a list or count of assets categorized in a particular asset category, or the zone a particular asset is in at a particular time. (For more about assets, see "Modeling the Network" on page 731.) • Case - Select Case if you want to report or view trends on the status of cases, such as number of cases opened and resolved. (For more about cases, see "Case Management and Queries" on page 585.) • Notification - Select Notification if you want to report or view trends on the status of events sent out in the notification workflow, such as number of events in the Investigate stage. (For more about notifications, see "Managing Notifications" on page 658.) • Session List - Select a Session List to query on or view trends on session activity. (For more about session lists, see "Managing Session Lists" on page 579.) • Trend - Select Trend if you want to report or maintain trend information on the data gathered in another trend. For instructions about how to build a trend, see "Building Trends" on page 369.

Query Fields	Description
Start Time	<p>This field only appears if you selected Event or Trend in the Query On field. Enter values depending on the data source you selected:</p> <ul style="list-style-type: none"> • Event - Specify the starting point for the data gathering from the events database. Event data is generally kept unarchived for 30 days by default, so specify a start time within that time frame. • Trend - Specify the starting point for the data gathering from the trends database. Be sure to specify a timeframe within the lifecycle of the trend (otherwise, the query returns an empty result set). <p>Tip: If the query is used as a base query in a trend, the trend start time overwrites the start time set here. See "Trend Parameters" on page 377.</p>
End Time	<p>This field only appears if you selected Event or Trend in the Query On field. Enter an end time depending on the type of source data you selected:</p> <ul style="list-style-type: none"> • Event - Specify the ending point for the data gathering that is some time after the starting point. Keep in mind that large time spans can mean large amounts of data, which can affect system performance. • Trend - Specify the end point for the data gathering that is some time after the starting point. <p>Tip: If the query is used as a base query in a trend, the trend end time overwrites the end time set here. See "Trend Parameters" on page 377.</p>
Use as Timestamp	<p>This field only appears if you selected Event or Trend in the Query On field. This field indicates which value to use as the timestamp for the report itself. This value helps with sorting and scheduling.</p> <ul style="list-style-type: none"> • End Time - Select End Time if you want to use the event or trend end-time you specified in the End Time field. The timestamp reflects the event end time. (If you are querying on a trend, select this option.) • Manager Receipt Time - Select Manager Receipt Time to use the time the event was received at the Manager. (If you are querying on a trend, this is probably not an appropriate option to choose because in that case "Manager Receipt Time" would indicate when the trend is run, rather than when events are received by the manager.)
Row Limit	<p>Set the row limit for the data table. (The default is 1000 rows.)</p> <p>Tip: If the query is used as a base query in a trend, the trend row limit overwrites the row limit set here. See "Trend Parameters" on page 377.</p>

The example below shows a query called *VPN Logins Outcome - Hourly* that returns VPN login attempts over a one day period each time it is run (Start Time is \$Now - 1d and End Time is \$Now).

Query	
Name	VPN Logins Outcome - Hourly
Query On	Event
Start Time	\$Now - 1d
End Time	\$Now
Use as Timestamp	End Time
Row Limit	10000
Distinct Rows	<input type="checkbox"/>
Database Hint	
Common	
External ID	
Alias (Display Name)	
Description	
Version ID	
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	



Tip

Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

Query Fields

The Query **Fields** tab contains the following main options with which to define query data and structure:

- [SELECT Query Fields](#)
- [GROUP BY Query Fields](#)
- [ORDER BY Query Fields](#)



Tip

Drag-and-drop is available on Query Structure panels. You can drag-and-drop items between options (for example, to group by Category Outcome, drag it from SELECT to GROUP BY. It stays in SELECT but is also used to GROUP BY)

Search Shortcuts

- Type part of the field name to find (for example, Name) in the Search box.
- Use the up/down arrow keys to jump to each instance of “Name” in the available fields.
- When you find the field name you want, press Return to add it to the condition statement under the selected section (SELECT, GROUP BY, or ORDER BY)
- Ctrl+F gets the Search box back in display if it’s hidden

Common Conditions Editor (CCE). The Query Editor, like other resource editors, uses the CCE for building conditional statements (query structure). For more tips on using the CCE, see [“Common Conditions Editor \(CCE\)” on page 846](#).

SELECT Query Fields

Click **Add SELECT columns** to select the data for the query. Data selected enters one big bucket, and any functions set for any of the data fields is performed on the entire bucket of data.

Drag and Drop items between options (e.g., to group by Category Outcome, drag it from SELECT to GROUP BY. It remains in SELECT but is also used to GROUP BY)

Select a Field Set:
Narrow the list of data fields to one designed for a particular use case.

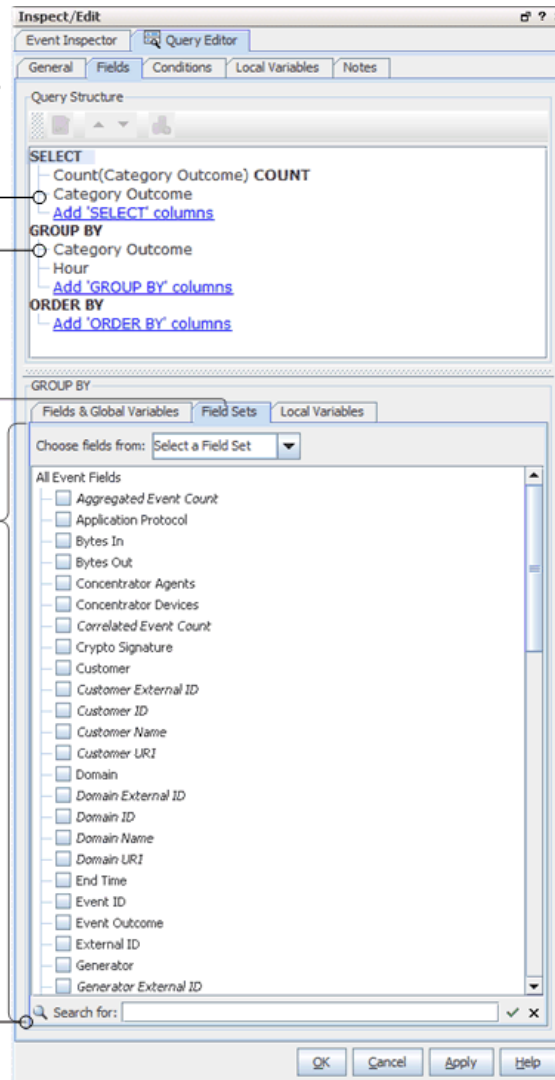
Choose Columns:
Select one or more data fields, then click the arrow to move it to the Query Columns area.

Search Shortcuts:
Type part of the field name you want to find (e.g., Name) in the Search box.

Use the up/down arrow keys to jump to each instance of "Name" in the available fields.

When you find the field name you want, hit Return to add it to the selected query structure sections (SELECT, GROUP BY, or ORDER BY)

Ctrl+F gets the Search box back in display if it's hidden



Query Structure:
Shows a summary of selected data and any optional functions and/or order-by and group-by conditions.



Tip



Fields shown in italics on the Data Options panel are derived, referenced, or side table fields (rather than "hard event data" in the main database tables). See also, "[Data Fields](#)" on page 867 and "[Variables](#)" on page 1006.

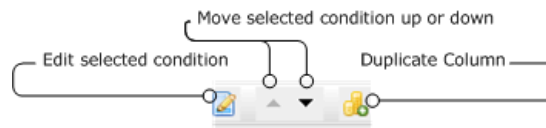
Query Structure (SELECT)

The Query Structure section at the top provides a summary of the fields selected in the SELECT section at the bottom. If you add GROUP BY or ORDER BY settings, these show up here also.

You can select from **Fields and Global Variables**, **Field Sets**, or **Local Variables** as data to build the query. Choosing a field set limits the fields shown to the selected field set.

- Click a field or variable (checkmark it) to select it.
- Click again (remove the checkmark) to deselect it.

- To edit a field or variable that you already have set as a query condition (showing under SELECT), simply double-click it or select it (click once) and click the Edit button () in the toolbar. (For example, you might want to edit the query by adding a function to it, as described in [“Applying Functions to SELECT Columns” on page 361.](#))
- To duplicate a field or variable that you already have under SELECT, select it (click once) then click the Duplicate Column button () in the toolbar.
- To move column up or down, select it and click the up or down arrow in the toolbar.



You can also select a condition item and right-click to get the various Edit options (**Edit**, **Copy**, **Delete**, **Duplicate**, etc.)

Applying Functions to SELECT Columns

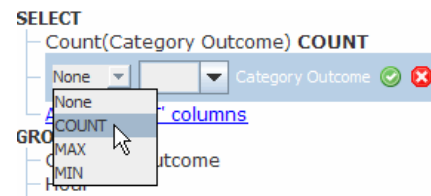
Optionally, you can specify an aggregate function on a particular column of data, such as a line item count, or in the case of numeric data, a sum or average

If the query is not grouped by one or more columns, then aggregate functions added here are applied to the whole result set.

If the query is grouped by one or more columns, then the aggregate function is performed on each group individually.

Adding a function adds a data field to the query schema that provides the results of the function, which can later be displayed in a report.

To specify a function for column data, double-click a field or variable in the top pane under “SELECT” and select a Function (from the drop-down menu) to apply to the column data.



The available functions are:

- **COUNT** - Count the number of line items returned in this column.
- **SUM** - Add all numerical data in a column, such as aggregated event count.
- **AVERAGE** - Calculate the average of all numerical data in a column, such as aggregated event count.
- **MAX** - Calculate the top values of the items returned in this column.
- **MIN** - Calculate the lowest values of the items returned in this column.
- **Standard Deviation (STDDV)** - Calculate the variation from the "average" (mean) for this column. (Square root of the variance.)
- **VARIANCE** - Calculate the amount of variation within the values returned for this column.

Select **Unique** to apply the function only to unique values in the column. (For example, the target address column may have 50 items in it, but only three are unique. To get a count of unique target addresses, check the Unique box.)

Click the green checkmark button (✓) to add the function.

To remove a function from a field, select the field, change the function selection to None, and click the green checkmark button again.

To cancel a modification to a function, click the (✗) button or simply click elsewhere on the UI (off of the Function menu.)

GROUP BY Query Fields

Click **Add GROUP By** to divide query results into separate buckets. For example, you could do a "group by" if you are interested in sorting items by timestamp, such as logins between 3 and 5 p.m. Functions on **GROUP BY** data apply to timestamp based fields only.

Drag and Drop items between options (e.g., to group by HOUR, drag it from GROUP BY to ORDER BY. It remains in GROUP BY but is also used to ORDER BY)

Query Columns: Shows columns selected for the group by.

Choose Columns: Select one or more data fields to determine which fields to group by, then click the arrow to move it to the Query Columns area.

Search Shortcuts:
 Type part of the field name you want to find (e.g., Name) in the Search box.
 Use the up/down arrow keys to jump to each instance of "Name" in the available fields.
 When you find the field name you want, hit Return to add it to the selected query structure sections (SELECT, GROUP BY, or ORDER BY)
 Ctrl+F gets the Search box back in display if it's hidden

The screenshot shows the 'Inspect/Edit' window with the 'Query Editor' tab active. The 'Query Structure' section displays a query with a 'SELECT' clause containing 'Count(Category Outcome) COUNT' and 'Category Outcome', and a 'GROUP BY' clause containing 'Category Outcome' and 'Hour'. The 'ORDER BY' clause is currently empty. The 'GROUP BY' section below shows a list of 'All Event Fields' with checkboxes next to each field name. A search bar is at the bottom of the field list. The 'Query Columns' section on the right shows the columns selected for the group by.



Fields shown in *italics* on the Data Options panel are derived, referenced, or side table fields (rather than “hard event data” in the main database tables). See also, [“Data Fields” on page 867](#) and [“Variables” on page 1006](#).

Query Structure (GROUP BY)

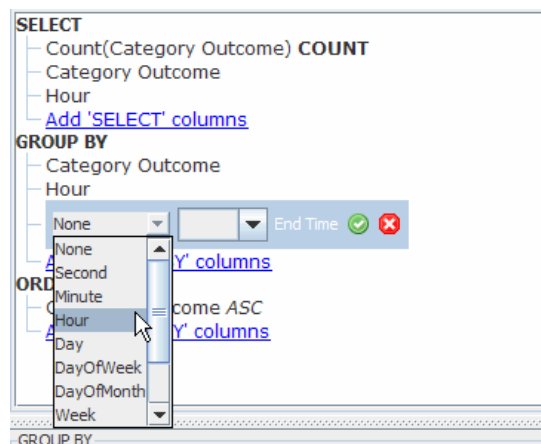
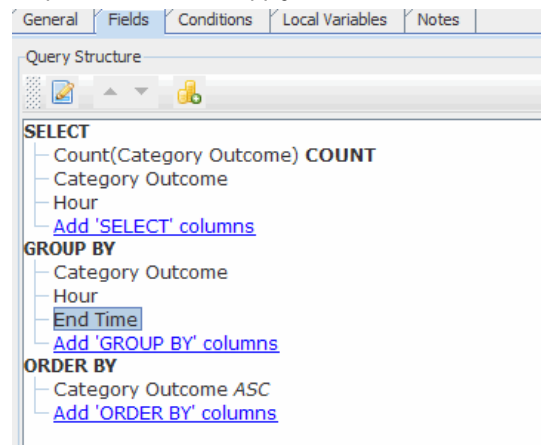
The Query Structure section at the top provides a summary of the fields selected in the GROUP BY section at the bottom. SELECT and ORDER BY settings show up here also.

Adding and editing fields and variables to order by works similarly to adding them for SELECT. See [“Query Structure \(SELECT\)” on page 360](#).

Applying Time-Based Functions to GROUP BY Columns

You can specify a time-based function on the group by column of data. Time-based functions apply only to time-based fields, such as event end time.

To specify a function for GROUP BY column data, double-click a field or variable in the top pane under “GROUP BY” and select one of the available time-based functions (from the drop-down menu) to apply to the column data.



Functions on items under GROUP BY create a separate bucket of data for each time function specified.

To specify a function for column data, select a data field in the Query Columns section then select a Function (from the drop-down menu) to apply to the column data:

- **Second** - Creates a new bucket for all events that occur in the same second.
- **Minute** - Creates a new bucket for all events that occur in the same 60-second period.
- **Hour** -Creates a new bucket for all events that occur in the same 60-minute period.
- **Day** - Creates a new bucket for all events that occur in the same 24-hour period.
- **DayofWeek** - Creates a new bucket for all events that occur on the different days of the week, such as Monday, Tuesday, and Wednesday.
- **DayofMonth** - Creates a new bucket for all events that occur on various days of the month, such as the first, second, and third.
- **Week** - Creates a new bucket for all events that occur in a week.
- **Month** -Creates a new bucket for all events that occur in a month.
- **Year** - Creates a new bucket for all events that occur in a year.
- **Quarter** - Creates a new bucket for all events that occur in a quarter.

ORDER BY Query Fields

Click **Add ORDER BY** columns to specify the order in which you want the data in your buckets sorted. For example, you might "order by" if you were interested in the numeric value of the items in your bucket such as the top 10 logins.

Drag and Drop items between options (e.g., to group by Category Outcome, drag it from SELECT to GROUP BY. It remains in SELECT but is also used to GROUP BY)

Query Columns Shows columns selected for the order by.

Choose Columns: Select one or more data fields to determine the sorting order by, then click the arrow to move it to the Query Columns area.

Search Shortcuts: Type part of the field name you want to find (e.g., Name) in the Search box. Use the up/down arrow keys to jump to each instance of "Name" in the available fields. When you find the field name you want, hit Return to add it to the selected query structure sections (SELECT, GROUP BY, or ORDER BY). Ctrl+F gets the Search box back in display if it's hidden.



Fields shown in italics on the Data Options panel are derived, referenced, or side table fields (rather than "hard event data" in the main database tables). See also, ["Data Fields" on page 867](#) and ["Variables" on page 1006](#).

Query Structure (ORDER BY)

The ORDER BY columns can be different than the ones you chose for the query data under SELECT. Also, you can apply functions to these columns.

Adding and editing fields and variables to order by works similarly to adding them for SELECT. See ["Query Structure \(SELECT\)" on page 360](#).

Applying a Column Function to Order By

Optionally, you can specify an aggregate function on a particular column of data to group by, such as a line item count, or in the case of numeric data, a sum or average.

You apply a function to ORDER BY columns the same as you do to a SELECT column, and the same functions are available depending on the fields or variables chosen. See [“Applying Functions to SELECT Columns” on page 361](#).

To specify a function for column data, double-click a field or variable in the top pane under “ORDER BY” and select a Function (from the drop-down menu) to apply to the column data.



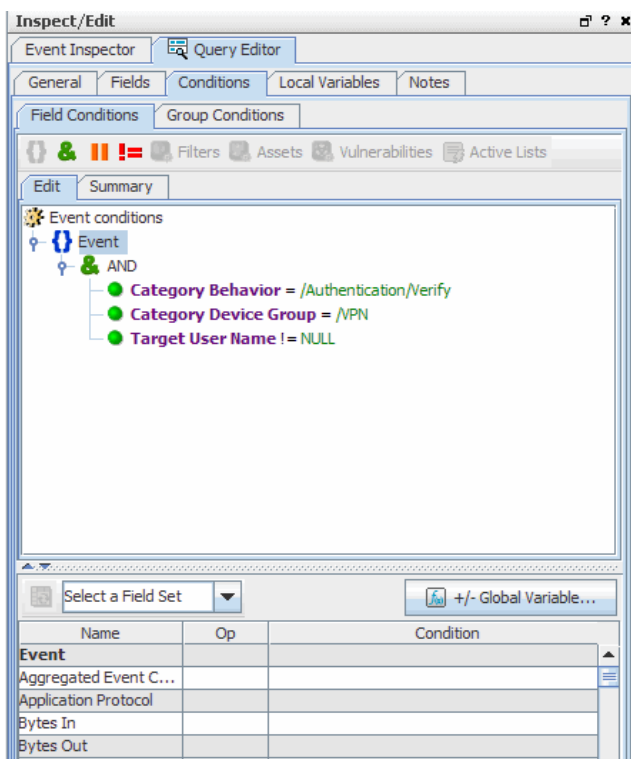
Sort Order

Under ORDER BY you can also set the sort order on the fields/columns. By default, the sort order is ascending (ASC). You can change it to descending (DESC)

Query Conditions

Optionally, you can create conditions on individual fields or on groups as part of the query. You can add filters, and conditions based on assets, vulnerabilities, and active lists.

Use the [Common Conditions Editor \(CCE\)](#) within the query editor to create query conditions as described in this section.





The Common Conditions Editor is used throughout the ESM Console for various resources. In addition to the topics that follow on defining conditions for a report query, see also [“Common Conditions Editor \(CCE\)” on page 846](#), [“Conditional Statements” on page 859](#), [“Conditions” on page 860](#), and [“Logical Operators” on page 947](#).

Creating Conditions on a Field

For information on how to create conditional statements, see [“Common Conditions Editor \(CCE\)” on page 846](#), [“Conditional Statements” on page 859](#), [“Conditions” on page 860](#), and [“Logical Operators” on page 947](#).

- 1 Click the **Conditions** tab and select data fields from the fields below list to build a condition statement in the display area at the top of the Edit sub-tab.

The data field table displays a **Name**, **Operator**, and **Condition** column. These three columns are combined to create <data field> <logic operator> <data field value> condition statements. For example, if monitoring a Cisco Router, you could define a condition statement to specify `Device Product = Cisco Router: Device Product` as the data field, `equals (=)` as the logic operator, and `Cisco Router` as the data field value.

- 2 In the Op column, double-click the cell and select a logic operator from the drop-down menu.
- 3 In the Condition column, type a data field value or double-click the cell and select a value from the drop-down menu. Press **Enter** to add the condition to the statement above.
- 4 Repeat this process to add more statements to the condition.
- 5 Click **Apply** or **OK** to save your changes and create the condition.

Here is some guidance on creating conditions.

- Drop-down menus appear if the selected data field has a set of value options.
- For example, if the Category Behavior data field is selected, a drop-down menu appears with the value options of `/Access`, `/Access/Start`, `Access/Stop/` and so on. One of the choices in this menu is `/Authentication/Verify`, which is the condition we selected for Category Behavior in our example condition.
- For date and time data fields, such as Detect Time, you can type an actual date value, such as `10/12/2002 8:54:00 AM`, or you can use special Time variables.
- The condition statement appears as a branch under the logical operator.
- To add a condition to an event field, click in its condition box and click the ellipses icon.
- To activate all operands on the top, select an item in the editor view, as shown above.

Creating Group Conditions

Creating a group condition is similar to creating a normal condition, except you pick an aggregate function to perform on the group.

You would use it if, for example, to group by event name and when you want to get only the events with more than 100 occurrences in the query. In this case, you would add a `Count()` aggregate function to the eventID field, for example, `count(eventId) > 100` to eliminate the events that have occurred less than 100 times.

Query Variables

Variables are run-time information derived from the source data (event, asset, case, notification, or trend, depending on the schema) that can be used in the query wherever normal fields can be used.



You can create local variables which are available only to the resource you are creating (in this case, a query), or use global variables. The following steps describe how to set a local variable. For information on creating global variables, see [Chapter 17, Global Variables, on page 477](#).

To set a local variable:

- 1 Click the **Variables** tab.
- 2 Click **Add** to launch the Variables dialog.
- 3 The Variables dialog displays different values depending on the function you choose. In the Variables dialog, enter the following values and click **OK**.

Options	Description
Name	Enter a name for the variable. This is the alias that appears in the Conditions editor when you can use the variable. Spaces and special characters are OK.
Function	From the drop-down menu, select a function. For a description of each function, click Help in the lower right corner.
Arguments	The arguments section contains a series of fields where you set the parameters for the variable. The available fields vary with the function you select.
Preview	The preview area provides an interface where you can enter values for the key variable fields so you can verify that the parameters you specified return the expected results. Enter test values and click Calculate .

Editing a Query

- 1 Navigate to **Reports** in the Navigator panel, select the **Queries** tab, and select the query you want to modify.
- 2 Double-click the query, or right-click and select **Edit Query** from the context menu. This launches the Query Editor in the Inspect/Edit panel, and shows the definition for the selected query.
- 3 Edit the query definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)



If the query is used in a trend, the query and associated schema referenced in the trend are set at the time the trend was created. After the trend is created, you can add columns to the base query, but columns added to the query after the trend is created are not used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to add or remove columns (data fields) in the query that are used in the trend, create a new trend and select that modified query.

Building Trends

A trend is an ArcSight resource that defines how and over what time period data are aggregated and evaluated for trends. A trend executes a specified query on a defined schedule and time duration.

The ArcSight trends engine evaluates source data for trends based on event conditions (such as number of worm outbreaks, incident time-to-close, or number of cases closed) or common network elements (such as operating system, business role, or regulatory compliance relevance).

Trends can be used as the primary data source for a report, or used as the data source input to another query which is then used in a report (perhaps along with other queries or trends).

Building trends is a component of ArcSight Reporting resource tools. Be sure to start with [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools, and [“Understanding Reporting Workflow” on page 331](#) to see how Trends fit in to the process of creating a report.

How Trends Work

A trend references a query, specifies a schedule on which the query automatically triggers, and provides mechanisms for efficiently storing, viewing, and leveraging the trend results for reporting. The trend results are stored in a trend table in the ArcSight database, and are themselves queryable.

Trends can be set to run indefinitely or to end at a specified date and time. A trend can be configured to start retrieving historical data from logs, start with current events, or at some specified time in the future. (You can also specify advanced options on how and when to build tables, store data, and partition it.)

Once trend data is collected, you can view the results in the Data Viewer table and generate a trend report that displays the results in tables and graphs.



Depending on the data gathered by the base query, the trend is either *snapshot trend* or an *interval trend*.

Snapshot Trend

A *snapshot trend* uses a query that operates on a fixed moment in time, for example, to gather information about assets on your network. Snapshot trends are built from queries based on assets, cases, or notifications. For example, snapshot queries and the trends built from them would be used to determine metrics such as current number of assets, number of systems with a particular operating system, or number of systems with particular vulnerabilities. A snapshot trend operates on data in the current moment in time, and only collects data going forward. Thus, trends cannot be used to answer the question, "how

many assets were there in this zone a month ago?" You can use trends to collect data from this point forward, however, and in a month from now, you have a month's worth of data telling you how many assets were in this zone at regular intervals over the last month.

Interval Trend

An *interval trend* uses a query that operates on events that happen over a specified time window, for example, to gather information about how many events of a particular description occurred daily over a 6-month period. Interval trends are event-based. For example, an interval trend using a base query with a time window could gather information to determine the number of login attempts in the past hour. You can "refresh" an interval trend manually as needed (by selecting the trend in the Navigator and clicking **Refresh** on right-click context menu). Interval trends are typically event-based.

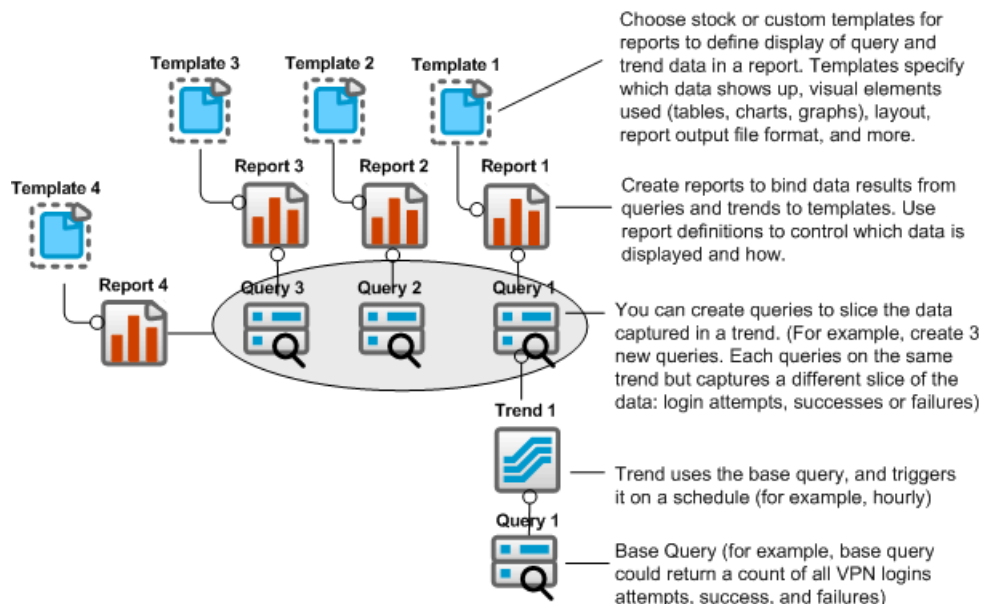
Query-Trend Relationships in Reporting



Note

Note that for a query used in a trend, the query and associated schema referenced in the trend are set at the time the trend was created. After the trend is created, you can modify some elements of the query if they do not affect the trend. For example, you can add or remove columns in the query if the related trend does not depend on them. Such modifications made to a referenced query are not reflected in the trend. If you modify aspects of the query that a trend depends on, the trend is disabled.

A base trend is made up of one query. Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.



For example, you could create a trend called "VPN Logins Outcome - Hourly" that references a query that returns all VPN login attempts, successful logins, and failed attempts. (You could schedule the trend to run hourly.) You can use this base trend directly in a report.

However, a more powerful approach would be to further refine the data results by creating three new trend queries, each of which takes the base trend as its data source but then sets further conditions on the query data to return one specialized slice of the results. One query could return only login attempts, another only successful attempts, and another only failed attempts. You could then draw on four queries in a single or multiple reports to show different views of the data. (The base query would show all types of login events, and the other three would show the focused views.)

Multiple reports can be generated from a single query or trend, and a single report can capture data from multiple queries and trends.

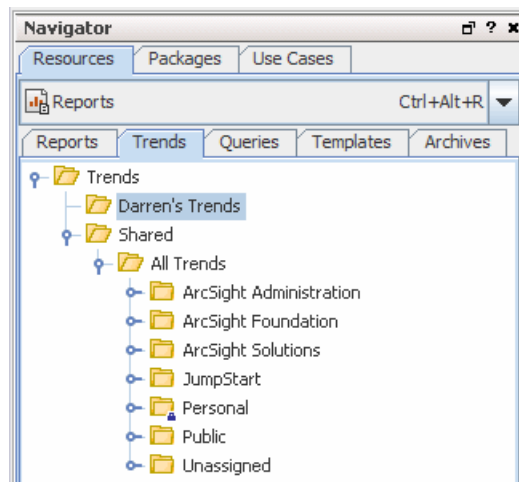
The ability to automate and refine queries by feeding them into trends and vice versa, along with the flexibility in populating reports solves many typical enterprise security reporting challenges. You can build a trend that gets a daily event count, feed the trend into a query that sums up the daily counts to get a monthly event count, and even feed that monthly count query into another trend and so forth. Managed Security Service Providers (MSSP) can use slicing and dicing query-trend approaches to create focused reports for multiple customers built from what are initially broad range queries.

Building a Trend

Before you begin building a trend, make sure that you have a query defined that captures the data you want to build a trend on. (See [“Building Queries”](#) on page 354 if you need more information.)

Navigating to Trends

In the Navigator panel, select the **Reports** resource from the drop-down menu and click the **Trends** tab.



Creating a New Trend

The high-level steps for creating a trend are as follows:

- 1 Right-click a trend group (folder) and select **New Trend**. This launches the Trend Editor in the Inspect/Edit panel. As a general rule, it is best to create new content in your own folder.
- 2 Define Trend attributes. At a minimum, fill in the required values (red asterisks) on the Attributes tab as described in the Trend Attributes topic below.
- 3 Verify the trend schema represented by the selected Data Fields is appropriate.

- 4 Test the trend schema to make sure it is returning the expected data as described in Testing a Trend.
- 5 Define a Trend schedule as described in Trend Schedule.
- 6 Click **Apply** or **OK** to create the new trend.

**Caution**

Do not click **Apply** or **OK** until you have defined the required values in the Trend section (trend name and query to use) and the trend schema in the Data Fields section of Trend Attributes. When you commit changes to the trend, the query and the schema are set and cannot be edited. If you decide to use a different base query or need to make a change to the schema, delete the trend and start fresh.

**Note**

A trend uses a "snapshot" version of the query as its data source. After you have used a query in a trend, you can modify some elements of the query if they do not affect the trend. For example, you can add or remove columns in the query if the related trend does not depend on them. Such modifications made to a referenced query are not reflected in the trend. If you modify aspects of the query that a trend depends on, the trend is disabled.

Defining Trend Settings

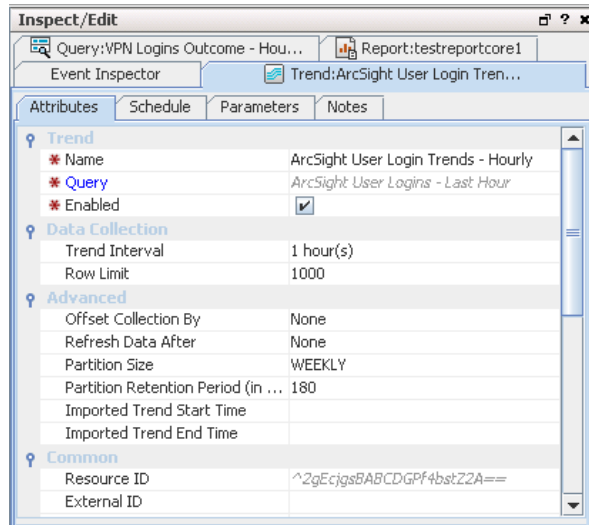
Use the Trend Editor to build a new trend or edit an existing one.

Trend Attributes

The following fields in the Trend section are required attributes to specify when creating a new trend.

Trend Fields	Description
Name	Name for the trend. Spaces and special characters are OK. The name you enter here is the alias that appears in data source pick lists in other editors.
Query	<p>Specifies the query that this trend uses.</p> <p>If you are creating a new trend, use the Query drop-down menu to select a query as the source data for your trend.</p> <p>Caution: Once the trend is created, you can add columns to the base query, but columns added to the query after the trend is created are not used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to remove columns (data fields) in the query that are used in the trend, create a new trend and select that modified query.</p>
Enabled	By default, the Enabled checkbox is checked. This activates the trend to begin working on live data as soon as the trend is created. Uncheck this box if you want to experiment with the trend before pushing it live.

The example below shows a trend that uses the "VPN Login Outcome - Hourly" query as its basis.



The **Data Collection** section provides default values for row limit and query duration. You can keep the defaults or modify as needed.

Data Collection Fields	Description
Trend Interval	Time span over which the trend operates. The default is one hour. For example, if the query counts the number of logins, this setting counts the number of logins every hour.
Row Limit	Maximum number of rows of data the trend captures. The default number is 1000.

The **Advanced** section provides optional settings to offset trend data collection and refresh trend data at a specified point in the future. By default, the offset and refresh values are set to "None". The Advanced section also specifies default values for data storage partitions. You can keep the defaults or modify as needed.

Advanced Fields	Description
Offset Collection By	Delays trend data collection by the time period specified. Offsetting trend data collection time enables you to compensate for events that arrive to the Manager late, either from a time zone lag or other data collection lag. Trend data collection starts after the time delay entered here. Enter a time delay and select Hours or Minutes from the drop-down menu. The default offset is None.

Advanced Fields	Description
Refresh Data After	<p>Triggers the system to automatically re-evaluate the query data at a later time to capture any additional events that may have come in late.</p> <p>Enter a refresh interval and select Hours or Minutes from the drop-down menu. The default refresh is None.</p> <p>Note: The Manager supports late arrival of events. For example, a SmartConnector can send a batch of events later if it is falling behind. You need to explicitly schedule a refresh of trend data only if SmartConnectors frequently lag behind in sending events to the Manager. If SmartConnectors rarely go down and are generally on time delivering events, there is no need to set this option.</p>
Partition Size	<p>Specifies the time range of the database partitions for this trend data, which in effect determines the partition size.</p> <p>The default "time slice" for trend tables is WEEKLY. That is, if the default setting is used, each partition would contain a week's worth of data. Partition size can be set to daily, weekly, or monthly. (You can always modify the Partition size as needed by editing the trend definition.)</p> <p>Database partitioning is for space and archive management purposes (keeping trend data organized for long term storage. It can also help to improve query performance.</p> <p>The Partition Size works in concert with the Partition Retention Period, described below.</p>
Partition Retention Period (in days)	<p>Specifies the number of days to retain the partitions from this trend as active in the ArcSight database. The default is 180 days. (You can always modify the Partition Retention Period as needed by editing the trend definition.)</p> <p>Note: The Partition Retention Period works in combination with the Partition Size. The system makes sure you always have as much data, if not more, than you specified in the configuration of these two settings. Similarly for factors such as time zones and daylight savings time, more data (never less) is retained. For example, if the Partition Size is set to MONTHLY and the Partition Retention Period is 45 days, the system stores two month's worth of data; two partitions. If the Partition Retention Period is set to 0 days, the data collected from one run of the trend is retained until the next partition is started. For example, if the Partition Size is MONTHLY and the Partition Retention Period is 0 days, then you keep one month's worth of data. Make sure that the trend start date is appropriate; a trend with a MONTHLY partition size, 0 days retention, and a start date near the end of the month would not maintain data for very long.</p>

Advanced Fields	Description
Query Overlap Time	<p>The query overlap time is the amount of time by which the next query should overlap with the previous query (overlapping the tail-end of the previous query).</p> <p>The default overlap is 0 ("None"), which corresponds to the normal non-overlapping trend query case.</p> <p>By setting a query overlap time, you can configure a trend to support calculations like moving averages. The query overlap time extends the trend to include overlapping query ranges.</p> <p>For example, to collect moving average data over a 10 day period, you could run the query each day over the previous 10 days. A query overlap time set to 0 (the default) would result in non-overlapping runs, such that the query would run every 10th day over the previous 10 days.</p> <p>On the other hand, to get an overlapping trend run, you could specify a 9 day overlap. With this setting, the query would run every day (10 day query - 9 day overlap) over the previous 10 days. The trend would gather data every day for days 1-10, 2-11, 3-12, etc.</p> <p>Notes:</p> <ul style="list-style-type: none"> Queries should not normally be run on the event table for anything longer than a day. Queries longer than a day should normally only run on other trend tables to allow the query to finish in a reasonable amount of time. This option is enabled for snapshot trends.
Imported Trend Start Time	<p>If the trend is exported without schedule start and end times, the trend start time specified here is used when the trend is imported.</p> <p>If the trend is exported without Schedule start and end times and no value is specified for Imported Trend Start Time, then when the trend is imported it defaults to use \$CurrentDate as the start time. (With this setting, the trend captures data starting from 12:00:00 AM of the current day.)</p> <p>Note: The imported trend start time takes effect only if the trend is exported without Schedule start time. To exclude the Schedule start time from a trend upon export, you must set the package "Format" option to "export". For information on this, see the description of the package "Format" options in "Creating Packages" on page 687.</p>
Imported Trend End Time	<p>If the trend is exported without schedule start and end times, the trend end time specified here is used when the trend is imported.</p> <p>If the trend is exported without Schedule end time and no value is specified for Imported Trend End Time, then when the trend is imported it defaults to using no end time. (With this setting, the trend runs indefinitely until it is manually disabled or edited to include an end time.)</p> <p>Note: The imported trend end time takes effect only if the trend is exported without Schedule end time. To exclude the Schedule end time from a trend upon export, you must set the package "Format" option to "export". For information on this, see the description of the package "Format" options in "Creating Packages" on page 687.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 684](#).

The **Data Fields** section is where you build the trend schema. This is populated automatically when you first select the query to use in this trend. The list shows the data fields collected by the query you chose. By default, all the query fields are selected for use in the trend. If you do not want to use a particular data field, uncheck the Use box for that item. Also, you can select which fields you also want to index. Indexing is done mostly for query efficiency. It is helpful if the query you are using returns a large amount of data, and you want to run sub-queries on the data.

Data Fields

Name	Use	Index
Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of Logins	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Category Outcome	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hour	<input checked="" type="checkbox"/>	<input type="checkbox"/>

The **Summary** box at the bottom displays a summary of the query interval and the schedule on which it runs.

Trend Schedule

Click the **Trend Schedule** tab to review or modify settings for the following parameters:

- **Schedule Frequency** - Specifies how often the query runs and gather data. The default is to run once every hour on the hour.
- **Schedule Range** - Specifies the timeframe (start and end date/time) during which the trend collects data at the scheduled collection times. By default, the date and time the trend was created is used as the trend schedule start time. The default is indefinitely; that is, No End date.

With the default settings, this trend would collect data once every hour on the hour until it is disabled manually.

A Summary of the configured schedule is shown at the bottom of the tab.

Trend Parameters

The Parameters tab lets you further refine the query results in terms of row limits, time zone restraints, filters, and start and end times. If you set parameters in the base query used by this trend, those parameters show up on the Trend Parameters tab. In the Trend, you can specify default parameters.

Then at Report building time, you can opt to run the report with the default parameters or "all parameters". You can also further refine parameter details for a specific run of a report. For more information on specifying parameters in reports, see ["Report Parameters" on page 401 in Creating Reports](#).



Note

Trend start/end times and row limits are used for gathering the data, and overwrite the start/end times and row limits set in the base query. If you do not customize the Trend Parameters, the defaults on this tab are used (not the start/end times and row limit on the Query General Attributes tab).

For reporting on the data (once it is collected), you can set new start/end times and row limit in the **Report Parameters** tab. The report parameters prescribe only the "outbound" or publishing data derived from the data already collected, not the how the data is gathered. (See ["Report Parameters" on page 401 in Creating Reports](#) and ["Running Reports" on page 423](#) for more information.)

Trend Actions (Add to Active List)

Trend actions give you the option to send specified columns (fields) in trend results to [Active Lists](#) (see ["Managing Active Lists" on page 571](#)). You do this by defining an **Add to**

Active List trend action. On the Actions tab for a trend, you can select to send data from one or more columns in the trend results to a specified active list.



Trend actions for active lists are similar to the **add to active list** rule action described in [“Rule Actions Reference” on page 455](#) and [“More Rule Actions” on page 460](#). Unlike rules, however, **add to active list** is the only action available for trends, and the settings are not as fine-grained as for rules; for example, thresholds, number of events, time units, and so on do not apply to trend actions.

How Trend Actions are Useful (Summary Views and Rules)

The “add to active list” trend action provides another mechanism to get information from trends outside of (and in addition to) reports, and supports summary views of information from multiple trends.

For example, you can build a single active list that gets updates from multiple trends (each trend updating different columns in the active list). Also, a single active list can receive updates and show information from trends as well as from other sources (for example, rules). Alternatively, you can build multiple active lists that get updates from a single trend.

Perhaps most importantly, the ability to populate active lists with trend data makes trend results readily available for use in rules, filters, active channels, and so forth. In previous releases, trends could not be easily leveraged in rules and other such resources.

Example Use Case

Consider the following example use cases for leveraging trend results in active lists:

- **Taking Action on Event-Based Trends.** Suppose an analyst wants to monitor the logins per hour by users based on their typical hourly login patterns and flag anything that is above a certain absolute threshold or more than *n* times a user's previous average.

The analyst can set up a trend to update the information in a trend table based on aggregation of per-user login events. The trend would have an **action** that updates an active list with the most recent results. Then, the analyst can configure a rule to update another active list when a user logs on and another rule to compare the current login count against what is normal for that user. Any gross discrepancy could be used to trigger an alarm about a possible threat.

- **Taking Action on Asset-Based Trends.** Suppose an analyst wants to monitor assets by how vulnerable they are, and watch for “unusual activity” on especially vulnerable assets.

The analyst can set up a trend to check vulnerability counts on assets and log the top *n* most vulnerable assets on a daily basis. The active list would have an **action** to update an active list. Incoming events on assets would trigger rules that would check this active list against the particular device and, if present, trigger extra processing.

Plan and Define Active Lists with Fields Mapped to Trend

As a first step in setting up trend actions, determine which active list(s) you want the trend to populate and with what data. You might have existing active lists to which you want to add trend data, or you might want to create new lists specifically for some trend results. (See [“Example: Populating Active Lists with Trend Results” on page 380](#) for an example of designing an active list based on the trend fields you want to monitor.)

Define a Trend Action

Use the Trend **Actions** tab to configure actions on a new or existing trend.

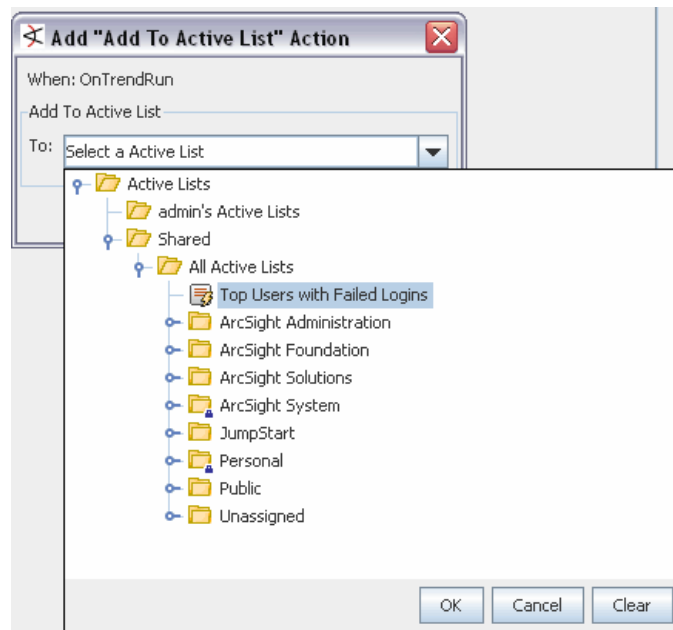
To define a trend action on an existing trend:

- 1 Select a trend in the Navigator, right-click and choose **Edit Trend**.
- 2 In the Trend Editor, click the **Actions** tab.
- 3 Select the action **On Trend Run**, right-click and choose **Add to Active List**.



Only a *fields-based* active list can be used in a Trend Action (not event-based lists). For more information on types of active lists, see ["Managing Active Lists" on page 571](#), especially the description of how to define data for the list (["Data: Event-based, Fields-based" on page 573](#)).

- 4 Select an active list from the dialog.



The active list you select here is updated by this trend.

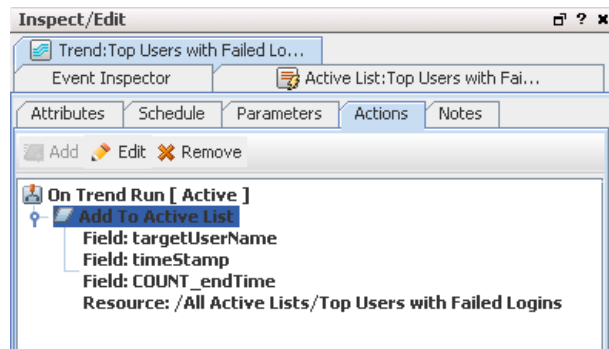
- 5 On the Add to Active List dialog, select fields from the trend (on the right side) to map to active list fields (on the left).



What you are doing in this step is mapping trend column names to active list column names. All the "key" columns required by the active list must have trend columns mapped to them so that the active list entry (row) is correctly updated by the trend.

However, not all of the active list value columns need to have trend columns mapped. Not specifying all the key columns is an error.

- 6 Click **OK** to add the action.



The action shows on the actions tab.

Note that you could add more actions here (by selecting the **On Trend Run** and clicking **Add**), edit this action, or remove it.

You can add multiple actions to a single trend (i.e., configure a single trend to update particular columns in multiple active lists with trend results).

- 7 Click **Apply** or **OK** to save the Trend Editor to save your changes.

Example: Populating Active Lists with Trend Results

Suppose you want to monitor top failed user logins daily and send that data to an active list. (You could then configure rules to interact with the active list and trigger an alarm based on some threshold; for example, a single user with a certain number of failed logins per day.) To do this, you could create an active list with fields that map to a trend that monitors “top users with failed logins”. To see the fields in this trend:

- In the Navigator, choose **Reports**, click the **Trends** tab, then navigate to [//Trends/Shared/All Trends/ArcSight Foundation/Intrusion Monitoring /SANS Top5 Reports/Top Users with Failed Logins per Day](#).
- Select the trend, right-click and select **Data Viewer** from the context menu to display the trend results in the Viewer. Note the columns included by default in this trend table ([TimeStamp](#), [Day](#), [User Name](#), and [Number of Failed Logins](#)).

You would need to have one or more of these fields in your active list to capture relevant data in the list, as we'll show in the next section where we define the trend.

Viewer

Top Users with Failed Logins Details | Top Users with Failed Logins per Day Details

Name: Top Users with Failed Logins per Day 25 shown / 25 matches

Start Time : 15 Jul 2009 00:00:00 PDT

End Time : 16 Jul 2009 11:39:17 PDT

Filter: No Filter

TimeStamp	Day	Username	Number of Failed Logins
15 Jul 2009 00:00:00 PDT	2009-07-15		55
15 Jul 2009 00:00:00 PDT	2009-07-15	lara	28
15 Jul 2009 00:00:00 PDT	2009-07-15	john	16
15 Jul 2009 00:00:00 PDT	2009-07-15	UNKNOWN	8
15 Jul 2009 00:00:00 PDT	2009-07-15	**unknown**	8
15 Jul 2009 00:00:00 PDT	2009-07-15	rajiv	8
15 Jul 2009 00:00:00 PDT	2009-07-15	shannon	7
15 Jul 2009 00:00:00 PDT	2009-07-15	michael	7
15 Jul 2009 00:00:00 PDT	2009-07-15	root	6
15 Jul 2009 00:00:00 PDT	2009-07-15	kashanmi	4
15 Jul 2009 00:00:00 PDT	2009-07-15	admin	3
15 Jul 2009 00:00:00 PDT	2009-07-15	dferrier	2
15 Jul 2009 00:00:00 PDT	2009-07-15	ram	2

To continue with our example, we could create a fields-based active list with fields that map to the trend “Top Users with Failed Logins per Day” as follows.

Inspect/Edit

Event Inspector | Active List: Top Users with Fai...

Attributes | Notes

+ Add Entry

Active List

- * Name: Top Users with Failed Logins
- Optimize Data: ☐
- * Capacity (x1000): 10
- * TTL Days: 1
- * TTL Hours: 0
- * TTL Minutes: 0
- Allow multi-mappings: ☐
- Partially cached: ☐

Common

Resource ID: HaZgngS1B8CF11taP+eRgQ==

External ID:

Alias:

Description:

(Name)

(Description)

* Data: ☐ Event-based ☒ Fields-based ☒ Key Fields

Name	Type	Sub-type	Key-field
User Name	String		<input checked="" type="checkbox"/>
Day and Time	Date		<input type="checkbox"/>
Number of Failed Logins	Long		<input type="checkbox"/>

Name	Type	Key Field
User Name	String	This is the key field.
Day and Time	Date	
Number of Failed Logins	Long	

When the trend runs, it populates the active list with data on top users with failed logins by user name, and list the count of failed logins for each user along with date/time information. This active list could be used as the basis for rules, filters, active channels, etc.

Viewer

Top Users with Failed Logins Details

Name: Top Users with Failed Logins

Last Update: 16 Jul 2009 11:33:13 PDT

Filter: No Filter

24 shown / 24 matches

User Name	Day and Time	Number of Failed L...	Creation Time	Last Modified Time	Count
unknown	15 Jul 2009 00:00:...	8	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
admin	15 Jul 2009 00:00:...	3	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
dferrier	15 Jul 2009 00:00:...	2	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
dsfdsa	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
fdgfdgd	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
fdsfds	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
fsaf	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
fsdfds	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
gfdgfd	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
john	15 Jul 2009 00:00:...	16	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
kashanmi	15 Jul 2009 00:00:...	4	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
lara	15 Jul 2009 00:00:...	28	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
michael	15 Jul 2009 00:00:...	7	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
oracle	15 Jul 2009 00:00:...	2	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
rajiv	15 Jul 2009 00:00:...	8	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
ram	15 Jul 2009 00:00:...	2	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1
ROOT	15 Jul 2009 00:00:...	1	16 Jul 2009 06:40:...	16 Jul 2009 06:40:...	1

Notes on Trend Action Behavior

- When it is mentioned that a trend "updates" the active list entry (row), what is meant is that either the row is inserted if it is not currently present, or if it is present, it is updated. Note that the update only populates / overrides the columns specified by the trend column mapping. Any other active list columns that do not have trend column mappings preserve their existing values. What this means is that it is possible for a single active list to be updated by multiple trends, each updating different columns. The active list is appropriately locked during read-modify-write cycle to avoid data corruption.
- A trend can be executed under a variety of circumstances, including refresh and backfill. However, for purposes of updating the active list, only the most recent data are entered into the active list. For example, no backfill data are added to the active list. A trend refresh run does not normally cause the active list to update, with the only exception being if it is the most recent data being refreshed.
- This trend action never removes entries from the active list. If the you want to have entries removed, use the active list's TTL (time-to-live) to have them expire. (For information on the TTL setting, see [related information on page 572](#) under [Creating an Active List](#).)

Editing a Trend Action

- 1 Navigate to the trend you want to edit.
- 2 Click the Trend **Actions** tab.
- 3 Select the action you want to edit and click **Edit**.
- 4 On the Add to Active List dialog, make changes to the field mappings as needed and click **OK**.
- 5 Click **Apply** or **OK** to save the Trend Editor to save your changes.

Removing a Trend Action

- 1 Navigate to the trend you want to edit.
- 2 Click the Trend **Actions** tab.

- 3 Select the action you want to remove and click **Remove**.
- 4 Click **Apply** or **OK** to save the Trend Editor to save your changes.

Testing a Trend

When you are creating a new trend or modifying an existing one, you might want to test it first to determine if you have defined the trend properly to return the data you want. To test the results of the schema you selected, make sure you are on the Schedule tab for the trend you want to test and click **Test**. Here are navigation instructions in case you are not already on that tab:

- 1 Navigate to Reports Trends in the Navigator panel, and select the trend you want to test.
- 2 Do one of the following:
 - ◆ Right-click and choose **Test** from the context menu

Or

 - ◆ Click **Edit Trend** to bring up the Trend editor in the Inspect/Edit panel. Within the editor for the selected trend, click the **Test** button at the bottom of any of the editor tabs (Attributes, Schedule, Parameters, and so forth).

This procedure evaluates the current event stream for matching events and populate the Test Trend pop-up dialog. The message "Success: x rows" at the bottom of the dialog tells you how many rows your trend returned.

The Test Trend sample shows a maximum of 25 rows. For interval queries, the sample also shows data from, at most, the last hour. If there is no match for the data, the trend returns no rows. This may mean that your current event query data contains no matching events or resources, or it may mean that your query needs to be refined.

Viewing Trend Data

- 1 Navigate to Reports Trends in the Navigator panel, and select the trend for which you want to view the data.
- 2 Right-click and select **Data Viewer** from the context menu. This launches the Trend Data Viewer in the Viewer panel and shows the query results. As with other ArcSight

event viewers, you can select an event or group of events, right-mouse click, and access various tools from the context menu to use for further investigation.

Viewer

ArcSight User Status \ Latest Events By Priority \ VPN Logins Outcome - Hourly Details

Name: VPN Logins Outcome - Hourly

Filter: No Filter

871 shown / 871 matches

Time	Number of Logins	Category Outcome	Hour
27 Jul 2006 12:48:26 PDT	26	/Attempt	12
27 Jul 2006 12:48:26 PDT	100	/Attempt	13
27 Jul 2006 12:48:26 PDT	12	/Failure	12
27 Jul 2006 12:48:26 PDT	47	/Failure	13
27 Jul 2006 12:48:26 PDT	13	/Success	12
27 Jul 2006 12:48:26 PDT	54	/Success	13
28 Jul 2006 08:48:26 PDT	22	/Attempt	8
28 Jul 2006 08:48:26 PDT	80	/Attempt	9
28 Jul 2006 08:48:26 PDT	10	/Failure	8
28 Jul 2006 08:48:26 PDT	38	/Failure	9
28 Jul 2006 08:48:26 PDT	12	/Success	8
28 Jul 2006 08:48:26 PDT	42	/Success	9
28 Jul 2006 09:48:26 PDT	23	/Attempt	9
28 Jul 2006 09:48:26 PDT	78	/Attempt	10
28 Jul 2006 09:48:26 PDT	13	/Failure	9
28 Jul 2006 09:48:26 PDT	35	/Failure	10
28 Jul 2006 09:48:26 PDT	11	/Success	9
28 Jul 2006 09:48:26 PDT	42	/Success	10

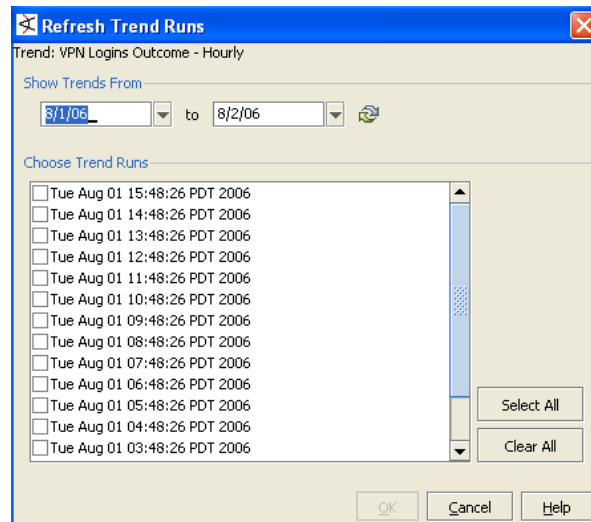
Refreshing Trend Data

In addition to relying on the scheduled execution of a query per its interval trend schedule, you can manually refresh the trend data at any time by using the trend refresh feature.

To manually refresh a trend table:

- Do either of the following:
 - Click the **Refresh Trend Runs** button on the Trends Attributes tab for the selected trend.
 - In the Navigator, select a Trend you want to refresh, right-mouse click and select **Refresh trend runs...** from the context menu.

This brings up the **Refresh Trends** dialog which displays the trend query start times of the selected trend.



- 2 Select a timeframe under **Show Trends From**, select one or more of the Trend Runs under **Choose Trend Runs**, and click **OK** to refresh the selected trend run(s).

This executes the base query and refreshes the trend table on the selected run(s). Trend refresh allows you to manually re-run a trend to compensate for events that arrive to the Manager late, either from a time zone lag or other data collection lag.



Also, you can configure data collection to be offset by some time period to compensate for late arrival of events. For more information, see Advanced settings for trends in this Help topic.

Editing or Viewing a Trend Definition

- 1 Navigate to **Reports** in the Navigator panel, select the **Trends** tab, and select the trend you want to modify.
- 2 Double-click the trend, or right-click and select **Edit Trend** from the context menu. This launches the Trend Editor in the Inspect/Edit panel, and shows the definition for the selected trend.
- 3 Edit the schedule, advanced settings, and so forth as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Trend editor without saving changes.)



The query used for a trend and the schema are set at the time the trend was created, and cannot be edited later. If you decide to use a different base query or need to make a change to the schema, delete the trend and start fresh. You can edit the base query by adding columns to it, but columns added to the query after the trend is created are not used by the trend. You can remove columns from the base query that are not used by the trend. However, if you want to add or remove columns (data fields) in the query that are used in the trend, create a new trend and select that modified query.

Using a Trend in a Query or Report

Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result.

For more information on next steps, see Building Queries and [“Creating Reports” on page 385](#).

Creating Reports

Reports are captured views or summaries of data that can be viewed in the ESM Console or exported for sharing in a variety of file formats. You can create reports by pulling together the result sets from one or more queries or trends.

For information on how to run an existing report, see [“Running Reports” on page 423](#).

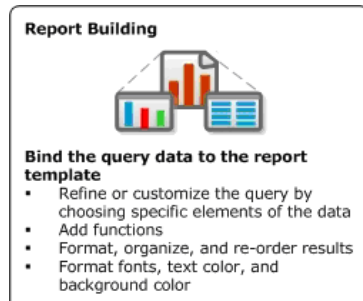
Creating Reports is a component of ArcSight Reporting resource tools. See also [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools, including how to build queries or trends and how to use a provided or custom template.

How Reports Work

When you have source data defined in queries and/or trends, you can design reports to present the data in charts and tables. You can use one of the templates provided with

ArcSight or design your own template using the Template Designer. This topic explains how to create a report that binds result data from queries and trends to a template, once you have one. (For information on accessing stock report templates or designing custom templates, see [“Using Report Templates” on page 335](#).)

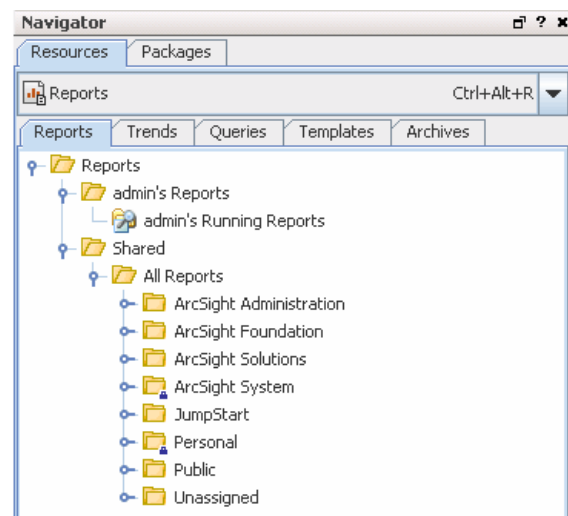
The reports resource defines how query data is bound to a report template. Depending on the report template you use, the reports editor exposes different parameters, variables, and conditions that enable you to choose which elements of the query data you want to show in the report. You can also apply additional functions to run on the data, and set numerous formatting options.



Building a Report

Navigating to Reports

In the Navigator panel, select **Reports** resource from the drop-down menu and click the **Reports** tab.



Creating a New Report

The high-level steps for creating a report are as follows:

- 1 Right-click a reports group (folder) and select **New Report** (or **New Report from Template** to start with a base template that you can refine later). This launches the Reports Editor in the Inspect/Edit panel.



As a general rule, it is best to create new content in the user's own folder.

- 2 Define Report Attributes such as report name, and optional aliases and owner/notification details.
- 3 Select the Report Template you want to use.
- 4 Choose Report Data by specifying what parts of the query data you want to use for each report element. Optionally, apply legends and top/bottom functions.
- 5 Specify Report Parameters output details, such as file format, paper size, and routing instructions. You can also set limits on the query return, such as row limits, time zone restraints, apply filters, and specify report start and end times.
- 6 Click **Apply** or **OK** to save settings and create the new report.



Note

Be sure to click **Apply** or **OK** frequently to save settings intermittently as you work through the above steps. Clicking **Apply** saves settings and leaves the Editor open. Clicking **OK** saves settings and closes the Editor for this query. If you do not apply or accept settings using these buttons, your settings are not saved.

- 7 Run the report to test it as described in Running a New or Archived Report.

The following sections provide details on how to use the Report editor to define report attributes, apply a template, choose report data, and specify report parameters.

Defining Report Settings

Report Attributes

The **Report Attributes** tab is where you define a report name, set alias report name and notification options, and view tracking details such as when the report was created and last updated.

The following fields in the **Report** section are required attributes that must be specified when creating a new query.

Report Field	Description
Name	Name for the report. Spaces and special characters are OK.



Tip

Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

The following example shows the Report Attributes for our VPN Logins Outcome report

The screenshot shows the 'Inspect/Edit' dialog box with the 'Attributes' tab selected. The dialog displays a table of report attributes for the 'VPN Logins Outcome Trend Report'.

Name	Value
Report	
Name	VPN Logins Outcome Trend Report
Common	
Resource ID	9RHoDVw0BABCfk2z4e1RyNA==
External ID	
Alias	
Description	
Version ID	
Deprecated	<input type="checkbox"/>
Assign	
Owner	
Notification Groups	
Parent Groups	
vicky's Reports	/All Reports/Personal/vicky's Reports
Creation Information	
Created By	vicky
Creation Time	28 Aug 2006 16:00:50 PDT
Time Since Creation	1 hour(s) 5 min(s) 57 sec(s)
Last Update Information	
Last Updated By	vicky
Last Update Time	28 Aug 2006 16:00:50 PDT
Time Since Last Update	1 hour(s) 5 min(s) 57 sec(s)

At the bottom of the dialog, there are buttons for 'Preview...', 'OK', 'Cancel', and 'Apply'.

Report Templates

The **Templates** tab is where you specify the template for the report. You can specify fonts, colors, page headers and footers, and the chart and table combinations and layout you want to use.

Report Template Selection

To populate the editor, select a template from the **Report Template** drop-down menu. ArcSight comes with six stock templates in the System templates folder, or you can navigate to your own template.

The example below shows the system template Three Charts Description Landscape.

Inspect/Edit

Report Editor \

Attributes \ Template \ Data \ Parameters \ Jobs \ Notes \

Report Template: Three Charts Description Landscape

Text Components

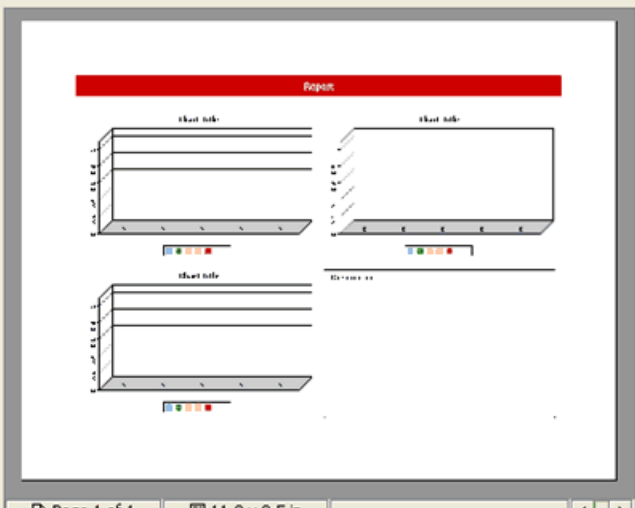
Header

Name	Value
Header	
Text	
Horizontal Alignment	left
Vertical Alignment	vertical center
Font	Serif, Plain, 10
Foreground Color	0, 0, 0
Background Color	255, 255, 255

Footer

Name	Value
Footer	
Text	
Horizontal Alignment	left
Vertical Alignment	vertical center
Font	Serif, Plain, 10
Foreground Color	0, 0, 0
Background Color	255, 255, 255

Preview



Page 1 of 1 11.0 x 8.5 in

Preview... OK Cancel Apply

Report Template:
Choose a template.
(Arcsight-provided or
custom template)

Text Components:
Specify Header,
Footer, and Text
formatting options for
the report.

Preview Area:
Shows the layout of
the Report Template
you chose.

Text Components

Text Components areas for Header, Footer, and Text sections provides fields to specify values for each of those sections of the report page.

Attribute	Description
Header	
Text	Type in the text you want to use as the header of your the pages in your report, such as the name of your department, or the series of reports to which it belongs. Note: You can use Velocity template references for fields that accept text, as described in "Velocity References for Reports" on page 1023 .
Horizontal Alignment	From the drop-down menu, select where you want the header to appear in the header area: left, right or center.
Vertical Alignment	From the drop-down menu, select where you want the header to appear in the header area: top, center, or bottom.
Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
Foreground Color	From the drop-down dialog, select a foreground color. This is the color of the lettering.
Background Color	From the drop-down dialog, select a background color. This color fills the header box.
Footer	
Text	Type in the text you want to use as the footer of your the pages in your report, such as the name of your company, a confidentiality statement, or the date. You can use the variables provided (such as \$currentpagenumber and \$totalpagenumber for page numbers). These are evaluated when you run the report to populate report output with appropriate numbering. Note: You can use Velocity template references for fields that accept text, as described in "Velocity References for Reports" on page 1023 .
Horizontal Alignment	From the drop-down menu, select where you want the footer to appear in the footer area: left, right or center.
Vertical Alignment	From the drop-down menu, select where you want the footer to appear in the footer area: top, center, or bottom.
Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
Foreground Color	From the drop-down dialog, select a foreground color. This is the color of the lettering.
Background Color	From the drop-down dialog, select a background color. This color fills the footer box.
Text	
Text	Type in the text you want to use as the title of your report, such Top 10 Attacks per Zone.
Horizontal Alignment	From the drop-down menu, select where you want the title to appear in the title area: left, right or center.

Attribute	Description
Vertical Alignment	From the drop-down menu, select where you want the title to appear in the title area: top, center, or bottom.
Font	From the drop-down dialog, select a font from the list of fonts available on your local system, font size, and style (bold, italic). The preview window indicates how the font will look.
Foreground Color	From the drop-down dialog, select a foreground color. This is the color of the lettering.
Background Color	From the drop-down dialog, select a background color. This color fills the title box.

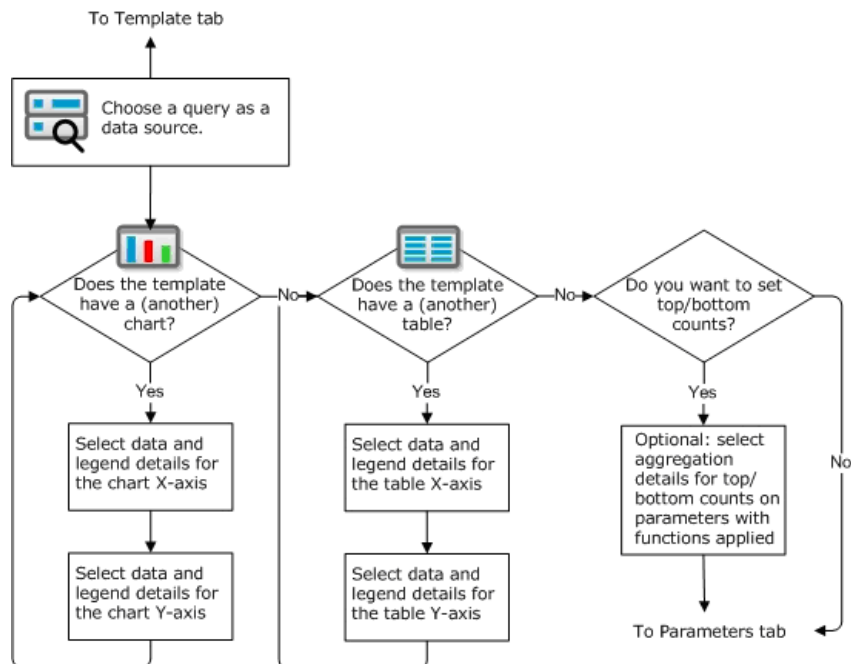
Preview Area

The Preview Area shows the layout of the report, and does not show the formatting updates as you go along. If you have designed other text boxes for your template, the attributes for those text boxes are displayed here using the same format as those shown above.

Report Data

Once the template is chosen and formatted, you are ready to populate the elements of the report with data.

The **Data** tab is where you choose which parts of the query or filter result data you want to use for each report element, apply legends and, optionally, top/bottom functions.



Use these options to select the data source (query or trend), chart and table type to use for the report, columns to include, and details on how the chart presents data.

Binding Data to Charts in Reports

Chart Data	Description
Data Source	<p>From the drop-down menu, select an existing data source you want to use for the chart in your report.</p> <p>The data source drop-down menu provides a list of existing resources based on the resource type you selected in the accompanying drop-down. You can report on queries, trends, active lists, or session lists.</p> <p>When the data source is selected, the remaining elements of the Data tab populate with the data available in the selected resource.</p>
Chart Type	<p>From the drop-down menu, select the type of chart you want to use for the chart part of the report. Depending on the template you use, you may have are several types of bar charts available as well as line charts, pie charts, speedometer, and so forth. The data source and chart type you choose apply to both the X and Y axes.</p>

Selecting Data for the X-Axis on a Chart

Data Source: Choose an existing resource on which to run the report. (Available sources will depend on which resource type is selected.) Data selected here apply to both X and Y axes.

Resource Type: Choose the resource type. You can report on queries, trends, active lists, or session lists.

Chart Type: Choose a chart type. (Bar chart, line chart, pie chart, and so on.)

X, Y Axis Tabs: Indicates which aspect of Data details you are working on. Optionally, you can Aggregate on one of the columns for this Report.

X-Axis Details: Choose and order the data you want to use on the X axis. Optionally, create and position a label for the data.

Display Options and Scale Format: Values set here apply to both X and Y axis data, and appear the same on both tabs.

If the report template you selected contains a **Chart**, bind your result data to the chart as described below.

	X-Axis Data Attribute	Description
Columns and Label	Available Columns	<p>Select the data field(s) from the query you want to show in the X-axis and use the right-hand arrow to move it to the Selected Columns area. The data you select here should be the item(s) you want to count</p> <p>For example, to build a trend report showing number of events over time, use a trend that captures the number of events per day. Add the end time to the X-axis to represent the day and add the count gathered for that day to the Y-axis. In this case, the X-axis is the data label, and the Y-axis is the count.</p>
	Selected Columns	The Selected Columns area shows which data fields you have selected for the X-axis, and provides the opportunity to change the sort order of the data. To change the sort order, select an item to activate the Sort checkbox. Select A-Z to sort data in ascending order; select Z-A to sort data in descending order.
	X-Axis Title	Specify a title for the X-axis.
	Label Rotation	<p>Select a rotation angle for the by entering a digit between 0 and 360.</p> <p>Labels refer to the individual X-axis data points, which are automatically derived from the data. The Label Rotation controls the angle of these labels.</p>
Display Options	Font	From the drop-down menu, select a font for the X and Y-axis text.
	Show Legend	Select this box to show a legend of the data elements. Keep in mind the number of different data elements your query may return. If the data you selected contains many elements, the legend may be large, which reduces the available space for the chart itself. If you choose to display the legend, you can move its location from choices in the Placement drop-down menu.
	Show Axis Grid	This setting displays the chart results in a table format along side the chart.
Scale and Format	Font	From the drop-down menu, select a font for the X and Y-axis text.
	Show Legend	Select this box to show a legend of the data elements. Keep in mind the number of different data elements your query may return. If the data you selected contains many elements, the legend may be large, which reduces the available space for the chart itself. If you choose to display the legend, you can move its location from choices in the Placement drop-down menu.

X-Axis Data Attribute	Description
Show Axis Grid	This setting displays the chart results in a table format along side the chart.

Selecting Data for the Y-Axis on a Chart

Y-Axis Details: Choose and order the data you want to use on the Y axis. Optionally, create and position a label for the data.

Summary Function: Optionally, you can enter a Summary Function on one of the columns and aggregate on that data for the Report.

Y-axis data should be numeric. If the data you select is a non-numeric data type, such as a string, apply a numeric *summary function* to it, such as **Count** or **Count distinct**.

Y-Axis Data Attribute	Description
Available Columns	Select the data field(s) from the query you want to show in the Y-axis and use the right-hand arrow to move it to the Selected Columns area. The data you select here should be the item you want to count by. For example, to show how many addresses each of your attacker zones have, you would select the attacker address.

Y-Axis Data Attribute	Description
Summary Function	<p>You can assign a summary function to one or more columns of data. (In the "Function" row for a column, click in the column to get a drop-down menu of functions.)</p> <ul style="list-style-type: none"> • Count - Provides a count of all line-items returned by the query. <p>Note: The Count function is a simple count of all events. It takes into consideration the <i>aggregated event count</i> and counts each event in an <i>aggregated event</i> individually. For example, if an event has an aggregated event count of 5, the Count function counts this event as equivalent to 5 events (with an <i>aggregated event count</i> of 1 each). Take this into account when comparing the number of rows in a report with the "grand total" count based on the Count function.</p> <ul style="list-style-type: none"> • Count Distinct - Provides a count of how many items are unique. For example, if there are 100 IP addresses but only 5 of them are unique, the system counts 5. • Average - Adds the results of numeric data and divides by the number of line items. • Sum - Adds the results of numeric data. • Max - For numeric data, Max calculates the line item with the highest value. • Min - For numeric data, Min calculates the line item with the lowest value. • Median - For numeric data, Median calculates the line item with the value closest to the middle between high and low. • Standard Deviation - For numeric data, measures the dispersion of the values in the data set (how spread out they are). If the data points are all close to the mean, then the standard deviation is close to zero. If many of the data points are far from the mean, then the standard deviation is further from zero. If all the data values are equal, then the standard deviation is zero. The Standard Deviation is the square root of the variance. • Variance - For numeric data, measures how spread out the distribution of data is. The variance is computed as the average squared deviation of each number from its mean. The variance and the standard deviation are closely related measures of dispersion and variability. <p>Selecting one of these functions activates the Aggregation tab, where you can set further parameters on these functions. To set a function, select a column, and choose a function from the Summary Function drop-down menu.</p>
Y-Axis Title	Type in a title for the Y-axis. Select a rotation angle by entering a digit between 0 and 360.
Label Rotation	<p>Select a rotation angle for the by entering a digit between 0 and 360.</p> <p>Labels refer to the individual Y-axis data points, which are automatically derived from the data. The Label Rotation controls the angle of these labels.</p>

Y-Axis Data Attribute	Description
Sort by	Optionally, choose a sorting order for the data on the Y axis. You can display data alphabetically (the default), reverse alphabetical, or sort by count.

Specifying Top/Bottom Filters Aggregation Filters for a Chart (Optional)

You can also set **Top/Bottom Counts** for a chart. This tab only becomes active when a summary function is applied to data in the Y axis. Settings in the **Aggregation** tab set top/bottom counts to data with summary functions applied. This is an optional step.

Inspect/Edit

Report:VPN Logins Outcome Tren...

Attributes Template Data Parameters Jobs Notes

Chart3 Chart2 Chart1

Data Source: s Outcome Trend Query - Attempt Queries

Chart Type: Line chart 2 sets of data (Z-axis)

Data (X-Axis) Value (Y-Axis) Aggregation

Set a top or bottom filter for the chart (optional)

How do you want to filter the chart data?

☒ None (Show all)

☐ Top 10 by means of Number of Logins

☐ Bottom by means of Number of Logins

Display Options

Font: Verdana, Plain, 8

☒ Show Legend

Placement: Bottom

☐ Show X-axis grid

☒ Show Y-axis grid

Scale and Format

Data (y-axis): ☐ Logarithmic Scale ☒ Show Value

Min Max Incr

Preview... OK Cancel Apply

Top Bottom Filter: Optionally, use aggregation to set top/bottom counts for Y-axis numeric functions.

On the Chart Aggregation tab, set the top or bottom filter for the chart. If there are more charts in your report, repeat these processes until data is bound to all the charts and laid out in your report template.

Aggregation Top/Bottom Filter	Description
None (Show all)	By default, no top/bottom filter is set.
Top	Select Top if you want to show the a certain number of entries with the highest values. Enter a digit in the text box, and from the drop-down list, select an appropriate Y-axis data column with a function applied.
Bottom	Select Bottom if you want to show a certain number of entries with the lowest values. Enter a digit in the text box, and from the drop-down list, select an appropriate Y-axis data column with a function applied.

Binding Data to Tables in Reports

If the template you selected contains a table, use the Table **Fields** tab to build a visual representation of a table in which to display the query result. You can choose the type of data source (trend, query, active list or session list) and the particular data source (which query, trend, etc.) to report on. Then you can select which fields from the data result you want to show up in your report (with the "Use" checkbox). Use Groups to combine fields into a single column in your Report table (drag and drop or menu commands).

Table Data	Description
Data Source	<p>From the drop-down menu, select an existing data source you want to use for the table part of your report.</p> <p>The data source drop-down menu provides a list of existing resources based on the resource type you selected in the accompanying drop-down. You can report on queries, trends, active lists, or session lists.</p> <p>When the data source is selected, the remaining elements of the Data tab populate with the data available in the selected resource.</p>

Data Source: Choose an existing resource on which to run the report. (Available sources will depend on which resource type is selected.)

Resource Type: Choose the resource type. You can report on queries, trends, active lists, or session lists.


Fields and Groups: Select the data fields you want to display in the table (by enabling **Use** for a field you want to show).
Provide a display name alias and specify data sort order in the column by dragging and dropping fields to desired location in column order.
Group multiple fields in a single column by dragging fields into Groups.

Display Options: Select a column or group to set font, foreground, and background display options.

Global Options: Global options apply to the whole table.

Specifying Fields for a Table

In the **Available Columns** area, you can select the fields you want to display in the table, group multiple fields into a single column as needed, assign Alias names for column headings, specify a data sort order, and set column size and alignment options.

Attribute	Description
Groups	<p>Optionally, you can sort data results from queries by grouping two or more fields into a single column.</p> <p>To create a group: Right-click in the Groups row for a column and choose Make Group. This brings up a dialog where you can name a new group and add the selected field.</p> <p>To add fields to a group: Drag fields from the Fields row to the Groups row. Alternatively, right-click a field and choose Add to Group. This brings up a dialog where you can name the group to which you want to add the selected field.</p>
Function	<p>To set a function on a field, right-click in the Function row for that field's column. Select the function you want to apply to the column from the Function drop-down menu. Once the function is set, the field appears with the function icon (.</p>

Attribute	Description
Use	<p>By default, all data entries are selected for use in the table. If you do not want to use all the available columns, uncheck the corresponding checkbox.</p> <p>Caution: If you de-select a data entry to indicate you do not want to use that column in report, the column is automatically pushed to the far right (the end of the table) to move it out of the way so that you can focus on the columns you are using. If you then select "Use" again for that same data entry, its column is inserted back into its original position along with the other columns you have selected to use.</p>
Field	This displays the name of the field as it is referred to in the ArcSight database. This field is not editable.
Alias	Enter a display name alias for the data column. For example, if the column is referred to as Source Translated Zone Name in the ArcSight database, this name can be shortened to Zone Name or Src Zone for display in the report table. In our example, we provide the aliases Time instead of Timestamp and Number of Logins for Category Outcome (Count).
Width	<p>Set column Width to either of the following options:</p> <ul style="list-style-type: none"> • Auto - Automatically divides column width evenly among the selected columns • User Specified Layout - This option requires that you enter numbers to specify percentage widths for individual columns.
Sort	Indicate the sort order for the data in each column.
H Align	Right-click in the H Align row to get a drop-down menu for specifying horizontal alignment of text in a given column. You can select for left-aligned, centered, or right-aligned text in the corresponding column.
V Align	Right-click in the V Align row to get a drop-down menu for specifying vertical alignment of text in a given column. You can select for top, bottom, middle, or baseline text in the corresponding column.
Page Break	Right-click in the Page Break row in a column to get options for specifying a page break before or after the that column.
Re-order Column Arrows	To specify a different order for how the columns are displayed, select a column and use the up/down arrows to move it up or down in the order.

With the **Custom Layout** options, you can specify custom column widths for the data in the table. By default, the **Custom Layout drop-down** menu shows User Specified Layout, which enables you to enter a numeral to specify a percentage for individual columns. Select one of the following:

- **Fit content** - Adjusts the column width to accommodate its content without wrapping. If the content is wider than the table, the table is extended to multiple pages.
- **Fit content one table area per page** - Adjusts the column width to accommodate its content without wrapping, and breaks each column onto its own page.
- **Fit content to page** - Adjusts the column width to accommodate its content without wrapping, and stretches the last column to fill the page.
- **Equal width columns** - Each column receives the same width to fit across a single page.

- **User specified layout** - Enables you to enter a numeral that represents a percentage of the overall page width. You can set a percentage for each column that totals 100%, or enter a percentage for one column, and the others selected receive an even percentage of the space remaining.

The **Display Options** area provides format options for each individual data column. This enables you to set different font style, size, and color and column background colors for each data column. To activate the display options, select one or more data columns:

- **To select one field:** click the field.
- **To select one or more contiguous fields:** click a field, hold down the Shift key, and select the remaining fields.
- **To select one or more non-contiguous fields:** click a field, hold down the Ctrl key and select the remaining fields

Attribute	Description
Font	From the drop-down menu, choose a font for the selected column(s).
Foreground Color	Foreground color for text, any visible lines that describe rows/columns, and other elements in the foreground. The example above shows all columns using black (RGB 0,0,0).
Background Color	Background (field) color for the data column. The example above shows the Count line with a pale yellow background (RGB 255, 255, 153).

In the **Global Options** area, you can set formatting options that apply to the whole table (not just one column).

Attribute	Description
Merge cells	Indicates whether to merge cells for grouped columns. When this option is enabled, identical values in grouped columns show only once. When this option is disabled, identical values show as many times as they occur (regardless of whether they are grouped).
Show group header	Indicates whether to show a group header row. This is a group label for when you have a summary function that adds one more rows at the end of the section. If this option is enabled, the table includes an extra column with a header derived from the content by which the section is grouped.
Show group columns	Enable this option to populate the grouped columns with data. (If this option is disabled, grouped columns are empty.)
Grand total	If you want to provide a grand total of all the sections, check the Show grand total box.
Label	If you selected a grand total, you can apply a label for the grand total. (For example, Total VPN Login Attempts.)

Click the **Preview...** button to preview the report table with the current configuration.

Set Top/Bottom Counts in Table Aggregation Tab (Optional)

This tab only becomes active when a function is applied to a column on the **Fields** tab. Settings in the Aggregation tab set optional top/bottom counts to data with summary functions applied to individual fields.

Report Parameters

The **Parameters** tab is where you set report output details such as file format, paper size, and routing instructions. From here you can also set limits on the query return such as row limits and time zone restraints, apply filters, and specify report start and end times.

Report Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input type="checkbox"/>
Run as User	Select a User	<input type="checkbox"/>
Email to		<input type="checkbox"/>
Email Format	Send URL	<input type="checkbox"/>

Query Parameters

Name	Value	Use Default
Table		
Row Limit	10000	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart2		
Row Limit	50	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart1		
Row Limit	50	<input type="checkbox"/>
Time Zone	Manager Time Zone	<input type="checkbox"/>
Filter by	Select a Filter	<input type="checkbox"/>

Report Parameters: Set Report output details.

Add Custom Parameters: Add and Edit custom parameters.

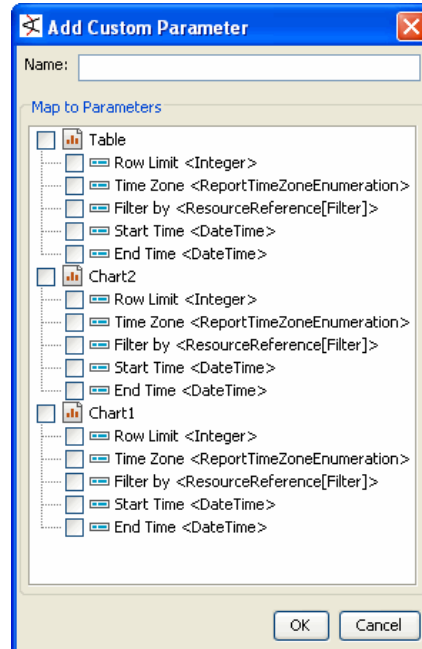
Query Parameters: Set override parameters for query data selected for each element of the report.

Buttons: Add..., Edit..., Remove, Preview..., OK, Cancel, Apply

In the **Report Parameters** area, enter the following values. The Use Default checkboxes do not apply to these items. Note that users can re-set most of these parameters at report runtime. See also [“Report Parameters” on page 425 in Running and Managing Reports.](#)

Common Parameters	Description
Report Format	<p>From the drop-down menu, select one of the following report output formats:</p> <ul style="list-style-type: none"> • pdf - Outputs the report as an Adobe PDF file. • xls - Generates a Microsoft Excel file for tables and charts. <p>Note: XLS reports run with <i>Microsoft Excel 2002</i> might have page break format problems (misalignments, column spillover) due to default page size settings in Excel. To correct this problem, open the resulting XLS report in Excel, choose File > Page Setup from the menus, change the paper size to Letter (instead of Legal), and click OK to save your changes. The report has the appropriate page break formatting. <i>This problem does not occur in newer versions of Microsoft Excel.</i></p> <p>Note: XLS report formats display speedometer charts as pie charts. This is a known limitation in Microsoft Excel.</p> • rtf - Produces a rich-text format document. • csv - Creates tabular data as a list of comma-separated values. <p>Note: Reports generated in CSV format are not the full equivalent of exports to other formats like PDF or HTML. CSV format is useful for loading report data into a spreadsheet for further manipulation. Since CSV is meant to contain tabular data, only the table data of a report is normally useful. Therefore, ArcSight exports only the table data portion of a report to CSV format, ignoring any other report information such as charts or text, including report titles.</p> • html - Generates the report in a Web page displayed by the default web browser.
Page Size	From the drop-down menu, select a paper size.
Run as User	<p>Run the report as a particular user. From the drop-down menu, select the user name by which you would like to run the report.</p> <p>For example, this option would allow an administrator for an Managed Security Service Provider (MSSP) to run report for a customer. The administrator would need write permissions to the user.</p>
Email to	<p>You can have the report sent as e-mail to one or more users.</p> <p>From the drop-down menu, select the users to whom the report should be e-mailed.</p>
Email Format	<p>You can e-mail a link (URL) to the report or send it directly as an e-mail attachment.</p> <ul style="list-style-type: none"> • If the report is large and is saved (archived) to a network-accessible location, you may want to select Send URL to point users to the report. • If you want to send the report directly to the user's e-mail box, select Attach Report.
Row Limit	You have the option of setting a row limit (for example, 1,000) if you think the generated table could exceed a manageable size.

To add a custom parameter that applies to the Report data, click the **Add** button. Parameters added here override those set in the query. For example, if you want all the report elements to report on events for the past 2 hours, you can create a start-time parameter of `$Now-2h`, which sets both table and chart start times to `$Now-2h`. Custom parameters are saved locally to the report definition, and are not persisted back in the query.



Set parameters and click **OK** to apply them to the report definition.

Back in the **Parameters** tab in the **Custom Parameters** section, enter an override parameter for the field(s) you selected from the Add Custom Parameters dialog.

In the **Query Parameters** area, enter any override values for the parameters in your query data. The Use Default checkboxes are only activated for items where default parameters exist and override values can be entered.

Enter these override parameters as needed for each chart and table.

Query Parameters	Description
Row Limit	You can limit the number of rows in the table to a number specified. Select a row limit value from the drop-down list.
Time Zone	By default, the Manager time zone is used. Choose the Console time zone, or another of the time zones from the drop-down list.
Filter By	Set a filter to operate on the query conditions.
Start Time	To set a start time that overrides the one set in the query, disable Use Default for this field and specify a start time here. For example, if you want all the report elements to report on events for the past 2 hours, you can create a start-time parameter of <code>\$Now-2h</code> , which sets both table and chart start times to <code>\$Now-2h</code> . This setting is saved locally as part of the report definition, not as part of the original query upon which the report is based.

Query Parameters	Description
End Time	To set an end time that overrides the one set in the query, disable Use Default for this field and specify an end time here. This setting is saved locally as part of the report definition, not as part of the original query or trend upon which the report is based.

Be sure to click **Apply** to save settings or **OK** to save settings and close the Inspect/Edit details for this report.

Setting Special Parameters for Running Large or Complex Reports

A very large report (for example, a 500 MB PDF report) might require so much virtual machine (VM) memory that it can cause the ArcSight Manager to crash and re-start. To prevent this scenario, you can set up the Manager to expose a special report parameter for generating the report in a separate process. The separate process has its own VM and heap, so the report is more likely to finish. Even if the memory allocated is still not enough, the report failure will not crash the Manager. This option must be set up on the Manager to expose it in the ESM Console report parameters list. The steps are as follows:

- 1 On the ArcSight Manager in the `server.properties` file, set `report.canarchiveinseparateprocess=true`. (This makes a new report parameter available on the ESM Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ESM Console, open the report that you want to run in a separate process in the Report **Editor**, and click the **Parameters** tab. Set the parameter **Generate Report In Separate Process** to **true**.

- 4 Run the report. The report should run like a normal report, but it does not consume the resources of the Manager VM. See notes below for more information.



Tips:

- If a report is saved with the parameter set to **"true"**, the report is archived as a separate process even if the property `report.canarchiveinseparateprocess` in `server.properties` is set back to **false** later on.
- This property indicates whether reports are allowed to be archived in a separate process. When this property is set to **"true"**, the option to run and archive the report in a separate process is available in the common properties in the Report Editor. Setting the value to true causes the report to be archived in a separate process. The benefit of archiving a report in a separate process is to avoid consuming Manager resources and potentially crashing the Manager.
- Refer to the *Administrator's Guide* for more information on setting server properties on the Manager. The property `Canarchiveinseparateprocess` is also documented in the `server.defaults.properties` file.
- Use this parameter only in special circumstances as needed. For example, if archiving a report is causing the Manager to crash then you might apply this solution. Generally, if a report contains tables that have more than 500,000 rows with 4 or 5 columns per row it is likely that the report is large enough over-tax the Manager VM memory. However, the tipping point may vary depending on the Manager heap size and the details and data in the tables so it is best to only resort to this solution if you encounter problems archiving a particular report.

Reports that query over a large time range with complex joins run much faster if the query contains a full scan database hint. This option must be set up on the Manager to expose it in the ESM Console report parameters list. The steps are as follows:

- 1 In the Manager in the `server.properties` file, set `report.canquerywithfullscanhint=true`. (This makes a new report parameter available on the ESM Console.)
- 2 Save the `server.properties` file and restart the Manager.
- 3 On the ESM Console, open the report that you want to contain the full scan hint in the Report **Editor**, and click the **Parameters** tab. Set the parameter **Query with Full Scan Hint** to **true**.
- 4 Run the report.



If a report is saved with the parameter **"true"**, the full database optimization hint is applied even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to **false** later on.

When the property is set to **"true"**, the report uses the FULL_SCAN hint in the SQL queries it generates to query the database. The content of the report does not change, but the queries logged in `server.report.log` contain the hint. FULL_SCAN hint can significantly reduce the runtime for SQL queries that query events within a large time range and contain complex joins.

Refer to the *Administrator's Guide* for more information on setting server properties on the Manager. This property is also documented in the `server.defaults.properties` file.

Use this parameter only in special circumstances if your organization has determined with the help of ArcSight support or professional services that it is appropriate.

Setup and Parameters to Generate PDF Reports with Asian Fonts

To generate reports in PDF with Asian fonts, the appropriately localized Adobe Reader 8.0 (for the language of your platform) must be installed on the ArcSight Manager with the OpenType fonts for Asian languages. (The font files you need are included as part of the localized Adobe Reader 8.0 installation.)

Additionally, font paths in `server.properties` need to map to the Adobe Reader 8.0 fonts. On the Manager edit `server.properties` as follows:

- Set `report.font.truetype.path` property to point to the directories that contain the TrueType and OpenType fonts. On Windows systems, these paths are typically "`C:\\WINNT\\fonts;C:\\Program Files\\Adobe\\Reader 8.0\\Resource\\CIDFont`", where ";" is used as a path separator to separate the multiple paths. (In the properties file, use backslashes as shown to escape the backslashes for the Windows-style path separators.) On UNIX systems, these paths are typically `"/usr/lib/font:<Adobe_Reader_Directory>/Resource/CIDFont"` where ":" is used as the path separator.
- Set `report.font.cmap.path` property to point to Adobe Reader's CMap directory. On Windows systems, this is typically "`C:\\Program Files\\Adobe\\Reader 8.0\\Resource\\CMap`". (In the properties file, use backslashes as shown to escape the backslashes for the Windows-style path separators.) On UNIX systems, the path is typically `"/usr/lib/font:<Adobe_Reader_Directory>/Resource/CMap"`.

Since the Adobe Reader supports OpenType fonts but does not directly support TrueType fonts, the ArcSight Manager provides default mappings between TrueType and OpenType fonts in

`<arcsight_home>\\il8n\\server\\reportpdf_config_<locale>.properties` file. Generally, the default mappings suit your purpose but if not, you can edit the `reportpdf_config_<locale>.properties` file to change mapping of any TrueType font to a different OpenType font.

After making these configuration updates, save the `server.properties` and `reportpdf_config_<locale>.properties` files, and restart the Manager. (Be sure to download and install the Adobe Reader and font files first, then change and save the settings in the properties files based on installed font paths, and restart the Manager.)

If you try to generate PDF reports with Asian fonts without the above setup, the Asian language strings appear mangled. For more information, see the *Administrator's Guide* "Troubleshooting" section.

Editing a Report

- 1 Navigate to **Reports** in the Navigator panel, select the **Report** tab, and select the report you want to modify.
- 2 Double-click the report, or right-click and select **Edit Report** from the context menu. This launches the Report Editor in the Inspect/Edit panel, and shows the definition for the selected report.
- 3 Edit the report definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)

End-to-End Reporting Examples

This topic includes two examples:

Quick-start example with Report Wizard - An introductory example of how to create a simple report on the results of a single, stock query with the Report Wizard.

Advanced example - A more in-depth example reporting on the results of several trend-queries and using a heavily-modified 3-charts template. This example walks you through creating the following resources for example queries, trend, and report:

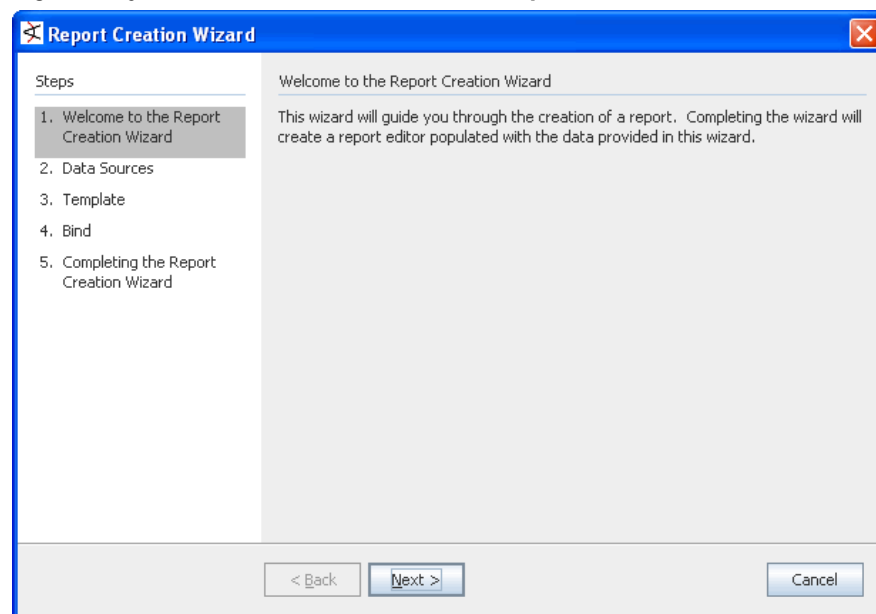
- A base query that captures data about number of VPN login attempts per hour.
- A trend that takes the base query as input, executes it, and stores captured data per a schedule you define.
- Queries that build on the trend to filter on various VPN login outcomes.
- A report that uses the complex queries as data sources and provides visual representations of query results in charts and tables based on an ArcSight provided template.

Even if you do not anticipate immediately having to create these elements from scratch (ArcSight provides a starter set of stock reporting content), we suggest working through both the simple example and the more complex one to gain an understanding of how queries, trends, and templates work together in the context of reporting.

Refer also to other topics in [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools.

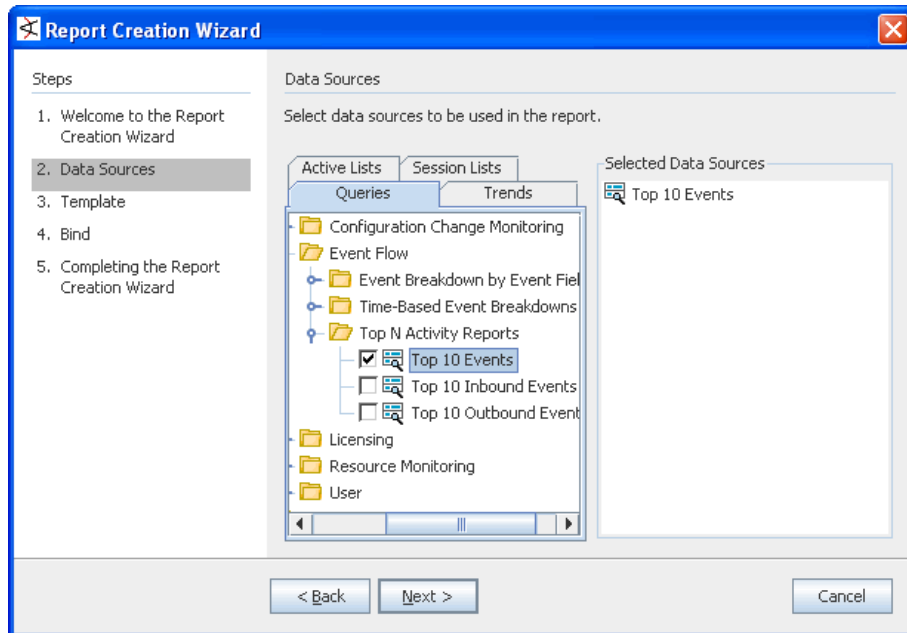
Quick Start Example of Creating a Simple Report with the Wizard

- 1 Navigate to the Reports resource in the Navigator panel and click the **Reports** tab. Right-click your user folder and choose **Start Report Wizard**.



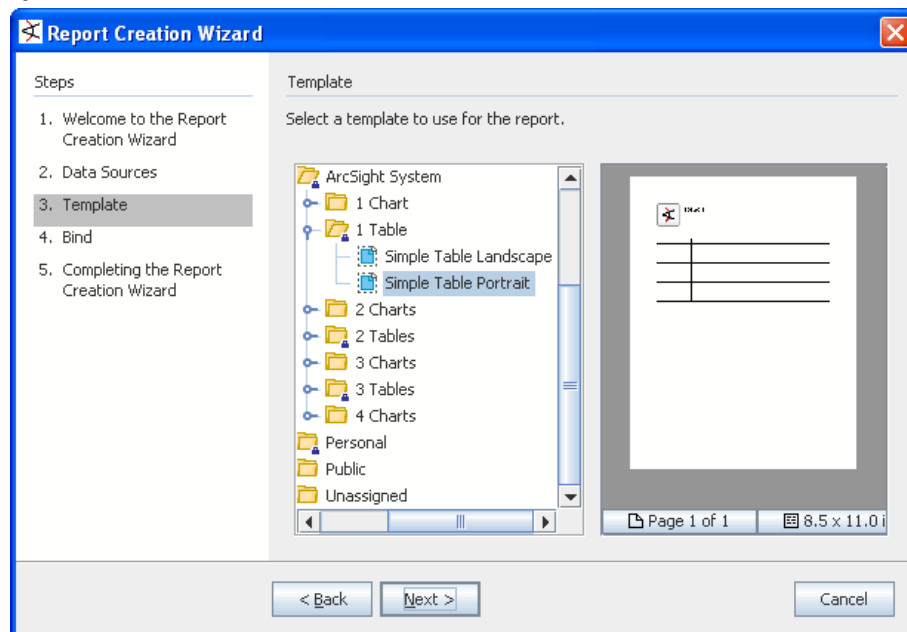
Click **Next**.

- On the **Data Sources** page, select the **Queries** tab (if not already selected, and navigate the Queries tree to choose an existing query. For this example, we select the **Top 10 Events query**, which you can find in Queries/Shared/All Queries/ArcSight Administration/Event Flow/Top N Activity Reports/.



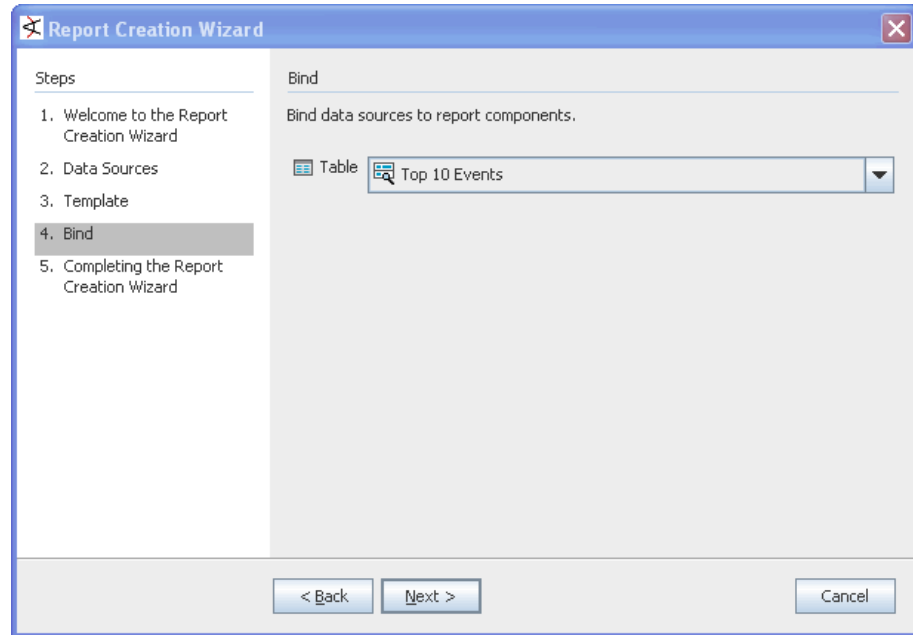
Click **Next**.

- On the **Template** page, select a template. For this example, select the **Simple Table Portrait** template under /Report Templates Shared/All Report Templates/ArcSight System/.



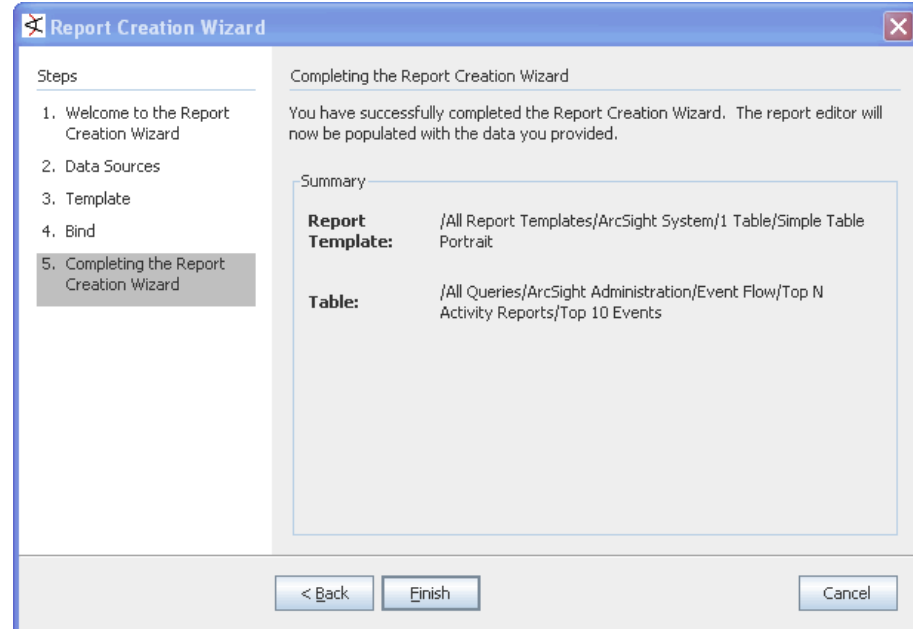
Click **Next**.

- 4 On the **Bind** page, select a template. For this example, select the **Simple Table Portrait** template under /Report Templates Shared/All Report Templates/ArcSight System/.



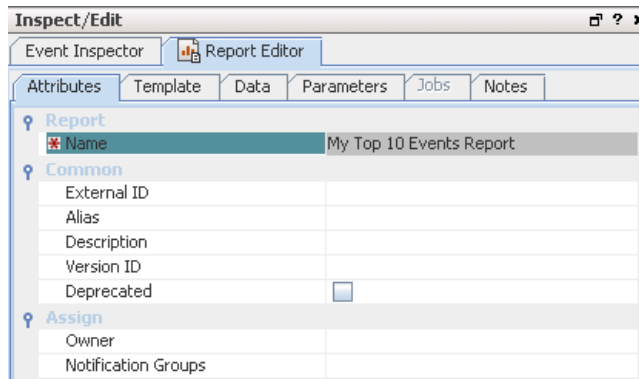
Click **Next**.

- 5 Review the report configuration summary.



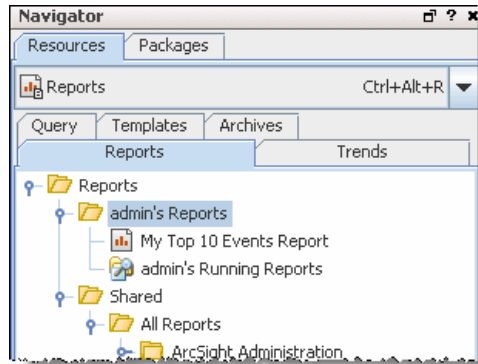
When you are satisfied with the report configuration, click **Finish** on the last page of the Report Wizard.

- 6 On the **Report Editor Attributes tab** (which is automatically displayed), enter a **Name** for the report. For this example, we name the report "My Top 10 Events Report".



Click **Apply** or **OK** on the Report editor to apply the report name and create the report.

- 7 The new report is added to your Reports folder shown in the Navigator.



- 8 On the Navigator panel Reports tree, open your Reports folder, right-click the new report and select **Run > Report with defaults**.

Advanced Reporting Example Overview

We build an example query that shows the number of login attempts on a virtual private network (VPN). Then, we use the query in a trend to collect data on VPN login attempts on an hourly basis. Next, we build several more focused queries on top of the trend to get views into particular slices of the data (all login attempts, successful logins, and failed logins).

Finally, we use the data results from the queries and trends to create a report. To format the report, we use one of the ArcSight provided templates.

Start by navigating to the Reports resource in the Navigator panel, then follow these steps to build the example report:



You need a set of canned VPN login events to properly verify the query and trend resources created for this example.

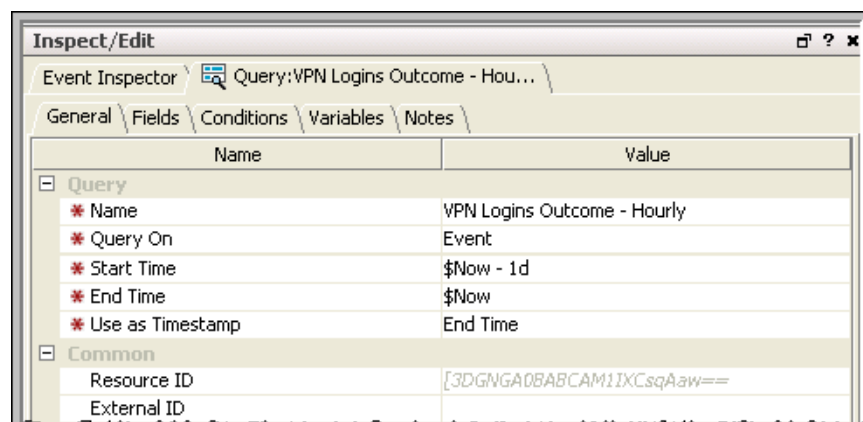
1. Build the VPN Logins Outcome Query

Start by building a base query that captures VPN Login Data to return a count of hourly VPN login attempts. Following is a summary of configuration details you can use to create this query. (If you need more general help on creating queries, refer to Building Queries.)

Query Name and Other General Attributes

Create a new query, name it, and set general attributes for it on the Query **General** tab as shown.

Query Attributes	Value
Name	VPN Logins Outcome - Hourly
Query on	Event
Start Time	\$Now - 1d
End Time	\$Now
Use as Timestamp	End Time

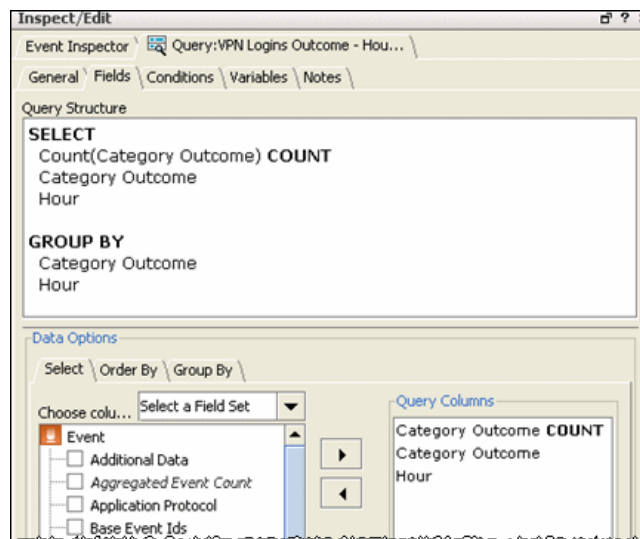


Fields to Include in Query Result

On the Query **Fields** tab, select fields and apply functions as shown to populate columns in the table of result data.

Selected Fields	Description
Category Outcome (COUNT)	To get this, first add Category Outcome to the Query Columns list. Then select it from the Query Columns list and use the Function drop-down menu to apply the COUNT function to it.
Category Outcome	Add the Category Outcome field to the Query Columns list again, but do not apply any function to it. This column contains the outcome of each login attempt (success or failure).
Hour	To get this, define a variable called Hour and assign the GetHour function to it, which returns the hour value based on the end time of the event. (Click the Variables tab to define the Hour variable first. Then you can return to the Select tab to add the Hour variable to the Query Column list.) This column contains the date and time of the login attempt.

Group by Category Outcome and Hour.



Query Conditions

On the Query **Conditions** tab, define some logical conditions for the login data that narrow the query result to return only the data you are interested in. Filter on VPN Logins by specifying that each login attempt must be categorized in a specific event category and device group:

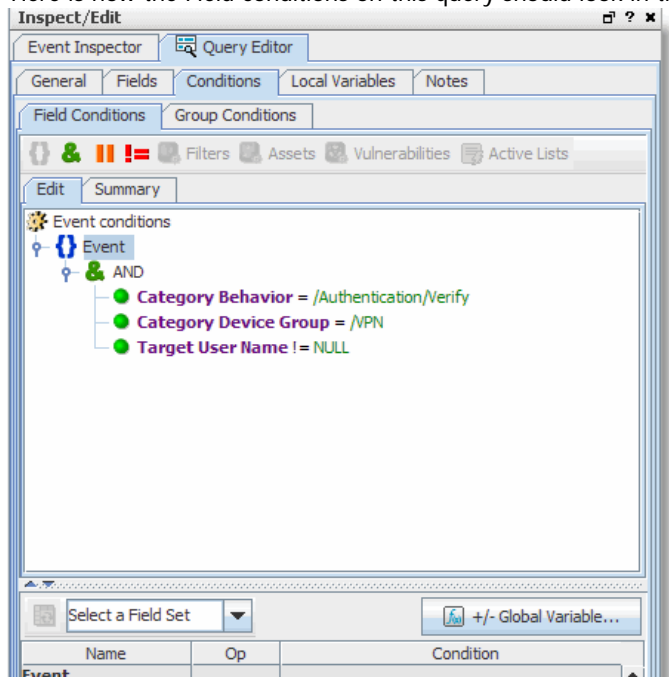
Category Behavior = /Authentication/Verify

Category Device Group = /VPN

Also, each login attempt must have a target user name value:

Target User Name Is NOT NULL

Here is how the Field conditions on this query should look in the display:

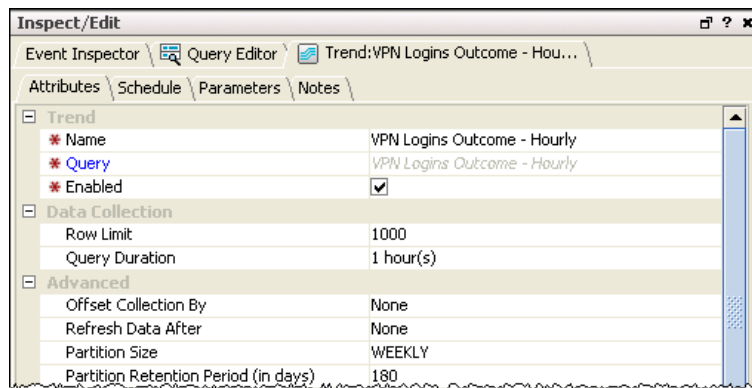


Click **Apply** or **OK** in the Query Editor to save the new query.

2. Build the VPN Logins Outcome Hourly Trend

Next, create a new trend, name it, and set general attributes for it on the Trend **Attributes** tab as shown. This trend uses the data results from the VPN Logins Outcome Query you just created. Keep the defaults for Trend Interval (1 hour to collect data on an hourly basis) and row limit at 1,000 (it stops collecting data when the table is filled at that limit).

Trend Attributes	Value
Name	VPN Logins Outcome - Hourly
Query	VPN Logins Outcome - Hourly
Enabled	On
Trend Interval	1 hour(s)
Row Limit	1000



Under Data Fields, you can see the fields the trend is getting from the query initially reflected with the original field names: TimeStamp, COUNT(CategoryOutcome),

CategoryOutcome, Hour. For readability, change these to the aliases Time, Number of Logins, Category Outcome, and Hour as shown below.

Description
Enter a description

Data Fields

Name	Use	Index
Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Number of Logins	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Category Outcome	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hour	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Summary

Occurs **Hourly**.
Schedule will start on **Tue Aug 29 18:07:15 PDT 2006**.

Refresh Trend Runs Test OK Cancel Apply

From here, you can test the trend to ensure you are getting correct data. To do this, click the **Test** button on the Trend **Attributes** tab. The Test Trend dialog returns an example result set. For each row, the Trend should return Timestamp, count of login attempts, Category Outcome (Attempt or Failure), Hour (from the Hour variable).

Trends also have schedules. On the Trend **Schedule** tab, define a schedule that specifies how often you want to run the trend. For the example, define this one to run every hour on the hour (Hourly, every 1 hour at "0 minutes after").

A Trend's range defines when to start and terminate the data collection.

The Trend starts as you specified and keep going until it is manually terminated.

Here is the data collected from a trend that ran hourly for a few days. You can view result data from your trend in the grid view by selecting the trend in the Navigator and clicking the Data Viewer for it in the right-click menu.

Time	Number of Logins	Category Outcome	Hour
27 Jul 2006 12:48:26 PDT	26	/Attempt	12
27 Jul 2006 12:48:26 PDT	100	/Attempt	13
27 Jul 2006 12:48:26 PDT	12	/Failure	12
27 Jul 2006 12:48:26 PDT	47	/Failure	13
27 Jul 2006 12:48:26 PDT	13	/Success	12
27 Jul 2006 12:48:26 PDT	54	/Success	13
28 Jul 2006 08:48:26 PDT	22	/Attempt	8
28 Jul 2006 08:48:26 PDT	80	/Attempt	9
28 Jul 2006 08:48:26 PDT	10	/Failure	8
28 Jul 2006 08:48:26 PDT	38	/Failure	9
28 Jul 2006 08:48:26 PDT	12	/Success	8
28 Jul 2006 08:48:26 PDT	42	/Success	9
28 Jul 2006 09:48:26 PDT	23	/Attempt	9
28 Jul 2006 09:48:26 PDT	78	/Attempt	10
28 Jul 2006 09:48:26 PDT	13	/Failure	9
28 Jul 2006 09:48:26 PDT	35	/Failure	10
28 Jul 2006 09:48:26 PDT	11	/Success	9
28 Jul 2006 09:48:26 PDT	42	/Success	10

When you are satisfied that the Trend is set up correctly, click **Apply** or **OK** in the Trend Editor to save the trend.

3. Filter the Trend Data (Login Attempts, Successes, Failures)

You can further refine the VPN login query data by creating separate queries based on the trend, each of which capture information a particular aspect of VPN login events. Developing several trend-based queries like this (to show different data slices of common scenarios), gives you a rich set of data views from which to run reports later.

Create three more queries all of which use the original trend as their data source, and then further filter the data to show only attempts, failures, or successes, respectively. Use each of these queries, **Attempt**, **Failure**, and **Success**, to further filter the login data captured in the trend:

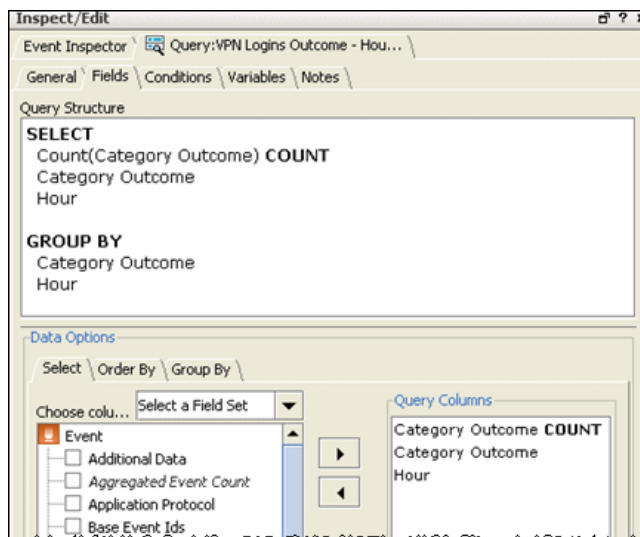
- **Login Outcome Trend Query - Attempt**
- **Login Outcome Trend Query - Failure**
- **Login Outcome Trend Query - Success**

As an example of how this is done, here are the details for creating one of these; the **Failure** Query definition.

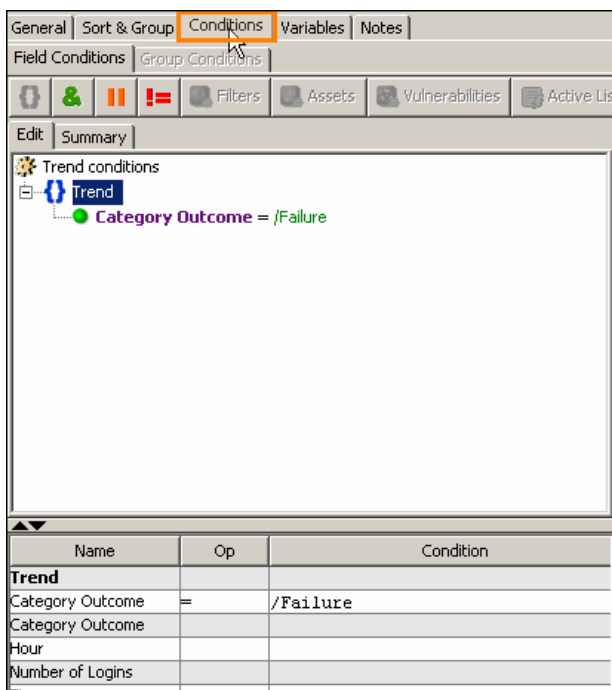
Create a new query and name it **Login Outcome Trend Query - Failure**.

As the query's data source type, choose **Trend** and select the "VPN Logins Outcome - Hourly" trend.

In the Query **Fields** tab, choose the same fields as in the original query to populate columns.



On the **Conditions** tab, specify **Category Outcome = /Failure**. The query only returns the login attempts that failed.



Save your changes. You have now built a query that reports on failed VPN login trends.

Create the other two queries (Login Outcome Trend Query - Attempt and Login Outcome Trend Query - Success) the same way specifying the appropriate Category Outcome condition for each.

Now you are ready to report on the Trend data.

4. Create the VPN Logins Outcome Report on Trend Data

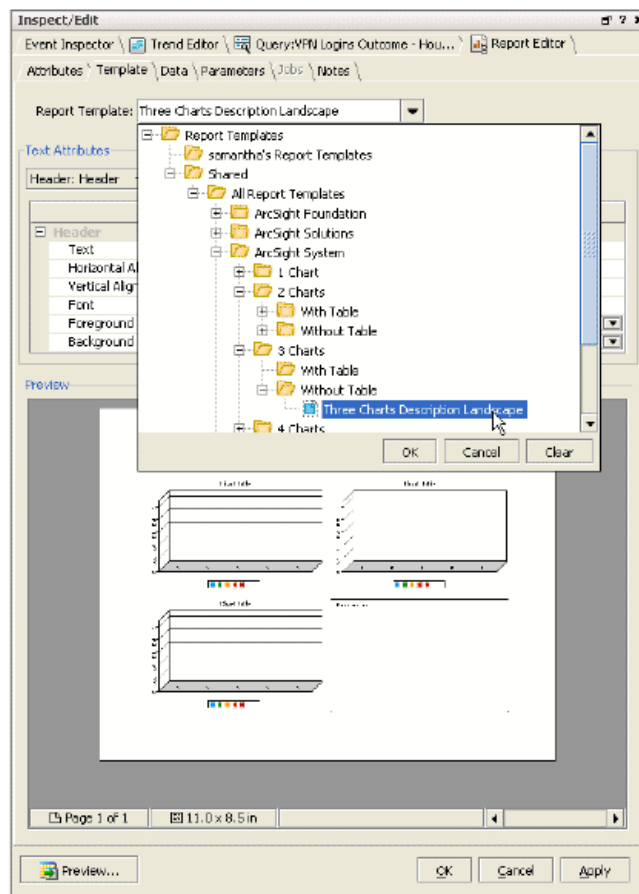
You can leverage multiple data sources in your report. For this example, you can use all three of the VPN Login trend-based queries you just built to create a report.

On the **Reports** tab, create a new report in your user folder and name it **VPN Login Outcome Trend**.

Choose a Template and Bind it to Result Data

A Template defines the visual constructs of a report such as layout, portrait or landscape, number of tables, number and types of charts, placeholders for text areas, and so on. You can find the ArcSight provided templates under **Report Templates/Shared/All Report Templates/Arcsight System/**.

In the Editor (Inspect/Edit panel) for your new report, click the **Template** tab and select the **Three Charts Description Landscape** to use as the Report Template. (Look in the drop-down tree under 3 charts/Without Table/ to find this template). In the preview panel you can see what the report template looks like. Double-click the template preview to open it in the viewer. Here you can see what the report looks like before adding the data.



On the Reports **Data** tab, you can bind each of the three charts in the template to each of the VPN login "trend" queries. (The data source type for each of these charts is a query, but remember that each of the queries uses a trend as its data source, which, in turn, was built on our original query.)

Chart	Description
Chart 1	<p>On the Report Data Chart 1 tab, select Login Outcome Trend Query - Attempt as the Data Source for the first chart. This query returns the number of login attempts over the last hour.</p> <p>On the X-Axis (horizontal) tab, add the Hour value to the Selected Columns. We'll show the Hour value on the X axis of the chart.</p> <p>On the Y-Axis (vertical) tab, place the Number of Logins (Category Outcome with "Count" applied to it) in Selected Columns. This shows on the Y axis of the chart.</p> <p>For Chart Type select a line chart.</p>
Chart 2	<p>On the Report Data Chart 2 tab, select Login Outcome Trend Query - Failure as the data source for the second chart. This query returns the number of failed logins per hour.</p> <p>Configure this chart also to show the Hour value on the X (horizontal) axis, and the number of failed logins on the Y (vertical) axis.</p>
Chart 3	<p>On the Report Data Chart 3 tab, select Login Outcome Trend Query - Success as the data source for the third chart. This Query returns the number of successful logins per hour.</p> <p>Specify the same assignments as the other charts for X and Y axis.</p>



At this point since you have selected some data for the report, you can click **Apply** to create the new Report and then continue working. It is a good idea to save frequently.

Using Custom Parameters

On the Report **Parameters** tab, you can view all the common parameters for the report (in Report parameters area), and all the parameters required for each chart (in Query Parameters area).

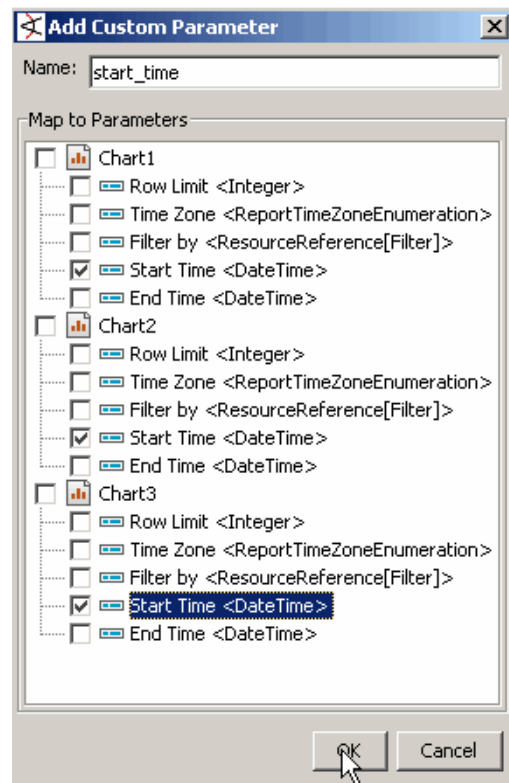
You can also provide Custom parameters. You can use Custom parameters to tie together similar parameters from multiple queries for one consistent value. For example, we could do this with Start Time and End Time.

Use Custom Parameters to tie together similar parameters (like Start Time and End Time) from multiple queries for one consistent value.

Query Parameters			
	Name	Value	Use Default
Chart3	Time Zone	Manager Time Zone	<input type="checkbox"/>
	Row Limit	25	<input checked="" type="checkbox"/>
	Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
	End Time	\$Now	<input checked="" type="checkbox"/>
Chart2	Time Zone	Manager Time Zone	<input type="checkbox"/>
	Row Limit	25	<input checked="" type="checkbox"/>
	Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
	End Time	\$Now	<input checked="" type="checkbox"/>
Chart1	Time Zone	Manager Time Zone	<input type="checkbox"/>
	Row Limit	25	<input checked="" type="checkbox"/>
	Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
	End Time	\$Now	<input checked="" type="checkbox"/>

Create a new Custom parameter called "start_time".

Click the **Add** button on the **Parameters** tab, and create a new parameter called start_time to prompt for Start Time field values. Map it to "Start Time" for all three charts (Chart 1, Chart 2, and Chart 3).



The custom parameter is added to the list of report parameters under Custom Parameters.

Similarly, add an End Time by adding a new parameter called "end_time" and map it to End Time for all three charts.

On the Parameters tab under Custom Parameters, use the drop down menus to choose the following values for your new parameters:

- Set **start_time** to \$Now-1d
- Set **end_time** to \$Now

Inspect/Edit

Event Inspector | Report:VPN Login Outcome Trend

Attributes | Template | Data | **Parameters** | Jobs | Notes

Report Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input type="checkbox"/>
Run as User	Select a User	<input type="checkbox"/>
Email to		<input type="checkbox"/>
Email Format	Send URL	<input type="checkbox"/>
Custom Parameters		
start_time	\$Now - 1d	<input type="checkbox"/>
end_time	\$Now	<input type="checkbox"/>

+ Add... | Edit... | Remove

Query Parameters

Name	Value	Use Default
Chart3		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart2		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>
Start Time	\$Now - 1d	<input checked="" type="checkbox"/>
End Time	\$Now	<input checked="" type="checkbox"/>
Chart1		
Time Zone	Manager Time Zone	<input type="checkbox"/>
Row Limit	25	<input checked="" type="checkbox"/>

Preview... | OK | Cancel | Apply | Help

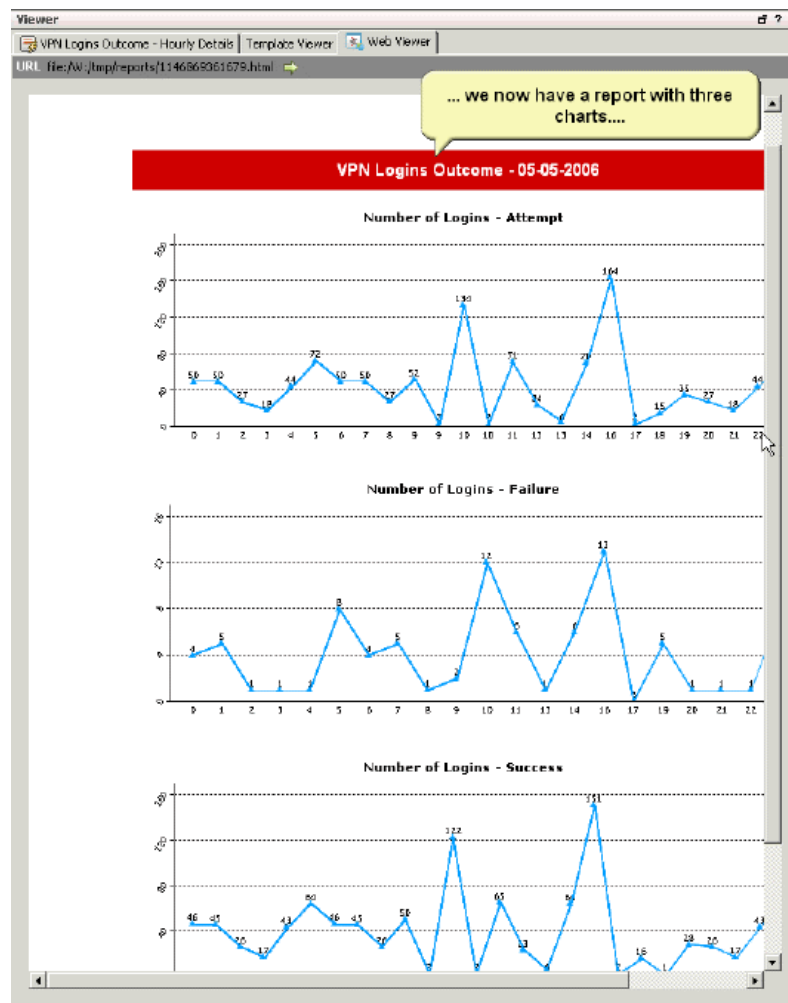
Click **Apply** or **OK** in the Report Editor to save the new report.

5. Run the Report

To run the report, select the VPN Login Outcome Trend report in the Navigator panel and choose **Run > Report with defaults** from the right-click menu to run and view the report.

In the Web Viewer we now have a report with three charts each showing a different slice of the data:

- Number of login attempts
- Number of failed logins
- Number of successful logins



Running and Managing Reports

This topic describes how run and manage various types of reports. Information is included on working with ad hoc reports, archived reports, focused reports, delta reports, and scheduled reports. The topic on Running Reports includes detail on setting report parameters at run-time. Also included is information on how to import and export reports, and work with report groups.

[“Running Reports” on page 423](#)

[“Managing Reports” on page 428](#)

[“Archiving and Scheduling Reports” on page 431](#)

Running Reports

Defined reports are usually run on a schedule and their output archived automatically. But there are also many occasions when you need to run the basic report types directly.

See also [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools, including how to develop new reports, queries, or trends using a provided or custom template.



Tips:

- No more than 5 reports can be run at the same time. The number of reports allowed to run simultaneously is a configurable parameter on the Manager in [ARCSIGHT_HOME/config/server.properties](#).
- If you are having problems running a large or complex report, refer to the topic [“Setting Special Parameters for Running Large or Complex Reports” on page 404](#).
- If you are having problems running PDF reports with Asian fonts, see the topic [“Setup and Parameters to Generate PDF Reports with Asian Fonts” on page 406](#).

Running a New or Archived Report

When you run reports, you most often use an existing report definition, or a copy of a report already defined, run, and archived for later use. Defining new reports is a separate

topic described in [Creating a Report](#). Please see also [“Archiving a Report” on page 431](#) and [“Scheduling Report Tasks” on page 433](#).



Tip

If you are having problems running a large or complex report, refer to the topic [“Setting Special Parameters for Running Large or Complex Reports” on page 404](#).

If you are having problems running PDF reports with Asian fonts, see the topic [“Setup and Parameters to Generate PDF Reports with Asian Fonts” on page 406](#).

Running a Defined Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 Click the **Reports** tab.
- 3 Navigate the Reports tree, and select the report you want to run.
- 4 Right-click the selected report to bring up the Context menu, and select **Run** with one of the report-type options described in [Run-Report Options](#) below.

Name	Value
Common Parameters	
Report Format	pdf
Page Size	Letter [8.5x11 in]
Email to	
Email Format	Send URL
Email Subject	\${ReportName}
Row Limit	25

Name	Value
Output Parameters	
Archive Report Folder	Select a Archived Report Group
Archive Report Name	\${Today}/\${ReportName}_\${Now}
Archive Report Expiration Time	\$Now+6M

☒ Save Output

OK Cancel Help

- 5 Select **Save Output** if you want to save a copy of the report to disk.

If this option is selected, additional archive parameters are displayed. You can override any of these defaults also. You can select a group in which to archive the report, provide a report name, and specify an expiration time at which to discard the report from the archive. By default, the report is saved in the archive for 6 months from the time it was run.



Tip

You can use Velocity template references for fields that accept text, such as Archive Report Name and Archive Report Expiration Time. See [“Velocity References for Reports” on page 1023](#) for details.

- 6 In the Report Parameters dialog box, enter new parameters if available and appropriate.

- 7 Click **OK**.
- 8 In the options dialog box click **Open** to open the report, **Save** to choose a location and format for the output file, or **Cancel** to quit. The Save option applies to all but HTML files.

Run-Report Options

To run a report, right-click a report in the Navigation panel, select **Run** from the Context menu, and choose one of these report-type options.

Report Type	Description
Report	Run the report, but with the opportunity to edit its current parameters (if present). If you choose this option, the Report Parameters dialog is displayed before the report is run. You can override the default report parameters for just this run of the report.
Report with defaults	Run the report directly, using its defined parameters, if present. For focused reports, this is the only option.
Report with selected event	Run the report using as parameters the fields of an event selected in a Viewer panel grid view.
Delta report	For reports based on bar charts, run the report after selecting another report as the comparison for the delta.

Report Parameters

You can override the following default report parameters at the time you run a report. Other parameters are set when the report was created (as described in Report Parameters in [“Creating Reports” on page 385](#)).

Parameter	Use
Report format	<p>The format in which to generate the report. Note that HTML output now appears in the Web Viewer tabs of the Viewer panel rather than in a browser client. Further, RTF appears by default in Word documents, XLS in Excel worksheets, CSV in Excel worksheets, and PDF in browser windows. Please note that the CSV-Plain format intentionally has fewer report header lines.</p> <p>Notes:</p> <ul style="list-style-type: none"> • CSV Report Format. Reports generated in CSV format are not the full equivalent of exports to other formats like PDF or HTML. CSV format is useful for loading report data into a spreadsheet for further manipulation. Since CSV is meant to contain tabular data, only the table data of a report is normally useful. Therefore, ArcSight exports only the table data portion of a report to CSV format, ignoring any other report information such as charts or text, including report titles. • XLS Report Format. XLS reports run with <i>Microsoft Excel 2002</i> might have page break format problems (misalignments, column spillover) due to default page size settings in Excel. To correct this problem, open the resulting XLS report in Excel, choose File -> Page Setup from the menus, change the paper size to Letter (instead of Legal), and click OK to save your changes. The report will have the appropriate page break formatting. <i>This problem does not occur in newer versions of Microsoft Excel.</i> <p>If your chart type is set to speedometer, the XLS report form displays the speedometer as a pie chart.</p>

Parameter	Use
Page size	Choose one of the available standard page sizes for the report.
Run as User	Optionally choose an existing ArcSight user's identity as a report constraint. The user identity can serve as a type of filter on the report's output, or it may be desirable to run a report on behalf of a user, as in a provider/customer (MSSP) circumstance. This capability is sometimes called "impersonation."
E-mail to	One or more e-mail addresses to send notifications to when the report runs. Separate multiple addresses with commas.
Email Format	<p>Specify whether to e-mail a link (URL) to the report or send it directly as an e-mail attachment.</p> <ul style="list-style-type: none">• If the report is large and is saved (archived) to a network-accessible location, you may want to select Send URL to point users to the report.• If you want to send the report directly to the user's e-mail box, select Attach Report.

Displaying an Archived Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 On the **Archives** tab, right-click a report and choose **Show Archive Report**.

Running a Delta Report

Delta reports show the difference between two sets of parameters, within a single comparative report. Defining new reports is a separate topic described in [Creating a Report](#). In order to run a delta report, you must have an existing report first. You can also set up a delta report to run and archive on a schedule. Please see also ["Archiving and Scheduling Reports" on page 431](#) and ["Scheduling Report Tasks" on page 433](#) for more information.

- 1 From the Navigator panel drop-down menu, select the **Reports** resource.
- 2 On the **Reports** tab, right-click a report and choose **Run**, then **Delta Report**.



The **Run Delta Reports** option is available only for reports with a bar, 3D bar, or inverted bar chart. The report must contain one chart only (no tables). The X and Y axis must have at least one column each, and no Z-axis. The chart must not have any summary function or top N filter applied. For more information about creating reports with these characteristics, see the ["Report Data" on page 391](#) section (under ["Creating Reports" on page 385](#)).

- 3 Select the parameters for the first report, select a report format from the drop-down menu, and click **OK**.
- 4 Select the parameters for the second report and click **OK**.
- 5 Select **Save Output** if you want to save a copy of the report to disk.

If this option is selected, additional archive parameters are displayed. You can override any of these defaults also. You can select a group in which to archive the report, provide a report name, and specify an expiration time at which to discard the report

from the archive. By default, the report is saved in the archive for 6 months from the time it was run.



You can use Velocity template references for fields that accept text, such as Archive Report Name and Archive Report Expiration Time. See [“Velocity References for Reports” on page 1023](#) for details.

The Report Viewer appears and displays the delta report. The report shows the difference between two sets of parameters used on a single report. The report also shows the data for each of the parameters.

When a delta report is run or archived, an internal event is sent to the ArcSight Manager. This event contains the following data fields and values:

Delta Report Event-data Field	Description
Event Name	Delta Report Generated (Report: <ReportName>), where <ReportName> is the name of the report.


Rules can be created using the delta report data fields.

Running Reports from a Grid View

You can define reports on-the-fly based on specific events in grid views in the Viewer panel.

Running a Rule-Context Report from a Grid View

- 1 In a grid view, select a correlation event.
- 2 Right-click it and choose **Report > Rule Context Report**.
- 3 In the **Report Parameters** dialog box, enter the time, in minutes, before and after this event's occurrence and click **OK**.
- 4 You can choose to Open or Save the report file.

In the grid view, a correlation event is marked with a **Flash** icon (). A report showing the correlation event and the events that triggered the rule appear.

Running an Event Context Report from a Grid View

- 1 In a grid view, select an event.
- 2 Right-click and choose **Report > Event Context Report**.
- 3 In the **Report Parameters** dialog box, enter the time, in minutes, before and after this event's occurrence and click **OK**.
- 4 You can choose to Open or Save the report file.

The report shows the events that occurred, within the specified time before and after this event appears.

Running a Channel Report from a Grid View

- 1 In a grid view, select an event.
- 2 Right-click and choose **Report > Channel Report**.

- 3 The Report Parameters dialog is displayed, and its fields are automatically populated with the event data fields. You can enter new parameters to limit or extend the report.
- 4 Choose a Report File Format from the drop-down menu.
- 5 Click **OK**.
- 6 You can choose to Open or Save the report file.



The channel report exports all of the events in the channel into a report. A channel report refers to the whole channel, not the selected event. However, you do need to select an event in the grid view in order to "select" the channel and get the Report > Channel Report menu option.

Managing Reports

Managing reports includes editing existing reports, importing/exporting, and organizing reports into groups.

Editing a Report

Over time, reports often need to be adjusted to keep them appropriate and useful. For more information, see ["Creating Reports" on page 385](#).

- 1 Navigate to **Reports** in the Navigator panel, select the **Report** sub-tab, and select the report you want to modify.
- 2 Double-click the report, or right-click and select **Edit Report** from the context menu. This launches the Report Editor in the Inspect/Edit panel, and shows the definition for the selected report.
- 3 Edit the report definition as needed and click **Apply** or **OK** to save your changes. (Click **Cancel** to exit the Query editor without saving changes.)

Creating Focused Reports

In addition to using the reports already available in the Navigator panel's Reports resource tree, you can easily make and save refinements to these definitions. These more narrowly defined or focused reports are also stored in the resource tree, so other people can also use them.

Focused reports are identical to other reports. They differ only in being useful variations on already defined reports. You create focused reports when you want to make a special variation available to other ArcSight users through the Reports resource tree.

Creating a Focused Report

- 1 In the Navigator panel, choose the **Reports** resource tree.
- 2 On the **Reports** tab, right-click a report and choose **New Focused Report**.
- 3 In the Focused Report Editor, select the **Attributes** tab and name the report. Name focused reports in a fashion that properly distinguishes them from their originals.

- 4 Click the **Parameters** tab and change any of the values as appropriate. These values are the same ones you set when Running a New or Archived Report.



Tip

You can use Velocity template references for parameter fields that accept text, as described in [“Velocity References for Reports” on page 1023](#).

- 5 Click **Apply** to make changes and keep the editor open. Click **OK** to store the definition in the resource tree in the same folder as the original report and close the editor.



Note

A focused report reflects changes made to the report on which it is based.

Importing and Exporting Reports



Caution

To import and export reports, use the packages feature. Since the reporting capabilities involve using queries, trends, and templates as a part of building reports, the import/export tool must track and manage dependencies across resources. Packages gives you this capability. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. Please see the information on packages in [“Managing Packages” on page 686](#).

You can import or export reports by following these procedures.

Importing Reports

- 1 In the **Reports** resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report group where you want the imported report to be placed and select **Import Report**.
- 3 In the window, select a file to import to the report group.
- 4 Click **Open**.

Exporting Reports

- 1 In the Reports resource tree, select the **Report** tab.
- 2 On the Reports tab, right-click a report and select **Export Report**.
- 3 In the window, select the directory to save the report.
- 4 Click **Save**.

Moving or Copying a Report

You may need to move or duplicate report definitions to better organize your work, to publish your definitions, or to make editable copies of enterprise reports.

- 1 In the Reports resource tree, navigate to a report and drag and drop it into another group.

- 2 Select **Move** to move the report, **Copy** to make a separate copy of the report, or **Link** to create a copy of the report that is linked to the original report.

If you select **Copy**, you create a separate copy of the report that is not affected when the original report is edited. If you select **Link**, you create a copy of the report that is linked to the original report. Therefore, if you edit a linked report, whether it be the original or the copy, all links are edited as well. When deleting linked reports, you can either delete the selected report or all linked report copies.

Managing Report Groups

Report groups store similar reports, and control access to reports, using access control lists (ACLs). When editing access control permissions, permissions given to a report group are also given to all groups and reports within that group.

Groups and reports can be managed with drag and drop functionality. You can move or copy groups and reports into other groups from the Reports resource tree. If a group is deleted, the reports within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Report Group

- 1 On the **Navigator Panel** drop-down menu, select **Reports**.
- 2 In the Reports resource tree, right-click a group and select **New Group**.
- 3 Enter a report group name in the "name" text field.
- 4 Press **Enter**.

Renaming a Report Group

- 1 In the Reports resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing a Report Group

- 1 In the Reports resource tree, right-click a group and select **Edit Group**.
- 2 In the Report Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying a Report Group

- 1 In the Reports resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Report Group

- 1 In the Reports resource tree, right-click a group and select **Delete Group**.
- 2 Click **Yes** in the dialog box.

Archiving and Scheduling Reports

You can schedule reports to archive automatically with the scheduler. The scheduler accepts multiple schedules by year, month, week, day, or hour. For example, a report can be archived automatically on the first of January at both 5 AM and 6 PM. The scheduler also sends e-mail notifications informing users when a scheduled report has been archived. Report Archiving is a component of ArcSight Reporting resource tools. Be sure to see [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools.

Archiving a Report

To archive a report:

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report and select **Schedule for Archiving > Report**. (This opens the report definition in the Editor with the **Jobs** tab showing.)
- 3 Click **Add** on the Jobs tab, and choose either **Schedule Report** or **Schedule Delta Report**.



The option to **Schedule a Delta Report** job is available only for certain types of event-based reports, and only when a previously-run report is available in the archives. Otherwise, clicking Add on the **Jobs** tab takes you directly to the job scheduler to schedule a standard report. For more information about Delta reports, see ["Running a Delta Report" on page 426](#).

- 4 Enter a name and description for the job.
- 5 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency** to get the Job Frequency dialog, and configure the schedule.

The Job Frequency dialog box is used to configure the schedule for a report job. It contains the following sections and controls:

- Schedule Frequency:** A group box containing radio buttons for **Hourly**, **Daily**, **Weekly**, **Monthly**, and **Yearly**. The **Hourly** option is selected. To the right of the radio buttons is a text field labeled "Every" followed by a spinner box containing the number "1", then "hour(s) at" followed by a spinner box containing the number "0", and finally "minutes after".
- Schedule Range:** A group box containing:
 - Start:** A text field with the value "8 Dec 2008 15:40:10 PST" and a dropdown arrow.
 - End:** A group box with two radio buttons: **No End date** (selected) and **End on**. The **End on** option has a text field with the value "8 Dec 2008 15:40:10 PST" and a dropdown arrow.
- Buttons:** At the bottom of the dialog are three buttons: **OK**, **Cancel**, and **Help**.

In the Job Parameters section, select or enter values for the parameter fields as necessary. For date parameters, enter values in the text fields, click the drop-down arrows or click the time buttons to select a time range. For time data, you can enter a specific value, such as 8:54:00 AM or you can use special timestamp variables.

Click **OK** to save changes to the Job schedule.

To view all scheduled jobs, click the **Open scheduled jobs list** tool button (🕒). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

For more information on setting up and viewing scheduled jobs, see ["Scheduling Jobs" on page 977](#).

- 6 Back in the report editor Jobs tab, under the **Job Parameters** section, enter values for the report parameters by clicking off the "Use Default" check marks, or change nothing here to keep the defaults. You can set the report format, e-mail options, output parameters, start and end times, and so on. These are the same parameters described in ["Report Parameters" on page 425](#).

Inspect/Edit

Report: Top 10 Events

Attributes Template Data Parameters **Jobs** Notes

+ Add ✕ Remove ↺ Frequency

Jobs	Description
Top 10 Events	Top 10 Events archive report

Next Run Time **8 Dec 2008 15:00:00 PST**

Job Parameters

Name	Value	Use Default
Common Parameters		
Report Format	html	<input checked="" type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input checked="" type="checkbox"/>
Run as User	Select a User	<input checked="" type="checkbox"/>
Email to		<input checked="" type="checkbox"/>
Email Format	Send URL	<input checked="" type="checkbox"/>
Email Subject	ReportName	<input checked="" type="checkbox"/>
Output Parameters		
Archive Report Folder	Select a Archived Report G...	<input checked="" type="checkbox"/>
Archive Report Name	{Today}-{ReportName}...	<input checked="" type="checkbox"/>
Archive Report Expir...	Now+6M	<input checked="" type="checkbox"/>
Custom Parameters		
StartTime	Now - 1d	<input checked="" type="checkbox"/>
EndTime	Now	<input checked="" type="checkbox"/>
Subtitle		
Text		<input checked="" type="checkbox"/>
Chart		
Time Zone	Manager Time Zone	<input checked="" type="checkbox"/>
Filter by	Select a Filter	<input checked="" type="checkbox"/>
Row Limit	10	<input checked="" type="checkbox"/>
Start Time	Now - 1d	<input checked="" type="checkbox"/>
End Time	Now	<input checked="" type="checkbox"/>
Title		
Text	Top 10 Events	<input checked="" type="checkbox"/>
ChartTitle		
Text		<input checked="" type="checkbox"/>

Summary

Occurs **Hourly**.

Schedule will start on **8 Dec 2008 14:05:24 PST**.

Preview... OK Cancel Apply Help

- 7 Click **Apply** or **OK** on the report Editor to save your changes for this report.


Parameterized Report Entries

The top portion of the dialog may or may not exist, depending on whether you chose any parameterized conditions while creating the report. A typical example of a parameterized condition is: detect time between `$CurrentDate-1d` and `$CurrentDate`. If such parameters exist, they are used for both immediate as well as scheduled generation of reports. While scheduling reports for archiving, these parameters are displayed in the Edit Parameters dialog. It is possible to independently modify the dates specified in the parameter text fields. In addition to relative dates, absolute dates can be specified as parameter values. Examples of valid absolute dates are: `01/01/2001` and `01/01/2000 11:00:00 AM`.

Viewing an Archived Report

To view an archived report, select the **Reports** resource in the Navigator (if it is not already selected) and click the **Archives** tab. Navigate the Archived Reports tree to find the archived report you want, then right-click the report and choose **Show Archive Report**. The report is displayed in the Viewer.

If you do not find the report you are looking for, you might want to check to see if it has

run yet. To view all scheduled jobs, click the **Open scheduled jobs list** tool button (). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

Scheduling Report Tasks

You can schedule some tasks to occur automatically. Specifically, this feature is available for archiving reports individually or by group, for taking pattern discovery snapshots, and for scheduling rules. This topic discusses the scheduler as it relates to scheduling reports (For more information on job scheduler in general, see also ["Scheduling Jobs" on page 977](#).)

Scheduling Individual-Report Archiving

- 1 Choose the Reports resource tree in the Navigator panel, select the **Reports** tab, and right-click the report you want to schedule.
- 2 Choose **Schedule for archiving**, then **Report** or **Delta Report** for delta reports. (This opens the report with the Jobs tab showing.)

- 3 Click **Add** on the Jobs tab.

The screenshot shows the 'Inspect/Edit' dialog box for a report job. The 'Jobs' tab is selected. The 'Jobs' table is empty with headers 'Jobs' and 'Description'. Below it is the 'Job Parameters' section with 'Common Parameters' and 'Output Parameters' groups. At the bottom is a 'Summary' section with a link 'Click here to set up schedule frequency'.

Jobs	Description
Please Enter a Name	Please Enter a Description

Next Run Time --

Job Parameters

Name	Value	Use Default
Common Parameters		
Report Format	pdf	<input checked="" type="checkbox"/>
Page Size	Letter [8.5x11 in]	<input checked="" type="checkbox"/>
Run as User	Select a User	<input checked="" type="checkbox"/>
Email to		<input checked="" type="checkbox"/>
Email Format	Send URL	<input checked="" type="checkbox"/>
Output Parameters		
Archive Report Fol...	Select a Archived Report ...	<input checked="" type="checkbox"/>
Archive Report Name	\${Today}}\${ReportName...	<input checked="" type="checkbox"/>

Summary

[Click here to set up schedule frequency](#)

Preview... OK Cancel Apply Help

- 4 Enter a name and description for the job.
- 5 In the Job Parameters section, select or enter values for the parameter fields as necessary.
- 6 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency**.
- 7 Click the schedule-building buttons in sequence from left to right, as appropriate according to the definitions below, providing specific timing information.
- 8 Repeat Step 3 to add another schedule for the same group.
- 9 Click **OK**.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and appear differently. In addition, Excel format is more memory-intensive than PDF.

- 10 Select the **e-mail scheduled reports to** checkbox and a user from the drop-down menu to automatically send an e-mail notification when the report is archived.

The user receives an e-mail notification stating that the report has been successfully archived. The e-mail also contains a URL to the report so that the user can view the report from the URL. The e-mail notification is sent to the e-mail address listed in the user's profile. The user must have an e-mail address in their user profile.

- 11 For the **Archive Folder** text field, click the archive report group button to select where to list the archived report.
- 12 In the Archive Report Selector, select a report archive group and click **OK**.
- 13 In the Report Parameters window, click **Update**.
- 14 For delta reports, in the Schedule Summary, right-click **Default** under the **Param Set 2** column and select **Edit Parameters** to change the second parameter set, if any. Click **Update**.
- 15 In the Schedule Summary, click **Close**.



You can use Velocity template references for fields that accept text, such as Archive Folder and Archive Report Selector. See [“Velocity References for Reports” on page 1023](#) for details.

Scheduling Report Archiving by Resource Group

- 1 In the Reports resource tree, navigate to a particular group.
- 2 Right-click the group and choose **Schedule for archiving>Report group**. (This opens the report with the **Jobs** tab showing.)
- 3 Click **Add** on the **Jobs** tab.
- 4 Enter a name and description for the job.
- 5 In the Job Parameters section, select or enter values for the parameter fields as necessary.
- 6 In the Jobs scheduler, click the link labeled **Click here to set up schedule frequency**.
- 7 Click the schedule-building buttons in sequence from left to right, as appropriate according to the definitions below, providing specific timing information.
- 8 Click **OK**.
- 9 Repeat Step 3 to add another schedule for the same group.

The following table shows Group Scheduling Buttons

Button	Usage
Type	Choose a timing scope for the archiving schedule. The typical choices are self-explanatory: hourly, daily, weekly, monthly, and yearly.
Month	For schedules that are yearly in scope, choose a month.
Date	For schedules that are yearly or monthly in scope, choose a date.
Day	For schedules that are weekly in scope, choose a day of the week.
Hour	For schedules that are daily or larger in scope, choose an hour of the day.
Min	For schedules that specify hours, optionally set the minute as well.
AM	Toggle between AM and PM for hourly schedules.

Standard Time Transitions

If the trigger time for a particular scheduled task run happens to fall during the transition time from daylight savings time (DST) to standard time (ST) or vice versa, the interval for that particular run will not be the expected interval.

Time zones that honor DST have a period of time that occurs twice during the transition from DST to ST. For example, in the US when changing from DST to ST, this hour occurs once while the DST is still in effect and again after switching to the Standard Time. The transition period occurs at 2 am, therefore 1:00:00 am - 1:59:59 am occurs twice (1:00:00 am PDT - 1:59:59 am PDT and 1:00:00 am PST - 1:59:59 am PST), where 1:00 am PST is 60 minutes after 1:00 am PDT. In this example, if the scheduled task is due to trigger any time between 1:00:00 am - 1:59:59 am, the interval for that particular run of the scheduled task will not be as expected.

Similarly, when the time changes from ST to DST, the 1:00:00 am - 1:59:59 am hour does not occur at all. The local time changes directly from 12:00 am to 2:00 am. So, if your scheduled task run was scheduled to trigger between 1:00:00 am - 1:59:59 am, the interval for that particular run will be off by an hour.

The interval calculation for subsequent scheduled runs do not get affected.

Currently, there are four time zones that are not supported in ESM:

- Kwajalein
- Pacific/Kwajalein
- Pacific/Enderbury
- Pacific/Kiribati

These time zones fall in two countries, Marshall Islands and Kiribati.

Editing a Report Archiving Schedule

You can change the archiving schedule for report definitions in your Reports resource folders.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Reports tab, right-click a report and select **Schedule for archiving**, then **Report** or **Delta Report** for delta reports.
- 3 In the Schedule Summary, right-click in the braces { } column and select the **Parameters** option to change report parameters set for the specific scheduled report. To delete a current scheduled archive report, right-click in the braces { } column of an existing schedule and click **Delete**.
- 4 To change the interval scheduling of a report, click the report interval button and **Yearly**, **Monthly**, **Weekly**, **Daily**, or **Hourly**, click the date and time buttons.
- 5 If editing within the same time frame, click the **Month**, **Date**, **Day**, **Hour**, **Min**, **AM/PM** buttons to specify changes to the report schedule.
- 6 When you've finished editing the schedule, click **OK**.

Editing Report Archiving Parameters

You can change the archiving parameters of the report definitions in your Reports resource folders.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Report Definitions tab, right-click a report and select **Schedule for archiving**, then **Report** or **Delta Report**.
- 3 Right-click in the braces { } column for a scheduled report and select the **Parameters** option.
- 4 In the Report Parameters window, type in the report parameter text fields, if any.

For date and time data fields, such as Detect Time, you can type an actual date value, such as 10/12/2002 8:54:00 AM, or you can use special timestamp variables.
- 5 Select the **E-mail scheduled reports to** checkbox, and a user from the drop-down menu, to automatically send an e-mail notification when the report is generated.

The user receives an e-mail notification stating that the report has been successfully archived. The e-mail also contains a URL to the report so that the user can view the report from the URL.

The e-mail notification is sent to the e-mail address listed in the user's profile. The recipient must have an e-mail address in their user profile.
- 6 For the Archive Folder text field, click the archive report group button to select where to list the archived report.
- 7 In the Archive Report Selector, select a report archive group and click **OK**.
- 8 In the Report Parameters window, click **Update**.
- 9 For delta reports, in the Schedule Summary, right-click **Default** under the **Param Set 2** column and select **Edit Parameters** to change the second parameter set, if any. Click **Update**.
- 10 In the Schedule Summary, click **Close**.

Deleting a Report Archiving Schedule

You can remove individual archiving schedules for reports in the Scheduled Tasks list.

- 1 In the Reports resource tree, select the **Reports** tab.
- 2 On the Report Definitions tab, right-click a scheduled report (showing a calendar icon) and choose **Schedule for archiving**, then **Report** or **Delta Report**.
- 3 On the line for the schedule to remove, right-click in the braces { } column and choose **Delete**.
- 4 In the confirmation dialog box, click **Delete** to remove it or **Cancel** to let it remain.

Chapter 16

Rules Authoring

This section explains how to use rules to correlate events in your environment.

["Designing Rules" on page 439](#)
["Managing Rules" on page 440](#)
["Managing Rule Groups" on page 441](#)
["Specifying Rule Conditions" on page 442](#)
["Specifying Rule Thresholds and Aggregation" on page 449](#)
["Creating Rule Actions" on page 451](#)
["Applying Rule Actions" on page 460](#)
["Enabling and Disabling Rules" on page 461](#)
["Importing and Exporting Rules" on page 463](#)
["Scheduling Rules" on page 463](#)
["Verifying Rule\(s\) with Events" on page 470](#)
["Deploying Real-time Rules" on page 473](#)
["Loading Rules" on page 474](#)

Designing Rules



Creating rules involves defining the events the rule evaluates, thresholds, and actions you want the rule to trigger. Conditions define which events trigger the rule, thresholds determine when a condition is met and a correlation event is generated, and actions state what responses are taken when a correlation event is generated. To define rule events and conditions, thresholds, and actions, begin by determining:

- Which event occurrences do I want to be aware of? This determines the rule's **events** and **conditions**.
- How many times do I want the event or events to occur and within what time frame? This determines the rule's **threshold**.
- What actions should automatically occur when an event is generated? When should those actions occur? This determines the rule's **actions**.

Before you create rules, determine which events you want to monitor. Be specific and as clear as possible. For example, monitoring all events from a Cisco Router would not be as useful as monitoring all denied events from that Cisco Router. In addition, the more conditions you add to a rule, the more specific the rule becomes. Use the ArcSight data

fields to guide you in selecting and specifying conditions. For more information, see [“Data Fields” on page 867](#).

Managing Rules

Like other resources, the rule-management tasks include creating, changing, deleting, and placing them.

Creating Rules

Before creating rules, determine which events you want to monitor. Be as specific and as clear as possible. For example, monitoring all events from a Cisco Router would not be as useful as monitoring all **denied** events from that Cisco Router. In addition, the more conditions you add to a rule, the more specific the rule becomes.

Use the ArcSight data fields to guide you in selecting and specifying conditions.

To create a rule:

- 1 From the Navigator Panel drop-down menu, select **Rules**.
- 2 Right-click a group and select **New Rule**.
- 3 On the General tab, type a name in the **Rule Name** text field.

The Rule Name text field is required and restricted to 25 characters. The Rule Name should be as descriptive as possible. It is stored in the Event Name data field and if the rule has a Send to Console action, the Rule Name appears in the Event Name column of the grid view.

- 4 Type a description in the **Description** text field.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

- 5 Define conditions on the **Conditions** tab following instructions See [“Specifying Rule Conditions” on page 442](#).
- 6 Add correlating events, specify thresholds and time windows to qualify events, and aggregate incoming event data based on matching fields on the **Aggregation** tab. See [“Common Conditions Editor \(CCE\)” on page 846](#), and [“Specifying Rule Thresholds and Aggregation” on page 449](#) for more information.
- 7 Click **OK** to save and close the rule. You can also click **Apply** to save changes but keep the rule open.

Editing Rules

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **General** tab to edit the rule name and description.
- 3 Select the **Conditions** tab to edit events, logical operators, and condition statements as described in Common Condition Editor.
- 4 After editing the conditions and other elements of the rule, click **OK** to save and close the rule. You can also click **Apply** to save changes but keep the rule open.

Moving or Copying Rules

- 1 In the **Rules** view, navigate to a rule and drag and drop it into another group.
- 2 Select **Move** to move the rule, **Copy** to make a separate copy of the rule, or **Link** to create a copy of the rule that is linked to the original rule.

If you select **Copy**, you create a separate copy of the rule that is not affected when the original rule is edited. If you select **Link**, you create a copy of the rule that is linked to the original rule. Therefore, if you edit a linked rule, whether it be the original or the copy, all links are edited as well. When deleting linked rules, you can either delete the selected rule or all linked rule copies.

Deleting Rules

- 1 In the **Rules** resource tree of the Navigator panel, right-click a rule and choose **Delete Rule**.
- 2 Click **Yes** in the confirmation dialog box.

Managing Rule Groups

Rule groups are created to store similar groups or rules in a single location. Groups can be created within groups to meet enterprise needs.

Groups and rules can be managed with drag and drop functionality. You can move or copy groups and rules into other groups from the Navigator panel's Rules resource tree. If a group is deleted, the rules within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating Rule Groups

- 1 In the Navigator panel's drop-down menu, choose **Rules**.
- 2 In the Rules resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 Type a name in the "name" text field.
- 4 Press **Enter**.

Renaming Rule Groups

- 1 In the Rules resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing Rule Groups

- 1 In the Rules resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.

- 3 Optionally, you can designate owners of a rule, and specify user groups that are notified of rules changes.
- 4 Click **OK**.

Moving or Copying Rule Groups

- 1 In the **Rules** resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting Rule Groups

- 1 In the **Rules** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Specifying Rule Conditions

After creating a new rule or opening an existing rule for editing, you can specify conditions on which a rule triggers, based on specific event, filter, asset, or vulnerability criteria. Like other ArcSight analysis components, rules editing uses the [Common Conditions Editor \(CCE\)](#). See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under “[Common Conditions Editor \(CCE\)](#)” on page 846.

Creating New Rule Conditions

The Conditions tab provides a default event alias, **event1**, which you edit and to which you add condition statements for evaluation.

To specify rule conditions:

- 1 In the Rules Editor, select the **Conditions** tab.
- 2 To edit the event alias (give it a name), right-click **event1** and select **Edit**. Type a new name for the alias in the text field and click **OK**.

Since rules can have numerous events, aliases should be unique and descriptive. For example, if monitoring Cisco Router denied events, **Cisco Router denied** could be the alias name. The name appears as a branch under the **Event conditions** tree.

- 3 Add a condition statement to the event alias using the Common Conditions Editor table (usage rules and features of this editor are described in “[Common Conditions Editor \(CCE\)](#)” on page 846):
 - a Locate the event name you want to use as in the condition statement.
 - b Choose the logical operator (for example, =) to be used for comparing values. If you need help, see “[Logical Operators](#)” on page 947 for descriptions.

- c Choose the value from the drop-down list under the Condition column to use as the basis for comparison.



If you want to use a global variable for the condition statement, you can attach one by clicking the **+/- Global Variables** button and then choosing the global variable from the selector dialog. The selected global variable will be added to the Common Conditions Editor table at the bottom. See [“Global Variables” on page 943](#) for more information.

- 4 To add more event aliases, select **Event conditions** and click the **New Event Definition** button; or right-click **Event conditions** and choose **New Event Definition**. Type an event name in the **Alias** text field and click **OK**.

If you have more than one event alias, a **Matching Event** branch appears. This enables you to define a join relationship on the multiple event aliases. For more information on joining two events, see [“Creating Matching or Join Conditions” on page 447](#). Other important references are Logical Operators and Conditional Expressions.

- 5 On the Conditions tab, click **Apply**.

The rule with the default threshold and action is created and listed in the Rules resource tree.

See [“Specifying Rule Thresholds and Aggregation” on page 449](#) for aggregation time-frame options.

Adding Filter Conditions

You add filters to rules as new conditions. It is usually more desirable to use an existing filter resource, if possible.

If there are other conditions in the rule, you choose whether to tie them to the filter condition with AND, OR, or NOT logical operators. For more information on filters, see [Chapter 11, Filtering Events, on page 223](#).

To add a filter condition to a rule:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab and select the event alias to which you want to add a filter condition.
- 3 Click the **And**, **Or**, or **Not** button; or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.
- 4 Right-click the logical operator and select **New Matches Filter Condition**.
- 5 In the Filter Selector, select a filter and click **OK**.
- 6 On the Conditions tab, click **OK**.

The Common Condition Editor's buttons and commands are discussed further in [“Creating Filters” on page 223](#).

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under [“Common Conditions Editor \(CCE\)” on page 846](#).

Negating Event Conditions

Rather than specifying event conditions to monitor, you can specify which event conditions **not** to monitor by negating them. When event conditions are negated, all but the selected event conditions are monitored.



Prior to using the following procedures, make sure multiple event conditions exist so you can negate at least one. To create event conditions, see [“Creating Rules” on page 440](#).

To negate event conditions:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Right-click an event alias and select **Negated**.

On the Conditions tab, the negated event is preceded by an exclamation point (!) as in the following example.

! <EventName>

- 4 To remove the Negated flag, right-click the event and select **Negated** again.

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under [“Common Conditions Editor \(CCE\)” on page 846](#).

Adding Asset Conditions

Asset conditions state whether your enterprise assets are targets or sources of events. An asset condition states “if an event occurs and the selected asset is the source or target, generate a correlation event”. For more information on assets, see [Chapter 28, Modeling the Network, on page 731](#).

To add an asset condition to a rule:

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Click the **And**, **Or**, or **Not** button, or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.

If there are existing conditions, you can tie them to the asset condition with either the AND, OR, or NOT logic operator. If AND is used, all the existing conditions and the asset condition must occur in the event. If OR is used, either the existing conditions or the asset condition must occur. If NOT is used, all but the asset condition must occur.

- 4 Select the logical operator and click the Assets button or right-click the logical operator and select **New Assets Condition**.
- 5 In the Assets panel below, select **Source Asset ID** to monitor if an asset is the source of an event or **Target Asset ID** to monitor if an asset is the target.
- 6 Select an asset or group and click **Apply**.

The asset condition appears in the Correlate section and is tied to any existing condition statements with the logic operator selected.

- 7 On the Conditions tab, click **OK**.

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under “Common Conditions Editor (CCE)” on page 846.

Adding Vulnerability Conditions

You can use an existing enterprise vulnerability to create a rule condition. A vulnerability condition states “if an event occurs with the vulnerability selected, generate a correlation event”. For more information on vulnerabilities, see [Chapter 28, Modeling the Network](#), on page 731.

To add a vulnerability condition to a rule:

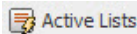
- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Click the **And**, **Or**, or **Not** button or right-click a logical operator and choose **New Logical Operator**, then **And**, **Or**, or **Not**.

If there are existing conditions, you can tie them to the vulnerability condition with either the AND, OR, or NOT logic operator. If AND is used, all the existing conditions and the vulnerability condition must occur in the event. If OR is used, either the existing conditions or the vulnerability condition must occur. If NOT is used, all but the vulnerability condition must occur.
- 4 Choose the logical operator and click the **Has Vulnerability** button or right-click the logical operator and choose **New Has Vulnerability**.
- 5 In the **Vulnerability Selector**, select a vulnerability and click **OK**.

The vulnerability appears on the Conditions tab and is tied to any existing condition statements with the logic operator selected.
- 6 On the Conditions tab, click **OK**.

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under “Common Conditions Editor (CCE)” on page 846.

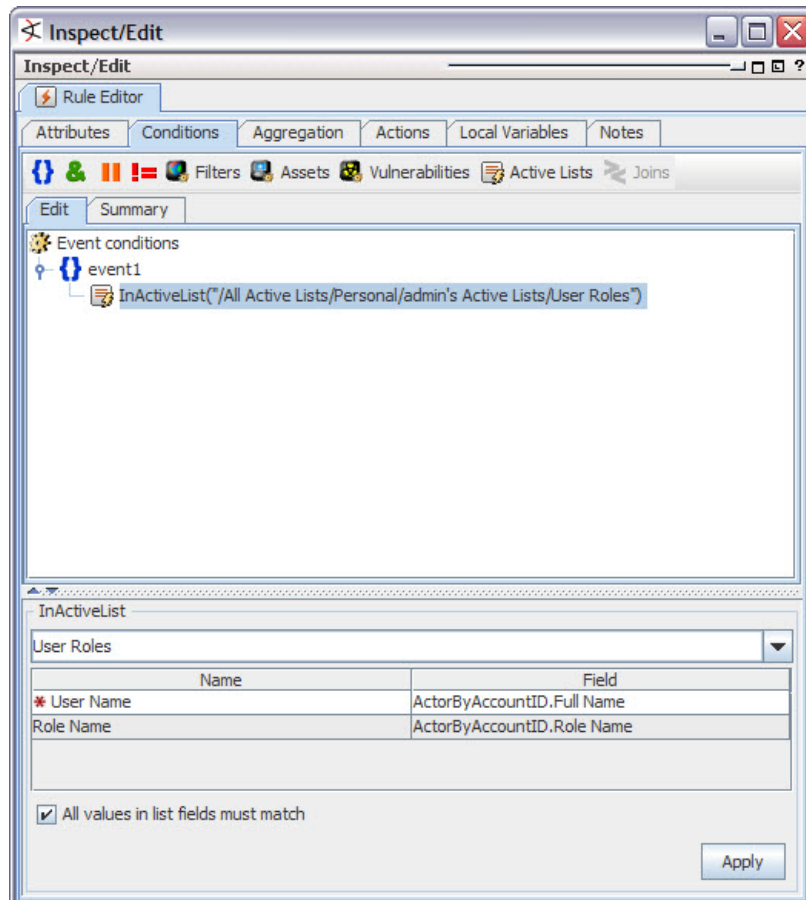
Adding Active List (InActiveList) Conditions

Use the Active List selector  to identify a particular active list that contains the argument for a condition. This condition evaluates whether an item or list of items is in an active list. You can use this to map a field or a global variable in the event schema to a corresponding field in an active list. It does not evaluate items in other non-event schemas (such as cases or assets).

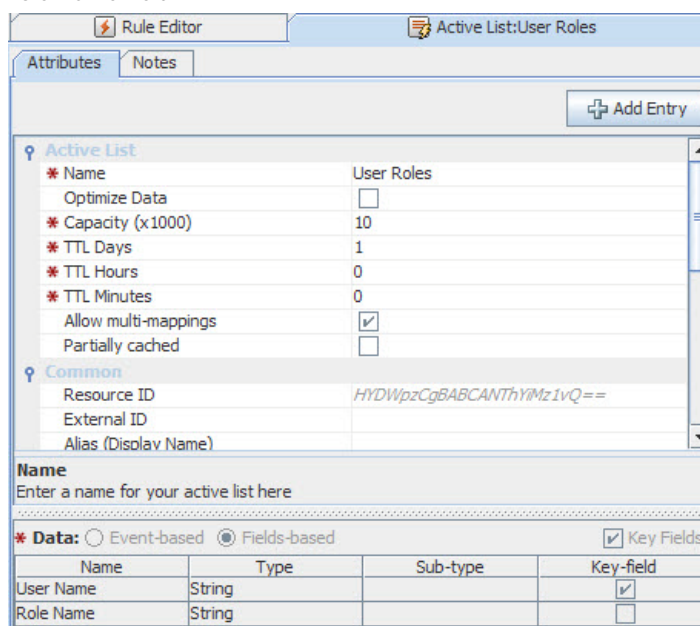
When the InActiveList condition is used to compare values in two lists, an additional option is shown where you can specify whether **All values in list field must match**.

- If “All values in list field must match” is checked (selected), the Active List condition evaluates to true only if all values in both lists match (i.e., all values must be in both lists for the condition to be true).

- If “All values in list field must match” is *not checked* (de-selected), then if any field matches (is in both lists), the condition statement evaluates to true. (This is the default behavior for queries.)



For example, suppose you have a fields-based multi-mapped active list that has User Name as a key field and accepts entries with multiple roles for the same user in the Role Name field.



Then suppose you set up an Active List (InActiveList) rule condition to compare the value of Role Name to a list type string field, like ActorByAccountID.FullName. If you then get list entries in your active list (e.g., user “Samantha Stevens” with roles as both “Administrator” and “Development Lead”), then your rule results in a comparison of two lists:

- ◆ The list of Samantha Steven’s roles
- ◆ The ActorByAccountID.FullName list

This product ships with several global variables that deal with actor-based lists. (See [“Actor Resource Framework Global Variables” on page 278.](#))



Note

- The InActiveList operator option evaluates single-value attributes and multi-value attributes. The field you map could return multiple values (e.g., a user could have multiple roles). In the case of multi-value attributes, if any one value matches, the condition evaluates to true.
- A condition that tests for whether all or any values in a list match is only available to specify on in-memory operations (e.g., in rules, filters, data monitors).

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under [“Common Conditions Editor \(CCE\)” on page 846.](#)

Creating Matching or Join Conditions

A matching or join condition is a condition statement that joins two data fields with the Matching or Join condition logic operator on the Conditions tab. Creating matching or join conditions using data fields provides the flexibility of creating conditions without knowing the specific data field’s values. The following join data field conditions can be created:

- Same data field for two events: `EventOne <data field A> <logic operator> EventTwo <data field A>`. For example, `EventOne Source Address = EventTwo Source Address`. In this example, both event data field must have the same value. This rule is useful when monitoring activity from an unknown Source Address that is generating numerous events.
- Different data fields for two events: `EventOne <data field A> <logic operator> EventTwo <data field B>`. For example, `EventOne Source Address = EventTwo Target Address`. In this example, the Source Address of the first event must equal the Target Address of the second event.
- Different data fields for the same event: `EventOne <data field A> <logic operator> EventOne <data field B>`. For example, `EventOne Source Address = EventOne Target Address`. In this example, the Source Address must equal the Target Address of the same event.



Note

There is a relatively high memory cost for join rules with low-selectivity join conditions (such as same source IP or same target IP). Just like queries in SQL, the more selective the conditions (the conditions on the individual events as well as the join conditions), the less expensive it is to execute, because fewer conditions match.

When authoring a rule you should order conditions on the events to be correlated (or joined) by placing the most restrictive conditions first; for example, adding join conditions like `event1's Source Address = event2's Source Address` or `event2's Detect Time = event1's Detect Time`. This dramatically reduces the memory consumption by the Correlation Engine, as much as 50% in some cases.

The following procedure can only be used with rules that involve two or more events.

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab.
- 3 Select the **Matching Event** branch and select **New Logical Operator**, then **And**, **Or**, or **Not**.

When adding join conditions, you need to decide how the new condition ties to the existing events in the rule. If AND is used, the new join condition must occur, in addition to the existing events, to trigger the rule. If OR is used, the new join condition or the existing events must occur. If NOT is used, all but the new join condition must occur. The logical operator appears as a branch under Joins.

- 4 Click the **Join Condition** button or right-click the logical operator and select **New Join Condition**.

A condition statement appears displaying event, data field, and logic operator text fields. These fields are combined to create <event> <data field> <logic operator> <event> <data field> condition statements. For example, if monitoring for the same Source Address data field in EventOne and EventTwo, the condition statement would be EventOne Source Address = EventTwo Source Address.

- 5 Select one of the following join data field conditions to use in the following steps:
 - ◆ When monitoring for the same data fields for two events use `EventOne <data field A> <logic operator> EventTwo <data field A>`.
 - ◆ When monitoring for different data fields for two events use `EventOne <data field A> <logic operator> EventTwo <data field B>`.
 - ◆ When monitoring for different data fields for the same event use `EventOne <data field A> <logic operator> EventOne <data field B>`.
- 6 In the text fields, choose an event and data field from the drop-down menus.

Select data fields that you want to monitor but for which you don't have values. For more information, see ["Data Fields" on page 867](#).
- 7 Choose a logic operator from the drop-down menu.
- 8 Choose an event and data field from the drop-down menus.
- 9 Click **OK**.

The join data field condition appears as a branch under the Matching Event logical operator.

- 10 On the Conditions tab, click **OK**.

See also [Condition Tree Command Buttons](#), [Condition Tree Context Menu Commands](#), and [Adding Conditions](#) under ["Common Conditions Editor \(CCE\)" on page 846](#).

Editing or Deleting Join Data Field Conditions

- 1 In the Rules resource tree, right-click a rule and select **Edit Rule**.
- 2 In the Rules Editor, select the **Conditions** tab and do the following:
 - ◆ To edit the logical operator, right-click the logical operator and select **Edit** or select the logical operator and press **Enter**. In the text field, select a logical operator and click **OK**.

- ◆ To edit the condition statement, right-click the condition statement and select **Edit** or select the condition statement and press **Enter**. In the text field, make edits and click **OK**. For more information, see [“Creating Rules” on page 440](#).
- ◆ To delete the Matching Event event, right-click **Matching Event** and select **Delete**. In the dialog box, click **Yes**. The event, its logical operators, and condition statements are deleted.
- ◆ To delete the logical operator, right-click the logical operator and select **Delete**. In the dialog box, click **Yes**. The logical operator and all its condition statements are deleted.
- ◆ To delete the condition statement, right-click the condition statement and select **Delete**. In the dialog box, click **Yes**.

3 Click **OK**.

Specifying Rule Thresholds and Aggregation

Thresholds are defined as an aggregate number of occurrences within a time span. When a threshold is met, the rule triggers.

Setting or Changing Rule Thresholds

- 1 In the Rules Editor, select the **Aggregation** tab.
- 2 In the **Number of Matches** field, enter a number if you want more than one matching event.
- 3 In the **Time Frame** field, enter an appropriate value and choose a time unit.
- 4 If you want to aggregate on the basis of certain fields' content being distinct, click **Add** under the **Aggregate only if these fields are unique** pane to select the fields to use. Select fields from global variables, field sets, and local variables.



Fields are *unique* only when the combined value of all fields is unique. For example, suppose you wanted to aggregate on three fields: Event Name, Event Message, and Category Outcome, with a threshold of two matches. If you got two events both with values of **Failed Login**, **Attempt**, and **Failure** for these fields, respectively, these events would be aggregated.

However, if you got only one event like this, and another with values of **Failed Login**, **Attempt**, and **Success**, these two events would not be aggregated because the combined value is not the same for the given threshold number of events.

- 5 If you want to aggregate on the basis of certain fields' content being identical, click **Add** under the **Aggregate only if these fields are identical** pane to select the fields to use. Select fields from global variables, field sets, and local variables.
- 6 Click **OK**.

The choices you make are expressed as a conditional statement in the **Summary** panel.

Aggregation Time Criteria

The ESM Console provides time-evaluation criteria that can affect event-occurrence aggregation and rule-triggering. You apply these to rules through the Aggregation tab and the statement panel of the Conditions tab.



If you set a rule to aggregate over fields of a **multi-mapped active list** or **overlapping session list**, the rule might fire multiple times, once for each field value in the corresponding list entries. The Console displays a warning to this effect when such a list field is selected in the Aggregation tab.

We recommend that you do not set rules to aggregate over multi-mapped active list or overlapping session list fields, *and also* add entries to the same list in a rule action ([“Adding a Rule Action” on page 452](#)). Setting *both* aggregation and rule actions to add entries to the same multi-mapped or overlapped list can cause the number of rules triggered to increase to an unmanageable level.

See also [“Allow multi-mappings” on page 572](#) in Active List topics and [“Overlapping Entries” on page 580](#) in Session List topics.

Criteria	Application
Time Frame	<p>Set on the Aggregation tab, Time Frame establishes the time span for occurrence aggregation. Event-occurrence aggregation is always controlled by Time Frame. Secondarily, Time Frame becomes the default for global and alias expiration time, if these are not set separately.</p> <p>Note: The Rule Action trigger “On Time Unit” can be set in conjunction with the Aggregation Time Frame to limit the number of times a rule is triggered. (See related information on page 454.)</p>
Global Expiration	<p>Set on the Conditions tab, a global expiration applies to an entire rule. This is the amount of time that qualifying events for all aliases are retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. To set Global Expiration, right-click the rule's root node (Correlate) in the Conditions tab and choose Set Global Expiration Time.</p>
Alias Expiration	<p>Set on the Conditions tab, an alias expiration applies to a single alias within a rule. This is the amount of time that a qualifying event for this alias (only) are retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. To set Alias Expiration, right-click an event alias in the Conditions tab and choose Set Alias Expiration Time.</p> <p>An event with an expiration time is displayed with an indicator, for example:</p> <p style="padding-left: 40px;">event1 (Wait time: 5m)</p> <p>To remove the alias expiration time, expiration time right-click the event alias that is configured for expiration time, then change the time to 0.</p>
Matching Time	<p>Set on the Conditions tab, a matching time creates a time-proximity comparison for multiple-alias rules, based on events' actual creation times. When two or more rule-condition aliases are present, a Matching Event node appears. You can right-click this node and choose Set Matching Time to require events' original timestamps (specifically, the event's original end-time) to fall within a range. Note that this time-proximity test is independent of and different than the memory-retention parameter set by global or alias expiration.</p>

Deleting Aggregation from a Rule

- 1 In the Rules resource tree, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, select the **Aggregation** tab.
- 3 In the **Aggregate only if these fields are unique** or **Aggregate only if these fields are identical** lists select the fields to delete and click **Remove**.
- 4 Click **OK**.

Creating Rule Actions

The Actions tab of the Rules Editor offers a consistent interface for defining actions to take based on the thresholds of the events that trigger them.

In the Actions tab, you click the buttons in the top row to Add, Edit, or Remove event-action sets for rules. Click **Hide Empty Triggers** to hide or show triggers not currently used.

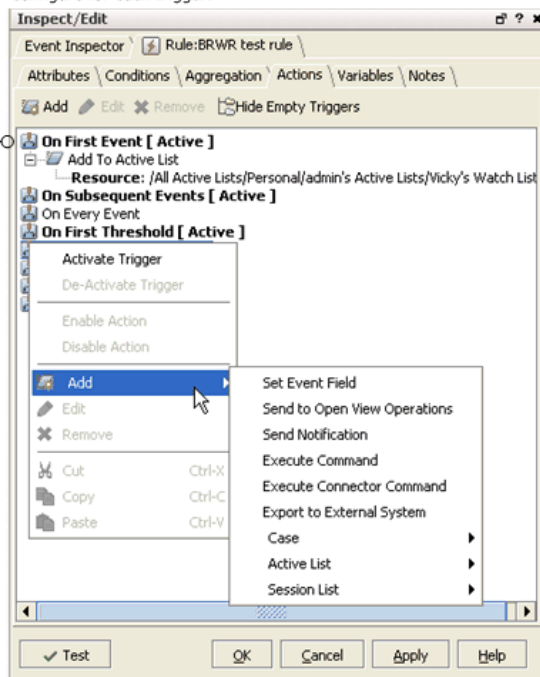


Note

Rules, rule triggers, and rule actions can be enabled or disabled at various levels. The rule itself can be enabled or disabled, the trigger on a particular rule can be activated or deactivated, and a rule action associated with a particular trigger can be enabled or disabled. Details on rule triggers and rule actions are described in this topic. For more information and a summary, see also [“Enabling and Disabling Rules” on page 461](#).

In the **Rules “Actions”** tab, you can define actions to take based on thresholds of the events that triggered them. In this example, “On First Event” is a trigger which is currently activated. The user has configured an action associated with this trigger to add events to the specified active list.


The Add list is expanded here to show all the actions you can configure for each trigger.



Adding a Rule Action

You add rule actions by choosing an event threshold trigger, clicking **Add**, choosing an action, then setting the action's parameters.

To add a rule action:

- 1 Choose **File > New > Rule** from the Console menu bar.
- 2 In the Rules Editor, click the **Actions** tab.
- 3 Select an applicable threshold trigger.
- 4 Click **Add** () , then choose an action from the menu.
- 5 In the **Add "Action Name" Action** dialog box, set the action's parameters, if present. See ["Rule Actions Reference" on page 455](#) for information about rule actions. Right-click the trigger and choose **Activate Trigger** to generate a descriptive event each time this rule action occurs. A rule must have at least one active trigger.
- 6 Click **OK** to add the new action to the rule's threshold trigger.

Editing a Rule Action

You edit rule actions by choosing an event threshold trigger, clicking **Edit**, then changing the action's parameters.

To edit a rule action:

- 1 In the Navigator panel, right-click a rule and choose **Edit Rule**.
- 2 In the Rules Editor, click the **Action** tab.
- 3 Select an action below a threshold trigger.
- 4 Click **Edit** to open that action's Add Action dialog box.
- 5 Change the action's parameters as appropriate.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See ["Velocity Templates" on page 1019](#).)

- 6 Optionally, right-click the trigger and choose **De-activate Trigger** to stop generating a descriptive event each time this rule action occurs.
- 7 Click **OK** to record the changes.

Removing a Rule Action

To remove a rule action, select an action below a trigger in the **Actions** tab and click **Remove**.

Activating or De-activating a Rule Trigger

When a trigger is activated, all enabled rule actions it contains are triggered when conditions are met.

- To activate a rule trigger, select the trigger in the **Actions** tab and click **Activate Trigger**.

- To de-activate a rule trigger, select the trigger in the **Actions** tab and click **De-Activate Trigger**.

Enabling or Disabling a Rule Action

For finer-grained control over which rules are triggered when, you can enable or disable a rule action associated with any of the triggers.

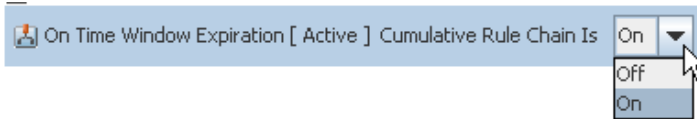
- To disable an action, select an action below a trigger in the **Actions** tab and click **Disable**.
- To enable an action, select an action below a trigger in the **Actions** tab and click **Enable**.

Threshold Triggering Options

Consider the following points when you are determining your triggering options:

- The minimum threshold value you can set is **2**.
- Triggering actions on every or subsequent occurrence can quickly use up resources. Use these options conservatively.
- For threshold-based triggers only a single correlation event are triggered on receipt of any single incoming event, even if that event has an aggregated event count high enough to trigger multiple firings. This is by design to prevent excessive firings. For example, if a rule has a threshold of 10, an event with an aggregated event count of 200 triggers only one rule firing (not 20).

Trigger	Threshold
On First Event	The first time rule conditions are met, overriding aggregation threshold settings.
On Subsequent Events	The second and subsequent times rule conditions are met (not the first), overriding aggregation threshold settings.
On Every Event	Every time rule conditions are met, overriding aggregation threshold settings.
On First Threshold	For the number of matches greater than 1, the first time rule conditions and threshold settings are met.
On Subsequent Thresholds	For the number of matches greater than 1, the second and subsequent times rule conditions and threshold setting are met, not the first.
On Every Threshold	Every time rule conditions and threshold settings are met.

Trigger	Threshold
On Time Unit	<p>Defines an action to take if the given threshold is met in the specified number of minutes specified. (When: On Time Unit: Every <NumberOfMinutes>).</p> <p>This setting can be configured to work in conjunction with aggregation to limit the number of times a rule is triggered. For example, if aggregation is set to 2 matches in 1 minute and you get 50 matches in 1 minute (depending on how you set the rule actions). If you then specify the rule to trigger "On Time Unit" of one minute for example, then even if there were 50 matches in 1 minute, the rule would only trigger once per minute when the aggregation threshold is met.</p> <p>Notes:</p> <ul style="list-style-type: none"> The list of correlated events attached to the On Time Unit trigger excludes the events composing the first threshold. For example, if the threshold is 2 and 5 matching events are found, the first 2 events are excluded and only the remaining 3 are included in the list of correlated events. If you want to include the missing first two events for the threshold rule firing, you can additionally use On First Threshold or On Every Threshold in conjunction with On Time Unit. In this case, you will not see the first two events as part of On Time Unit. Instead, the first two events will be part of On First Threshold or On Every Threshold. Activating On Time Unit does not imply that a rule is triggered on the first event, on subsequent events, or on every event that meets conditions. This specifically sets the rule to trigger for every given time unit <i>if</i> aggregation thresholds are met. Be sure to set On Time Unit to less than or the same value as the Aggregation "Time Frame" (related information on page 450) to prevent getting an extra correlation event for the rule itself.
On Time Window Expiration	<p>When the threshold settings have expired.</p> <p>Note: When the On Time Window Expiration (TWE) trigger is activated, it includes an option to display a cumulative rule chain (a summary of triggered rules) at the end of the triggered rules list.</p> <p>By default, the cumulative rule chain option on an activated TWE trigger is off. To toggle the option on or off:</p> <ol style="list-style-type: none"> Click the Rule Editor Actions tab for a selected rule. Make sure the On Time Window Expiration trigger is active. (See "Activating or De-activating a Rule Trigger" on page 452 for information on activating triggers.) Right-click the <i>active</i> TWE trigger and select On or Off on the cumulative rule chain option as needed.  <p>When a TWE trigger activates a rule, a Correlation Event is generated. If the cumulative rule chain option is <i>on</i>, the correlation event contains all the base events from the first threshold to the TWE.</p> <p>If the cumulative rule chain option is <i>off</i>, the generated correlation event contains events from the last threshold to the TWE.</p>

Rule Actions Reference

Consider the following points:

Action sequence

Always add actions in the order in which you want them to be executed. For example, to set a static value in an active list with values, first add the action to Set Event Field, then add the action to Add to Active List.

Please note that the Editor display does not always match the internal representation of the specified order of rule actions. However, if you add rule actions in the proper order, that order is maintained internally.

Actions added to a rule show up the first time in the order you add them. You can continue to modify these and they show up in this order. After you click **Apply**, the display reorders the actions so that **Add to Active List** shows up first even though the internal representation has not been modified. Even so, rule actions continue to work as expected unless you change the order. For example, if you delete the Set Event Field action then add it back in after Add to Active List action is already configured, the rule actions are mis-ordered and do not trigger as expected.

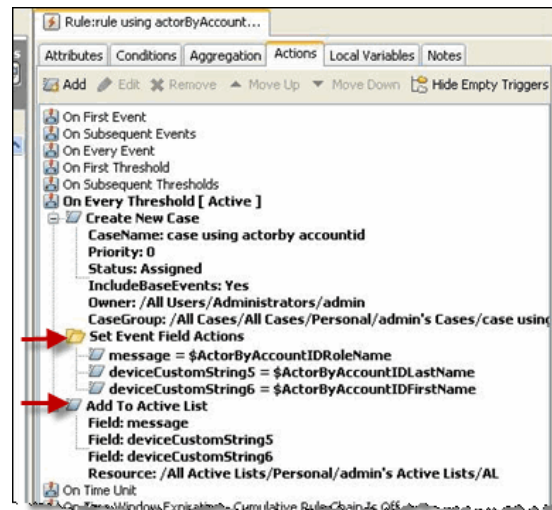
Use of velocity expressions in rule actions involving lists

You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (For additional details, see [“Velocity Templates” on page 1019.](#))

If you are using velocity expressions to derive values from variables and your rule is acting on an active or session list, perform these extra steps in conjunction with your action:

- 1 Aggregate over the field(s) of interest on the rule's Aggregation tab.
- 2 Use the **SetEventField** action to set unused field(s) to the field(s) in [Step 1](#). Start with the \$ symbol followed by the exact name of the variable but without any special characters like spaces and dots. For example:

`$ActorByAccountIDLastName`



- 3 Specify the list to be acted on by the rule.

The following table contains rule actions that are available if you right-click a trigger on a rule's Actions tab and select **Add**.

Action	Description
Set Event Field	Fills in a data field value for correlation events generated by the rule. You specify the data field and the value to place in the field. If the correlation event already has a value for the selected data field, that value is overridden with this rule action.
Send to OpenView Operations	<p>Sends the triggered rule's associated events to a special ArcSight SmartConnector within the Manager. The connector forwards the information to an HP OpenView Operations installation.</p> <p>This applies only where you have specifically integrated OpenView with ArcSight. Request the ArcSight Tech Note concerning HP OpenView Operations for more information.</p>
Send Notification	<p>Sends e-mail, pager, or cell phone messages to the ArcSight users in the notification group when rules are triggered. Specify a notification group in the Event Group drop-down menu.</p> <ul style="list-style-type: none"> Click Ack Required if you want to begin an escalation chain. In this case those notified must acknowledge that they received the notification. If you do not select Ack Required, the message is merely informative. For more information, see "Managing Notifications" on page 658.
Execute Command	<p>Executes a command when the rule triggers. Select an operating system platform from the drop-down menu.</p> <ul style="list-style-type: none"> Enter the command string in the Command field. Enter any required parameters in the Parameters field. Otherwise the command cannot execute without user intervention. Select the Action Type: <ul style="list-style-type: none"> Automatically run on manager: executes the command at the ArcSight Manager without further intervention. Run on Manager with Console confirmation: requires an operator at a Console to approve the command before it executes. Run on connector(s): Sends the command to the connector(s) that report the events.
Execute Connector Command	<p>Executes a SmartConnector command applicable to the device reporting the events. This is also known as the CounterACT feature.</p> <p>Select the SmartConnector to execute the command. When you select a connector, the command field is populated with the commands available for that connector. Only certain SmartConnectors can process commands beyond the basic set that all SmartConnectors support (start, stop, pause, continue, and terminate). This is similar to "Sending Control Commands to SmartConnectors" on page 715.</p>
Export to External System	Sends the rule and the triggering events to an external system that is integrated with ArcSight. The export is in the form of XML on the ArcSight Manager's archive/exports directory.

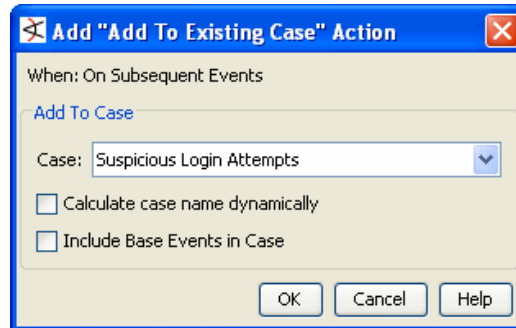
Action	Description
Case Create New Case	<p>Creates a new case when the rule is triggered. Specify a case name, optional description, case group, consequence severity, and owner.</p> <p>The maximum number of rule-associated events a case can hold is 1000. If this limit is reached, the Console sends a warning message and disables the action until the number of events in the case drops below the maximum. To decrease the number of events, manually remove them from the case.</p> <p>In the example shown in the following figure, an action to create a new case called Suspicious Login Attempts that is created in conjunction with an existing field value from an event, for example, Attacker Address. The case name format is <i>Suspicious Login Attempts \$attackerAddress</i> and case creation is triggered <i>On First Event</i> for this rule.</p>

You have the option to include the base events (non-correlation events) in the case or not.

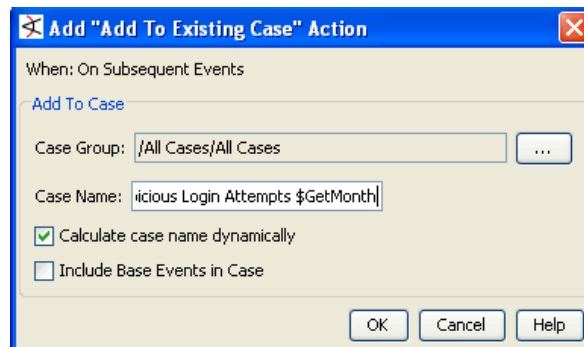
Tip: A suggested approach for updating cases based on triggered rules is to:

- 1 Configure an action to create a case on first event or some threshold, and then
- 2 Add to that same case when subsequent events or thresholds are triggered for that same rule. (For more on this, see the following information on the rule action to [“Add to Existing Case” on page 458.](#))

Action	Description
Add to Existing Case	<p>Adds the associated events to an already-defined case.</p> <p>The maximum number of rule-associated events a case can hold is 1000. If this limit is reached, the Console sends a warning message and disables the action until the number of events in the case drops below the maximum. To decrease the number of events, manually remove them from the case.</p> <p>You can choose one of two main options:</p> <ul style="list-style-type: none"> Select an existing case. Use the Case drop-down menu to navigate the Cases resource tree and select a case.



- Select **Calculate case name dynamically** to specify a case defined in another rule action. This setting inherently depends on another rule action to first create the case. *In this scenario, the referenced case will not be available until the rule action set to create it is triggered.*



To specify Case Group, browse to the group you defined as the case location in the other rule action that creates the case.

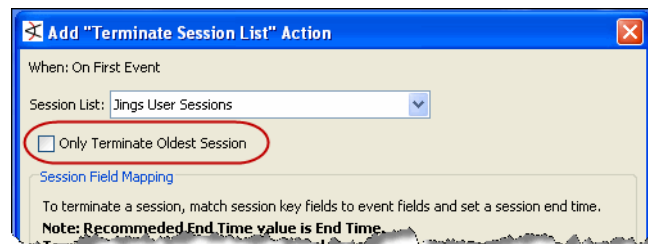
For Case Name, specify the dynamic name based on the same case name you provided in the other rule action that creates the case. An example of a dynamic case name is one that includes a variable. In the example, **GetMonth** is a variable name, and so the entry is **Suspicious Login Attempts \$GetMonth**. If your variable name has spaces, replace the spaces with the underscore character. For example, if your variable is **Get Month** instead of **GetMonth**, then your case name is **Suspicious Login Attempts \$Get_Month**. To calculate the case name, the rule action evaluates this dynamic case name and picks the existing case with the matching name. (See also the information on rule actions to ["Create New Case" on page 457.](#)) You also have the option to include base events (non-correlation events) in the case or not.

Action		Description
Active List	Add to Active List	<p>Add the associated events to an existing active list that you select.</p> <p>When you are specifying fields to be added to the active list, you have the option to select local variables from the Fields tab or global variables from the Global Variables tab.</p>
	Remove from Active List	<p>Remove the associated events from an existing active list that you select.</p> <p>When you are specifying fields to be removed from the active list, you have the option to select local variables from the Fields tab or global variables from the Global Variables tab.</p>

Notes:

- See [related information on page 450](#) about aggregation settings combined with rule actions that add entries to multi-mapped active lists and overlapping session lists.
- See [related information on page 455](#) about using velocity expressions in rules that act on lists.

Session List	Add to Session List	<p>Add the associated events to an existing session list that you select.</p> <p>When you are specifying fields to be added to the session list, you have the option to select local variables from the Fields tab or global variables from the Global Variables tab.</p>
	Terminate Session List	<ul style="list-style-type: none"> • Add the events to the session list when a session terminates. When you are specifying events to be terminated, you have the option to select local variables from the Fields tab or global variables from the Global Variables tab. • Terminate the oldest session. If checked, the oldest session is added to the "terminate" session list. Oldest time is based on the session's Start Time.

**Notes:**

- See [related information on page 450](#) about aggregation settings combined with rule actions that add entries to multi-mapped active lists and overlapping session lists.
- See [related information on page 455](#) about using velocity expressions in rules that act on lists.

Asset	Add Asset Category To Asset	<p>Add the asset category to the associated asset.</p> <p>This supports the automated discovery and categorization of assets (web servers, mail servers, firewalls, etc.) based on the type of events each asset is sending. Rules can be constructed to listen for certain types of events, and then categorize the associated asset appropriately. (You also set up a condition based on which to Remove Asset Category From Asset.)</p>
	Remove Asset Category From Asset	<p>Remove the asset category from the associated asset.</p> <p>This supports automated categorization (or de-categorization) of assets along with the Add Asset Category To Asset rule action.</p>

Applying Rule Actions

Rule actions are automatic procedures that occur when all rule conditions and threshold settings have been met. You can choose to be notified of a triggered rule at the ESM Console or through the Notifier, have information about the events that triggered the rule sent to a case or an active list, or automatically execute a command-line function. You can also assign more than one rule action to any rule.

More Rule Actions

Defining a New Rule Action

To define a new rule action, select the **Actions** tab of the rule you're creating or editing. Select an active trigger or activate an inactive one. Then right-click in the activated trigger and choose **Add**. The Console now displays a list of options for each of the action types you may want to add, for example, **Set Event Field**, **Send Notification**, **Execute Command**, **Add to Active List** or **to Session List**, **Create New Case**, and so on.

Some additional actions you can specify for a rule include the following.

- **Add To Active List, Add to Session List** - When triggered, adds the qualifying item to the specified active or session list.
- **Remove From Active List** - When triggered, clears the qualifying item from the active list.

Add To Active List and **Remove From Active List** either take no arguments (if acting on an event-bound active list) or a list of event fields (if **not** dealing with an event-bound active list). The values from the specified fields (those specified either by an event-bound active list or by the argument list) form an item that is added to, or removed from, the active list. Removing an item that is not present does not cause an exception. Adding an item that is already present simply increments that item's counter. You can see this counter in the Active Lists Editor. (See [“Active Lists” on page 790](#) and [“Managing Active Lists” on page 571](#) for more information.)

- **Add to Existing Case:** Adds to a case all the events that have triggered the rule. When the rule is triggered, all events associated with the rule are sent to a case for further investigation. The maximum number of rule-associated events a case can hold is 1000 (as controlled by `rules.max_events_in_case` server property).

When this limit is reached, a warning message goes to the ESM Console. The Add to Case action deactivates and further events are not sent to the case. When the number of events in the case reduces, the Add to Case action re-activates, and it resumes sending events to the case.

- **Create New Case:** Creates a new case and adds all events that have triggered the rule to the case. When the rule triggers, all events associated with the rule are sent to a case for further investigation. The maximum number of rule-associated events a case can hold is 1000.

Once this limit is reached, a warning message is sent to the ESM Console and the Create New Case action deactivates and further events are not sent to the case. When the number of events in the case reduces, the Create New Case action reactivates, and it resumes sending events to the case.

- **Execute Command:** Executes a command-line function when the rule triggers. The command-line function can be executed immediately or sent to the ESM Console prior to execution. For example, you could specify an action to perform the bin/ping command on a specific IP address.

In the ESM Console, you can decide whether to execute or clear the rule action during real-time monitoring.

- **Export to External System:** Sends the rule and the triggering events to an external system that is integrated with ArcSight. The export is in the form of XML, in the ArcSight Manager's archive/exports directory.
- **Send to Console:** Sends a correlation event to the ESM Console when the rule triggers. A correlation event is generated by a rule when its conditions and threshold settings are met. The Send to Console rule action should always be used. Setting this action displays the "flash" triggered-rule event on the Console.
- **Send Notification:** Sends e-mail, pager, or cell phone messages to ArcSight users when rules are triggered. The Send Notification rule action can send an informative message or can begin an escalation chain that requires an acknowledgment from a user. Informative notifications are sent to all destinations in a notification group to relay a message. They do not need to be acknowledged. If the **Ack Required** checkbox is selected, the notification must be acknowledged. For more information, see ["Managing Notifications" on page 658](#).

To generate a correlation event the rule is triggered. You can specify a Set Event Field rule action. This rule action fills in a data field value for correlation events generated by the rule. You specify the data field and the value to place in that field. If the correlation event already has a value for the data field selected, that value is overridden with this rule action.

See ["Creating Rule Actions" on page 451](#) for more information on defining rule actions and associated triggers.

Enabling and Disabling Rules


You can enable (set to on) or disable (set to off) rules. Rules can also be automatically disabled by ArcSight.




Note

Keep in mind that only rules deployed in Real-time Rules show up in a live channel when they are triggered. Therefore, once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules as described in Deploying Real-time Rules.


Enabling Rules

In the **Navigator** panel's **Rules** resource tree, right-click the rule and choose **Enable Rule**. The rule is displayed as enabled or on () in the Navigator.

Disabling Rules



In the **Rules** resource tree, right-click a rule and choose **Disable Rule**. The rule is displayed as disabled or off () in the Navigator.

Automatically and Manually Disabled Rules

If a rule is **disabled** or off () , the rule is grayed out on the **Navigator** panel in the Rules resource tree.

A rule can be manually disabled by an administrator or automatically disabled by the ArcSight system. A rule is disabled by the ArcSight system for either of the following

reasons. When a rule is automatically disabled, it generates an audit event indicating that this happened so that administrators can follow up as needed.

Cause for Automatically Disabled Rule	Description
Rule is invalid	<p>An invalid rule is automatically disabled and displayed as broken  in the Navigator.</p> <p>If an administrator configures a rule or related resource in a way that "breaks" the rule and leaves it in an invalid state, the system automatically disables the rule.</p> <p>If a rule is disabled automatically due to an invalid configuration, an "Invalid Reason" is displayed in the Rule Editor on the Inspect/Edit panel. When the rule is reconfigured to a valid state and enabled, the "Invalid Reason" field is no longer displayed.</p> <p>The "Invalid Reason" field is not displayed for rules that are manually disabled.</p>
Rule is recursive	<p>Rules that trigger themselves in a recursive loop is automatically disabled <i>temporarily</i>. A rule that is automatically disabled due to recursion is re-activated after a time frame that matches the aggregation time frame for the rule. (The default aggregation time frame is 2 minutes.)</p> <p>An auto-disabled rule is displayed with a special icon  in the Navigator. (It shows with the "broken" symbol, overlaid by an ArcSight logo to indicate that the system disabled it.)</p> <p>A rule can be inherently recursive due to a flaw in its design, or temporarily recursive because of some particular events involved. In the first case, temporarily disabling the rule often clears out the problem, and allows the rule to run normally when it is re-activated.</p> <p>If the rule is inherently recursive, it is continuously re-enabled and auto-disabled. The solution in this case is to redefine the rule logic and redeploy it, since it is effectively a "broken" rule.</p>
Number of rule triggers exceeds configured limits	<p>Number of rule triggers exceeds configured limits A rule that exceeds configured limits show as disabled () in the Navigator, and offer a right-click option for the user to manually disable it permanently.</p> <p>The system disables a rule if the rule exceeds the configured limits on number of rules triggered per minute or ratio of base events to triggered rules, as defined in the file ARCSIGHT_HOME/config/server.defaults.properties on the Manager.</p> <p>A rule in this state continues to attempt to run until the user disables it permanently by right-clicking it in the Navigator and choosing Disable.</p>

For rules that are disabled automatically by ArcSight, right-clicking the disabled rule in the **Navigator** provides a manual **Disable** option so that users can permanently disable the rule until it is fixed. If these rules are not manually disabled, they make continued attempts to run and get intermittently enabled/disabled by the system. This can impact system performance.

Disabling Rule Components

You can also disable certain components of a rule, such as particular rule triggers or a rule actions associated with particular triggers. For information on this, see [“Activating or Deactivating a Rule Trigger” on page 452](#) and [“Enabling or Disabling a Rule Action” on page 453](#) (in [“Creating Rule Actions” on page 451](#)).

Importing and Exporting Rules

Rules are created in a readable XML format. You can export a rule or rule group to an external file to modify it. After modification, you can import it back into the ArcSight Manager.



To import and export rules, use the packages feature. Packages supersedes the import/export facility provided in previous releases and offers enhanced functionality, including version support, dependency management, and import/export capabilities. Portable ArcSight packages can automatically manage dependencies across resources and other packages. Please see the information on packages in [“Managing Packages” on page 686](#).

Scheduling Rules

You can schedule rules to run at a specified time interval (such as hourly, daily, or monthly).

Scheduled Rules are a useful alternative to real-time rules in situations where you want to deploy rules that take into account historical data along with live data, or when you simply want to control when the rules are run. The scheduled rules engine can process historical data, take real actions, and generate correlated events which are the same as those generated by the real-time rules engine.

Scenarios for Using Scheduled Rules

- **Batched Events.** In many environments, certain types of events are not immediately available to the Manager, but instead are sent in batches infrequently; sometimes once a day, or once a week. Such events have different Manager receipt times and end times. Manager receipt times are current (when the batches are submitted), but the event end times are in the past, since the events actually happened in past. Common examples of events that are sent in batches are those involving physical security devices and represent individuals gaining entry to buildings or offices by means of badge readers and card keys.

Since these events (like an employee entering an office) arrive late to the Manager, they cannot be effectively correlated with other events (like a user login) by typically deployed rules that use the real-time rules engine. When the real-time rules engine receives login events, it waits for 1 minute (or whatever the time window for this rule is) and then throws out the login event, since the other event did not arrive within rule's time window. Suppose you have a rule that looks for a badge swipe event and a login event within 1 minute of each other (aggregates on 1 minute). The login events are received by the Manager real time as they occur. But the badge swipe events are collected and submitted only once a day at 10 p.m.

A real time rule would not correlate the two events because it would throw out the login event before it ever gets the batched event. But if you scheduled your rule to run at midnight with the scheduled rules engine, it could correlate the actual end times of batched events and login events that occur within 1 minute of each other. Scheduled rules can correlate these types of events because (a) rules can be scheduled to run

when both the login and batched events are available within the database and (b) although the Manager receipt times for these events would be different, their end times are close together within the aggregation window. Correlations are based on end times of events.

- **Historical Data.** You may want to capture and correlate other kinds of historical data (other than batched events). For example, if you have observed a pattern of events over the last several weeks, decide to write rules to take actions on some of those events, and correlate not only future occurrences of them but also the past events. This is possible to do by scheduling rules to run on events with end times in the past.
- **Optimized Rule Schedules.** Another scenario in which you might want to use scheduled rules is for rules that are more appropriate to run after business hours (for example, in the middle of the night). The job scheduler on rule groups lets you specify the appropriate schedule, and the rules are deployed as correlated events but are executed on off-hours.

In all such cases, scheduled rules generate correlation events and take real actions when triggered, just like deployed real-time rules.

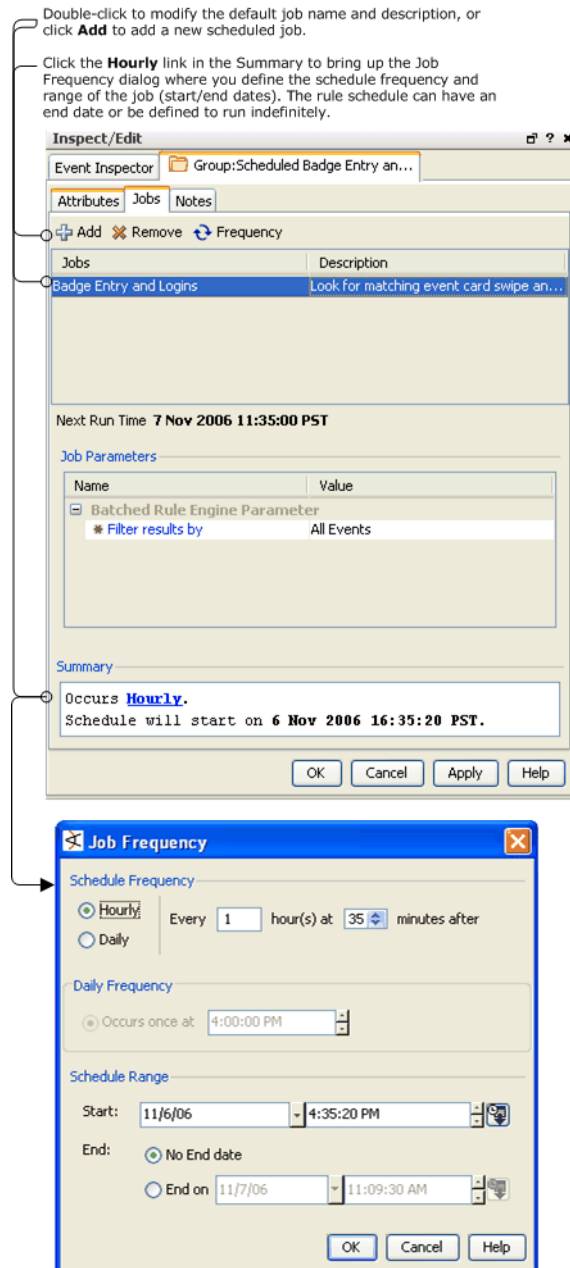


Although scheduled rules that correlate batched events work in part with historical data, these are deployed rules (not tests) that take actions as appropriate and do affect the live system.

Scheduling a Rule Group

- 1 Click the **Rules** resources on the Navigator.
- 2 Identify the rule(s) you want to schedule. (For information on how to create new rules, see [“Managing Rules” on page 440.](#))
- 3 If these rules are not already in a rule group, create a new rule group and link or move rules into it. (For information on how to create and work with rule groups, see [“Managing Rule Groups” on page 441.](#))
- 4 Select a rule group, right-click, and choose **Edit Rule Group** from the context menu.
- 5 Click **Jobs** in the Rule Group editor.
- 6 Add a job, name and describe it, and specify a schedule on which to run the rule group.

- 7 Specify a filter for these rules. (By default the filter is set to All Events. Click **Filter Results by** to refine the filter to display only events relevant to the rule. Narrowing the filter optimizes performance when the rule is run.)



- 8 Click **Apply** or **OK** to deploy.

The rule(s) are deployed according to the schedule specified in the Rule Group editor on the Jobs tab, and are triggered if the rule conditions are met.



You cannot schedule a single rule outside of a group, but you can schedule it as a "group of one" contained in a folder. To schedule one or more rules, place them in a folder. Multiple rules in the same folder run together per the schedule as part of the rule group.

Example of a Scheduled Rule (Badge Swipes and Logins)

As an example, here are the **conditions statements** for a rule that correlates Badge swipe events, which are sent to the Manager in a batch file once per day, with login events which are sent to the Manager frequently in real-time. The example rule looks for an event with "swipe" in the name and an event with "login" in the name.

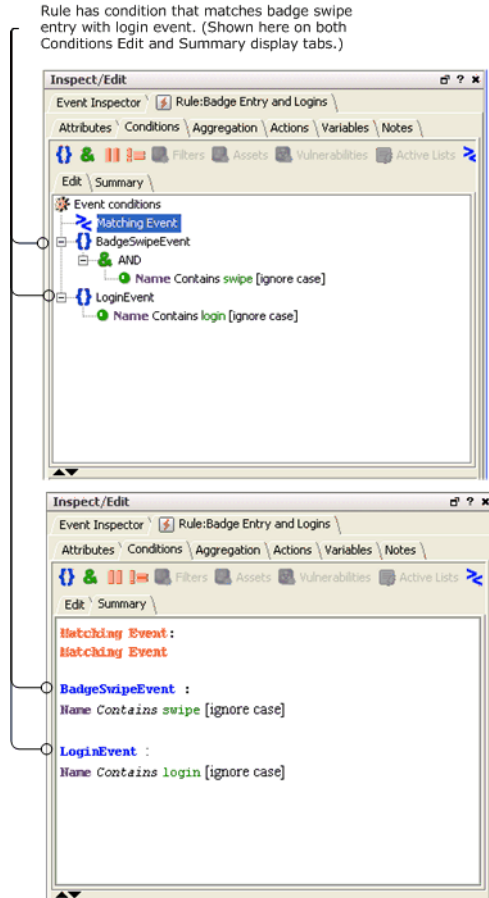


Figure 16-1 Example Scheduled Rule: Condition Statements

This rule sets an **aggregation time window** to correlate these events at 2 minutes. This means that a login event (end time) must occur within 2 minutes of a badge swipe event (end time) in order for the rule to be triggered.

The rule aggregates on 1 or more matching conditions within a 2 minute time window. A badge swipe and login entry must occur within 2 minutes of each other to be correlated and trigger the rule.

The screenshot shows the 'Inspect/Edit' dialog box for a rule named 'Rule:Badge Entry and Logins'. The 'Aggregation' tab is selected. The '# of Matches' is set to 2, and the 'Time Frame' is set to 1 Minute. There are two sections for aggregation criteria: 'Aggregate only if these fields are unique' and 'Aggregate only if these fields are identical', each with an 'Add...' button. A 'Summary' section at the bottom states 'Aggregate if at least 2 matching conditions are found within 1 Minutes'. At the bottom are buttons for 'Test', 'OK', 'Cancel', 'Apply', and 'Help'.

Figure 16-2 Example Scheduled Rule: Aggregation

Note that if you deploy this rule in real-time rules, the rule is not triggered to capture the events you want to correlate. Although the badge swipe events are actually occurring within 2 minutes of login events (according to event end times), the ArcSight Manager Receipt Time for badge swipe events is always hours later (whenever they are submitted as batched events). In this kind of scenario, the real-time rules engine would never correlate these events because the badge swipe events (with late Manager Receipt time) would be read in so much later.

If, however, you deploy this as a scheduled rule to run on a nightly basis, the rule is triggered and capture the correlated events. This is because the scheduled rules engine is designed to correlate historical data with live data.

To configure this as a scheduled rule, you would create a new folder (group) for it under Rules resources in the Navigator, link or move the rule into the folder, then edit the rule group to add a scheduled job (on Jobs tab). The job schedule defines when the rule runs. Once the job schedule is applied to the rule group, the rule is deployed as a scheduled rule.

To create and test the example rule:

- 1 Create a rule called "Badge Entry and Logins".
- 2 On the Conditions tab for this rule, set a condition to look for two events joined by "AND"; an event with "swipe" in the event name and an event with "login" in the event name.
- 3 Save the new rule.
- 4 Create a new rule group folder called "Badge Entry and Logins" and link or move the rule into that folder.
- 5 Edit the "Badge Entry and Logins" rule group to add a scheduled job for rule of the same name.
- 6 Save the new rule group.

After you save the rule group with the scheduled job, the rule is deployed.

For testing purposes, schedule the job to start in 5 minutes from the current time and then use the ArcSight Test Alert connector to test sending events to the Manager with end times within two minutes of each other and different Manager receipt times. (For example, to model a real-world scenario: set Manager receipt time for badge swipes to several hours later than for logins.)

Make sure that the start time of your scheduled job is earlier than the event end times on your test events (so that the scheduled job is running to capture the events). You should see the scheduled rule triggered on correlated events.

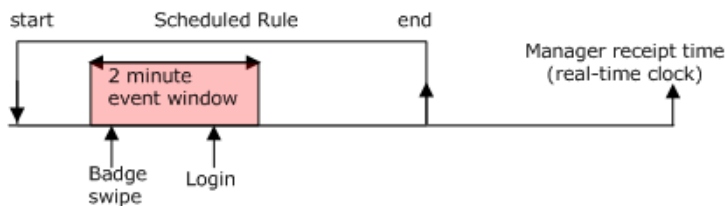


Figure 16-3 Start Time on Example Scheduled Rule is Set Earlier than End Times of Events

As a comparison, deploy the same rule in a real-time rules folder and send the test events again. Note that the same rule is not triggered by the real-time rules engine because it is not designed to correlate historical data.

In every scheduled run of a rule, only events arriving between that run and the earlier run are considered for input.

Testing Rules

You can test rules against copies of active channels for valid conditions logic, verify that rules are triggered by the events they are supposed to capture, and that they generate correlated events as expected.

The ESM Console provides two different ways of getting to tools for testing and verifying rules against events before deploying the rules in real time:

- Test a single rule from within the rule editor by clicking the Test button
- Test rules and rule groups from the navigation tree with the Verify Rules with Events option

These options are somewhat similar. They differ in the navigation paths to select or set up the channels, and more importantly in that from the rule editor you can test only the selected rule but from the navigation tree you can test several selected rules or rule groups. This Help topic explains how to test a single rule from the rule editor. See also [“Verifying Rule\(s\) with Events” on page 470](#).

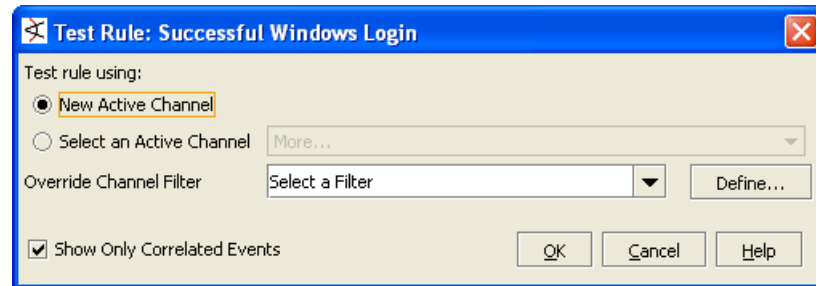


Keep in mind that only rules deployed in Real-time Rules act on live events and show up in a live channel when they are triggered. For more information, see [“Deploying Real-time Rules” on page 473](#).

Testing a Rule from the Rule Editor

- 1 Choose the Rules resource in the Navigator, and select the rule you want to test.
- 2 Right-click and choose **Edit Rule** to bring up the Rule editor for that rule in the Inspect/Edit panel.
- 3 In the editor for the selected rule, click **Test**.

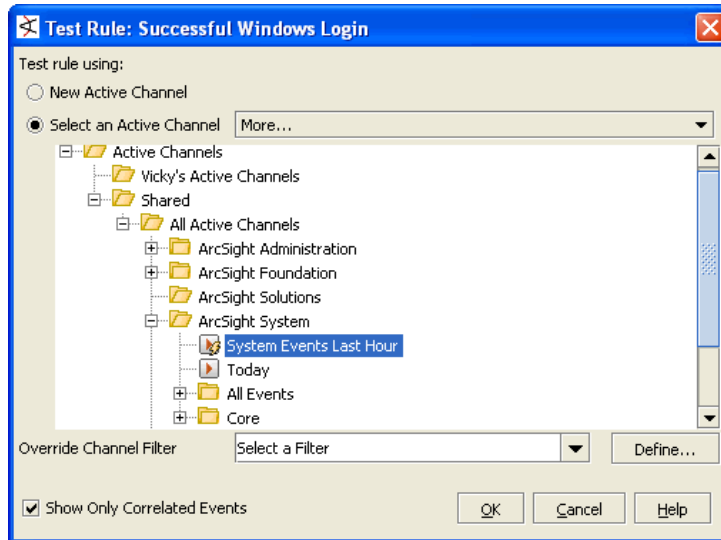
This brings up the Test Rule dialog where you can choose an existing active channel or create a new channel in which to verify the rule.



- 4 Select either **New Active Channel** or **Select an Active Channel** depending on whether you want to test the rule in a new or existing channel.

You can set override channel filters on either a new or existing active channel.

If you choose **Select an Active Channel** (which means you are opting to use an existing channel rather than create a new one), an inline browser is displayed where you can navigate to and choose an existing channel.



- 5 Once you have set up the channel, click **OK**. (If you need more help on setting up channels, see [“Viewing and Using Channels” on page 130](#).)

The channel is displayed in the Viewer panel.

Showing Rule Errors

If rules have errors, the rule icon () changes to indicate it.

In the Rules resource tree, right-click the rule-error icon and choose **Show Error**. The error appears in a dialog box.

Verifying Rule(s) with Events

The ESM Console provides two different ways to test or verify rules before deploying them. These options are somewhat similar. They differ in the navigation paths to select or set up the channels, and more importantly in that from the rule editor you can test only the selected rule but from the navigation tree you can test several selected rules or rule groups.

This topic explains how to test multiple rules or rule groups from the navigation tree using “Verify Rule(s) with Events”. See also [“Testing Rules” on page 468](#).

“Verify rules with events” is an enhanced version that replaces “replay with rules” in previous versions. You can test rules by running them against a set of captured events for forensic analysis. Now you can replay events to verify rules in existing active channels or, as before, create new channels for this purpose. Also, you can select a single rule, multiple rules, or a rule group to verify. (In earlier releases, only the last of these options was available.)

To verify rules with events, select an existing active channel or create a new one, and then scan the list of events in the channel to verify that the rule is triggered and that it generated correlated events as expected.

Existing active channels have a sliding time window for events (based on the channel filters).

New active channels created as "replay with rules" channels have a fixed time window for qualifying events, and the events are those that qualify under the rules in the selected group. These active channels incorporate the conditions, aggregation characteristics, and actions defined for the rules in the selected group.



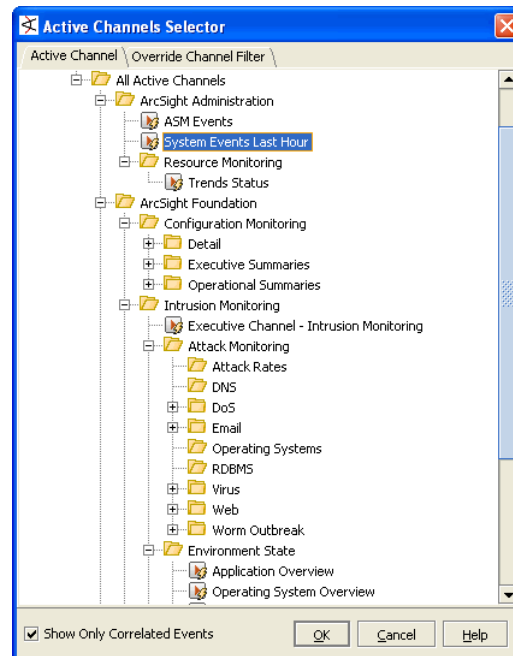
Note

Rules tested against pre-existing active channels are actually executed on copies of active channels the system automatically generates for this purpose. Rules run in verify mode do not generate real rule actions correlated with live or historical system events and, therefore, when they are triggered no real rule actions are impacting the system state. Only real-time rules or scheduled rules (set up to capture batched and other types of historical data) trigger real rule actions.

Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. For more information, see ["Deploying Real-time Rules" on page 473](#) and ["Scheduling Rules" on page 463](#).

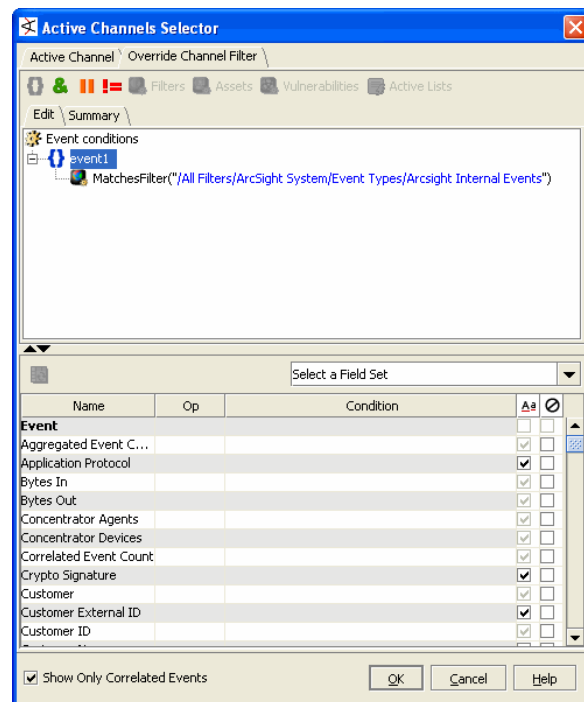
Verify Rule(s) from the Resource Tree

- 1 In the Rules resources tree, right-click an appropriate group and choose **Verify Rule(s) with Events**.
- 2 From the sub-menu, choose **Most Recent Opened Active Channels, More, or New Active Channel**.
 - ◆ **Most Recent Opened Active Channels**. Choose from the list of recently opened channels. The selected channel is displayed in the Viewer panel.
 - ◆ **More...** This brings up the Active Channel Selector dialog. Use this dialog to navigate to the channel you want.



If you want to redefine or further narrow the stream of events in the selected channel, click the Override Channel Filter tab to add filters to it. The Override

Channel Filter tab shows the conditions on the currently selected channel. You can add, remove, or modify the filters here.

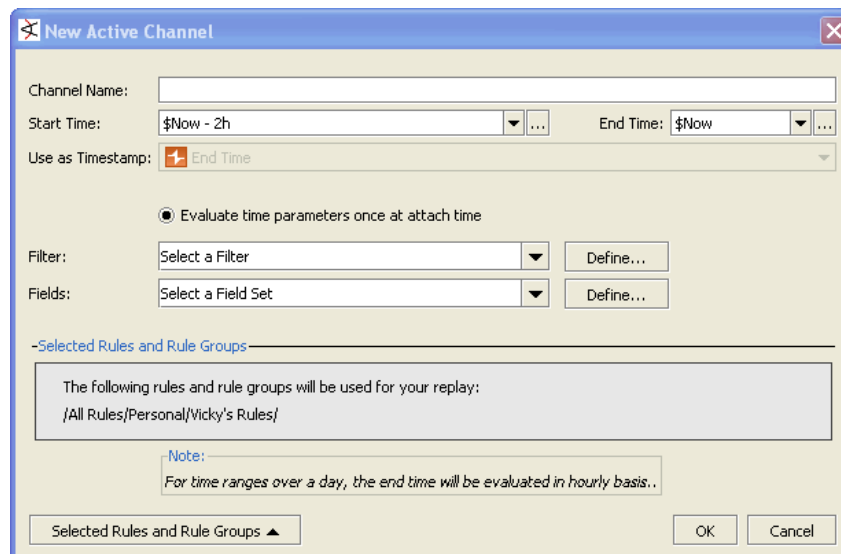


Click **OK** to choose the selected channel with filter modifications (if any).

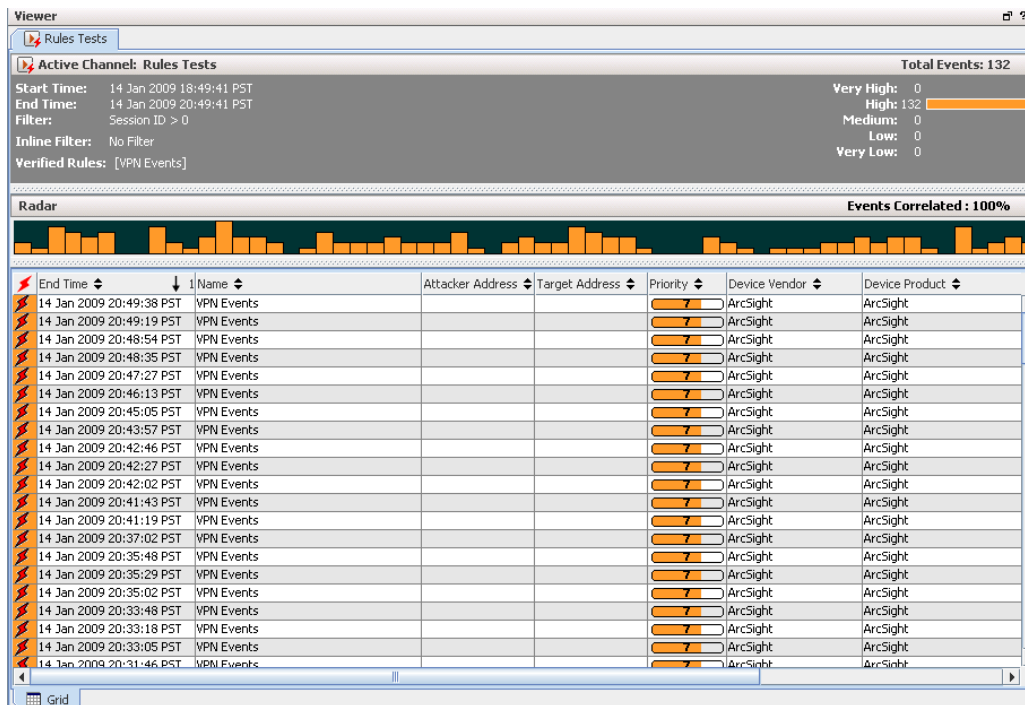
The selected channel is displayed in the Viewer panel.

◆ New Active Channel...

Selecting this option brings up a dialog where you can set up the parameters for the active channel that displays the rules in action. Provide a name for the new channel and set the other channel options as described in [“Viewing and Using Channels”](#) on page 130.



Click **OK** to create the new channel with your chosen settings. The new channel is displayed in the Viewer panel.



About Test Channels: A lightning bolt icon on a channel indicates it is a test channel created as a result of choosing **Verify Rules with Events** on a rule. Test channels cannot be re-used, even for the same rule. Remove test channels from the Active Channels folder in the Navigator.

Alternatives to Test Channels: If you would like to re-use a channel to test various rules, create a standard active channel e.g., "My Rules Test Channel" (see ["Creating an Active Channel" on page 131](#)), then send rules test results to that channel. You can re-use a standard channel as many times as you want to test rules (i.e., *verify rules with events*).



Note Filters shown on rule verification channels are not designed for copying and re-use outside of these special rule testing channels. Rule verification channels show rule-triggered events and other non-correlation events in the channel, but the complete filtering logic that accomplishes this is not exposed.

Filter conditions on these channels display the original filter (if one is applied) and "Session ID > 0". The session ID statement is a simplified representation of the back-end filtering taking place in the special rule verification channel to limit this particular channel to show only new rule-triggered events.

Deploying Real-time Rules

Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules.

Rules run in verify or test rule mode do not generate real rule actions correlated with live or historical system events and, therefore, when they are triggered no real rule actions are impacting the system state.

Only real-time rules show up in a live channel, generate correlation events, and trigger real rule actions.



A special category of rules called scheduled rules can capture batched and other types of historical data, generate correlation events, and trigger real rule actions. These act similar to real-time rules, but are deployed differently. They are evaluated according to a schedule, and trigger off of historical/past events. See [“Scheduling Rules” on page 463](#) for more information.

Deploying a Rule

In the **Navigator** panel's **Rules** resource tree, right-click a rule or a rule group (folder) and choose **Deploy Realtime Rule(s)**.

The rules you deploy are linked into the Real-time Rules folder (Shared/All Rules/ Real-time Rules). This means that if you change something in the working copy of a rule (in your user folder), those changes also take effect in the deployed rule and vice versa.

You can also manually copy, link, or move rules from your working user folder to a user folder in Real-time Rules. To do this, click and drag a rule or rule group to the Real-time Rules folder, then choose an option in the dialog (Copy, Link, or Move). Using this method of deploying real-time rules is useful if you want to copy or move the rule(s) rather than link them.

If a rule is already enabled (🔴), it is deployed as enabled. If a rule has been disabled (🔴) during testing phase, it is deployed into real-time rules but remain disabled until you enable it. Rules must be both enabled and deployed in real-time rules to take effect in the live system. (If you enable or disable a deployed, linked rule in the original location it is also enabled or disabled in real-time rules and vice versa.) For more information, see [“Enabling and Disabling Rules” on page 461](#).

Removing or Un-deploying a Rule

You can remove rules from the Real-time Rules folder, thereby “un-deploying” them from the live system.

To un-deploy a rule (beyond disabling it), select the rule in the Real-time Rules folder, right-click, and choose **Delete Rule** from the context menu.

Depending on whether the rule was linked, moved, or copied into the Real-time Rules folder, you get different options at this point.

- If the rule has been moved or copied into your working folder, you get an option to remove it or to cancel the operation.
- If the rule is a link to the original rule in your working folder, you get options to remove it from this group only, delete it entirely from all locations, or cancel the operation. (A linked file is treated as a single entity, so edit actions taken on the file in any location affect all instances of it.)

Loading Rules

Creating custom rules does have an effect on the load placed upon the ArcSight Manager. This load is a function of how many partial and full matches are generated by those rules. Since partial matches occur when any condition of a rule is met and full matches occur

once all conditions of a rule have been met, poorly written rules can generate many partial matches without generating any full matches.

Also, poorly written rules can generate, in a worst case scenario, one additional event for every incoming event. However, well-written rules have conditions that are restrictive enough to limit partial matches to those events that are likely to participate in a full match. Such rules are also likely to generate very meaningful derived events and they also impose a smaller load on the ArcSight Manager. Therefore it is very important that you carefully plan, write, and test all your custom rules.

Automatic Disabling

ArcSight automatically disables improperly written rules that would produce excessive or meaningless events. The conditions that cause rules to be disabled are described below.

The factors that control rule disabling are shown in the table below.

Rule Disabling Factor	Operation
Alias Matches	If an alias is defined in the rule, this is the number of events matching that alias, independent of other defined aliases.
Partial Matches	If more than one alias is defined in the rule, this is the number of events matching the aliases defined before the current one, and for the current one, and for their join condition (if present).
Generated Events Counts	The number of correlation events generated.
Base Event Counts	The number of base events used by the rule to generate correlation events.
Time Unit Counts	The number of time units (minutes) that passed since the current rule activated.

Therefore, the conditions that can result in rule disabling are:

- The number of matching aliases would exceed the default limit of 100000.
- The number of partial matches for any of the aliases would exceed the default limit of 100000.
- The rule generates more than five correlation events for each base event it processes.
- The rule generates more than 1000 correlation events in one time unit.

The above values are defaults that may be adjusted differently for your enterprise.

Chapter 17

Global Variables

This topic describes global variables, which enable you to create a variable that derives data from fields in the resource and event schema and can be used and re-used in monitoring and authoring contexts throughout the Console.

[“About Global Variables” on page 477](#)
[“Creating a Global Variable” on page 478](#)
[“Promoting a Local Variable to a Global Variable” on page 480](#)
[“Editing a Global Variable” on page 483](#)
[“Navigating to Global Variables” on page 484](#)
[“Adding a Global Variable to a Resource” on page 484](#)
[“Chaining a Global Variable” on page 489](#)
[“Global Variables in Standard Content” on page 490](#)

About Global Variables

ArcSight provides the ability to create variables that derive values from existing data fields, which you can create locally in the resource you're working on to make monitoring and correlation more specific to particular scenarios.

In addition to these local variables, there is a global variable resource, which makes it possible to define a variable once, then re-use it in multiple places wherever conditions can be expressed (active channels, rules, filters, data monitors, and queries), and wherever fields can be selected (CCE, field sets).

Global variables are centralized and reusable, which makes them an essential building block for user correlation in the Actors feature, and other advanced correlation scenarios.

Once created, global variables can be selected in the [Common Conditions Editor \(CCE\)](#) as additional fields on the Filters or Conditions tabs, as [Group By](#) arguments for data monitors and queries, and in rule conditions and actions. You can add variables to field sets in the Field Set Editor to extend the event and resource schema with values derived from other data fields.

The global variables feature also makes it possible to easily promote local variables defined for a particular resource into a global variable, where it can be re-used in other condition statements.

Global variable dependencies

Global variables depend on a pre-defined schema, so ad hoc data gathered during run-time in active channels, active lists, session lists, query viewers, queries, domain fields, and trends cannot be used to define a global variable.

Ad-hoc (in-memory) global variables can be displayed as columns in active channels, but not used as part of a condition or filter (for example, to derive a list or query result).



Remote variables processing

Variables using Group, List, and Category Model functions are evaluated on the Manager, not directly on the Console, and are referred to as **remote** variables.

These remote variables are evaluated only once on the console for any given event or resource. These remote variables are evaluated only once on the console for any given event or resource. Therefore, the value of the variable on the Console does not change if the underlying data is modified that would result in a different value for the variable. New events (in events channels) and resources (in resource channels) evaluate the variable again, and you see the updated value. Because not all variables can be calculated on the Console, there may be a delay in returning values from variables that are calculated remotely on the Manager.

This topic describes how to use Console tools to create global variables, and how to leverage them in other resources. For details about the supported variable types and functions, see [“Variables” on page 1006](#).

Creating a Global Variable

Here are the high-level steps for creating a global variable:

- 1** In the Navigator panel, go to **Field Sets** and click the **Fields & Global Variables** tab.
- 2** In the Fields tree, right-click the group to which you want to add the global variable, such as **<user's> Fields**, and select **New Global Variable**.
- 3** In the Global Variable Editor in the Inspect/Edit panel, define the global variable.
 - a** In the *Attributes* tab, name the global variable, specify its type, and specify the group in which to place it to help others find it in pick lists. For details, see [“Global Variable Editor: Attributes Tab” on page 479](#).
 - b** In the *Parameters* tab, define the parameters the variable use and the function(s) it performs. For details, see [“Global Variable Editor: Parameters Tab” on page 479](#).
 - c** In the *Local Variables* tab, you can optionally add a local variable, which extracts data from a field that can be used for the overall global variable. For details, see [“Global Variable Editor: Local Variables Tab” on page 479](#).
- 4** Click **Apply** to apply the changes and keep the editor open; click **OK** to save changes and close the editor.

Global Variable Editor: Attributes Tab

Field	Description
Name	<p>Enter the variable name (which must be unique in the containing group)</p> <p>NOTE: The value you enter here cannot be changed once the global variable is saved. If you want to change the name of the global variable after it is saved, make note of the variable attributes and re-create the variable with the desired name.</p> <p>NOTE: Global variable names cannot be SQL or Oracle keywords.</p>
Type	<p>From the drop-down selector, select the type of global variable you want to create: The type you choose here determines the type of fields available to this variable, and which resources can use the data derived from it.</p> <ul style="list-style-type: none"> • Event Global Variable. Select this default option if you want the global variable to operate on event fields. • Asset Global Variable. Select this option if you want the global variable to operate on fields associated with assets in the network model. • Case Global Variable. Select this option if you want the global variable to operate on fields associated with cases. • Actor Global Variable. Select this option if you want the global variable to operate on fields associated with actors.
Group	<p>From the drop-down menu, select the group in which to place your global variable. This is the group where you find the global variable in field pick lists in the CCE and Field Sets editor. The Variables group is selected by default.</p>

For a description of what to enter in the Common fields, see [“Common Resource Attribute Fields” on page 684](#).

Global Variable Editor: Parameters Tab

- 1 On the parameters tab in the Function field, select the function that the variable evaluates.
- 2 In the Arguments fields, specify the arguments (number and type parameters depending on the function), each of which may be a constant value, a field from the parent field set, or another global variable (see [“Chaining a Global Variable” on page 489](#)).
- 3 For relevant functions, you can verify that the arguments you entered in the Function and Arguments fields return the values you want by entering sample parameters in the *Preview* fields.

For details about how to fill out the Function and Arguments fields, see [“Variable Definition Fields” on page 1009](#).

Global Variable Editor: Local Variables Tab

Use the Local Variables tab to extract a value from a field that you want to use in the overall Global Variable.

- 1 Click **Add**. This launches the Add Local Variable editor.

- 2 In the Add Local Variable editor, enter a name for the local variable, specify a function, and add arguments (number and type parameters depending on the function).
- 3 Verify that the arguments you entered in the Function and Arguments fields return the values you want by entering sample parameters in the *Preview* fields.

For details about what to enter in the Function and Arguments fields, see [“Variable Definition Fields” on page 1009](#).

Creating a Global Variable from a Domain Field

You can define a set of fields outside the standard event schema for tracking activity pertaining to use cases beyond standard network security. You can create global variables on these user-defined domain fields for use anywhere that fields can be selected.



Create the domain field and add it to a domain field set first

Before creating a global variable for a domain field, make sure that the domain field you want to use is created and added to a domain field set. The domain field set is what makes the field available to the global variable editor.

- 1 In the Global Variable Editor > Attributes tab, give the global variable a name, type, and group.
- 2 In the Parameters tab, select a function and data type for the global variable function you are creating. For example, if you want to perform an arithmetic function, the domain field data type should be NUMBER.
 - a In the Arguments section, select the domain field from the Fields tab.
 - b Verify that the arguments you entered in the Function and Arguments fields return the values you want by entering sample parameters in the *Preview* fields.

Promoting a Local Variable to a Global Variable

If you have an existing resource (such as a field set or rule) that contains one or more local variables that you want to re-use in other resources, it is easy to convert that variable to a global variable.

This feature is available in the following resource editors: active channels, data monitors, field sets, filters, rules, and queries.

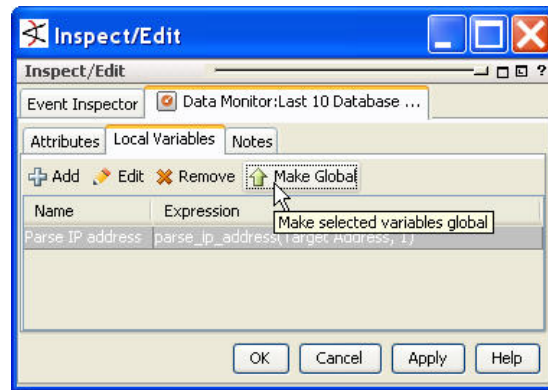


Local variables defined for data from events, actors, cases, and assets can be promoted to a global variable

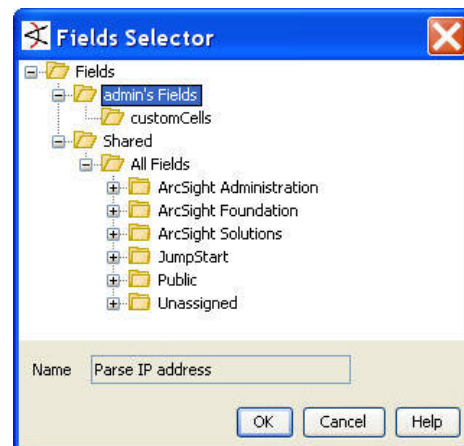
Local variables defined for a query viewer cannot be promoted to a global variable. Query viewers operate on queries, which have their own distinct schema for each instance. A local variable defined for a query viewer is likely only applicable to the specific query viewer it applies to.

To promote a local variable:

- 1 At the Local Variables tab in the resource editor, select the local variable you want to promote. This activates the Make Global button in the local variable toolbar.



- 2 Click the **Make Global** button. This launches the Fields Selector, where you can choose the group to which you want to save the global variable.

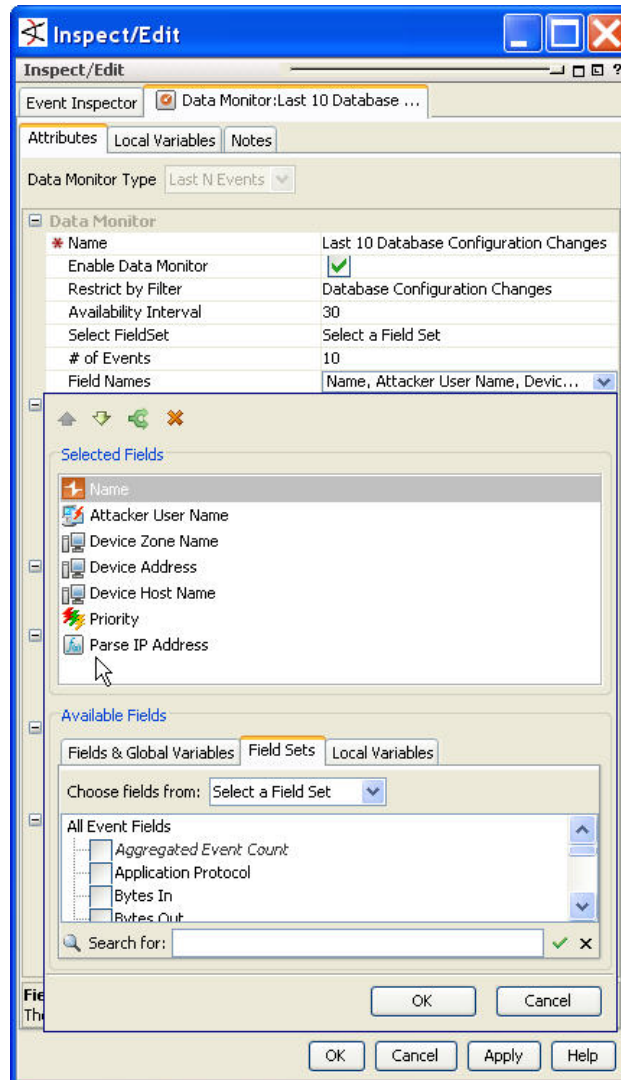


- 3 The system prompts you to decide whether to use the global variable you just promoted in the resource.

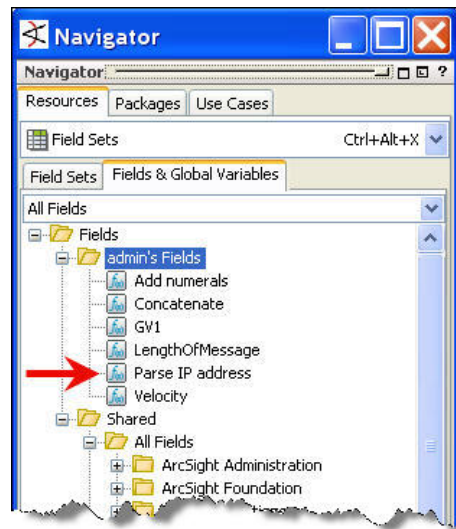


- ◆ Click **Yes** to promote the local variable to a global variable. This removes the variable from the local variables list and makes it available to the resource as a global variable.
- ◆ Click **No** to keep the variable local in the host resource.

If you opted to replace the local variable with the global version, you can see it by viewing the condition or selected fields tab, depending on what type of resource you are working in.



- 4 You can find the new global variable you just promoted from the global variables tree. Go to **Field Sets > Fields & Global Variables** and navigate to the group in which you saved the global variable.



The new global variable appears in the Variables hierarchy and be available for use in other resources.

A global variable may also chain (use as parameters) other variables that are local to a resource. A common use case is to create a complex chain of variables, and expose only the variable representing the final result as a global variable, keeping the chained intermediate variables local to their host resource.

Editing a Global Variable

To edit an existing global variable:

- 1 In the Navigator panel, go to **Field Sets > Fields & Global Variables**. Right-click the global variable you want to edit and select **Edit Field**.
- 2 In the Global Variable editor, you can only make edits to the group in which the global variable is stored, and the function parameters, since changes to the variable name and type could impact other resources that link to the variable.
- 3 Click **Apply** to save the global variable and leave the editor open, or click **OK** to save and close the editor.

Moving or Linking a Global Variable

A global variable can be moved or linked in the Navigator the same way other resources can be moved or linked. Global variables cannot be copied. For details, see [“Move, Copy, or Link a Resource” on page 120](#).

Deleting a Global Variable

To delete a global variable:

- 1 In the Navigator panel, right-click the global variable and select **Delete Field**.
- 2 At the confirmation dialog box, click **Delete**.

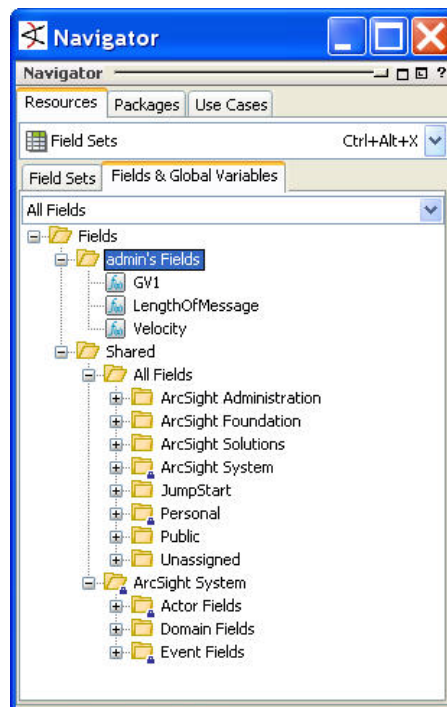
If any resources depend on this variable, a warning is displayed containing the URI of the impacted resources. You can override the warning and force-delete the variable. In such cases, the dependent resources are marked invalid; you can then edit those resources and remove any orphaned references.

Navigating to Global Variables

The console Navigator contains a new resource tab called Field Sets with a tab called Fields & Global Variables. This tab displays:

- Global variable resources defined by users and in standard content
- Standard event schema fields
- User-created domain fields (part of the Domain Field Sets feature described in ["Domain Field Sets" on page 491](#)).

Local variables contained in other resources are not displayed here.



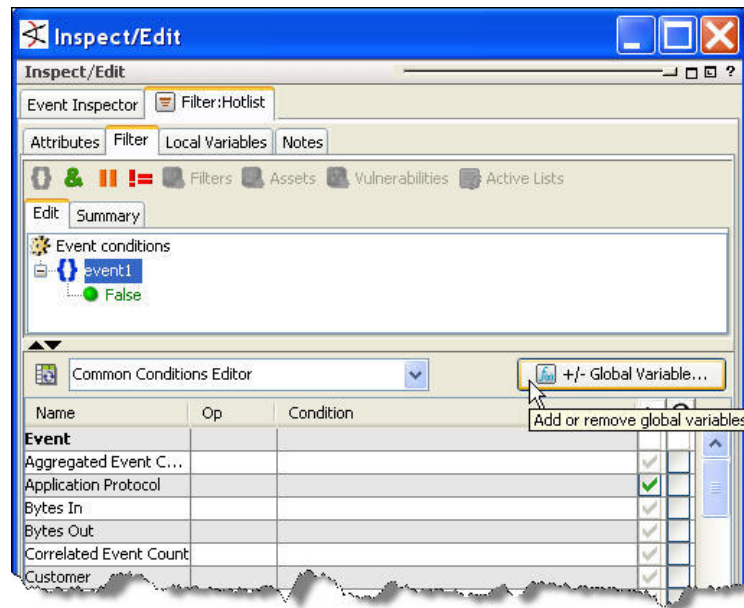
To view fields in the standard schema, including device custom fields, go to Fields & Global Variables > [All Fields/ArcSight System/Event Fields](#).

Adding a Global Variable to a Resource

You can add a global variable to any resource in which you can express a condition in any resource that uses the [Common Conditions Editor \(CCE\)](#), as well as data monitors and field sets. Global variables are made available to query viewers via the queries the query viewer is based upon.

Adding a Global Variable Using the CCE

Resources that use the CCE provide a button that enables you to add a global variable to a condition statement.



To add a global variable using the CCE:

- 1 In the CCE for a given resource, click the **+/- Global Variable** button.
- 2 On the Global Variable Selector dialog, select one or more variables you want to add and click **OK**.

Only variables whose schema type matches the given resource are displayed. For example, an actor-based global variable can be added to an actor-based query, not an event-based or other resource-based queries.

- 3 The added variables appear in the field list under the group selected for it in the Global Variables editor (such as the Variables group). You can use these variables in condition statements for this resource.

For details, see [“Adding or Removing Global Variables Using the CCE” on page 857](#) in the reference topic on the [Common Conditions Editor \(CCE\)](#).

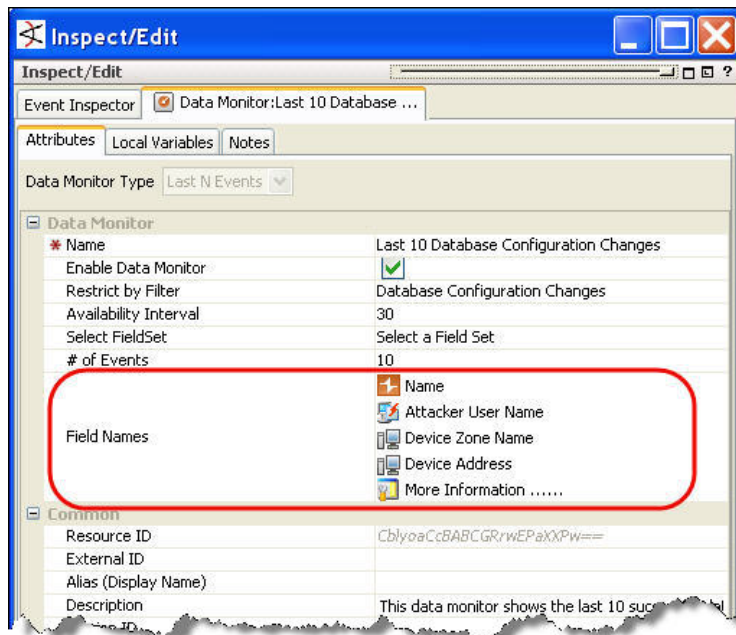
If the resource you are working in uses a field set that contains global variables, any global variable fields included in the selected field set are also available for selection in the CCE.

Adding a Global Variable to a Data Monitor

You can add a global variable to any fields-based data monitor on the attributes tab where fields are selected. Field-based data monitors include:

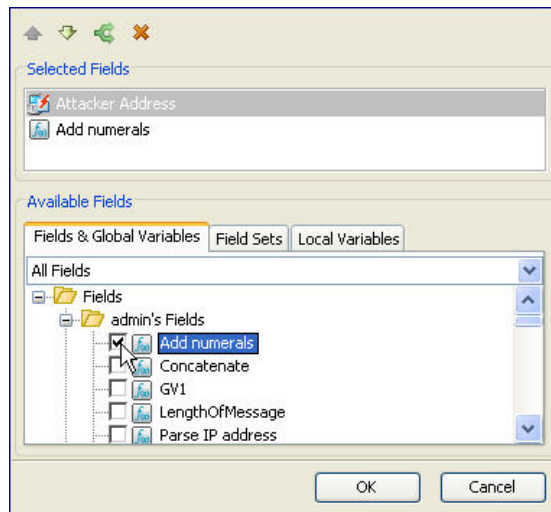
- Event graph
- Hierarchy Map
- Last N Events
- Last State
- Moving Average

- Statistics
- Top Value Counts (bucketized)



To add a global variable to a data monitor:

- 1 Go to **Dashboards > Data Monitors**. Either create a new data monitor (right-click > **New Data Monitor**) or edit an existing data monitor (right-click > **Edit Data Monitor**).
- 2 In the Data Monitor editor where you can select fields, click the value field to launch the field selector. The available fields vary depending on the type of data monitor you selected.
- 3 In the field selector, click the Fields & Global Variables tab and select an available global variable. Click **OK**.



For details about how to use the data monitor editor, see [“Using Custom View Dashboards”](#) on page 167.

Adding a Global Variable to a Field Set

You can also add a global variable to a field set. Once you add a global variable to a field set, whenever you apply that field set in a resource, you can select the global variable directly without having to add it first.

There are five different types of field sets:

- **Actor field set.** An actor field set contains only actor-related fields. Only a global variable created using actor fields can be added to an actor field set.
- **Asset field set.** An asset field set contains only asset-related fields. Only a global variable created using asset fields can be added to an asset field set.
- **Case field set.** A case field set contains only case-related fields. Only a global variable created using case fields can be added to a case field set.
- **Event field set.** An event field set is a named subset of available data fields from the security event schema.

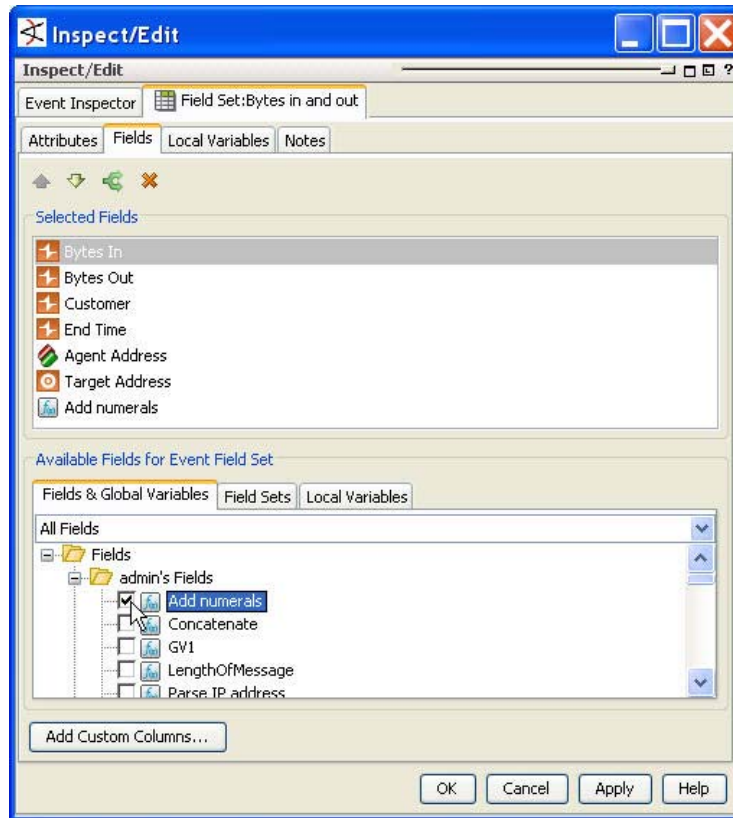


There are also domain field sets, but you cannot create a global variable using domain fields and you cannot add a global variable to a domain field set.

To add a global variable to a field set:

- 1 Go to **Field Sets > Field Sets**. Either create a new field set (right-click > **New Field Set**) or edit an existing field set (right-click > **Edit Field Set**).

- 2 In the Field Set editor Fields tab where you can select fields, click the Fields & Global Variables tab and select an available global variable. Click **OK**.



For details about creating a field set, see [“Creating a Field Set” on page 205](#).

Adding Global Variables to an Active Channel

When you initially create an active channel, you can only apply fields that are defined as a field set, either an existing one, or an ad hoc one you define one when setting up the active channel.


Global variables can only be added to an active channel from an existing field set that contains them. If an existing field set contains one or more global variables, those global variable fields become part of your active channel.

However, if you are defining the fields ad hoc from the New Active Channel dialog, the Define Grid Fields selector does not present global variable fields.



Viewing global variables in the Event Inspector

When you view events in an active channel and open an event that contains a global variable field in the Event Inspector, you may need to refresh the Event Inspector view to see the global variable fields, because the Manager processes global variable data differently from regular event data.

- If your Hide Empty Rows icon  is toggled on (so that empty rows are not displayed), you may not see the global variable field(s) in the event inspector.
- To refresh the view, de-select, then re-select the Hide Empty Rows icon.

Chaining a Global Variable

You can “chain” variables, that is, use one variable as a function parameter for another variable. The parent (outer) variable doing the chaining can be either a local or global variable.

A variable (local or global) may be chained inside another variable only if the child (inner) variable's return type is compatible with the outer variable's parameter type. For example, an ADD function variable can be chained inside a variable that takes a numeric parameter.

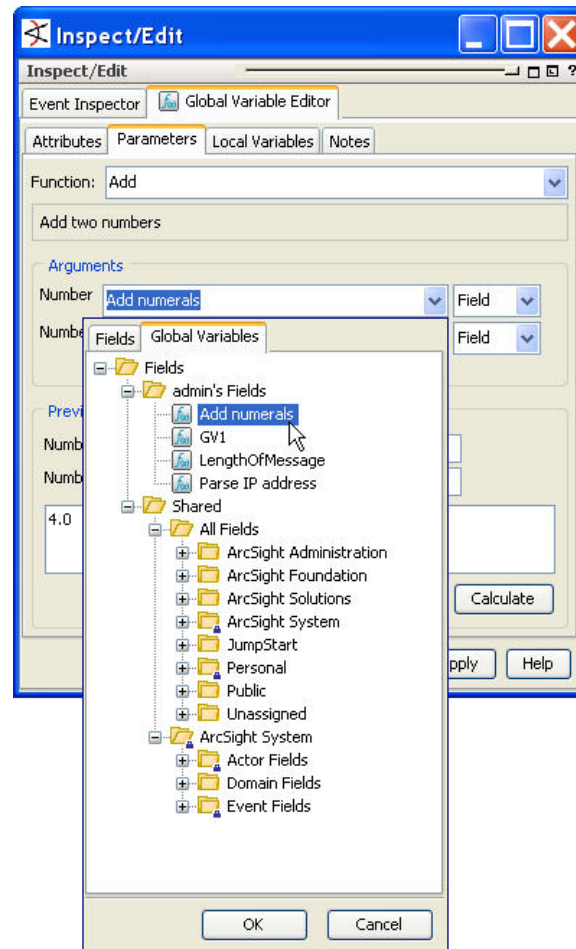


Create the inner variable first, and verify that its data type is compatible with the outer variable

Before making one variable a function parameter of another variable, create the inner variable first, and make sure that its data type is compatible with the function you want the outer variable to perform.

These steps assume you are chaining two global variables. You can also chain a global variable in the parameters of a local variable defined in the Local Variable tab of the Global Variable editor.

- 1 In the Global Variable Editor: Parameters tab, select a function that matches the data type of the global variable function you want to chain. For example, if you want to perform an arithmetic function, the child (inner) variable should be a NUMBER.



- 2 In the Arguments section, select the inner global variable from the Global tab.
- 3 Verify that the arguments you entered in the Function and Arguments fields return the values you want by entering sample parameters in the *Preview* fields.

In the case of global variables that perform lookups from Active or Session Lists, the nested sub-fields (representing the list columns) are also available for selection, provided the sub-fields are the required data type.

Global Variables in Standard Content

There is a library of global variables already defined that support actors and that cover basic event throughput scenarios.

Actors Global Variables

Standard content provides a series of global variables that support the actors feature in All Fields/ArcSight System/Actor Variables. These variables support the actors infrastructure, and are described in more detail in [“Actor Resource Framework Global Variables” on page 278](#).

Variables Library

There is a library of variables that deal with basic event throughput in [All Fields/ArcSight Foundation/Variables Library](#).

Device, Protocol, and Total Bytes Global Variables

The Device, Protocol and TotalBytes variables operate on commonly used root event fields, and are used in v5.0 and later standard content resources to reduce the number of columns processed while still returning all the relevant event data.

Asset Information Global Variables

Asset Information global variables present information related to a given asset (for example, zone, address, host/asset name, and so on).

Host Information Global Variables

Host Information global variables provide asset details for devices that are either not modeled in the network model as individual assets, or are represented in an asset range, and whose traffic is processed by devices that report to the Manager through SmartConnectors.

Timestamp Formats Global Variables

Timestamp Formats global variables provide a consistent way of displaying various timestamp data in some consistent formats, since different installations may use different formats (even from Console to Console in the same installation).

User Information Global Variables

User Information global variables are similar to the Asset and Host Information global variables, but are focused on the user, rather than a system. Since user information can be mapped to user name, user ID or both, it is useful to have the information combined for display and processing, so that you don't have reports with a lot of blank fields.

Chapter 18

Domain Field Sets

Domain field sets make it possible to monitor, correlate, and analyze events that pertain to different business verticals (domains), such as credit card transactions, online banking, or stock transactions, as well as traditional security use cases.

This topic describes domain field sets and the tools used to build them, and describes how to use them for monitoring events that pertain to different business verticals.

[“About Domain Field Sets” on page 491](#)

[“Implementing Domain Field Sets: Process Overview” on page 496](#)

[“Domain Modeling” on page 497](#)

[“Creating Domain Field Sets” on page 498](#)

[“Configuring FlexConnectors for Domains” on page 501](#)

[“Using Domain Field Sets in Correlation, Monitoring, and Investigation” on page 503](#)

About Domain Field Sets

ArcSight ESM's centralized schema and the correlation resources that leverage it have traditionally focused on providing an integrated view of the security status of relevant IT systems, and integrating security into your existing management processes and workflows.

But having events consolidated and normalized into a single schema and the power of ESM's correlation engine offers the opportunity to analyze event data for other business-related use cases beyond traditional network security.

Domain field sets are a construct in the centralized ESM schema that makes it possible to distinguish between events that pertain to different business verticals, such as credit card transactions, online banking, or stock transactions.

Once created, domain field sets make it easy to monitor, correlate, and analyze events for traditional security use cases and specialized business-related use cases.

The domain field sets feature is separately licensed, and requires some additional configuration on the Manager as well as FlexConnector development to supply the supported data.

Anatomy of Domain Field Sets

The ESM schema is the culmination of the normalization process, and the backbone of the data structure that drives ESM correlation. The 400+ data fields in the schema represent

attributes that are common across different types of devices, and attributes of certain ESM resources, such as assets, actors, and cases.

ESM has always preserved additional data processed by the SmartConnector that was not captured by the standard ESM schema as additional data, which is viewable in the Console from the [Event Inspector](#).

The domain field sets feature makes it possible to extend the standard ESM schema by binding the additional data from a device that you define in a FlexConnector to special *domain fields* you define. When you add the domain fields to a *domain field set*, your additional event data becomes available to view in channels and other resources, such as queries and rules.

How Domain Field Sets Work

ESM offers a series of special *domain fields*, which you can configure to identify a business-related attribute from additional data available in an event. When one or more of these domain fields is added to a *domain field set*, ESM can use it to evaluate incoming events and identify them as relevant to a particular business vertical or domain for event monitoring, investigation, and analysis.

A domain field can be a member of more than one domain.

When events come into the Manager, they are evaluated against the available domain field sets. If the event matches the fields in a domain field set, the event is tagged as relevant to that domain. Those domain fields defined for that event appear in the event inspector, and anywhere that domain field set is referenced.

To find the appropriate domain for an event, the Manager finds the one with the best fit:

- The Manager finds which of the additional data fields are domain fields.
- For all the candidate domains, the Manager selects the one with the most domain field hits. The relevance percentage must be at least 80%. That percentage is the number of matched fields divided by the total number of fields defined for the domain.
- If there is a tie, the selected domain is the one with the highest relevance percentage.
- If there is still a tie, it uses the oldest domain.
- If no matching domain can be found, the fields are left as additional data and the Manager specifies No Domain.

Like event fields and field sets, domain fields and field sets are also available for monitoring and investigation in active channels in the ArcSight Web interface.



Content, such as rules and filters, does not work if it uses a domain field and the domain field set is missing. If you export and import such content, either include the domain field set in the package, or make sure that the domain field set pre-exists on the import system.

Standard ESM Schema: the Static Schema

The standard ESM schema, also referred to as the “static schema,” is the traditional set of 400+ fields used to normalize event data from devices and applications across the network. The data fields included in the basic ESM schema are discussed in more detail in [“Data Fields” on page 867](#).

The standard ESM schema can also accommodate additional data from the SmartConnector using *device custom fields*, which can be used to extend the ESM schema with attributes not captured by the base schema for simple use cases.

Device Custom Fields

Device Custom fields are extra fields in the ESM schema reserved for attributes generated by a device that the schema does not already capture. These fields are defined by ArcSight or by a SmartConnector author who develops custom SmartConnectors to customer specifications. Each Device Custom field binds additional data to the ESM schema using a label-and-value pair, which can be used in filters, rules, or data monitors to make correlation more specific.

Previous releases of ESM offered 11 Device Custom label+value pairs for three different data types. ESM v5.0 keeps these same Device Custom fields, and adds two new data types to the original three:

Label	Data type	Quantity
Date	Date/Time	2
Number	Long	3
String	String	6
IPv6 (new for v5.0)	IPv6	4
Floating Point (new for v5.0)	Floating Point	4

All custom string fields have been expanded in ESM v5.0 from 1023 bytes to 4000 bytes.

For a complete list of the device custom fields ESM supports, see [“Device Custom Group” on page 880](#).

Device Custom fields are generally adequate if you are monitoring for use cases that fall into a single business vertical, such as standard network security.

Domain Fields: the Dynamic Schema

For business environments that must support monitoring, investigation, and analysis for use cases in multiple business verticals, the domain field sets feature enables users to define those business verticals using the fields unique to their devices and operating environments. Domain fields are “dynamic,” because they can mean different things for different events depending on the domain an event belongs to. When selecting a domain field, you first select the Domain field set, so domain fields must be part of a field set to be used.

The domains schema is made up entirely of user-configurable data fields that support the data types shown in the table below. The feature also offers significantly more label+value

pairs than standard device custom fields, and enables you to customize the name of the label to make it easier to identify them according to function.

Data type	Quantity	Description
Date	6	<p>Values that represent dates ranging from January 1 of the year 0001 through December 31 of the year 9999, and times from 12:00:00 AM (midnight) through 11:59:59 p.m.</p> <p>ESM supports the following date formats:</p> <p>02/09/2010 13:35:53.000 -0800</p> <p>02/09/2010 13:35:53.000</p> <p>02/09/10 1:35:53.0 PM</p> <p>2/9/10 1:35 PM</p> <p>2/9/10 1:35:53 PM</p> <p>2/9/10 1:35:53 PM PST</p> <p>2/9/10 1:35:53 PM PST</p> <p>Feb 9, 2010 1:35 PM</p> <p>Feb 9, 2010 1:35:53 PM</p> <p>Feb 9, 2010 1:35:53 PM PST</p> <p>Feb 9, 2010 1:35:53 PM PST</p> <p>February 9, 2010 1:35 PM</p> <p>February 9, 2010 1:35:53 PM</p> <p>February 9, 2010 1:35:53 PM PST</p> <p>February 9, 2010 1:35:53 PM PST</p> <p>Tuesday, February 9, 2010 1:35 PM</p> <p>Tuesday, February 9, 2010 1:35:53 PM</p> <p>Tuesday, February 9, 2010 1:35:53 PM PST</p> <p>Tuesday, February 9, 2010 1:35:53 PM PST</p> <p>09 Feb 2010 13:35:53 PST</p> <p>Feb 09 2010 13:35:53</p> <p>02/09/2010</p>
Number	13	Whole numbers containing no decimals.
String	34	A flexible sequence of up to 4000 characters.
IPv6 Address	4	A sequence of characters that represent an address in IPv6 format.
IPv4 Address	4	A sequence of characters that represent an address in IPv4 format.

Data type	Quantity	Description
Floating Point	8	<p>Double-precision numeric fields with decimal points that can appear in different places.</p> <p>NOTE: The way Java processes floating point numbers may sometimes produce imprecise results in situations where numbers are rounded off for display purposes.</p> <p>For example, (2.0 - 0.1) will be displayed as 1.9, but the actual result will be 1.8999999999999999.</p> <p>Such accuracy differences are a well-known issue with binary floating point representations.</p> <p>Be aware of this when using floating point fields, especially when using the Equals (=) operand.</p> <p>Further information about the Java implementation of the IEEE 754 Standard for Binary Floating-Point Arithmetic can be found here: http://java.sun.com/docs/books/jls/third_edition/html/typesValues.html#4.2.3.</p>
CLOB	4	<p>Character Large Object fields, such as text, memo or long character fields.</p> <p>ESM displays the first 4000 characters of CLOB data in the event inspector, but it is not available for viewing or correlation operations.</p>
BLOB	4	<p>Binary Large Object fields, such as images, audio or other multimedia objects.</p> <p>BLOB data is stored in the database, but is not operable, and thus is not available for viewing or correlation operations.</p>
Resource Reference	4	<p>Event fields used for internal ESM audit events that need to refer to an ESM resource.</p> <p>Event attributes (event name, URI, event ID, and external ID) are presented in a single string.</p>

Example Scenarios for How to Apply Domain Field Sets

To illustrate how the domain field sets feature works, we'll use the example of a company that needs to monitor and investigate event traffic for potential fraud involving credit card transactions and online banking.

In this scenario, you might want to create the following domain fields for two business scenarios: Credit Card Transactions, and Online Banking. Data types for each field are included in parentheses. The fields in bold are fields the domain field sets share in common.

Credit Card Transactions	Online Banking
Credit card number (Number)	Bank account number (Number)
Credit card account number (Number)	Transaction amount (Floating Point)
Transaction amount (Floating Point)	Transaction currency (String)
Transaction currency (String)	Authorization required (String)

Credit Card Transactions	Online Banking
SSN (String)	Authorization ID (Number)
	Authorization Server (IP Address)
	SSN (String)

None of these fields are part of the standard ESM schema, but the domain field sets feature enables you to add these fields to the ESM schema. These additional fields officially become a domain when they are added to a domain field set.

We'll use this example in ["Using Domain Field Sets in Correlation, Monitoring, and Investigation" on page 503](#) to demonstrate how to model domain field sets, how to create them, best practices for handling shared domain fields, and how to leverage domain fields in ESM resources for monitoring, investigation, and analysis.

Implementing Domain Field Sets: Process Overview

Implementing the domain field sets feature is a process that requires some preparation. This section provides an overview of preparing for and implementing the domain field sets feature.

- 1 **Obtain license.** The domain field sets feature is a separately licensed feature. To activate The domain field sets feature in your environment, contact ArcSight Customer Support.

- ◆ For new ESM installations, the license is applied using the Manager Setup tool during ESM installation.
- ◆ For existing ESM installations, the license is applied using the Manager Setup tool and restarting the Manager.

For details about these processes, see the *ESM Installation and Configuration Guide* for new installations, and the *ESM Upgrade Guide* for existing ESM installations.

- 2 **Assign user permissions.** By default, the Admin user has permission to create domain fields and domain field sets. The Admin user can assign permissions for Domain Authoring and read/write privileges for domain fields and domain field sets to other users.

The Admin user can grant Domain Authoring rights to any user group.

- a In the Navigator panel, go to Users.
- b Right-click the user group to which you want to grant domain authoring privileges and select **Edit Access Control**.
- c On the Operations tab, click **Add...** and check the [/All Permissions/ArcSight System/Domain/Author](#) permission.

- 3 **Model the domain use case.** This is a planning process that involves knowing the business use case you want to address, then identifying the data fields you need from devices, and the data types best suited for them. For example, you may be interested in discovering potential credit card fraud by tracking particular attributes of credit card transactions. This process is described in more detail in ["Domain Modeling" on page 497](#).
- 4 **Create domain fields.** Define the domain fields you need using the Domain Fields editor as described in ["Creating Domain Fields from the Console" on page 498](#).

- 5 **Create domain field sets.** Create a domain field set for each situation you want to monitor (such as credit card or online banking transactions). For complete instructions about how to create domain field sets, see [“Creating Domain Field Sets from the Console” on page 500](#).
- 6 **Develop FlexConnector(s) to send additional data.** To leverage domain field sets for devices that do not currently report to ESM using an standard ArcSight SmartConnector, you can build a FlexConnector, or modify an existing one. For an overview of how to accommodate the additional data types supported by domain field sets, see [“Configuring FlexConnectors for Domains” on page 501](#). For complete instructions about how to develop a FlexConnector with the additional fields required to support your domain use case, see [“Configuring a Connector for ArcSight ESM Domain Field Sets” in the *ArcSight FlexConnector Developer’s Guide*](#).

To leverage domain field sets for devices that report to ESM using a standard ArcSight SmartConnector, contact ArcSight Professional Services, or your ArcSight representative.
- 7 **Leverage domain fields and domain field sets in content.** You can use domain fields and domain field sets for correlation, monitoring, and investigation. For details about how to use domain field sets, see [“Using Domain Field Sets in Correlation, Monitoring, and Investigation” on page 503](#).

Domain Modeling

Domain modeling is concerned with understanding the use case you want to track, then identifying the data you need to track it, the devices that send the data, and the data types best suited for processing that data. Once this information is modeled in detail, you can use it to create the necessary domain fields and field sets in ESM, and develop the relevant FlexConnector(s) to send the additional event data using the appropriate data type to the ESM Manager.

The objective of domain modeling is to identify:

- The devices that will send the information you’re interested in
- The exact name and data type of the event attributes you’re interested in. The field name you give to a particular attribute from a device in the FlexConnector must be the exact name you enter in the domain field editor for that field. This process is case sensitive.

For example, if you named the social security number field “SSN” in the domain field editor, you must enter `SSN` as the field name in the FlexConnector. `Ssn` or `ssn` will not work.



Caution

Know your field names and data types before configuring the FlexConnector

When developing a FlexConnector, you set the exact name of the field and its data type that you want to add as a domain field to the ESM schema.

Data types cannot be changed once an event reaches the Manager, so be sure to set the data type to one that’s appropriate for the type of data you’re collecting.

For more about the data types available for domain fields, see [“Domain Fields: the Dynamic Schema” on page 493](#).

For instructions about how to accommodate the additional data types supported by domain field sets, see [“Configuring FlexConnectors for Domains” on page 501](#).

Creating Domain Field Sets

This topic describes how to create domain fields and domain field sets, and how to use them once they are added to ESM.

The process of creating a domain field set involves creating domain fields, then binding them to a domain field set. Once domain fields are created, they can be leveraged for correlation, monitoring and investigation only when they are added to a domain field set.

Admin users and those who have been granted Domain Authoring privileges can create domain fields and domain field sets.



Note

Domain Authoring privileges are required to add domain fields and domain field sets

By default, the Admin user has full privileges to add domain fields. The Admin user can grant Domain Authoring permission and read/write privileges for domain fields and domain field sets to other users.

For basic instructions, see [Step 2](#) in “Implementing Domain Field Sets: Process Overview” on page 496.



Note

Domain fields and field sets can only be created in /ArcSight System

To ensure that only those with the correct permissions have access to domain feature resources, Admins and those with Domain Authoring privileges can create domain feature resources in the [/ArcSight System](#) folder only:

- Domain fields: [/All Fields/ArcSight System/Domain Fields](#)
 - Domain field sets: [/All Field Sets/ArcSight System/Domain Field Sets](#)
-

Creating Domain Fields from the Console

Admin users and those with Domain Authoring privileges can create a domain field in the [/All Fields/ArcSight System/Domain Fields](#) group.

- 1 In the Navigator panel, go to **Field Sets** and select the **Fields & Global Variables** tab.
- 2 Navigate to [/All Fields/ArcSight System/Domain Fields](#). Right-click **Domain Fields** or any group in this branch in which you want to create the new field, and select **New Domain Field**.
- 3 In the Domain Field Editor in the Inspect/Edit panel, enter attributes for the field, assign it to one or more existing field sets (or assign the field to a new field set when creating a field set later), and click **OK**.

Domain Field Editor: Attributes Tab

This topic describes the attributes to enter in the Attributes tab of the Field Editor when creating a domain field using the Console.



Caution

Field Name Must Match Data from FlexConnector

The name you enter for the field must match the field name for the data coming from the FlexConnector. For example, if the field for social security number is called SSN on the device, enter SSN for the field name.

For domain modeling tips, see “[Domain Modeling](#)” on page 497.



Domain field attributes cannot be changed once created

Data entered in the domain field Attributes tab cannot be changed once changes to the domain field are applied or saved. After a domain field is created, you can add or remove field sets the domain field belongs to from the Field Sets tab.

Domain Field Attribute	Description
Name	<p>Enter the name for the field.</p> <p>The name of the field must match the field name for the data coming from the FlexConnector. For example, if the field for Social Security Number is called SSN, enter SSN here.</p> <p>A domain field name cannot be the same as another domain field name, even if it is created in a different group.</p> <p>NOTE: Special characters exclamation point (!), <space>, and ampersand (&) are rendered internally by ESM as an underscore (_). If you create multiple domain fields with these characters as the only difference (for example, DF!20, DF 20, DF&20), the system sees all these as the same field name and it will only create the first field.</p> <p>NOTE: Domain field names cannot be SQL or Oracle keywords.</p> <p>NOTE: Once changes to the domain field are applied or saved, the name cannot be changed.</p>
Data Type	<p>From the drop-down menu, select the data type of the field:</p> <ul style="list-style-type: none"> • BLOB • CLOB • DATE • FLOATING POINT • IP ADDRESS • IPv6 ADDRESS • NUMBER • RESOURCE REFERENCE • STRING <p>For a description of these data types, see “Domain Fields: the Dynamic Schema” on page 493.</p>
Field Type (Usage)	<p>When creating a domain field from the ArcSight System/Domains folder, the field type Domain is automatically selected and cannot be edited.</p>

For a description of what to enter in the Common fields, see [“Common Resource Attribute Fields” on page 684](#).

Domain Field Editor: Field Sets Tab

The field sets tab enables you to add the field you are creating or editing to one or more existing field sets. Domain fields can be added to domain field sets or event-based field sets only.

If the field set to which you want to add the domain field does not yet exist, you can create the field set later and add the field to that field set through the Field Set Editor. For more about using the Field Set Editor, see [“Creating Domain Field Sets from the Console” on page 500](#).

To add the domain field you are creating or editing to an existing domain field set:

- 1 In the *Available Field Sets* panel, navigate to the field set to which you wish to add the field.
- 2 Select the field set by checking its checkbox. The field set will appear in the *Selected Field Sets* panel.
- 3 Click **Apply** to add the field to the selected field set(s).
- 4 To remove the field from a selected field set, click the field set in the *Selected Field Sets* panel and click the delete button (✕).
- 5 When you are finished editing the field attributes, click **OK** to close the Field Editor.

Deleting a Domain Field

- 1 In the Navigator panel at the Fields and Global Variables tab, right-click the domain field you want to delete and select **Delete Field**.
- 2 In the confirmation dialog box, click **Delete** to delete the field.



If you have already received events associated with a deleted domain field...

If you have already received events with that field, you can still delete that field. The event data pertaining to that field will be stored in the ESM database, but it will not be available for display.

Creating Domain Field Sets from the Console

Admins and users with Domain Authoring privileges can create a domain field set in the [/All Field Sets/ArcSight System/Domain Field Sets](#) group.

- 1 Domain field sets can only be created in the [All Field Sets/ArcSight System/Domain Field Sets](#) group, or subfolders within this group, by the Admin user and users who have been granted Domain Authoring privileges.

Existing domain field sets cannot be copied into any group.

To create a domain field set, right-click the group in the [ArcSight System/Domain Field Sets](#) branch and select **New Field Set**.

- 2 In the Field Set Editor in the Inspect/Edit panel, enter attributes for the field set and assign it one or more existing domain fields.
- 3 Click **Apply** to save the field set in the resource tree and continue editing. Click **OK** to save the field set in the resource tree and close the editor.

For details about what to enter in each field of the Field Set Editor, see the next section, [“Field Set Editor: Attributes Tab” on page 501](#).

Field Set Editor: Attributes Tab

The attributes tab is where you name the field set and specify what type of field set it is.

Field	Description
Name	Enter a name for the field set that identifies what it represents.
Type	The type Domain Field Set is set by default and is read-only.

For a description of what to enter in the Common fields, see [“Common Resource Attribute Fields” on page 684](#).

Field Set Editor: Fields Tab

The Fields tab is where you add existing domain fields to the domain field set. (For instructions about how to create a domain field, see [“Creating Domain Fields from the Console” on page 498](#).)




- Fields and Global Variables tab.** In the Fields and Global Variables tab in the *Available Fields for Domain Field Set* panel, select the existing domain fields you want to add to this field set.



Global Variables are not available to domain field sets.

You can only add existing domain fields to a domain field set.

The selected field will appear in the *Selected Fields* panel.

- ◆ To re-order the fields in the list, select a field and use the up /down  arrows to place it in the desired order.
- ◆ To remove the field from the list, select the field and click the delete button .

- Field Sets Tab.** Other field sets cannot be added to a domain field set.
- Local Variables tab.** Local variables cannot be added to a domain field set.
- Click **Apply** to add the selected domain field(s) to the domain field set. Click **OK** to close the Field Set Editor.

Field Set Editor: Local Variables Tab

Local variables cannot be added to domain field sets, and this tab is unavailable for edit.

Configuring FlexConnectors for Domains

To leverage domain field sets for devices that do not currently report to ESM using a standard ArcSight SmartConnector, you can build a FlexConnector, or modify an existing one.

To leverage domain field sets for devices that report to ESM using a standard ArcSight SmartConnector, contact ArcSight Professional Services, or your ArcSight representative.

Before developing a FlexConnector or modifying an existing one to send additional data to support domains, first model your domain scenarios as outlined in [“Domain Modeling” on page 497](#), and create the domain fields and domain field sets that will consume the additional data as described in [“Creating Domain Field Sets” on page 498](#).

With ESM v5.0, supported data types are listed below. The names used for the supported data types in the FlexConnector are listed on the left; the corresponding names used for those same data types in the ESM Console are listed on the right.

Data type (FlexConnector)	Data type (Console)
String	String
Long	Long
TimeStamp	Date
IPAddress	IPv4Address
Integer	Number
IPv6Address	IPv6Address
Double	Floating Point

You can modify an existing FlexConnector or create a new FlexConnector to take advantage of the fields you have defined as part of the domain field set. For example, you may have created a domain field set as follows for credit card transactions:

Field	Type
Credit Card Number	Integer (Number)
Transaction Amount	Double (Floating Point)
Currency	String
Transaction Host IP	IPv6Address
Transaction Time	TimeStamp (Date)

You can add mappings for these fields in the FlexConnector parser as additional data fields.

For example, for this sample domain field set, you can add the following entries to the FlexConnector parser you are developing:

```
token[0].name=Credit Card Number
token[0].type=Integer

token[1].name=Transaction Amount
token[1].type=Double

token[2].name=Currency
token[2].type=String

token[3].name=Transaction Host IP
token[3].type=IPv6Address

token[4].name=Transaction Time
token[4].type=TimeStamp

additionaldata.Credit Card Number=Credit Card Number
additionaldata.Transaction Amount=Transaction Amount
additionaldata.Currency=Currency
additionaldata.Transaction Host IP=Transaction Host IP
additionaldata.Transaction Time=Transaction Time
```

The connector processes the additional data fields with the data type you assigned along with the token names.

Start the FlexConnector to begin the flow of additional data to ESM.

Using Domain Field Sets in Correlation, Monitoring, and Investigation

This section provides details and examples about how to use domain fields and domain field sets in different types of ESM resources for correlation, monitoring and investigation, and reporting.

Where to Find Domain Fields in the Event Inspector and Field Selectors

You can find domain fields in different places, depending on the context you are working with.

Where to Find Root Domain Fields in Field Selectors

You can find domain resource fields that describe the general attributes of a domain (for example, domain name and ID) among the Root fields in field selectors in the CCE and relevant right-click context menus.

Where to Find User-Created Domain Fields in Field Selectors

Finding the domain fields you created depends on the context from which you are selecting them.

- In some context field selectors, the domain field set appears as one of the groups from which you can select fields.
- In other contexts, you can find the domain fields by selecting the domain field set they belong to from the field set selector.
- When looking at event(s) in channels, domain field(s) will be displayed if they are relevant to the event(s).

Using Domain Fields and Field Sets for Correlation

Using the example outlined in [“Example Scenarios for How to Apply Domain Field Sets” on page 495](#), you can create a rule that detects if there are 3 or more credit card transactions over \$500 from the same SSN within 5 minutes, and put the matching SSNs into an active list.

- 1 First, create the active list with these attributes:

Field	Value
Name	Suspicious Credit Card Activity
Data	Select the Field based radio button
Fields	Create a new field called “SSN” with the data type <code>string</code> . The field name you enter here is used as a label within this active list to identify the data that will be displayed in this column. The name you enter here does not have to match the domain field names, but it is recommended that the name you use help you identify the data that goes in this column.

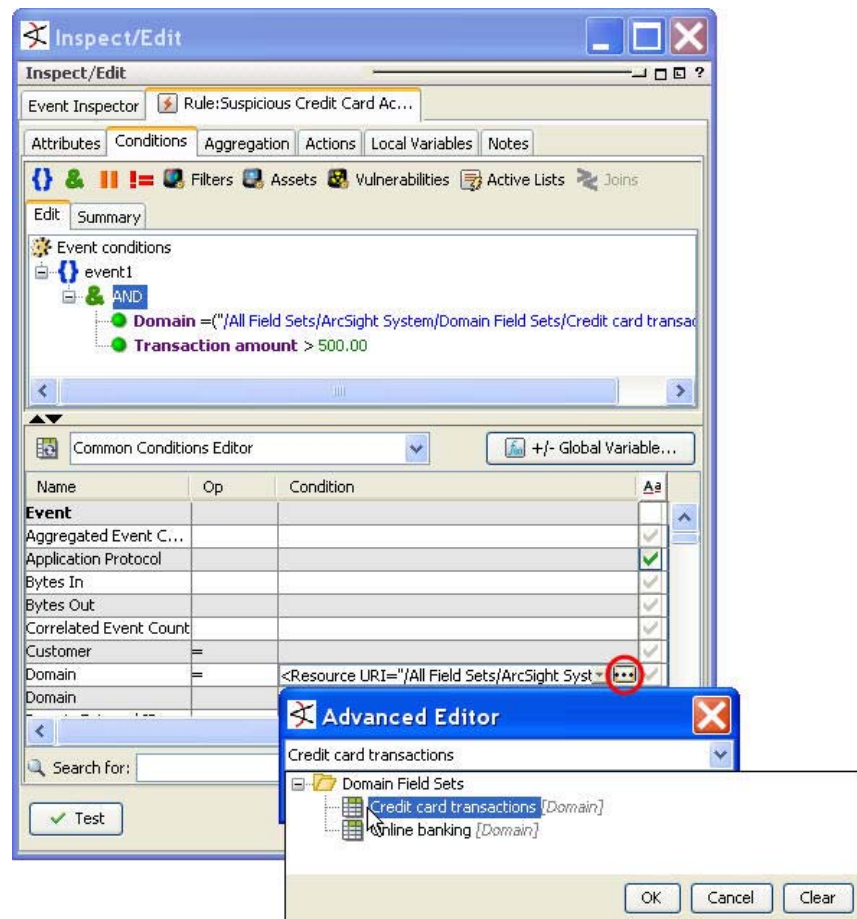


No Mapping Available for Active List Field of Type Integer

ESM currently provides no domain field mapping for active list or session list fields of the data type 'integer'. To map domain fields with the data type 'number' to an active list or session list, use the data type 'long.'

- 2 Next, create a rule that detects three credit card transactions over \$500 from the same SSN in an hour.
 - a Adding a condition that operates on a domain is a two-step process: first specify the domain field set to which the condition applies, then express the condition you want to perform on the domain data.

Field	Value
Field set drop-down menu	Start with the Common Conditions editor field set.
Condition	Specify the domain to which this condition applies by adding the following condition: <code>Domain = <domain field set ESM resource ID></code> Use the drop-down menu in the condition side to launch the Advanced Editor, from which you can select your Credit Card Transactions field set.
Field set drop-down menu	Select the domain field set you created for credit card transactions.
Condition	For Transaction Amount, select the greater than operator (>) and enter 500 in the Condition field.



- b** In the Aggregation tab, set number of matches to 3, timeframe to 5 minutes, and aggregate on identical **SSN** fields.

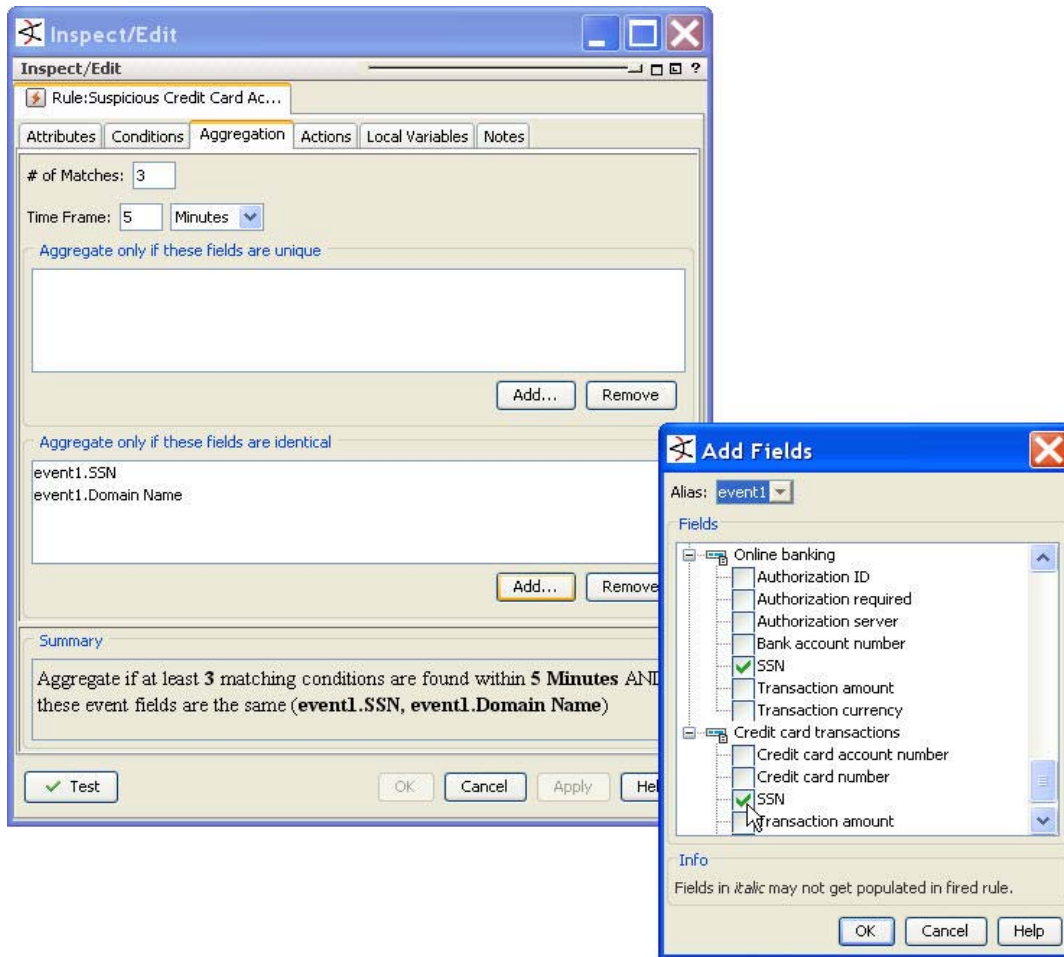
In the Add Fields dialog, find the **SSN** field in the domain field set you created for credit card transactions at the bottom of the pick list, past the groups.

Because the fields associated with the domain field set are going to be displayed in the active list, add the Domain Name attribute to the Aggregate statement.



ESM will prompt you to add the Domain Name field

If you forget to add the Domain Name field to the aggregation statement, ESM will offer to you add it for you, since the domain's derived fields are going to be added to the active list.



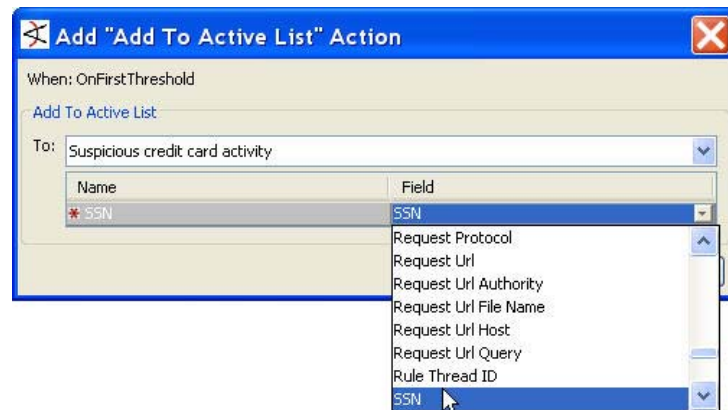
Shared domain fields appear as selected in all the domain field sets of which they are a member.

If a domain field is shared among multiple domain field sets, the domain field appears as selected in all the domain field sets of which it is a member.

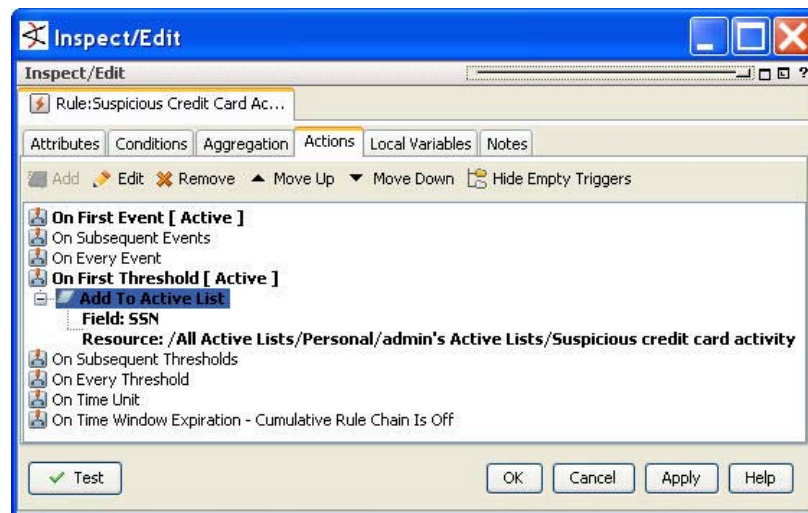
The example above shows the SSN field selected in both the Credit card transactions and Online banking field sets, even though it was selected from the Credit card transactions domain field set.

- c At the Actions tab, select the **On First Threshold** trigger and select **Add > Active List > Add to Active List**, and select the *Suspicious Credit Card Activity* active list you created in step 1. Select the SSN field to be added to the active list.

In the Add Action dialog, select the SSN field you created from the pick list.



The resulting trigger should look like this:



- d** To activate the rule on events, link the rule to the Real-Time Rules folder (drag-and-drop > link).

Using a Domain Field in a Global Variable

You can create a global variable for a domain field. For example, you can create a global variable that finds SSNs with 1234 as the last four digits.

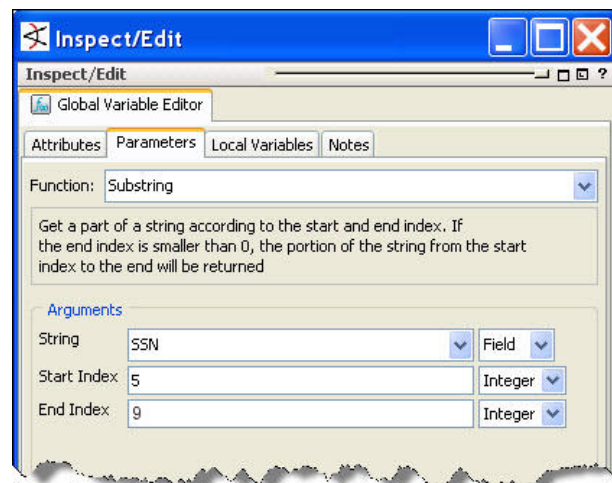
- 1** In the Navigator panel, go to **Field Sets > Fields & Global Variables**.
- 2** Right-click a group, such as <User's> Fields, and select **New Global Variable**.
- 3** In the Global Variable editor in the inspect/edit panel, define the attributes for a global variable that will find SSNs with the last 4 numbers in common.
 - a** In the Attributes tab, define the global variable's attributes.

Field	Value
Name	LastFourSSN

Field	Value
Type	Select Event Global Variable . Domain fields will come into ESM as part of the event stream from certain ESM-monitored devices.

- b** In the Parameters tab, select the function and parameters you want the global variable to perform.

Field	Value
Function	Category: String Function: Substring
Arguments	String (Type: Field): From the drop-down menu, navigate to the SSN domain field, which will appear alphabetically in the list of available fields. Start Index (Type: Integer): 5 End Index (Type: Integer): 9 Note: This example assumes that the data contains no dashes between the SSN elements. If the data contains dashes, adjust these numbers to accommodate the extra characters.



- 4** Once created, the global variable can be added to a condition expressed in the CCE, `LastFourSSN=1234`. For more details, see [“Adding a Global Variable to a Resource” on page 484](#).

What Correlation Functions Support Which Data Types

Some of the fields added for ESM v5.0 are only supported by certain correlation functions. The matrix below describes which functions support which field.

Correlation Function	Domain Fields	Custom Fields	Floating Point	IPV6	CLOB	BLOB
Event-based active list		X	X			
Field-based active list	X	X	X			
Rule aggregation fields unique	X	X	X	X		
Rule aggregation fields identical	X	X	X	X		
Rule editor conditions tab InActiveList (Field based AL)	X	X	X			
Set event field action	X	X	X	X		
Add to active list action	X	X	X			
Trends on query with active lists	X	X	X			
Query viewer	X	X	X	X		
Query	X	X	X	X		
Filter	X	X	X	X		
Pattern Discovery		X	X			
Active Channel	X	X	X	X		
Report	X	X	X	X		
Data Monitor	X	X	X	X		

Chapter 19

Use Cases

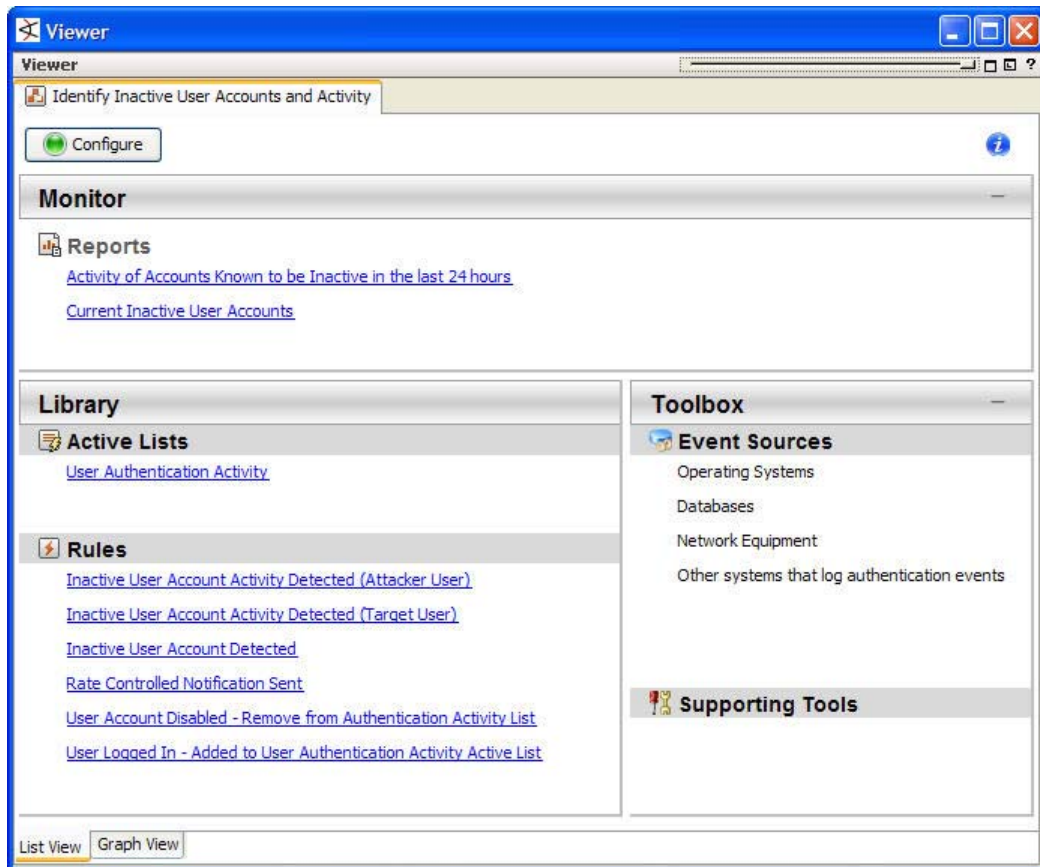
Use cases are a way to view, configure, and transport specially developed sets of related resources that address specific security issues and business requirements.

[“About Use Cases” on page 511](#)
[“Navigating to Use Cases” on page 513](#)
[“Master Use Cases” on page 513](#)
[“Standard Use Cases” on page 514](#)
[“Installing Use Cases” on page 516](#)
[“Viewing and Using Use Cases” on page 517](#)
[“Configuring Use Cases” on page 518](#)
[“Configuration Panels” on page 525](#)

About Use Cases

Use cases are special ArcSight content groupings that provide an integrated console-based alternative for viewing and interacting with resources to the standard one-resource-at-a-time viewing method offered in the Resource tree of the Navigator panel. Use cases also make it easy to configure shared resources in a single operation, and to export related resources in an ArcSight Resource Bundle for use in other ArcSight instances. Use cases are currently available only for ArcSight-provided content.

The example below shows all the resources that make up a comprehensive use case for monitoring inactive users. The resources are organized into the function they serve: monitoring resources, a library of correlation resources that drive the use case, and a toolbox of supporting tools, including event sources.



From this centralized home page, you can monitor the dashboards and channels, edit the filters, field sets, and data monitors, view the associated event sources and notification destinations, and perform other relevant workflow tasks related to the use case.

ArcSight provides use cases delivered in ArcSight Resource Bundles (.arb) ready to be installed from the `ARCSIGHT_HOME/current/jumpstart` directory. The Jumpstart directory delivers ArcSight start-up content designed to streamline the process of getting your environment customized and online analyzing events quickly. Learn more about the ArcSight Express use cases and those provided in the jumpstart directory in [“Standard Use Cases” on page 514](#).

For resources that require configuration with values specific to your operating environment, the Use Cases feature provides a Use Case configuration wizard to configure them in a simple, centralized operation as described in [“Configuring Use Cases” on page 518](#).



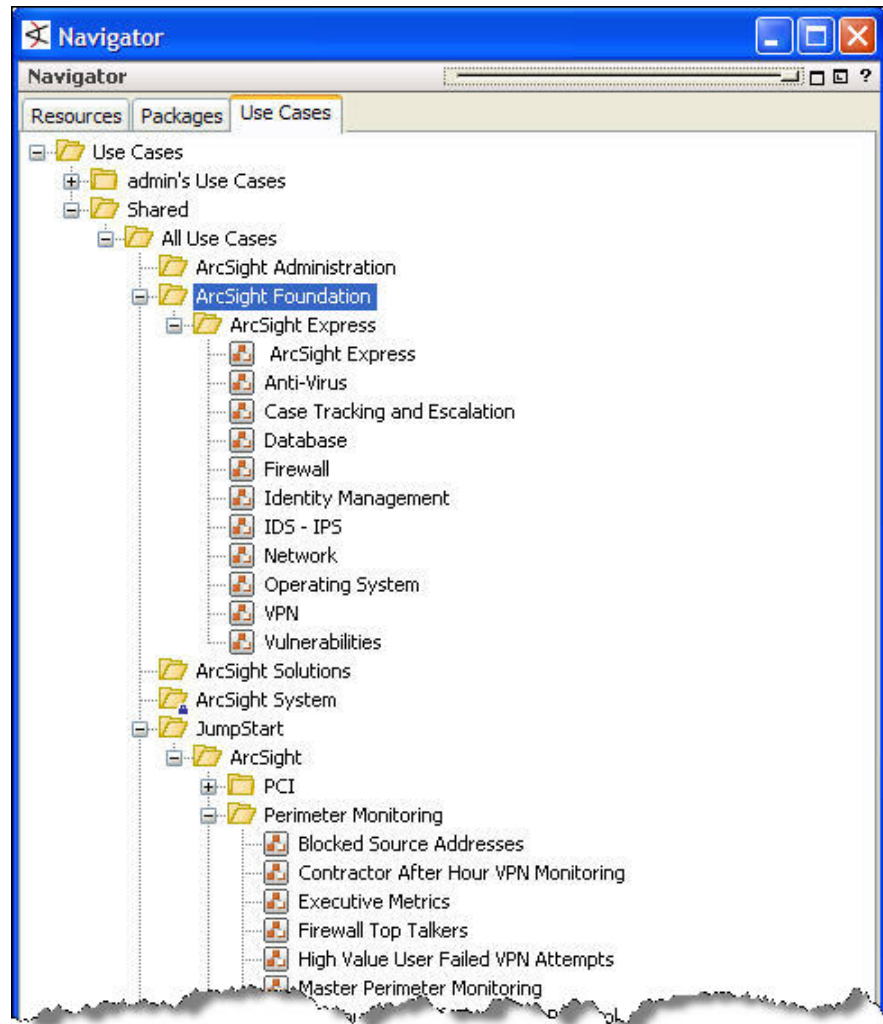
Note

Users with Admin privileges should use Configuration wizard

Because many different types of resources are included in a given use case from many different locations in the individual resource trees, ArcSight recommends that only users with Admin privileges run the use case configuration wizard. This ensures that the user performing the configuration has adequate permissions to access the configurable resources.

Navigating to Use Cases

Like packages, use cases span resources, so they are presented in their own tab in the Navigator panel parallel with resources and packages. The example below shows the standard use case resources installed automatically with ArcSight Express in the ArcSight Foundation tree, and the Perimeter Monitoring use case available for installation as a Jumpstart package.



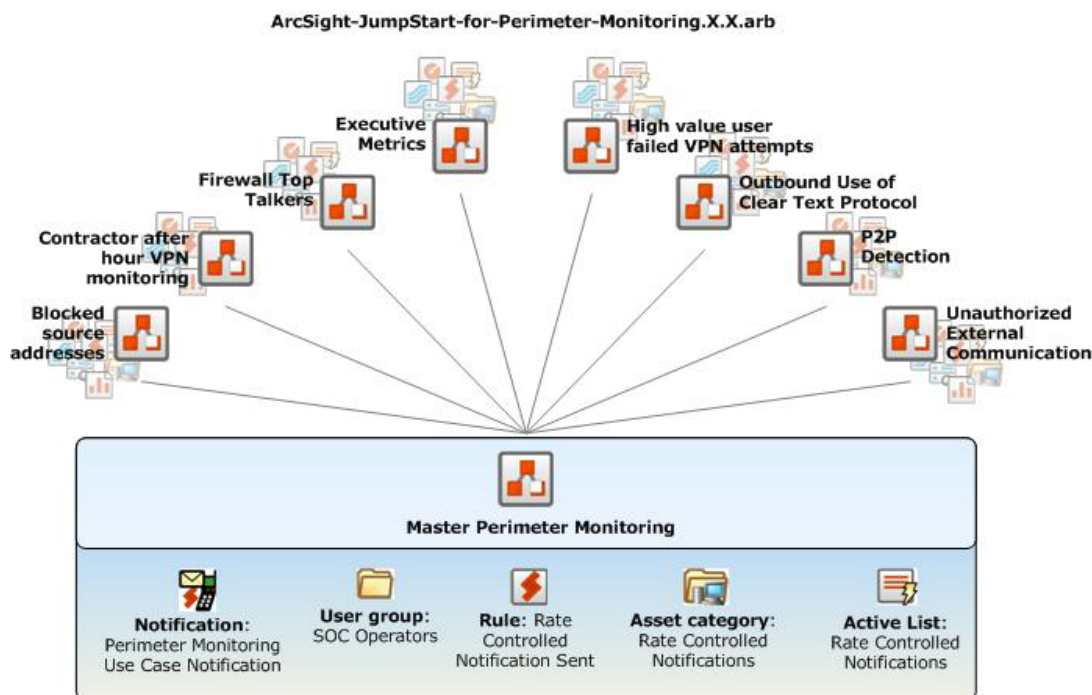
When a use case resource is installed, the resources that make up a use case are distributed in different locations throughout the individual resource trees in the Resources tab. When a use case home page is opened in the Viewer panel, the use case home page provides a right-click option that enables you to locate a given resource in the individual resource navigator.

Master Use Cases

For scenarios that call for multiple related use cases, any common resources shared by a group of related use cases can be managed by a master use case. A master use case is simply another use case that contains resources shared by other related use cases. Master use cases help centralize any configuration required to tailor the use case to your operating environment.

How Master Use Cases Work

A use case may contain several related use cases. Common resources that serve all the use cases are contained in a master use case. Running the use case configuration wizard on any use case configures that single use case as well as the master use case resources, if they are not already configured. The diagram below illustrates the use cases that make up the ArcSight Jumpstart for Perimeter Monitoring family of use cases.



When a master use case is present, the Use Case configuration wizard for the master use case is automatically launched when the ARB containing the group of related use cases is installed. The individual use cases that are part of that group all reference the configurations set in the master use case.

Standard Use Cases

The use cases provided with the product are designed to get it customized quickly to your environment and analyzing events quickly.

Pre-Installed Use Cases for ArcSight Express

Use cases for ArcSight Express are found in [All Use Cases/ArcSight Foundation/ArcSight Express](#).

Use Case	Description
ArcSight Express	The ArcSight Express use case contains several useful resources for monitoring network and network security devices, as well as a way to configure some of these resources. This is a master use case, which contains other device monitoring use cases and can configure common elements used by all of these related use cases.

Use Case	Description
Anti-Virus	The Anti-Virus use case contains several useful resources for monitoring anti-virus devices, virus and worm and other malware activity, as well as a way to configure some of these resources.
Case Tracking and Escalation	The Case Tracking and Escalation use case contains several useful resources for monitoring case workflow activity, from tracking the history of individual cases to being notified when a new case investigation has yet to be started within a policy time-frame.
Database	The Database use case contains several useful resources for monitoring database activity, as well as a way to configure some of these resources.
Firewall	The Firewall use case contains several useful resources for monitoring Firewall activity, as well as a way to configure some of these resources.
Identity Management	The Identity Management use case contains several useful resources for monitoring Identity Management activity, as well as a way to configure some of these resources.
IDS - IPS	The IDS - IPS use case contains several useful resources for monitoring Intrusion Detection/Prevention System activity, as well as a way to configure some of these resources.
Network	The Network use case contains several useful resources for monitoring Network device activity, as well as a way to configure some of these resources.
Operating System	The Operating System use case contains several useful resources for monitoring Operating System activity, as well as a way to configure some of these resources.
VPN	The VPN use case contains several useful resources for monitoring VPN activity, as well as a way to configure some of these resources.
Vulnerabilities	The Vulnerabilities use case contains several useful resources for monitoring Security Assessment and vulnerability activity, as well as a way to configure some of these resources.

ArcSight Jumpstart Use Cases

ArcSight provides use cases delivered in ArcSight Resource Bundles (.arb) ready to be installed from the [ARCSIGHT_HOME/current/jumpstart](#) directory. The Jumpstart directory delivers ArcSight start-up content designed to streamline the process of getting your environment customized and online analyzing events for perimeter monitoring and user monitoring, and addressing regulatory requirements for PCI and SOX. See [“Installing Use Cases” on page 516](#) for details on installing Jumpstart use cases.

Use Case Bundle	Description
ArcSight-JumpStart-for-PCI.1.0.5787.arb	Resources that can help determine when user accounts become inactive on PCI-regulated systems, part of a larger program for complying with Payment Card Industry regulations.

Use Case Bundle	Description
ArcSight-JumpStart-for-Perimeter-Monitoring.1.0.5788.arb	Resources that address activity coming into and going out of the network, such as VPN logins, outbound protocols, top firewall activity, blocked addresses, and P2P tracking.
ArcSight-JumpStart-for-SOX.1.0.5789.arb	Resources that address example accounting oversight use cases, part of a larger program for complying with the Sarbanes-Oxley act.
ArcSight-JumpStart-for-User-Monitoring.1.0.5790.arb	Resources that address general use cases relating to user activity on the network.

Once installed, the jumpstart use cases appear in the Jumpstart group in the Navigator panel.

Installing Use Cases


This topic describes how to install a use case from an ARB file in the [ARCSIGHT_HOME/current/jumpstart](#) directory.

- 1 Log into the ArcSight ESM Console as the ArcSight ESM Administrator.



Only Admin users should use the Configuration wizard

Because many different types of resources are included in a given use case from many different locations in the individual resource trees, ArcSight recommends that only users with Admin privileges run the use case configuration wizard. This ensures that the user performing the configuration has adequate permissions to access the configurable resources.

- 2 In the **Packages** tab in the Navigator panel, click **Import** ().
- 3 Browse to the [ARCSIGHT_HOME/current/jumpstart](#) directory, select a use case ARB file to import, and click **Open**.

When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.
- 4 In the Packages for Installation dialog box, verify that the package Install checkbox is selected and click **Next**.

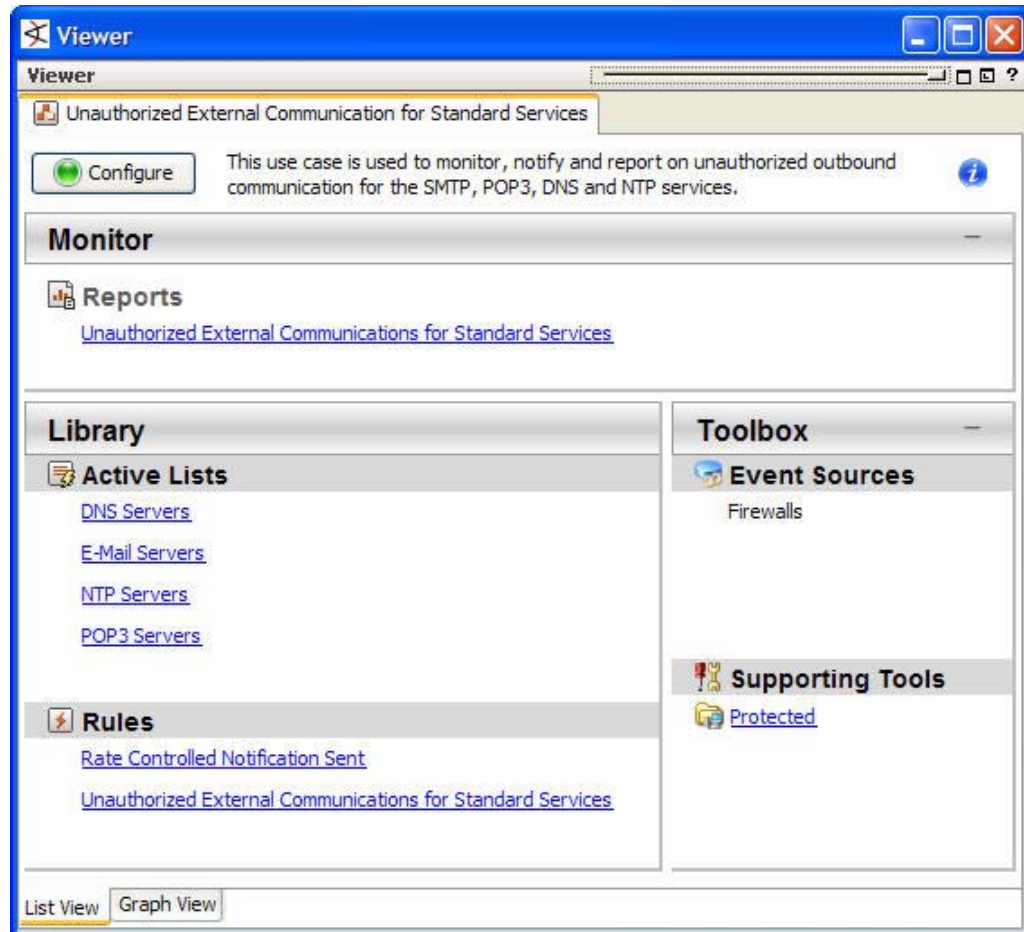
The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.
- 5 In the Installing Packages dialog, click **OK**.
- 6 In the Importing Packages dialog, click **OK**.

If a master use case is associated with a use case group in the ARB file, the Use Case wizard launches and starts configuring the master use case associated with the use case group. The master use case is provided so you can configure the common resources used by the use cases in the group in a single process using the configuration. For more information, see ["Master Use Cases" on page 513](#). For instructions on using the Use Case wizard, see ["Configuring Use Cases" on page 518](#).



For more information, see [“Importing Package Bundles” on page 689](#) and [“Installing Packages” on page 690](#).

Viewing and Using Use Cases

To open a use case in the Viewer panel, double-click the use case in the Use Cases tab of the Navigator panel, or right-click the use case and select **Open Use Case**. The Use Case opens in the Viewer panel.



The use case viewer is organized into the following sections:

Section	Description
	The Configure button launches the Use Case configuration wizard.
	The information section contains a description of the use case.
Monitor	The Monitor section contains monitoring-related resources: active channels, dashboards, reports, focused reports, and query viewers.
Library	The Library section contains a section for every type of correlation resource that drives the use case: active lists, session lists, field sets, filters, queries, rules, trends, actors, fields, and data monitors.

Section	Description
Toolbox	The Toolbox section contains event sources and supporting resources, such as notification destinations, groups, and other use cases.
Supporting Tools	The Supporting Tools section contains any other resource types included by the content author.



View the use case and its associated resources in a resource graph

You can view a resource graph of the use case and its associated resources by selecting the Graph View tab at the bottom of the Viewer panel.

Accessing Resources from the Viewer Panel

When a use case is open in the List View tab of the Viewer panel, you can view, edit, navigate, or graph a use case resource by right-clicking the resource and selecting from one of the following options:

- **View**—Open the resource in the Viewer panel to view the contents of the resource. This option is not available for all resources.
- **Edit**—Open the resource for editing in the Inspect/Edit panel. For more information, see [“Inspecting and Editing” on page 102](#).
- **Find in Navigator**—Open the resource in the Navigator panel. For more information, see [“Navigating” on page 94](#).
- **Graph View**—View the association between this resource with other resources using a graphical viewer. For more information, see [“Visualizing Resources” on page 674](#).
- **Rule**—Enable or disable the rule. This option is available with a rule resource.
- **Trend**—Schedule the trend. This option is available with a trend resource.



View the use case and its associated resources in a resource graph

You can view a resource graph of the use case and its associated resources by selecting the Graph View tab at the bottom of the Viewer panel.

Configuring Use Cases

ArcSight provides a Use Case configuration wizard to assist you in configuring all the resources in the use case to reflect your operating environment in a single operation.



You can still configure resources individually

If you need to change the configuration for a single resource in the use case, you can always use the individual resource editor.

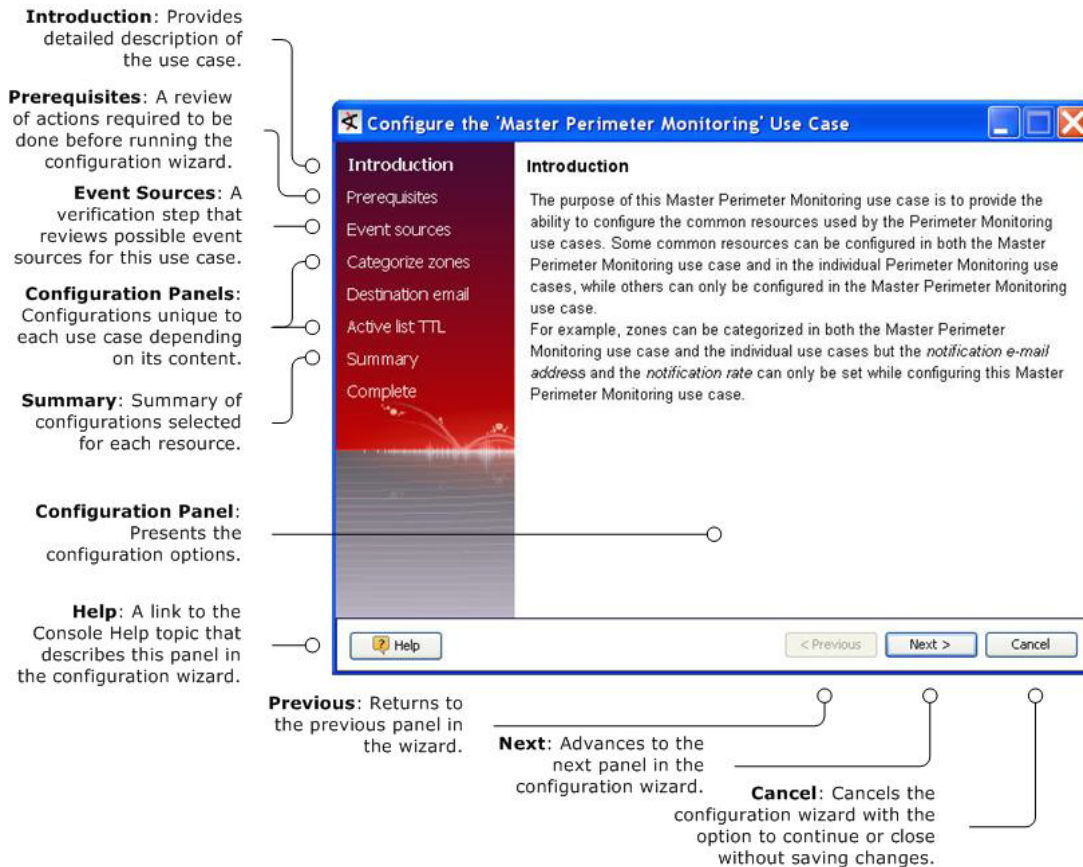


Only Admin users should use the Configuration wizard

Because many different types of resources are included in a given use case from many different locations in the individual resource trees, ArcSight recommends that only users with Admin privileges run the Use Case configuration wizard. This ensures that the user performing the configuration has adequate permissions to access the configurable resources.

Navigating the Use Case Configuration Wizard

The Use Case configuration wizard consists of the following features:



To use the Use Case wizard:

- "Step 1 - Model Your Network" on page 519
- "Step 2 - Install Use Case Package Bundles" on page 520
- "Step 3 - Launch the Use Case Wizard" on page 520
- "Step 4 - Introduction Panel" on page 520
- "Step 5 - Prerequisites Panel" on page 521
- "Step 6 - Confirm Event Sources Panel" on page 521
- "Step 7 - Configuration Panels" on page 523
- "Step 8 - Summary of Settings to Apply Panel" on page 523

Step 1 - Model Your Network

Model your network first as a part of the initial configuration of ArcSight ESM. Use case configuration requires having a network model in place. So, model your network before running the Use Case wizard.

To assist in modeling your network, a Network Model wizard is provided on the ArcSight ESM Console (menu option **Tools > Network Model**). For more information, see ["About the Network Model" on page 731](#).

Step 2 - Install Use Case Package Bundles

Do this step only if you plan to use one of the use cases supplied in the ArcSight jumpstart directory.

Import and install the use case package bundle that contains the use case (if it is not already installed). For more information, see ["Installing Use Cases" on page 516](#).

Step 3 - Launch the Use Case Wizard

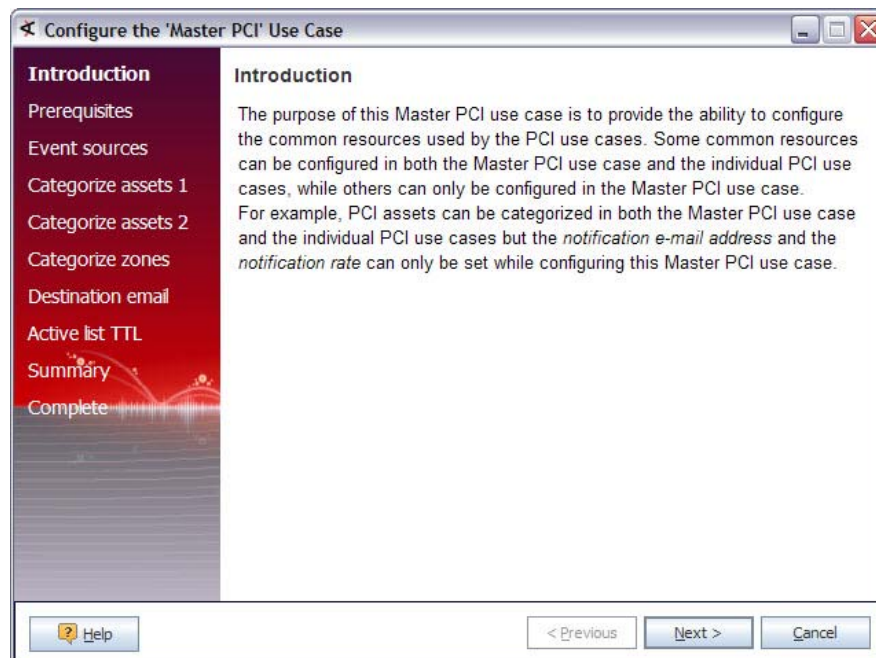
Launch the Use Case wizard using one of the following methods:

- **Browse from the Navigator panel**—In the Navigator panel, select the **Use Cases** tab, right-click a use case and select **Configure Use Case**.
- **From the ArcSight ESM Console menus**—Choose **Tools > Use Case** from the menus. Select a use case from the tree in the wizard and click **Next**.
- **From the Viewer panel**—In the Navigator panel, select the **Use Cases** tab, right-click a use, and select **Open Use Case**. In the Viewer panel, click **Configure Use Case**.

The Introduction panel of the Use Case wizard displays.

Step 4 - Introduction Panel

The Introduction panel describes the purpose of the use case. If you are configuring a master use case, the introduction specifies if there are essential common resources that can only be configured using the master use case. For more information, see ["Master Use Cases" on page 513](#).



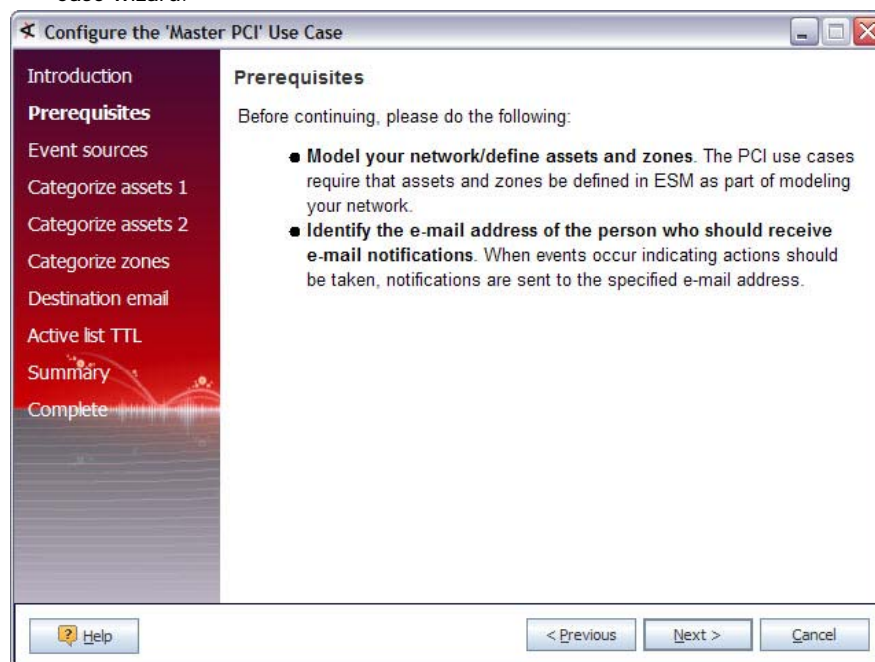
Click **Next**.

The Prerequisites panel displays as shown in [n](#).

Step 5 - Prerequisites Panel

The Prerequisites panel (n) describes required actions or information needed before continuing with the Use Case wizard:

- **Any actions that should be completed before running the Use Case wizard.** For example, your network should be modeled before using the Use Case wizard to configure the use case. A Network Model wizard is provided from the ArcSight ESM Console (menu option **Tools > Network Model**). For more information, see [“About the Network Model” on page 731](#). Complete these actions before continuing with the Use Case wizard.
- **The information that needs to be provided when running the Use Case wizard to configure the use case.** For example, the number of days before a user is required to change their passwords or the network devices on your network that are subject to the PCI regulation. Gather this information before continuing with the Use Case wizard.



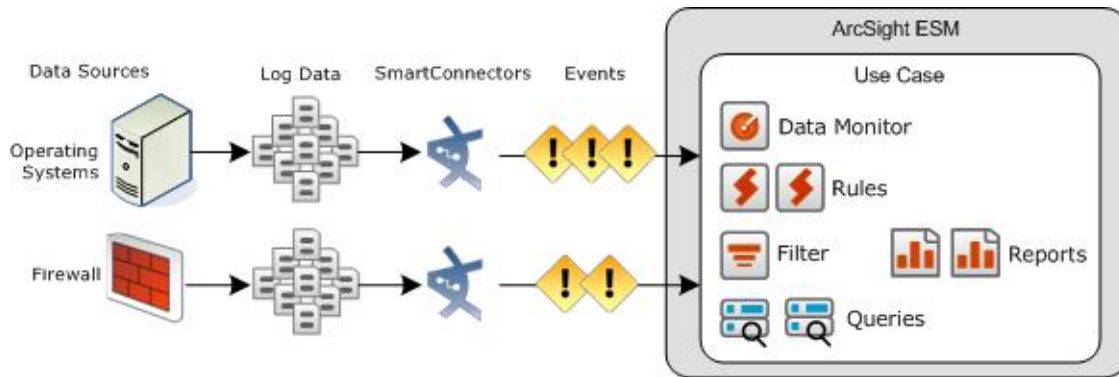
Click **Next**.

The Confirm Event Sources panel displays as shown in .

Step 6 - Confirm Event Sources Panel

The Confirm Event Sources () panel lists the event sources that send events to the Manager through a SmartConnector for the use case. SmartConnectors collect log data

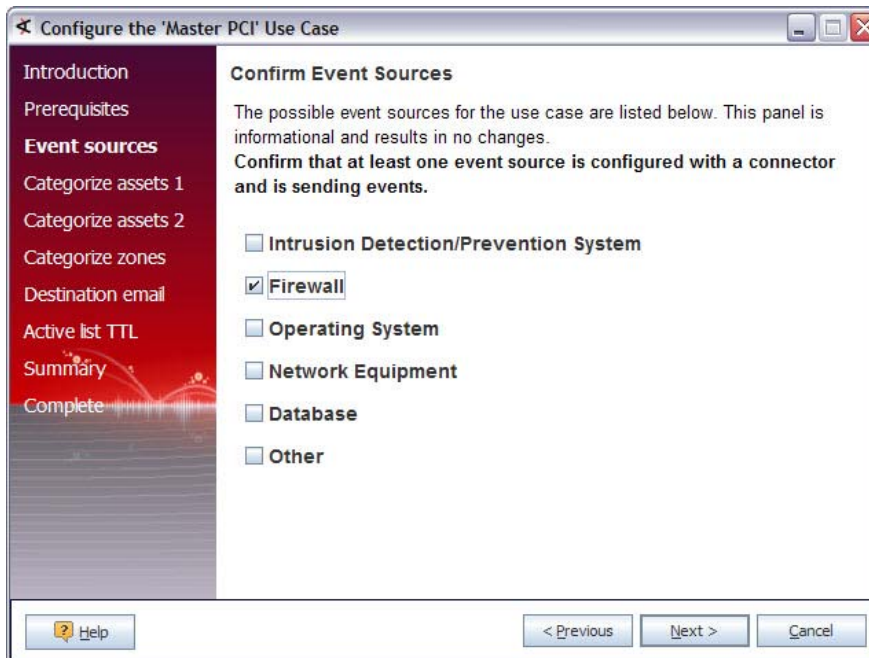
from event sources (such as firewalls and operating systems) and generate events that are sent to ArcSight ESM as shown in the following diagram:



The resources in the use case are driven by these events and without the event sources, the use case does not generate output. For more information, see *Devices and Connectors in a Network* in the *ESM 101 Guide* and [Chapter 27, Managing SmartConnectors, on page 695](#).

For your environment, confirm the event sources that are configured with a SmartConnector and supplying events to ArcSight ESM for this use case. For most use cases, you are asked to confirm that **at least one of the listed event source** is configured with a SmartConnector and sending events to ArcSight ESM.

Confirm the event sources and click **Next**.



Note

The Confirm Event Sources panel is informational. It simply lists the event sources that can provide data to the use case. The wizard does no configuration based on options you select in this panel.

After the Confirm Event Sources panel, a series of configuration panels display.

Step 7 - Configuration Panels

The series of configuration panels displayed depends on the resources that make up the use case and are different for each use case.

In these configuration panels, you are prompted to supply values that reflect your environment. The values you provide are used to populate the settings in the resources that make up the use case. After the series of configuration panels, the Summary of Settings to Apply panel appears. The settings are not actually saved to the resources until the Next button is clicked in the Summary of Settings to Apply panel. If you click Cancel in any of the configuration panels or in the Summary of Settings to Apply panel, none of the configuration settings specified in any of the configuration panels are saved.

The Use Case wizard displays the following types of configuration panels:

[“Categorize Assets/Zones Panels” on page 526](#)
[“Populate Active List” on page 527](#)
[“Specify the Notification E-mail Address Panel” on page 529](#)
[“Set the Inactivity Time Period Panel” on page 531](#)
[“Set the Notification Rate Panel” on page 531](#)
[“Schedule Daily Report Panels” on page 532](#)
[“Schedule Weekly Report Panels” on page 534](#)
[“Schedule Monthly Report Panels” on page 536](#)
[“Schedule Yearly Report Panels” on page 538](#)

For each configuration panel, follow the instructions in the appropriate configuration panel and Help topic and click **Next**. Repeat until the Summary of Settings to Apply panel appears as shown in [n](#) and described in [“Step 8 - Summary of Settings to Apply Panel” on page 523](#).

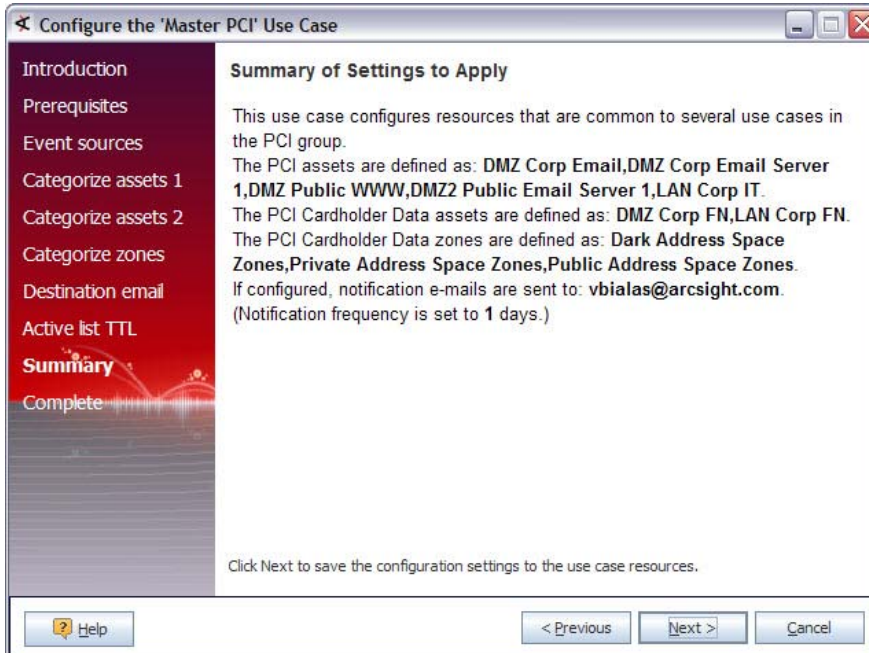
Step 8 - Summary of Settings to Apply Panel

The Summary of Settings to Apply panel ([n](#)) displays a summary of the settings you specified in the previous configuration panels.

Choose one of the following options:

- To apply the settings specified in the previous configuration panels to the use case resources, click **Next**.
- To cancel without applying settings, click **Cancel**.

- To go back to the previous panel, click **Previous**.

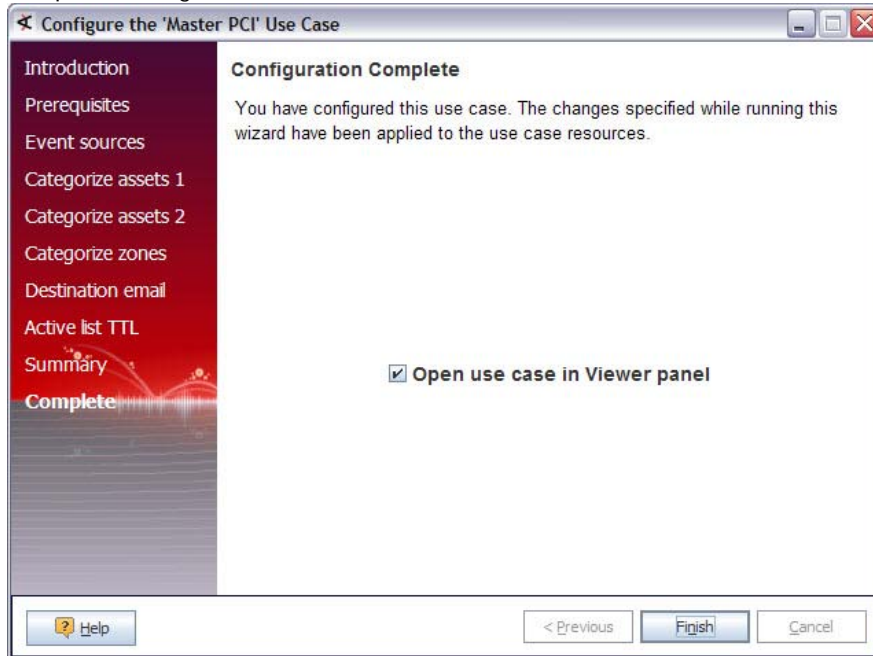


After you click Next, the settings are applied to the resources in the use case. If the use case contains data monitors, the data monitors are enabled.

A Commit Changes dialog briefly displays as the settings are applied to the use case resources. After the settings have been applied, a Configuration Complete panel displays as shown in .

Step 9 - Configuration Complete Panel

The Configuration Complete panel () displays a message indicating that you have completed configuration of the use case.



Leave the *Open use case in Viewer panel* checkbox selected and click **Finish**.

The Console displays the use case in the Viewer panel, and use case configuration is complete. If the event sources for this use case are configured with a SmartConnector and are sending events to ArcSight ESM, the following actions occur:

- The “library” resources in this use case, such as rules, data monitors, and queries, start processing events.
- If the conditions in the use case are met, data is provided to the output resources of the use case such as reports, active channels, dashboards, and cases.

In the future, you can reconfigure the use case resources, using either of the following methods:

- Run the Use Case wizard again—For more information, see [“Step 3 - Launch the Use Case Wizard” on page 520](#).
- Edit the resource directly in the Navigator panel—For more information, see [“Navigating” on page 94](#).

Configuration Panels

After the Confirm Event Sources panel, the configuration wizard presents a series of configuration panels. The set of configuration panels displayed depends on the content of the use case and is different for each use case.

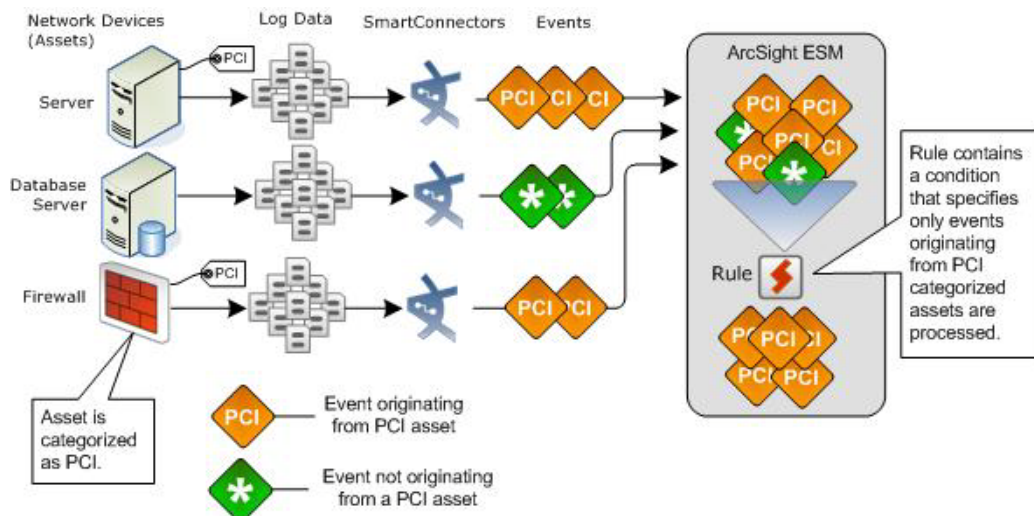
[“Categorize Assets/Zones Panels” on page 526](#)
[“Populate Active List” on page 527](#)
[“Specify the Notification E-mail Address Panel” on page 529](#)
[“Set the Inactivity Time Period Panel” on page 531](#)
[“Set the Notification Rate Panel” on page 531](#)
[“Schedule Daily Report Panels” on page 532](#)
[“Schedule Weekly Report Panels” on page 534](#)
[“Schedule Monthly Report Panels” on page 536](#)
[“Schedule Yearly Report Panels” on page 538](#)
[“Enable Rules Panel” on page 539](#)
[“Enable Rule Actions Panel” on page 540](#)
[“Set Session List Entry Expiry Panel” on page 541](#)

After preceding through the series of configuration panels, the Summary of Settings to Apply panel (n) displays. Return to [“Step 8 - Summary of Settings to Apply Panel” on page 523](#).

Categorize Assets/Zones Panels

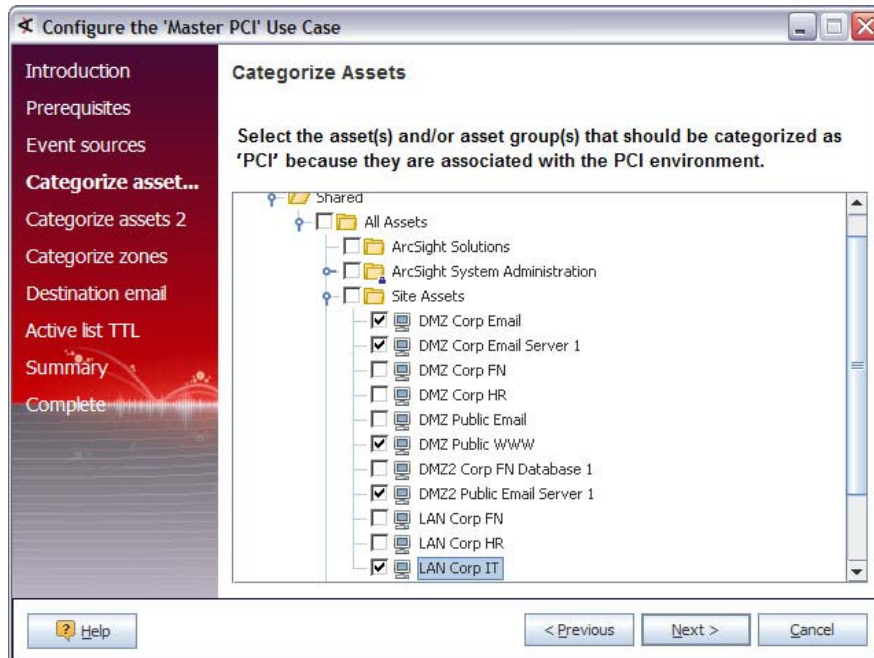
In the Categorize Assets or Zones panels, you are asked to classify assets or zones into an ArcSight ESM category. A logical category (such as [PCI](#) or [SOX](#)) can be applied to assets, asset ranges, asset groups, zones, or zone groups. These categories provide a cross-referencing capability that makes it possible to track and filter network activity based on business relevance. Using these categories, the events processed by the use case resources can be restricted.

For example, classifying assets into the [PCI](#) group can limit the set of events processed by the use case resources to only those events that originate from PCI assets. For example, a rule in a PCI use case may be configured to only process events originating from assets categorized as PCI as shown in the following diagram:



In the Categorized PCI Assets panel, you are prompted to supply the network devices (assets) that should be regulated by the Payment Card Industry (PCI) standard and therefore categorized as a PCI asset, as shown in . The assets and asset groups you select in this panel are classified as a PCI asset in ArcSight ESM.

For more information, see [“Network Model” on page 732](#), [“Categories” on page 836](#), and [“Asset Model” in the ESM 101 Guide](#).



If any assets/zones have already been categorized, a check mark displays next to the asset/zone name. If your assets/zones are already categorized and no revisions need to be made, click **Next** to skip this step. For example, if you already categorized your assets/zones in the master use case, you do not need to categorize your assets/zones again. You can however, revise your asset/zone categorization while configuring the individual use case.

Select the assets that should be categorized and click **Next**.



Note

The new categorization is not applied until **Next** is clicked in the Summary of Settings to Apply panel as described in [“Step 8 - Summary of Settings to Apply Panel” on page 523](#).

The categorization of assets, assets groups, zones, or zone groups is global in ArcSight ESM and not specific to a use case. Any categorization changes made in this panel (while configuring either an individual use case or the master use case) affect any resources that reference this category in any use case. The last set of categorization changes, applied by clicking Next in the *Summary of Settings to Apply* panel, overrides any previous settings.

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Populate Active List

If your use case includes one or more field-based (static) active lists for looking up non-event related data, the use case configuration wizard includes the Populate Active List panels.

In the Populate Active List panels, you are prompted for sets of data that are used to populate Fields-based active lists. Active lists store data over a period of time. Resources such as rules and data monitors can reference the data stored in active lists. For example, an active list could store the port numbers that are allowed access to the PCI Card Holder Data Environment (CDE). For more information, see *How Active Lists Work* in the *ESM 101 Guide*.

You may be prompted for a single column of data or multi-column sets of data. For example, you might be prompted to supply a set of trusted port numbers (one column of data) or a set of default User Accounts and associated Vendor Names (two columns of data). The data you provide in the panels is added to the data that may already exist in the active list.

To define the input data:

- 1 If you plan to import the data using a CSV file, create the CSV file to import. The data types of the columns and the number of columns in the CSV file must match the columns in the active list. For example, in the Define Default User Accounts panel, you are prompted to provide a set of default User Accounts and associated Vendor Names. The *Default User Account-Vendor List* active list is a two column active list that expects default User Accounts in the first column and associated Vendor Names in the second column.
- 2 Select a method for populating the active list. In the first Define Data Sets panel (u), select one of the following options:
 - ◆ **Import CSV file**—Provide the data by importing a Comma-Separated Value (CSV) file
 - ◆ **Manual data entry**—Provide the data by typing the values directly into a table

Configure the 'PCI 2.1 - Monitor Default User Accounts' Use Case

Define Default User Accounts

Supply the default user accounts and vendor names for your network e.g. scott Oracle. If a CSV file is used, it should contain two columns.

User Account	Vendor Name
jeff	Unix

Add Remove

Help < Previous Next > Cancel

- 3 If the **Import CSV file** option is selected, click... and browse for a CSV file to import. Select the file and click **OK**.
- 4 Click **Next**.

The second define data panel displays as shown in .



If you imported data using a CSV file, the data is displayed in the panel.

- 5 Enter values.
- 6 Add additional rows as needed:
 - a Click **Add**.
 - b Enter the data into the new row.
- 7 Click **Next**.

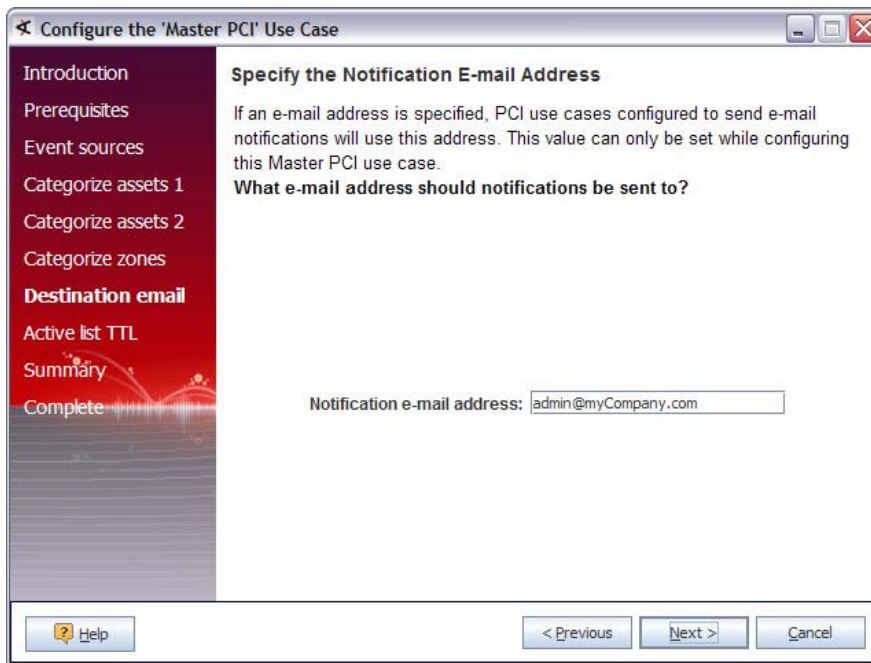
When Next is clicked in the Summary of Settings to Apply panel as described in [“Step 8 - Summary of Settings to Apply Panel” on page 523](#), the new values are added to the existing values already present in the active list. If you specify a value that already exists in the active list, an additional entry is added and the Count for that entry is increased by one.

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Specify the Notification E-mail Address Panel

In the Specify the Notification E-mail Address panel (), you are prompted to supply an e-mail address or an e-mail alias (distribution list). If an e-mail address is specified, a notification (alert) is sent to the specified e-mail address when the condition(s) described in the panel are satisfied. For example, the use case could contain a rule that tests when

default system accounts are used. Once the rule is triggered, an e-mail notification is sent to the specified e-mail address or distribution list.



The screenshot shows a configuration window titled "Configure the 'Master PCI' Use Case". On the left is a sidebar with a list of steps: Introduction, Prerequisites, Event sources, Categorize assets 1, Categorize assets 2, Categorize zones, **Destination email**, Active list TTL, Summary, and Complete. The "Destination email" step is highlighted in red. The main area of the window is titled "Specify the Notification E-mail Address". It contains the following text: "If an e-mail address is specified, PCI use cases configured to send e-mail notifications will use this address. This value can only be set while configuring this Master PCI use case." Below this is the question "What e-mail address should notifications be sent to?". A text input field is present with the value "admin@myCompany.com" and the label "Notification e-mail address:". At the bottom of the window are three buttons: "Help" (with a question mark icon), "< Previous", and "Next >", along with a "Cancel" button.



The e-mail address does not have to be an ArcSight ESM user.

In order for notifications to be sent to specified e-mail address, notifications must be configured. For more information, see ["Managing Notifications" on page 658](#) and ["Acknowledging Notifications" on page 110](#).

Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 523](#).

Set the Inactivity Time Period Panel

In the *Inactivity Time Period* panel, you are prompted to supply an expiration time period as shown in . In this example, an account expires if no logins have occurred within the specified time period.

The numeric value you specify sets the expiration time period in days. This expiration time period is the Time To Live (TTL) in days for an active list. Entries in the active list expire when the Time To Live (TTL) has been reached. This expiration causes an event to be generated. This event can be used by other ArcSight ESM resources such as filters and rules. For more information, see [“Managing Active Lists” on page 571](#).

For example, in the *PCI 8.5 - Identify Inactive User Accounts* use case, you are prompted to supply the Inactivity Time Period. If you answer 45 days, the Time To Live (TTL) for the *Users Who Accessed Cardholder Data* active list is set to 45 days which means once an account has been on the active list (indicating no activity) for more than 45 days, it expires. This expiration generates an event which triggers the *Inactive User Account Detected* rule.



Caution

The value specified in this panel is saved as Time To Live (TTL) in days for the active list. If other resources reference this active list, the change to the TTL value can affect the behavior of other resources listed in different use cases.

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Set the Notification Rate Panel

In the *Set the Notification Rate* panel, you are prompted to specify how often a notification e-mail should be sent—the notification rate. This rate is used to throttle the number of alert notifications sent. The rate specified in this panel sets the Time To Live (TTL) in days for the *Rate Controlled Notifications* active list.

If the notification rate is set to 0, only one e-mail is sent for every issue until the entry is manually removed from the *Rate Controlled Notifications* active list.

The screenshot shows a window titled "Configure the 'Master PCI' Use Case". On the left is a sidebar with a red background and white text listing steps: Introduction, Prerequisites, Event sources, Categorize assets 1, Categorize assets 2, Categorize zones, Destination email, **Active list TTL**, Summary, and Complete. The main area is titled "Set the Notification Rate" and contains the text: "Set the notification rate to throttle the number of alert notifications sent. **How often should e-mail notifications be sent?** This value can only be set while configuring this Master PCI use case." Below this text is a label "Send notifications every:" followed by a text input field containing the number "1" and the word "days". At the bottom are three buttons: "Help" (with a question mark icon), "< Previous", and "Next >" (with a right arrow icon), and a "Cancel" button.

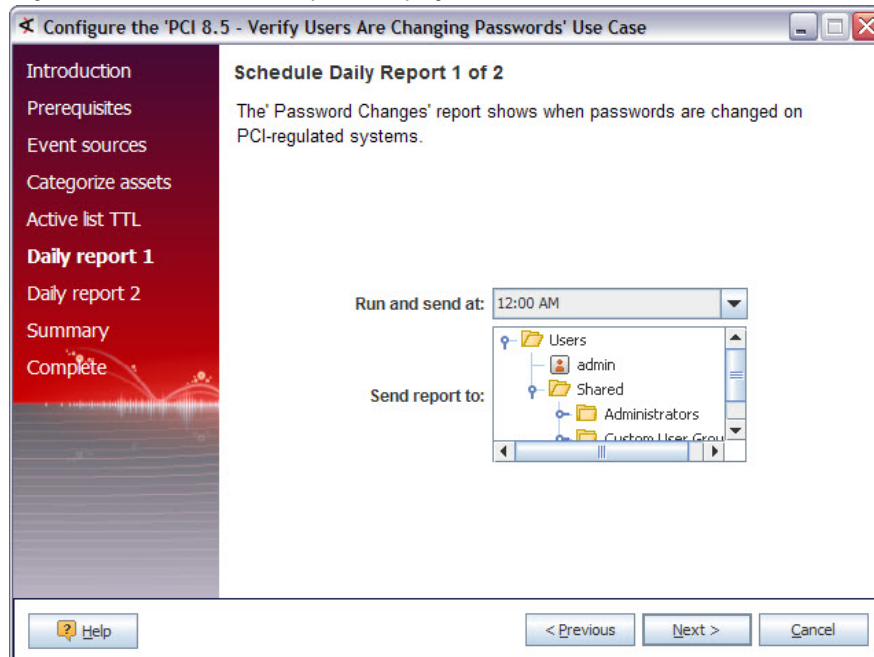
Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 523](#).

Schedule Daily Report Panels

In the *Schedule Daily Report* panel, you are prompted to schedule a daily report, as shown below.

The screenshot shows a window titled "Configure the 'PCI 8.5 - Verify Users Are Changing Passwords' Use Case". The sidebar on the left has the same red background and lists steps: Introduction, Prerequisites, Event sources, Categorize assets, Active list TTL, **Daily report 1**, Daily report 2, Summary, and Complete. The main area is titled "Schedule Daily Report 1 of 2" and contains the text: "The 'Password Changes' report shows when passwords are changed on PCI-regulated systems." Below this is the question: "Do you want to schedule the 'Password Changes' report to run daily?" followed by two radio button options: "Yes" (which is selected) and "No". At the bottom are three buttons: "Help" (with a question mark icon), "< Previous", and "Next >" (with a right arrow icon), and a "Cancel" button.

If you answer **Yes**, another panel displays as shown below.



In the **Run and send at** field, select a time during the day when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see ["Managing Users" on page 641](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

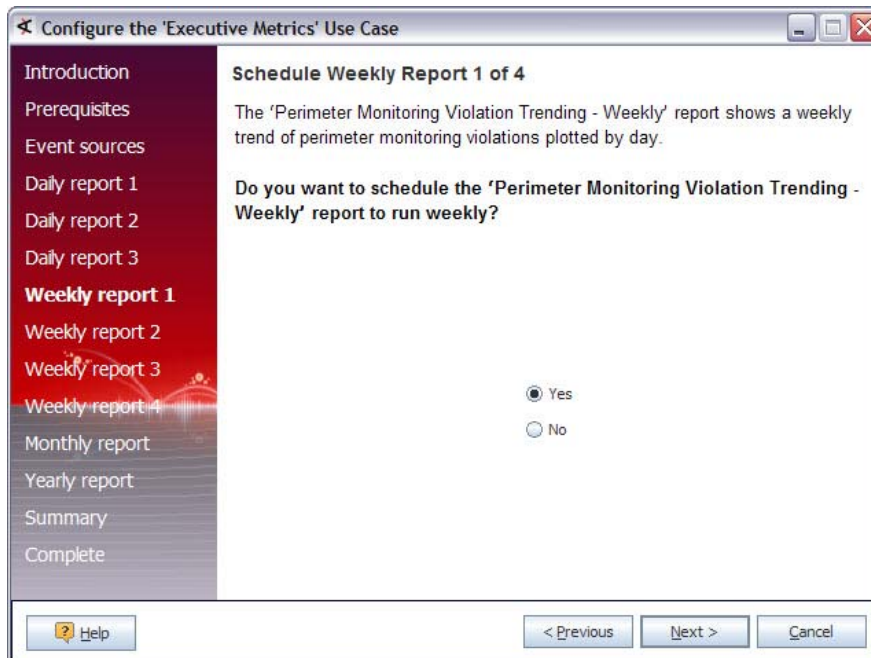
When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run daily. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.

For more information, see [Chapter 15, Running and Managing Reports, on page 423](#).

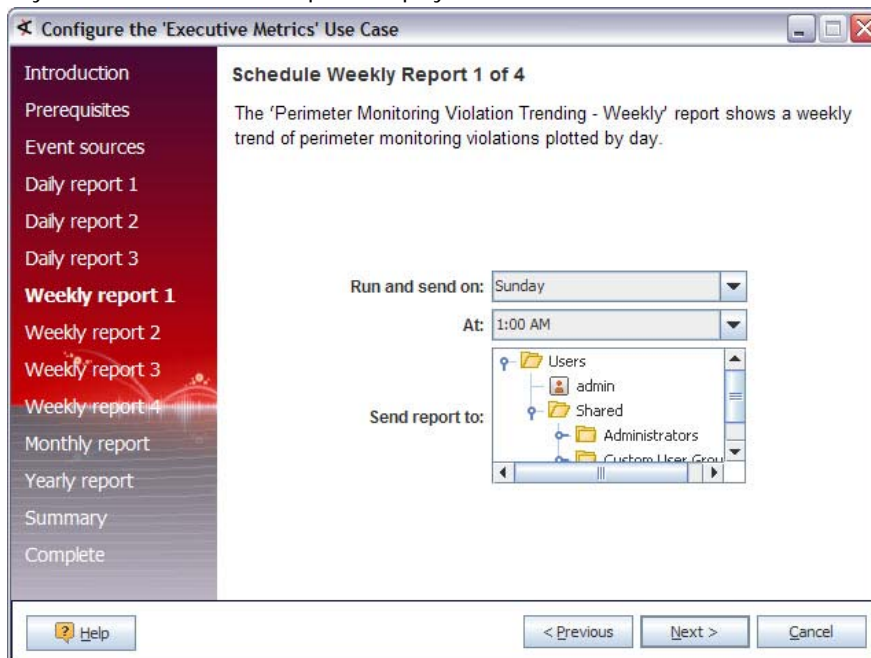
Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 523](#).

Schedule Weekly Report Panels

In the **Schedule Weekly Report** panel, you are prompted to schedule a weekly report, as shown below.



If you answer **Yes**, another panel displays as shown below.



In the **Run and send on** field, select the day of the week when the report should run.

In the **At** field, select a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see ["Managing Users" on page 641](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run weekly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



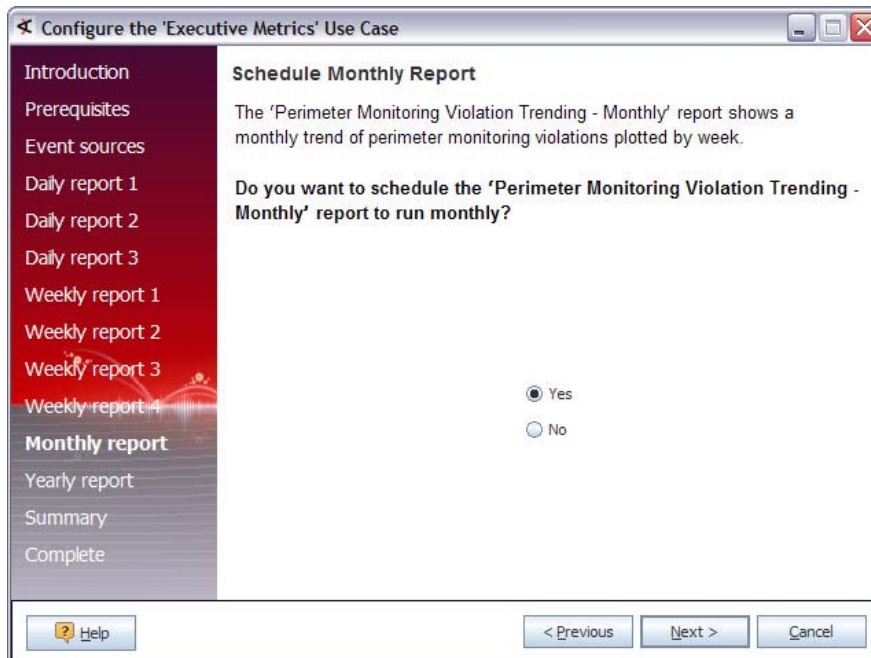
Weekly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

For more information, see [Chapter 15, Running and Managing Reports, on page 423](#).

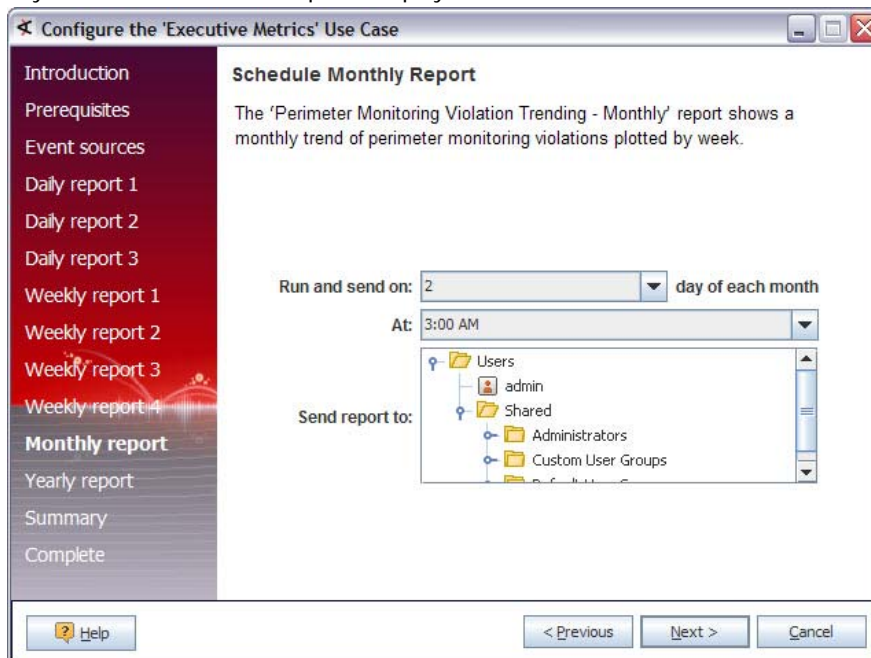
Return to the list of configuration panels in ["Step 7 - Configuration Panels" on page 523](#).

Schedule Monthly Report Panels

In the **Schedule Monthly Report** panel, you are prompted to schedule a monthly report, as shown below.



If you answer **Yes**, another panel displays as shown below.



In the **Run and send on __ day of each month** field, specify the day of the month when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **At** field, specify a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see [“Managing Users” on page 641](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run monthly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



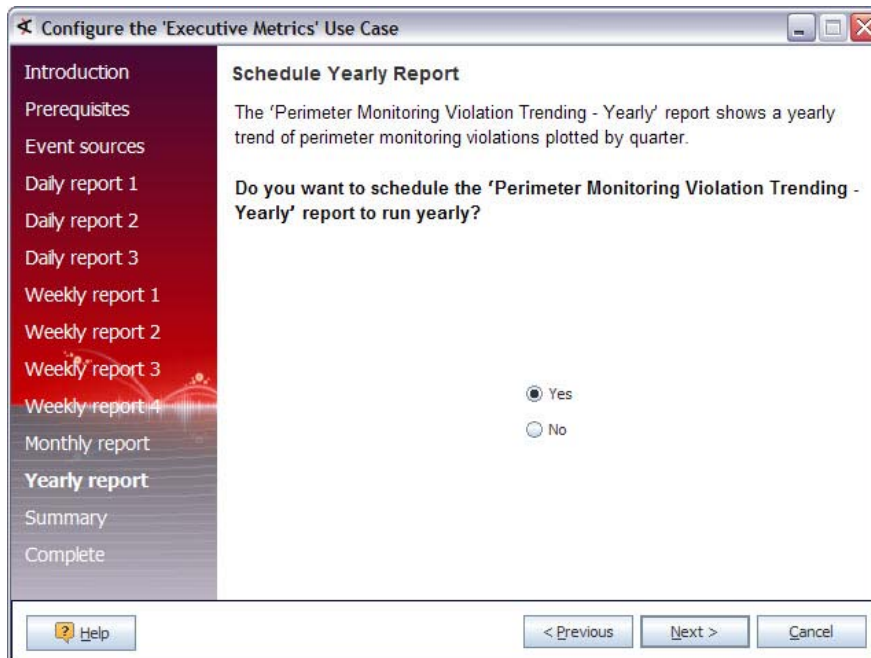
Monthly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

For more information, see [Chapter 15, Running and Managing Reports, on page 423](#).

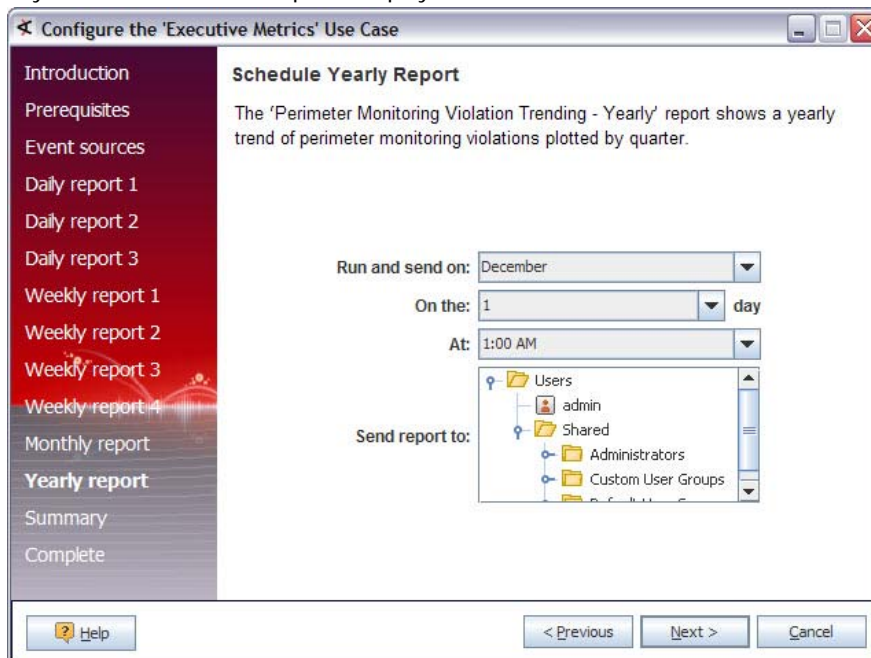
Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Schedule Yearly Report Panels

In the **Schedule Yearly Report** panel, you are prompted to schedule a yearly report, as shown below.



If you select **Yes**, another panel displays as shown in .



In the **Run and send on** field, specify the day of the month when the report should run. When a report runs, the output of the report is stored on the ArcSight ESM Manager. You can elect to send the report to the e-mail address associated with the ArcSight ESM user.

In the **On the _ day** field, specify the day of the month when the report should run.

In the **At** field, specify a time during the day when the report should run.



For best performance, schedule reports to run at different times during the day.

In the **Send report to** field, browse for an ArcSight ESM user.



In order for the report to be sent, an e-mail address must be specified for the selected ArcSight ESM user. For more information about creating an ArcSight ESM user or specifying an e-mail account for an ArcSight ESM user, see [“Managing Users” on page 641](#). If no e-mail address is specified, the report is archived on the ArcSight ESM Manager.

When the Next button is clicked in the Summary of Settings to Apply panel, the Use Case wizard creates a job for the report called [Use Case Scheduled Job](#) that is scheduled to run yearly. If you edit or remove the [Use Case Scheduled Job](#), this can cause inconsistencies between the report and the wizard.



Yearly reports do not display results immediately. It can take up to twenty four hours for the report to display results and results are only displayed if the conditions in the query invoked by the report are satisfied.

For more information, see [Chapter 15, Running and Managing Reports, on page 423](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

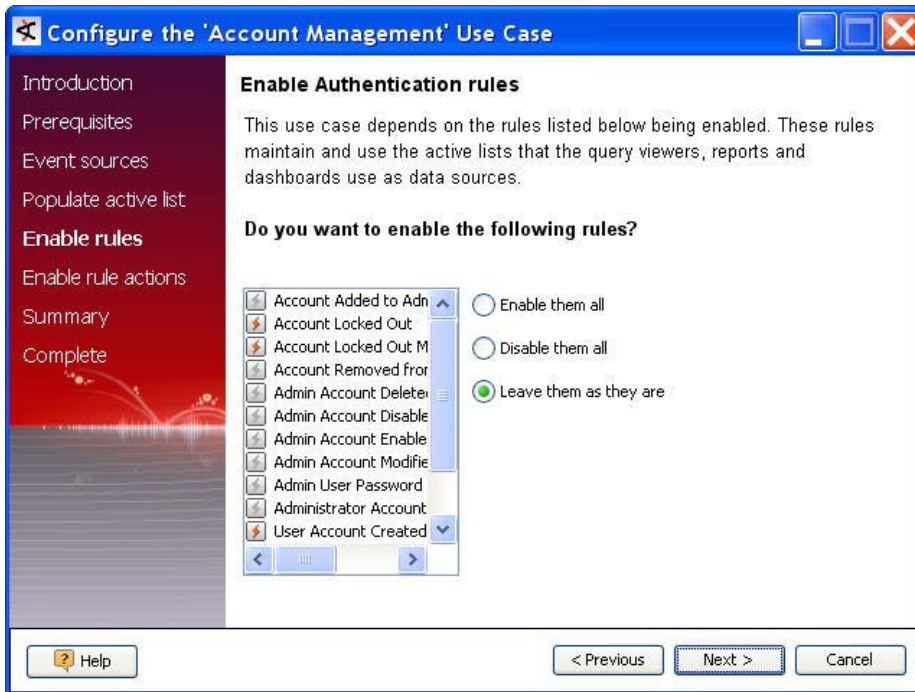
Enable Rules Panel

The Enable Rules panel provides the opportunity to enable (or disable) the rules associated with this use case in a single operation.

The Enable Rules panel of the use case configuration wizard presents a list of all the rules included in the use case. Some rules may be enabled by default, as shown in the example. In this panel, you can:

- **Enable them all:** Selecting this option enables all the rules in the use case.
- **Disable them all:** Disables all the rules in the use case, including those that are enabled by default.

- **Leave them as they are:** Keeps the rules as they are shown.



Changes appear after the configuration wizard is completed

Changes you make in this panel won't be visible in the list of rules until after the configuration wizard is completed.

You can also enable and disable rules individually outside of the use case configuration wizard. You can access the rule editor by right-clicking the rule list from the use case home page (right-click > **Edit Rule**) or from the Resources tree in the Navigator panel (**Resources** > **Rules** > right-click > **Edit Rule**). For instructions, see [“Enabling and Disabling Rules” on page 461](#).

For more about rules, see [Chapter 16, Rules Authoring, on page 439](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Enable Rule Actions Panel

The Enable Rule Actions panel provides the opportunity to enable (or disable) certain rule actions that require configuration for your environment for rules associated with this use case. This panel appears after the [Enable Rules Panel](#) panel.

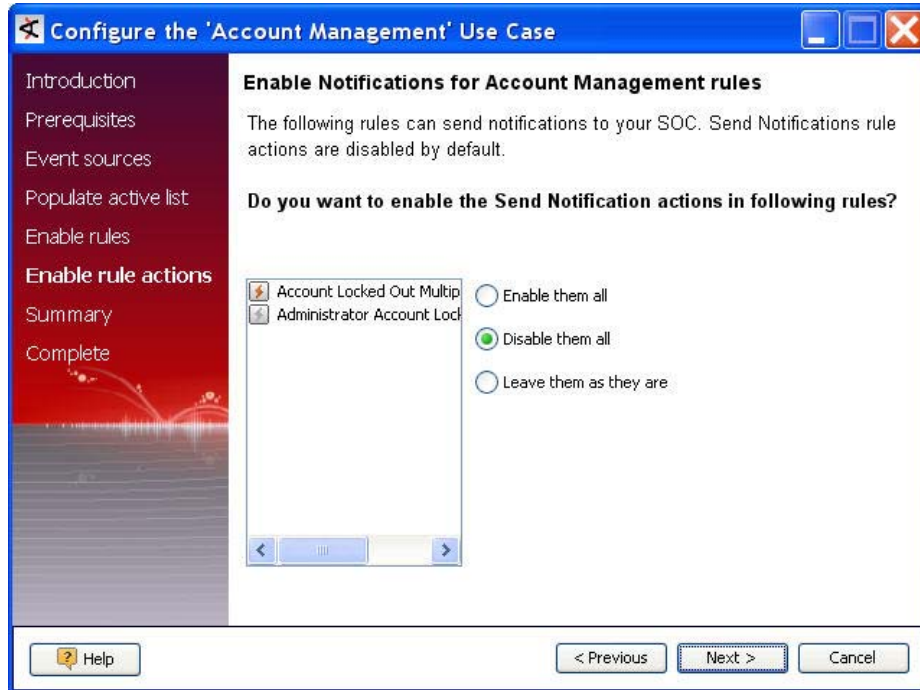


Changes appear after the configuration wizard is completed

The changes you make in this panel and the Rule Action panel won't be visible in the list of rules until after the configuration wizard is completed.

The Enable Rule Actions panel of the use case configuration wizard presents a list of the rules in the use case that have actions that require local configuration, such as Notifications, as shown in this example. In this panel, you can:

- **Enable them all:** Selecting this option enables the action for all the rules that have configurable actions associated with them.
- **Disable them all:** Disables the Notification action for all the rules that have configurable actions associated with them.
- **Leave them as they are:** Keeps the rule actions as they are shown.



You can also enable and disable rule actions individually outside of the use case configuration wizard. You can access the rule editor by right-clicking the rule list from the use case dashboard (right-click > **Edit Rule**) or from the Resources tree in the Navigator panel (**Resources** > **Rules** > right-click > **Edit Rule**). For instructions, see [“Enabling or Disabling a Rule Action” on page 453](#).

For more about rules, see [Chapter 16, Rules Authoring, on page 439](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

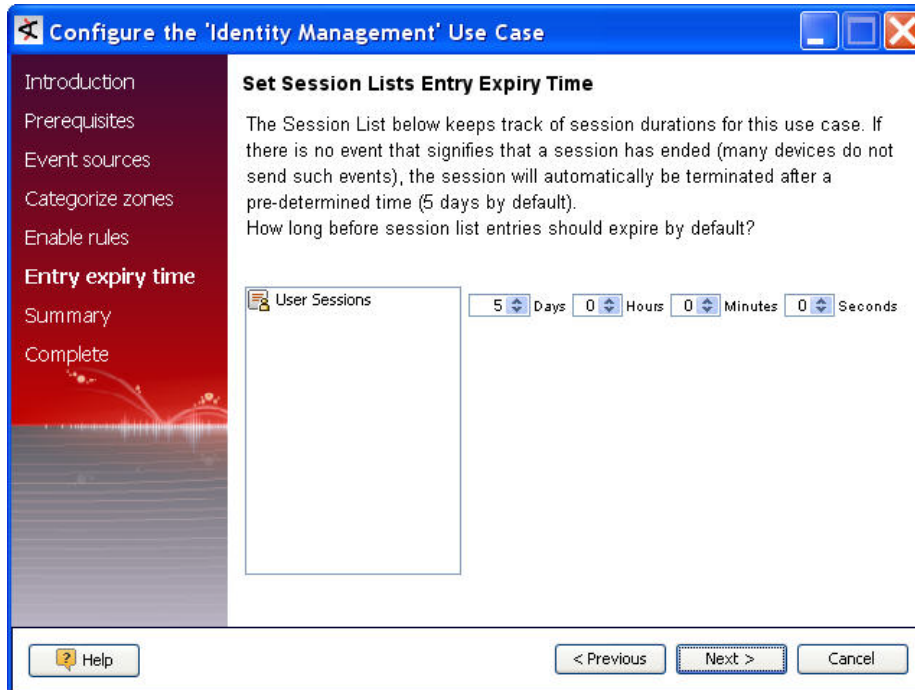
Set Session List Entry Expiry Panel

The Set Session List Entry Expiry panel provides the opportunity to set the expiration time on session lists that don't already have a specific end time already defined. The default expiration is 5 days. You can further refine this by adjusting the days, hours, minutes, and seconds.

The example shown in this topic comes from the Identity Management use case included with the ArcSight Express use cases (**Use Cases** > [All Use Cases/ArcSight Foundation/ArcSight Express](#)).

In this panel, you can use the up/down arrows to set the end-time parameters (days, hours, minutes, and seconds) for all the session lists in the use case.

Expiration time is calculated from the time the entry was made. For example, if an entry is made on Tuesday at 3 p.m. and the default is not changed, the entry would expire on Sunday at 3 p.m.



You can also set the session list entry expiration time individually outside the use case configuration wizard. You can access the session list editor by right-clicking the session list from the use case dashboard (right-click > **Edit Session List**) or from the Resources tree in the Navigator panel (**Resources** > **Lists** > **Session Lists** > right-click > **Edit Session List**). For details, see [“Terminating a Session List Entry” on page 551](#).

For more about session lists, see [Chapter 20, Identity Correlation, on page 543](#).

Return to the list of configuration panels in [“Step 7 - Configuration Panels” on page 523](#).

Chapter 20

Identity Correlation

Identity correlation provides the ability to model users and associate them with events. Identity correlation can be accomplished using **session lists** for some scenarios (*session correlation*) and **active lists** for others (*user or device correlation*).

You can capture and record session-related data in a user-defined *session list* where it can be used for a number of purposes in identifying and tracking users in relation to MAC addresses, IP addresses, machines, network logons, and so forth.

Also, you can use a pre-populated *active list* to find a value and then use the value (as a variable) in a rule. You can use this strategy to identify entities or objects in a variety of scenarios such as correlating various user IDs (logins, e-mail addresses, badge IDs) to unique IDs; mapping unique user IDs to user roles; and even finding the status of a machine by its host name.

The following topics describe scenarios for using both resources, and include step-by-step examples of using sessions lists and active lists with rules and variables for identity correlation.

[“Understanding Session Correlation” on page 543](#)

[“Managing Session Lists” on page 547](#)

[“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#)

[“Using Active Lists to Correlate Users \(Example\)” on page 561](#)

Understanding Session Correlation

You can leverage ArcSight provided resources (pre-defined [Session Lists](#) and [Rules](#)) or develop customized session lists to use for identity correlation, as described here.

How Session Correlation Works

Session correlation captures and records session-related data in a user-defined list, where it can be used by ArcSight's Correlation Engine to:

- Resolve event endpoints against DHCP sessions to identify which device was located at the reported IP address at the time of the event
- Utilize existing maps that link MAC addresses and/or host names to users, if available
- Attribute actions originating from a specific device to its owner
- Extract and resolve user information from VPN logins, including the VPN user name and session characteristics

- Track who accesses a given network node at a given time to trace events that originate from this device to users that were logged in at the time

Session correlation is a three-step process that involves three or more ArcSight resources.



The user defines a session list, then creates a rule to populate it. The results written to the session list can be used anywhere variables are used, such as to trigger other rules, or to populate active channels, dashboards, and reports.

The high-level steps are:

- 1 Create a session list (as described in [“Creating a Session List” on page 547](#)).
- 2 Create a rule to populate the session list (as described in [“Creating a Session List Rule” on page 544](#)).
- 3 Use the session list output wherever needed (as described in [“Using the Session List Output” on page 546](#)).

See also [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#) for a walkthrough of creating and populating a session list with Windows session information.

Creating a Session List Rule

To create a rule that writes new sessions into your session list or that re-sends session start times to your session list:

- 1 In the Navigator panel's drop-down menu, choose **Rules**.
- 2 In the Rules resource tree, right-click a group and select **New Rule**. The Rules Editor displays in the Inspect/Edit panel.
- 3 At the **General** tab, enter the following values:

In this field...	...enter this
Name	Enter a name in the Rule Name text field. The Rule Name should be as descriptive as possible. It is stored in the Event Name data field and if the rule has a Send to Console action, the Rule Name appears in the Event Name column of the grid view. The Rule Name text field is required and restricted to 25 characters.
Common: External ID, Alias	If this rule is referenced by an external system, such as Remedy or vulnerability scanner, enter the pertinent external ID information here. If not, leave these fields blank.
Description	Enter a description in the Description text field. The description should be meaningful and detailed. For example, This rule creates an entry to the DHCP session list when a new DHCP session starts.

In this field...	...enter this
Assign: Owner, Notification Groups	If you wish to specify an owner for this resource and to automatically notify other users when this rule is changed, select existing users and notification groups from the drop-down menu. This step is optional.

- 4 At the **Conditions** tab, enter the conditions that indicate a session start and click **Apply**.
- 5 At the **Aggregation** tab, specify the event fields from the session list that you want to have displayed in the event grid when the rule is triggered by the session conditions specified in the Conditions tab. You should probably aggregate all items you specified in your session list so that those values get populated when the event occurs.
- 6 At the **Actions** tab, set the trigger and the action you wish the rule to take when the conditions are met.
 - a Select the trigger you want to apply to this rule. **On First Event** is the default trigger. This determines which occurrence of the session start conditions trigger the action to write the event to the session list as the session start.

Trigger	Description
On First Event	Triggers the action the first time rule conditions are met.
On Subsequent Events	Triggers the action the second and subsequent times rule conditions are met (not the first).
On Every Event	Triggers the action every time rule conditions are met. This overrides threshold settings.
On Time Unit	Triggers the action based on the time increment specified in the Every... text field in the Add Action dialog box.
On Time Window Expiration	Triggers the action when the threshold settings have expired.
On First Threshold	Triggers the action the first time rule conditions and threshold settings are met.
On Subsequent Thresholds	Triggers the action the second and subsequent times rule conditions and threshold settings are met, not the first.
On Every Threshold	Triggers the action every time rule conditions and threshold settings are met.



You can use references to Velocity Templates as parameters for rule actions to derive values from event fields and variables. (See ["Velocity Templates" on page 1019](#).)

- b After you have selected a trigger, click **Add** to add an action. **Select Session List | Add to Session List**.
- c In the Add Action dialog box at the Session List drop-down menu, navigate to the session list you created earlier. The parameters you set for the session list are displayed in the Session Field Mapping area.

- d** In the Session Field Mapping area at the Start Time field, select which event time stamp you wish to use to record as the official start time.

Start Time	Description
End Time	The time the event ended.
Manager Receipt Time	The time the event arrived at the Manager.

- e** For the remaining fields you specified in your session list that have multiple choices, select which value you wish to use for your session list and click **OK**. You can find a description of the data fields, see [“Data Fields” on page 867](#).
- 7** When all parameters are entered, click **OK**. The relevant events matching this rule now populate the session list.

Using the Session List Output

Once the session list has been populated by events that trigger the session list rule, the session data can be accessed anywhere variables can be used:

- Active channels
- Data monitors
- Dashboards
- Filters
- Reports
- Rules

Creating a Variable

From the editor of one of the resources (active channel, data monitors, dashboards, filters, reports, rules), you can create a variable. This variable is derived from the session time-stamp data stored in the session list.

To create a variable:

- 1** In the Navigator panel's drop-down menu, choose the resource that you wish to consume the session list data. These steps use Filters as an example. Right-click a filter group and select New Filter.
- 2** At the Attributes tab, enter a name for the filter, and optionally, external ID and alias information, and/or owner and notification group information.
- 3** At the Variables tab, click **Add**, then choose either Local Variable or Global Variable (depending on whether you want this variable shared across all resources). In the "Add Variable" dialog, enter the following values and click **OK**:

In this field...	...enter this
Name	Enter a name for the variable. This name appears in the <Lists> menu available from the Common Conditions Editor (CCE) . Spaces and special characters are OK.
Function	In the Function pull-down menu, select List Functions > GetSessionData .
Arguments	In the <field name> pull-down menu, select the session list you created previously.

In this field...	...enter this
Preview	To preview the results, select an asset from the list of assets reporting events to ArcSight and click Calculate .

- 4 Perform any necessary Session Field Mapping.
- 5 In the Filters tab conditions editor, scroll down to the bottom of the Fields list until you see Variables. Here you see the name of the variable you created in [Step 3](#). In the Operator field, select an operator appropriate for the GetSessionFunction variable you created in [Step 3](#). In the Condition field, enter an appropriate value. Session lists that allow overlapping sessions would take a list of values separated by commas. Session lists that do not allow session overlapping would take a single value. This instructs the filter to derive its values from your session list.
- 6 When you have finished setting all the conditions, click **Apply** to save changes and keep the editor open; click **OK** to save the filter and exit the editor.

Populating a Session List Manually

Session lists are really designed to be populated automatically by rule actions, however, there may be times when you need to populate the list manually. For example, you may wish to enter known values to your session list for testing purposes, or to get session correlation started with known values while you are waiting for the event stream to populate the list with more session-related values.

To manually add data to the session list you just created, see [“Adding a Session List Entry” on page 550](#).

Managing Session Lists

While you can manually update session lists, their real value comes when you author automatic, rule-driven lists with dynamic content.

See also [“Understanding Session Correlation” on page 543](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#).



Note

As described in [“Creating a Session List” on page 547](#), filters improve session list performance by restricting the number of events that must be evaluated. Filters, such as DHCP IP address ranges, are installation-specific. Therefore, consider adding a filter to pre-defined session lists, such as /All Session Lists/ArcSight Foundation/Network Monitoring/DHCP, to improve performance.

Creating a Session List

Note that session lists are usually defined in conjunction with rules specifically tailored to interact with those lists dynamically. Lists not driven by rules are empty or contain only manually added entries that have not timed out.

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Session Lists** tab.
- 3 Right-click a session list group and choose **New Session List**.

- 4 In the Session List Editor, in the Inspect/Edit panel, define the following values.

In this field...	...enter this
Name	Enter a name for the session list. This name identifies the session list in ArcSight pick lists. Spaces and special characters are OK.
Overlapping Entries	Check this box to alert the system to allow multiple instances of key pairings, which keeps the previous session with the same key field open. For example, you might check this box if the list tracks activity for an asset that supports multiple-user logins.
In Memory Capacity (x1000)	This setting indicates the maximum number of session entries the system keeps in memory. 10,000 is the default value. For most cases, 10,000 is appropriate, however, you may wish to adjust this setting if the devices you are monitoring for this session list contain a lot of data to ensure you have adequate memory cache available.
Entry Expiration Time	<p>Enter an expiration time for session list entries. This indicates the time after which entries are marked as terminated (if no explicit termination event is received previous to this).</p> <p>The default is 0 seconds, which means the entry never expires. An entry with no expiry date/time can only be terminated explicitly (through user action on Console, rule actions, or archives).</p>

- 5 Set the **Common** and **Assign** fields as appropriate.
- 6 Define columns for session list entries by clicking the row of the lower panel labeled "<Enter Name>." Columns for Start Time, End Time, and Creation Time are pre-defined.

In this field...	...enter this
Name	Enter a name for each session parameter you wish to track; for example, IP address, zone, or MAC address. The name you enter here appears as a label in the session list, and in the Variable pick list. Names can contain spaces, such as "User name."
Type	<p>Type indicates the data type of the entry. Data types can be:</p> <p>Address (IP address or MAC address)</p> <ul style="list-style-type: none"> • Date • Double • Integer • Long • Resource Reference (with appropriate subtype) • String

In this field...	...enter this
Subtype	<p>There are only two data types that require subtypes: Address and Resource reference.</p> <ul style="list-style-type: none"> • Address – Choose IP address or MAC address. • Resource reference – A Resource reference can refer to any resource, such as Asset, Knowledge Base Article, or Zone.
Key Field	<p>Select one or more fields that must be unique to indicate a session start. In most cases, you would select at least two fields to make a key-value pair. For example, in the case of a DHCP login event, when a new IP and zone combination are written to the list, this indicates that a new session has started.</p>

Columns can only be defined when the session list is created. Column definitions cannot be added, removed, or changed once the new session list is saved.

- 7 Click the **Filter** tab in the Session List Editor and define a filter that limits the number of events considered for the new session list. Session lists without filters must evaluate every event, which can negatively affect performance. The Filter tab presents the familiar [Common Conditions Editor \(CCE\)](#). Although the filter editor is similar, session list filters are not the same as Filter resources. Session list filters use different fields than Filter resources, for one thing.

Session lists are often concerned with logins to specific machines. In this case, you would write a filter that would limit evaluation to IP address ranges of interest. By filtering out all events except those targeting IP addresses in the DHCP server's subnet, for example, you are effectively limiting session list evaluation to inside traffic, reducing the overhead of session list evaluation. Other uses of session lists suggest other installation-specific knowledge that can be used to create session list filters that restrict the number of events matched against the session list.

Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entry** button in the Session List Editor to manually create more entries for the current session list.

Editing Session Lists

- 1 In the Session Lists resource tree, right-click a session list and choose **Edit Session List**.
- 2 Make appropriate changes to the properties of the session list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Moving or Copying Session Lists

- 1 In the Session Lists resource tree, navigate to a session list and drag and drop it into another group.
- 2 Choose **Move** to move the session list, **Copy** to make a separate copy of the session list, or **Link** to create a copy of the session list that is linked to the original session list.

If you choose **Copy**, you create a separate copy of the session list that is not affected when the original session list is edited. If you choose **Link**, you create a copy of the session list that is linked to the original session list. Therefore, if you edit a linked session list, whether

the original or the copy, all links are edited as well. When deleting linked session lists, you can either delete the selected session list or all linked session list copies.

Exporting Session Lists

In the session list viewer, you can export selected entries from an session list to a CSV file. This is useful if you want to manage session list data external to the Console.

- 1 In the Session Lists resource tree, select a session list, and choose **Show Entries**. The data in the session list is displayed in the Viewer panel as session list details.
- 2 On the session list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting Session Lists

- 1 Right-click a session list and choose Delete Session List.
- 2 In the dialog box, click **Delete**.

Adding a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click an entry that is similar to the entry you would like to add. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to post the changed entry as a new one.

Adding a Session List Entry Based on an Existing Entry


- 1 Right-click an item in the Session List resource tree and choose **Edit Session List**. The Session List Entry editor appears in the Inspect/Edit window.
- 2 Click the **Add Entry** button.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to save the new entry. The **Reset** button clears all values.

Deleting a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to delete. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click the entry's **Value** to make changes. The column type may limit the kind of data that can be entered.

- 4 Click **Add** to post the changed entry as a new one.

Terminating a Session List Entry

- 1 In the Session Lists resource tree, right-click a session list and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to terminate. Choose **Terminate Session Entry**.
- 3 Enter the date and time for the session end time. Click the  button for a context menu containing relative times such as Now, 1 hour ago, 1 day from now, and so on. Click **OK**.

Using Session Lists to Correlate Session Data on User Logins (Example)

Using session lists for identity correlation is a three-step process that involves three or more ArcSight resources. The high-level workflow for creating and using session lists for identity correlation is:

- 1 Create a session list.
- 2 Create a rule to populate it.
- 3 Use the session list output.

The results written to the session list can be used anywhere variables are used, such as to trigger other rules, or to populate active channels, dashboards, and reports.

This Help topic steps through an example of building and populating a session list to track Windows user login sessions.

(For a full explanation of working with session correlation, see the overview list of topics in [Chapter 20, Identity Correlation](#), on page 543.)

Example Overview

This example shows you, first, how to create a session list (essentially, a container) with a schema appropriate for storing information about Windows logins and logoffs.

Next, we create two rules to populate the session list:

- A rule that is triggered at start of a successful Windows login and populates the session list with the successful login event data
- A rule that is triggered when a user logs off and populates the session list with the session termination event data

Then, we verify the rules using the Verify Rules with Events tool to make sure that the rules are triggered and that your session list is populated appropriately with session logins and start/end times.

Finally, we create a new report using the session list you just created as the data source, and run the report.



You need a set of canned or live Windows session events (user logins/logoffs) to properly verify the resources you create for this example.

1. Create a Session List to Store Windows Sessions

Start by creating a session list that serves as a container for Windows login sessions.

Choose the **Lists** resource in the Navigator, and click the **Session List** tab. Right-click a user folder and choose New Session List. (For more detailed help on creating session lists, see ["Creating a Session List" on page 547.](#))

In the Session List editor, name the session list, and add the fields as shown.

Session List Attributes	Value
Name	Windows Login Sessions
Overlapping Entries	Disabled (leave unchecked) This example assumes that the Windows server we are monitoring does not support multiple-user logins, which is why we leave Overlapping Entries unchecked.
In MemoryCapacity(x1000)	10



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 684.](#)

Add the following three fields with names and types as shown. Set "Username" as the key-field.

Field Names for Session Lists	Type	Key Fields
Username	String	Enabled
NT Domain	String	
Device	String	

Session List Name

Disable Overlapping Entries if server does not support multi-user logins

Fields: The session list will include these fields. Username, marked as the Key-field, must be unique to indicate a session start.

Name	Type	Sub-type	Key-field
Username	String		<input checked="" type="checkbox"/>
NT Domain	String		<input type="checkbox"/>
Device	String		<input type="checkbox"/>

2. Create Rules to Populate the Session List with Windows Logins

Create two rules with which to populate the session list:

- A rule that triggers on Windows session logins
- A rule that triggers when a Windows session terminates

To create a new rule, choose the Rules resource from the Navigator drop-down menu, right-click a user group, and select New Rule from the context menu. (If you need more help on creating rules, see [“Managing Rules” on page 440](#). For a general introduction to working with rules, see [Chapter 16, Rules Authoring, on page 439](#).)



For this example, first create rules in a user folder under Rules for testing purposes. Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. Only rules deployed in Real-time Rules filter on live events and show up in a live channel when they are triggered. See [“Deploying Real-time Rules” on page 473](#) for more information.

Rule 1: Triggers on Windows Session Logins

Create a rule to populate the session list. Use the following attributes, conditions, aggregation, and actions as shown below.

Attributes

On the **Attributes** tab, enter the name of the session login rule as follows.

- **Name:** Successful Windows Login

The screenshot shows the 'Inspect/Edit' window for the rule 'Successful Windows Login'. The 'Attributes' tab is selected. The rule name is 'Successful Windows Login'. The 'Common' section shows 'Resource ID' as '5+DQZ8Q0B8BCAEKKAQjivLA=='. The 'Assign' section shows 'Owner' as 'Vicky'. The 'Parent Groups' section shows 'Vicky's Rules' with a path of '/All Rules/Personal/Vicky's Rules/'. The 'Creation Information' section shows 'Created By' as 'Vicky', 'Creation Time' as '27 Sep 2006 14:05:35 PDT', and 'Time Since Creation' as '2 day(s) 3 hour(s) 32 min(s) 35 sec(s)'. The 'Last Update Information' section shows 'Last Updated By' as 'Vicky', 'Last Update Time' as '27 Sep 2006 17:06:13 PDT', and 'Time Since Last Update' as '2 day(s) 31 min(s) 57 sec(s)'.

Conditions

Click the **Conditions** tab for the login rule, and enter the following conditions.

- Target User Name Is NOT NULL
- Target Nt Domain Is NOT NULL
- Device Host Name Is NOT NULL

Setting these conditions causes the rule to be triggered on any event that includes a device host name and a user name where the target is a Windows NT domain. (For more information on using the Common Conditions Editor or "CCE", see ["Common Conditions Editor \(CCE\)" on page 846](#) and ["Conditional Statements" on page 859](#).)

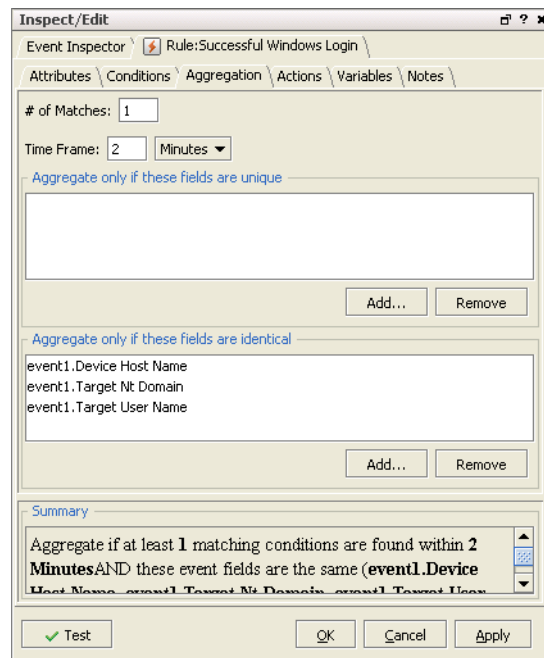
The screenshot shows the 'Inspect/Edit' window for the 'Rule Editor'. The 'Conditions' tab is selected. The 'Event conditions' section shows a tree view with 'event1' expanded, showing an 'AND' condition with three sub-conditions: 'Device Host Name != NULL', 'Target Nt Domain != NULL', and 'Target User Name != NULL'. The bottom section shows a table with columns 'Name', 'Op', and 'Condition'. The table contains two rows: 'Device Asset Local ID' and 'Device Direction'.

Aggregation

Click the **Aggregation** tab for the login rule. Under **Aggregate only if these fields are identical**, click **Add...** to bring up the Add Fields dialog. Select the following fields on which to aggregate and click OK to add them to the rule.

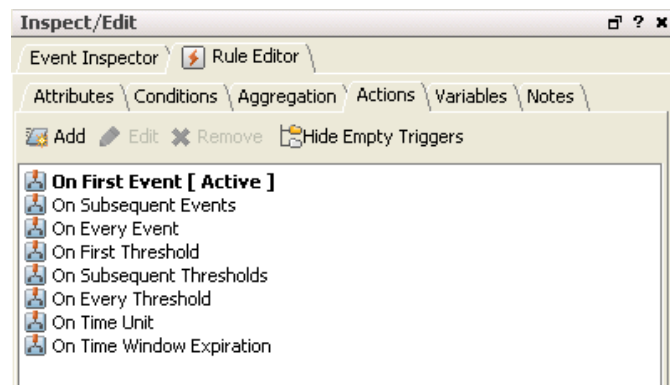
- Target User Name
- Target Nt Domain
- Device Host Name

Aggregation can be used to combine multiple events (as specified in the number of matches) into a single entry for the session list. But in this case (where we are aggregating events with identical fields on only a single match), we are specifying fields in the Aggregation tab for the purpose of making those same fields available in the Actions tab.



Actions

Click the **Actions** tab for the login rule.



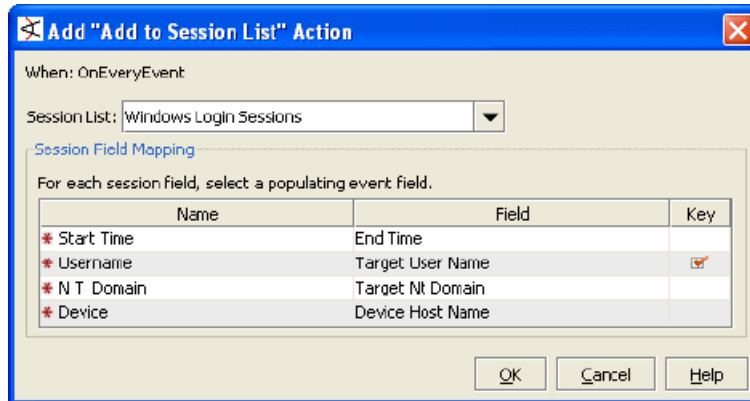
Select **On Every Event**, and click **Add | Session List | Add to Session List**.

In the Session List drop-down menu on the Add dialog, select the Windows Login Sessions session list you created in the first step.

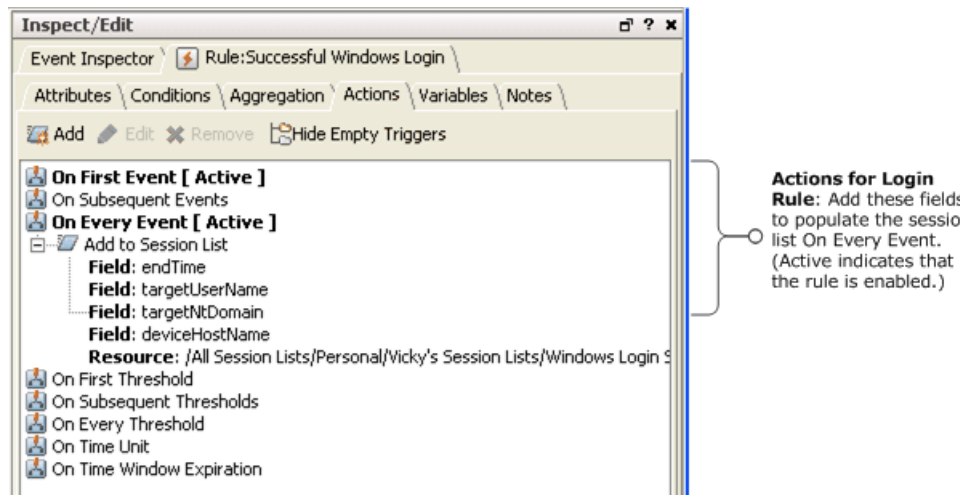
Map the fields as follows.

- Start Time: End Time
- Username: Target User Name
- NT Domain: Target Nt Domain
- Device: Device Host Name

This prompts the rule to add a login event to the Windows Login Sessions list every time a matching login event occurs.



Click **OK** on the Add to Session List dialog to add the actions to the rule. When the actions are properly configured, they are displayed under the "On Every Event" action as shown. Windows session logins are added to the session list on every event.



Click **OK** to save the session login rule.

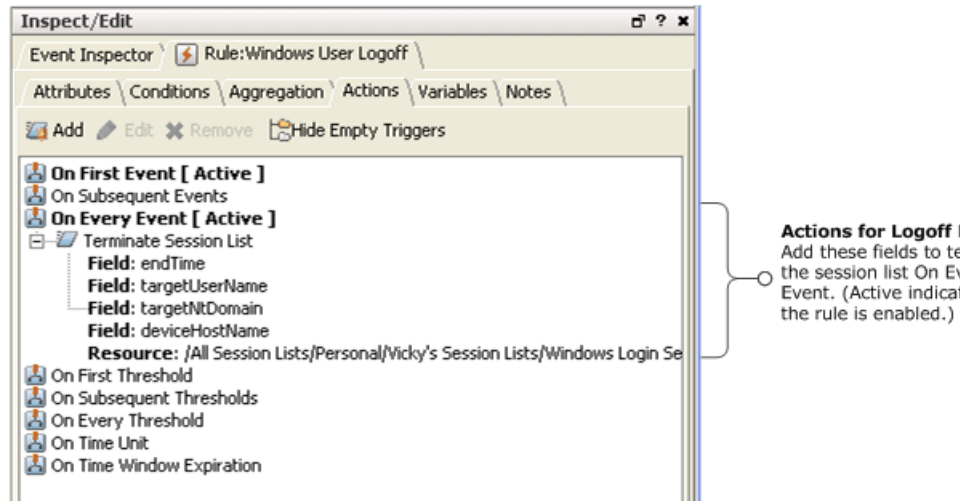
Rule 2: Triggers on Termination of Windows Sessions

Create a rule to populate the session list with Windows session termination information. Define this "terminate session list" rule with the same settings as the "add to session list" rule you just created, with the following differences specific to terminating the session:

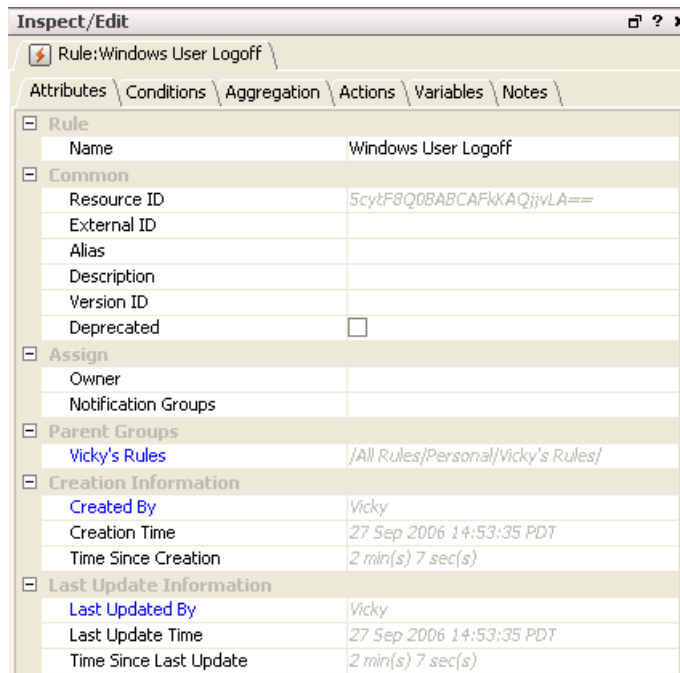
- On the **Attributes** tab, Rule Name is Windows User Logoff (instead of Login).
- On the **Conditions** tab, define the same Conditions as in the previous rule.
- On the **Aggregation** tab, aggregate on the same fields as in the previous rule.

- On the Actions tab, define the same actions as in the previous rule but add the actions to **Terminate Session List** instead of Add to Session List. (The menu path for adding the logoff rule is **Add | Session List | Terminate Session List**.)

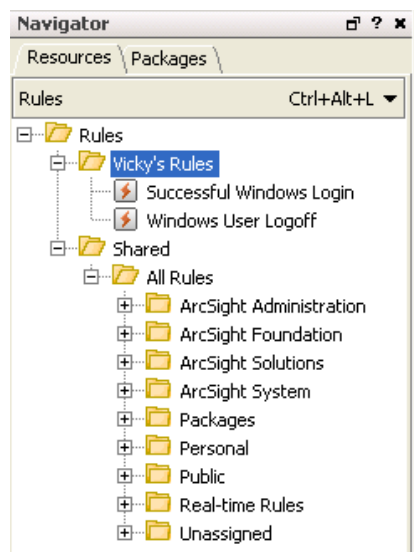
The **Actions** tab for the logoff rule is shown below. Notice that for Windows logoffs, the rule triggers the action to add an entry to the terminate session list on every logoff event.



Here is an example of the **Attributes** tab for the logoff rule when it is completely configured.



3. Verify Rules



For each rule, we want to answer some key questions to verify the rules are working as expected.

Rule	Verify Questions
Add to Session List	Is the rule triggered when a Windows logon occurs? Are the values inserted into the Session List?
Terminate Session List	Is the rule triggered when a Windows logoff occurs? Is the End Time in the Session List changing according to the rule (that is, is it terminating the session for this user)?

To test the rules before deploying in real time, we can use an active channel created from the Verify Rule(s) with Events option, and also view entries in the Windows Login session list we created in the first step of this example.

- 1 Select the Rules folder that contains them, right-click, and choose **Verify Rule(s) with Events** in the context menu. You can create a New Active Channel to test the rules.

For more information on testing rules, see [“Verifying Rule\(s\) with Events” on page 470](#) (formerly Replay-with-Rules).



Once you have created and verified rules and are ready to deploy them on real-time events, move or copy the rules to your user folder under Real-time Rules. Only rules deployed in Real-time Rules filter on live events and show up in a live channel when they are triggered. For more information, see [“Deploying Real-time Rules” on page 473](#).

4. Use the Session List in a Report

You can leverage session lists in a variety of resources including reports, active lists, active channels, data monitors, and as input to other rules. (For example, you could use a rule to correlate multiple failed VPN logins over a short timeframe with a particular user entry in the session list. You might specify that if both conditions are met, add the user to an active list such as /Active Lists/Shared/All Active Lists/ArcSight System/Threat Tracking/Suspicious List.)

For this example, use the session list in a simple report.

Create a new report on the session list for this example. The steps are:

- Create a report
- Choose a report template
- Choose the session list as the data source for the report
- Run the report

Here are step-by-step instructions for creating a report showing the Windows logins

- 1** In the Navigator, choose the **Reports** resource and click the **Templates** tab.
- 2** Expand the folder /Report Templates/Shared/All Report Templates/ ArcSight System/, right-click **Simple Table Portrait** and choose **New Report from Template**.
- 3** Provide a name for the report (for example, Windows Login Sessions).
- 4** Click the **Data** tab and select Session Lists for the Data Source type and the Windows Login Sessions list for the data source.
- 5** Click **Apply** or **OK** to save the report.
- 6** Still under the Reports resource in the Navigator, click the **Reports** tab. The report you created is displayed under your user folder.
- 7** Select the new report, right-click and choose **Run Report** or **Run Report with Defaults** from the context menu.

Following is an example of an HTML version of the Windows Login Sessions report.

Report					
Username	N T Domain	Device	Start Time	End Time	Creation Time
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15	Sep 27 2006 16:04:15	Sep 27 2006 16:23:06
shannon		churchill	Sep 27 2006 16:04:15		Sep 27 2006 16:23:06
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55
steve		belmont	Sep 27 2006 14:12:33	Sep 27 2006 14:12:33	Sep 27 2006 15:18:55

For more information on creating and using reports, see [“Creating Reports” on page 385](#) and [“Running Reports” on page 423](#).

Using Active Lists to Correlate Users (Example)

You can use active lists to find a value and then use value (as a variable) in a rule. You can use this strategy to identify entities or objects in a variety of scenarios; for example:

- Given that logins from the same attacker are showing up under multiple IP addresses, find out whether the attacks are coming from the same machine with different IP addresses.
- Correlate user logins (e.g., onto server machines) with physical building or room entry. A user's login ID is not the same as badge ID. You use an active list to map various user identifiers (login, e-mail, badge) to a unique user ID (UUID) for each user.
- Map UUIDs to user roles.
- Find the current status (e.g., up, down) of a given machine host name.

- Find the current status (e.g., up, down) of a given SmartConnector.

(The last two can be handled using data monitors also.)

This example shows how to build a rule that leverages unique user ID information from a pre-populated active list to correlate user logins on critical servers with badge swipe entries to the server room. The rule is triggered when a server user login does not have a matching badge swipe ID.

The example highlights how an active list with values can be leveraged for identity correlation. In this case, the active list collects target user IDs for the same user from different sources (e.g., user login, badge ID, e-mail address, phone number) and maps those different IDs to a unique user ID. The rule then uses the unique user ID to correlate badge swipe IDs with user login IDs.

(For a full explanation of working with identity correlation, see the overview list of topics in [Chapter 20, Identity Correlation, on page 543](#). For more about active lists, see also ["Managing Active Lists" on page 571](#), ["Case-Insensitive Lookup in Active Lists" on page 573](#), and ["Using Rules to Populate an Active List" on page 574](#).)

Example Overview

For this example, consider a scenario where server machines with critical data reside in a secure area. Only users in a specialized group are allowed physical access to the server room (with badge swipe on a card reader) and user login permissions to the servers. This example assumes a policy against remote logins to the server room machines.

We want to monitor and correlate user access to the server room (badge swipes) and user logins on the server machines, and take action (e-mail notification) if our access policies are violated. Some examples of policy violations that we want to catch are:

- Cases where someone logged into a server but no badge swipe is registered. This could indicate policy violations such as remote logins or unauthorized server room entry (e.g., server room door was left open)
- There is no matching badge swipe ID for a server console login (e.g., a user stole someone's badge to get into the server room, then logged in to the server with a different user ID)

This example assumes a pre-populated active list with values with a schema appropriate for storing information about user IDs. The active list keys off of user identifiers from various sources (e.g., user login, e-mail address, phone number) and map these variants to the same unique user ID (UUID).

The UUID can then be used as a variable in a rule for correlating user login IDs with badge IDs. We'll show how to create this rule, which leverages the user information collected in the active list.

1. Build and Populate the Active List with User IDs

This example assumes that you have a pre-populated active list that maps user identifiers from various sources (badge ID, user login, e-mail, phone number) to unique user IDs (UUIDs). For the purposes of the example, we are interested in correlating badge IDs and user logins for users who log into critical servers. The active list (populated with our list of users) provides the "User Map" we need to derive each user's unique ID.

The active list definition includes the following two fields with names and types as shown. "User Identifier" is set as the key-field. This information is available in incoming events

(badge swipes and user logins). Each user identifier is mapped to a UUID. Assume, for this example, that we got this mapping from IT or Human Resources departments. The UUID value is the information we'll want to extract from this list via a variable.

Field Names for Session Lists	Type	Key Fields
User Identifier	String	Enabled
UUID	String	

Inspect/Edit Active List: User Map

Attributes Notes

Active List

- Name: User Map
- Optimize Data: ☐
- Capacity (x1000): 10
- TTL Days: 0
- TTL Hours: 0
- TTL Minutes: 0

Common

- Resource ID: HwI3RHX8B8CAD5TxJ+nsKg==
- External ID:
- Alias:
- Description:
- Version ID: AAAAAJxPh56sdUzC
- Content Version ID:
- Deprecated: ☐

Assign

- Owner:
- Notification Groups:

Parent Groups

- All Active Lists: /All Active Lists/

Creation Information

- Created By: admin
- Creation Time: 30 Jan 2009 17:26:25 PST
- Time Since Creation: 4 day(s) 22 hour(s) 13 min(s) 35 se...

Last Update Information

- Last Updated By: admin
- Last Update Time: 3 Feb 2009 18:17:00 PST
- Time Since Last Update: 21 hour(s) 23 min(s)

(Name)
(Description)

Data: ☐ Event-based ☒ Fields-based ☒ Key Fields

Name	Type	Sub-type	Key-field
User Identifier	String		<input checked="" type="checkbox"/>
UUID	String		<input type="checkbox"/>

Annotations:

- Active List Name: Points to the 'Name' field in the 'Active List' section.
- Fields: The active list includes these fields. User Identifier, marked as the Key-field, is the value returned from various sources (badge, user login, etc.).
- The unique user ID (UUID) that the user identifier maps to is provided here through an LDAP system, or some other data source. This is the focus of this active list; to map various user IDs to this UUID. The UUID will be used as a variable in a rule.

Populating an Active List with User Data

There are various ways to populate an active list with this kind of user information:

- Human Resources (HR) or IT database
- Identity management system
- Import from a CSV file (in the Navigator, right-click the active list and choose **Import CSV File**. See ["Importing an Active List" on page 577](#))

■ Manually add names to the list



Note that this is a different type of task than populating an active list based on data gleaned from events (e.g., [“Using Rules to Populate an Active List” on page 574](#)).

In this example, we *already have the “map” and the values we need (the unique user IDs) provided in the active list*, and we are going to feed them into a rule as a variable.

In the other example (using rules to populate the active list), we are using a rule to add items to an active list and to discover and use values as items are added to the list.

Here is an example of an active list pre-populated with user information.

User Identifier	UUID	Creation Time	Last Modified Time	Count
badge0123	SamanthaStevens	3 Feb 2009 18:21...	3 Feb 2009 18:21...	1
badgeID4156	StephanieMartinelli	3 Feb 2009 18:17...	3 Feb 2009 18:17...	1
badgeID5245	RobertJackson	28 Jan 2009 16:3...	3 Feb 2009 18:18...	1
rjackson	RobertJackson	28 Jan 2009 16:3...	3 Feb 2009 18:18...	1
rjackson@xyz.com	RobertJackson	4 Feb 2009 15:50...	4 Feb 2009 15:50...	1
samstevens	SamanthaStevens	3 Feb 2009 18:21...	3 Feb 2009 18:21...	1
samstevens@abc.com	SamanthaStevens	4 Feb 2009 15:49...	4 Feb 2009 15:49...	1
stephmartinelli	StephanieMartinelli	3 Feb 2009 18:17...	3 Feb 2009 18:17...	1
stephmartinelli@xyz.com	StephanieMartinelli	4 Feb 2009 15:50...	4 Feb 2009 15:50...	1

If you want to follow along with the example but don't have a database or spreadsheet of user information handy, you can manually add example data:

- 1 Build and save the User Map active list definition as described in [“1. Build and Populate the Active List with User IDs” on page 562](#).
- 2 In the Navigator, right-click the User Map active list and choose **Show Entries**.
The list is shown in the Viewer panel.
- 3 Click the Add Entry button at the top right of the list to get the Active List Entry Editor.
- 4 Use the Active List Entry Editor to manually add user identifiers and unique user IDs. Click **Add** on the editor to add each line of data. To support the example, add at least two lines for each user. Keep the UUID the same, but the user identifiers different to illustrate the mapping.

User Identifier	UUID
badge0123	SamanthaStevens
samstevens	SamanthaStevens
badgeID5245	RobertJackson
rjackson	RobertJackson

2. Create a Rule that Uses Active List Values to Correlate User IDs

Now that we have an active list that maps various user IDs to unique user IDs (UUIDs), we can create a rule that makes use of the active list to correlate events coming from the same user with different user IDs (such as a badge swipe ID and a server login ID).

The following sections show how to define this example rule.

Attributes

On the **Attributes** tab, provide a name for the rule.

■ Name: Server Room Console Login Policy

Variable

Next, we'll define a variable we can use to find unique user IDs (UUIDs) in the active list we created in the previous step ("[1. Build and Populate the Active List with User IDs](#)" on [page 562](#)).

Create a variable called `UserMap`. (Click the **Variables** tab for your rule and click **Add** to begin). Provide these values for the variable definition.

Option	Specify this Value
Name	<code>UserMap</code>

Option	Specify this Value
Function	<p>GetActiveListValue</p> <p>Use the drop-down menu to navigate to this function, which is found under "List Functions".</p>
List	<p>UserMap</p> <p>This is the active list we created in the previous step ("1. Build and Populate the Active List with User IDs" on page 562).</p>
User Identifier (Active List Key field mapping)	<p>Target User ID</p> <p>Use the pull-down under "Field" to select Target User ID event field.</p> <p>For matching events, the rule uses the value in the Target User ID field as a lookup key in the active list.</p> <p>For example, if the Target User ID is a login ID of "samstevens", a badge ID of "badge0123", or an e-mail address of "samstevens@abc.com", all of these resolve to a unique user ID of "SamanthaStevens" in the active list mapping. The variable value passed to the rule to be evaluated in a condition would be SamanthaStevens, the UUID for any of those user identifiers.</p>

The following figure shows the example variable definition on the Add Variable dialog.

Add Variable

Name: UserMap

Function: GetActiveListValue

Retrieve ActiveList value

Arguments

List: User Map

Field Mapping

For each key field, select a matching event field.

Name	Field	Key
User Identifier	Target User ID	<input checked="" type="checkbox"/>

Preview

Set a value for each key field.

Name	Value
User Identifier	

Calculate

OK Cancel Help

Click **OK** to save the variable.

The new variable is listed on the Variables tab as shown below.

Name	Expression
UserMap	get_activelist_value(\"/All Active Lists/User Map\")

Conditions

We define the rule conditions so that each time a server machine login occurs, the rule conditions are evaluated. (The `ServerRoomConsoleLogin` condition causes this to happen.)



For more information on using the Common Conditions Editor (CCE), see [“Common Conditions Editor \(CCE\)” on page 846](#) and [“Conditional Statements” on page 859](#).

A comparison ([Matching Event](#)) is made between server room logins and badge swipe IDs in a 2-minute time window. The matching event uses our `UserMap` variable (see [“Variable” on page 565](#)) to get the unique ID from the active list we built in the previous step ([“1. Build and Populate the Active List with User IDs” on page 562](#)).

The rule is triggered in cases where you do not find a matching badge swipe ID for a user login.

We define the rule conditions as follows.

- ◆ The `ServerRoomConsoleLogin` condition finds server room machine logins via the event name and asset category. The summary of this condition is:

```
ServerRoomConsoleLogin : ( Name = Console Login AND Target
Asset ID InGroup("/All Asset Categories/Server Room
Machines/") )
```

This is the “start” condition that causes the rule conditions to be evaluated because **it is looking for server logins**.

- ◆ We define a [Matching Event](#) condition that correlates server machine logins (one type of user identifier) with badge IDs used for server room entry (another type of user identifier) based on the unique user ID (UUID) from the Active List.

We do this by using the `UserMap.UUID` variable we created for this purpose (see [“Variable” on page 565](#)).

Matching Event: `ServerRoomConsoleLogin.UserMap.UUID = BadgeSwipe.UserMap.UUID`

If we find a badge ID matches for all server logins, the rule is not triggered. If there is a server login with no matching badge ID within our time window, the rule is triggered.

- ◆ If someone logs in, we want to find a matching badge swipe ID for it. Since we are looking for users who logged in to servers but did not use their own badges to enter the room, we add a condition specifying that no badge swipe event occurred for this user. The summary of this condition is:

```
! BadgeSwipe : Name = Badge Swipe Event
```

The following figures show the rule conditions definition (Edit panel) and summary (Summary panel).

Matching Event Condition: Correlates server login IDs with badge swipe IDs based on unique IDs (UUIDs) gleaned from the active list. The UserMap variable is used to get UUID values from the active list.

Server Room Console Login Condition: Finds server room machine logins (via event name and asset category). This is the "start" condition that causes the rest of the rule conditions to be evaluated.

Not Badge Swipe Event Condition: We are looking for users who logged in but did not use their own badges to enter the room. Adding this condition completes the scope of the conditions. When there is a server login, the rule correlates IDs (via the Matching Event), but triggers only if there is no matching badge swipe (this condition).

Below is an example of a Rule Conditions Summary.

Matching Event:
`SeverRoomConsoleLogin.UserMap.UUID = BadgeSwipe.UserMap.UUID`

SeverRoomConsoleLogin :
`(Name = Console Login AND Target Asset ID InGroup(\"/All Asset Categories/Server Room Machines/\"))`

! BadgeSwipe :
`Name = Badge Swipe Event`

Aggregation

For this example, use default aggregation settings. Aggregate on 1 match in a 2 minute timeframe.

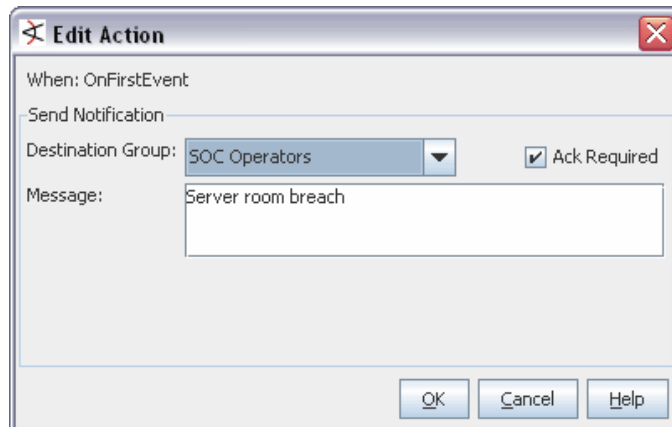
Actions

Click the **Actions** tab for the rule to set up an action to take if the server room is breached.

Select **On First Event** (this trigger is activated by default), right-click and choose **Add > Send Notification** to bring up the Add "Send Notification" Action dialog.

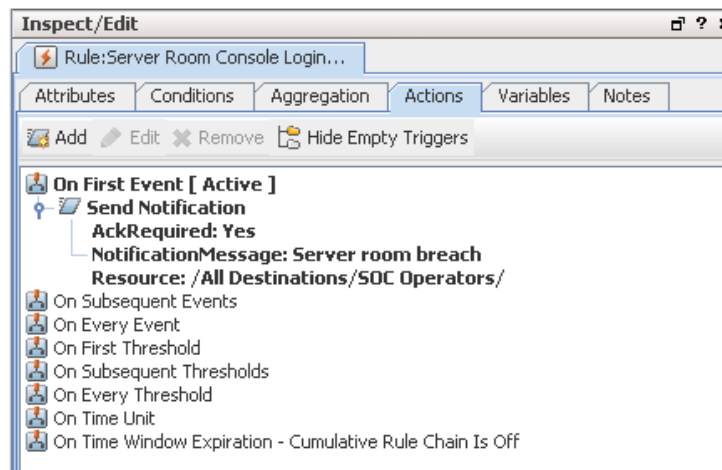
Choose the Destination Group for the e-mail, type in a message, and click **OK** to add this action to the On First Event trigger.

For this example, we chose **SOC Operators** as the Destination Group. Our message is **"Server room breach"**.



Click **OK** to save the notification definition.

When the action is configured, it is displayed under the "On First Event" trigger as shown in the figure. According to this rule, a message is sent on the first trigger event; the first event in every time window that indicates a server room policy violation.



Click **Apply** or **OK** on the rule editor to save the example rule.

Chapter 21

List Authoring

Active Lists and Session Lists are important tools for tracking traffic with IP addresses of interest.

- [“Managing Active Lists” on page 571](#)
- [“Managing Active List Groups” on page 578](#)
- [“Managing Session Lists” on page 579](#)

Managing Active Lists

While you can manually update active lists, their real value comes when you author automatic, rule-driven lists with dynamic content. See [“Creating an Active List” on page 571](#) and then [“Using Rules to Populate an Active List” on page 574](#).

Creating an Active List

Active lists are usually defined in conjunction with *rules* specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules are empty or contain only manually added entries that have not timed out. (See [“Using Rules to Populate an Active List” on page 574](#) and [“Rules Authoring” on page 439](#) for more information on how to create rules that work with active lists.)

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Active Lists** tab.
- 3 Right-click an active list group and choose **New Active List**.
- 4 Fill in fields and select options as follows.

In this field...	...enter this
Name	Enter a name for the active list. This name identifies the active list in ArcSight pick lists. Spaces and special characters are OK.
Optimize Data	If you want to create a hash-based list, click Optimize Data to toggle it on. This option reduces the memory usage of an active list. It is useful for active lists with more than 1,000 entries or for lists that contain a large amount of information per entry. See “Optimize Data with Hash-Based Active Lists” on page 792 (in the reference topic “Active Lists” on page 790).

In this field...	...enter this
Capacity (x1000)	<p>This setting indicates the maximum number of active list entries the system keep in memory. 10,000 is the default value. For most cases, 10,000 is appropriate, however, you may wish to adjust this setting if the devices you are monitoring for this active list contain a lot of data to ensure you have adequate memory cache available.</p> <p>Notes:</p> <ul style="list-style-type: none"> • This represents a limit on in-memory capacity only. (If you select Partially cached, more entries are retained but this has an impact on performance when it is necessary to retrieve active list items from the data base.) • If the maximum number of entries is reached, an existing entry is randomly selected and removed. • Capacity influences the maximum memory that can be consumed by the active list. The memory usage is proportional to the number of entries in the list, which usually are less than the capacity. Capacity affects memory usage, but has little if any impact on performance.
TTL Days, TTL Hours, TTL Minutes	<p>In the TTL (Time To Live) fields, set the number of Days, Hours, or Minutes an unused result should remain on the active list before it is removed. Use 0 (zero) to cause the field to never expire. The maximum number of days is 99999.</p>
Allow multi-mappings	<p>Check this box to allow multiple instances of key pairings. This enables a single key, such as an actor attribute, to map to multiple values, such as a set of roles. You can use this to return a list of entries with the same value for the key field.</p> <p>For example; with multi-mappings enabled, you can create an active list that could return multiple roles for an actor named Clark Kent (reporter, superhero, space traveller) or multiple names associated with a farmhouse in Kansas (Clark Kent, Superman, Kal-El).</p>
Partially cached	<p>When Partially cached is selected, additional entries beyond the in-memory Capacity (x1000) maximum are stored and retrieved from the database.</p> <p>Using "Partially cached" increases overall capacity but can impact performance (because it takes more time to retrieve list entries from the database).</p>
Common and Assign fields	<p>Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see "Common Resource Attribute Fields" on page 684.</p>

In this field...	...enter this
Data: Event-based, Fields-based	<p>In the Data panel, choose Event-based or Fields-based lists.</p> <ul style="list-style-type: none"> The Event-based option is convenient for choosing event attributes as found in existing events. When checking or adding to an Event-based list, you only need to supply an event. <p>Select event attributes or define arbitrary fields for list data collection.</p> <ul style="list-style-type: none"> The Field-based option offers detailed event and attribute selection controls that involve mapping fields to event attributes. <p>For Fields-based lists optionally check Key Fields to enable a per-field Key option, and then select one or more data fields that must be unique.</p> <p>For example, the Arcsight provided active list ArcSight Foundation/Configuration Monitoring/Assets with Recent Configuration Modifications uses fields-based data, and keys on unique values for asset address, zone, and name.</p> <p>Field-based lists that use "Key Fields" are known as active lists with values. (For more information, see "Active Lists with Values" on page 793.)</p>

5 Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entries** button in the Active List Editor to manually create more entries for the current active list.

Case-Insensitive Lookup in Active Lists

By default, active list lookups are case-sensitive. For example, suppose you create an active list designed to capture user logins, aggregated on user name. (If user "John" logs in 10 times and user "Ringo" logs in 7 times, you want the Active List to display two lines: one line showing John's 10 logins, and another showing Ringo's 7 logins.)

You then need to create a rule to populate the list with login information. (See ["Using Rules to Populate an Active List" on page 574.](#)) If all login names received from your devices are formatted in the same "case" (upper case, lower case, or initial caps), the list provides the desired display. However, if the user names arrive in different formats from active directories and other sources (e.g., John, JOHN, and john for a single user), by default the list and associated rule do not aggregate these different forms of the same user name on a single line, but rather treat them each as a different login names.

If you do not want case-sensitive results (as, in this example), you can use either the **ToUpper** function or the **ToLower** function in a **Variable** as a part of the rule(s) that populate your active list. You can use one of these functions as a variable in a rule, and map it (as a "DeviceCustomString") to any field in the active list for which you want to normalize upper/lower case format. The following topic provides a walk-through example that shows how to make case-insensitive active lists. See ["Using Rules to Populate an](#)

[Active List](#) on page 574, especially the sections [“Use Variable to Make Active List Case-Insensitive”](#) on page 575, [“Aggregation”](#) on page 575, and [“Actions”](#) on page 576.



Please keep in mind that more fine-grained conditions logic requires more processing and can have a performance impact. For example, specifying a case-insensitive active list requires more processing than a case-sensitive active list. Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation.

Using Rules to Populate an Active List

Typically, active lists are defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. (See [“Rules Authoring”](#) on page 439 for more information on how to create rules.)

Example

For example, to create an active list that captures information about VPN login events, you need to create both (a) the active list that forms the *table* or *shell* to store/display the data, and (b) the rule(s) to capture and send matching events to the list. The rules **populate** the list for you.

This example shows how to create an active list and a rule that work together to capture VPN login events. The active list shows the number of logins by user name.

Example Active List

To try out this example, first create a Fields-based active list named “VPN Events”, with fields named [User Name](#) and [Category](#), both of type [String](#). Set [User Name](#) as the Key field. Click **OK** to save this active list.

* Data: <input type="radio"/> Event-based <input checked="" type="radio"/> Fields-based <input checked="" type="checkbox"/> Key Fields			
Name	Type	Sub-type	Key-field
User Name	String		<input checked="" type="checkbox"/>
Category	String		<input type="checkbox"/>

Example Rule to Populate Active List

Next, create a rule also named “VPN Events” to populate the active list with user names and category information for matching login events.

What the Rule Does


The goal is to define this rule to look for VPN login events, using values found in [Event Name](#) and [Category Device Group](#) fields as indicators of such events. A matching event triggers the rule. When triggered, the rule interacts with our “VPN Events” active list as follows.

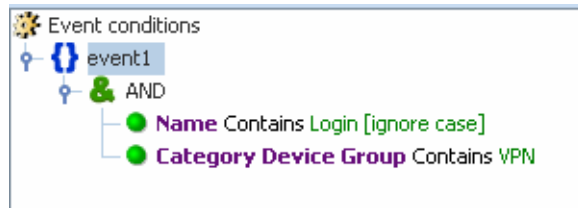
Populate this field in the Active List	With the value from this field in incoming events
User Name	Target User Name
Category	Category Device Group

Conditions

Set **Conditions** to capture events when the **Event Name** contains [Login](#) and **Category Device Group** Contains [VPN](#). To capture event names from various sources that might be

formatted differently (e.g., in all upper case, all lower case, or initial capitalization),

Uncheck the Case-Sensitive  option next to the Event Name field.



This shows up in the **Conditions Summary** tab as follows:

```
event1 :
( Name Contains Login [ignore case] AND Category Device Group Contains VPN )
```



Please keep in mind that more fine-grained conditions logic (as used in this example) requires more processing and can have a performance impact. For example:

- Specifying that a field be case-insensitive requires more processing than the default case-sensitive setting.
- Using "<SomeField> Contains <SomeString>" for a field lookup requires more processing than writing a field lookup like "<SomeField> = <SomeString>".
- Combining these types of conditions (as shown in this example) is even more performance-intensive (e.g., doing a lookup on <SomeField> Contains <SomeString> and making that case-insensitive).

Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation. Streamlining conditions wherever practical helps to optimize system performance.

Use Variable to Make Active List Case-Insensitive

For this example, we want to make our active list *case-insensitive*. That is, since **User Name** is the active list *key field*, we want to aggregate matching events from the same user regardless of the original capitalization format of the user name in the event. If 3 events come in with user name "Jeff", and 4 more come in with user name "jeff", these should be shown on a single line in the active list showing that Jeff logged in 7 times. As described below, we'll map a **Variable** String Function called **ToUpper** to achieve this. (You can also use **ToLower**.)

On the **Local Variables** tab in the rule, create a variable named **ConvertToUpperCase**, select the String Function **ToUpper**, and select Target User Name as the argument. Click **OK** to save the variable. In subsequent steps, this variable inserts Target User Name values in the active list. This way, all lookups from the active list use upper case key field values.



Please keep in mind that more fine-grained conditions logic requires more processing and can have a performance impact. For example, specifying a case-insensitive active list requires more processing than a case-sensitive active list. Use conditions logic like this only as necessary, and weigh your performance requirements as a part of content creation.

Aggregation

On the **Aggregation** tab in the rule, select the fields for aggregation *only if they are identical*. In the Add Field dialog, set Aggregation for event1 on **Category Device**

Group, `ConvertToUpperCase` (our variable, which you select in Add Field's Local Variables tab), and `Device Custom String`.

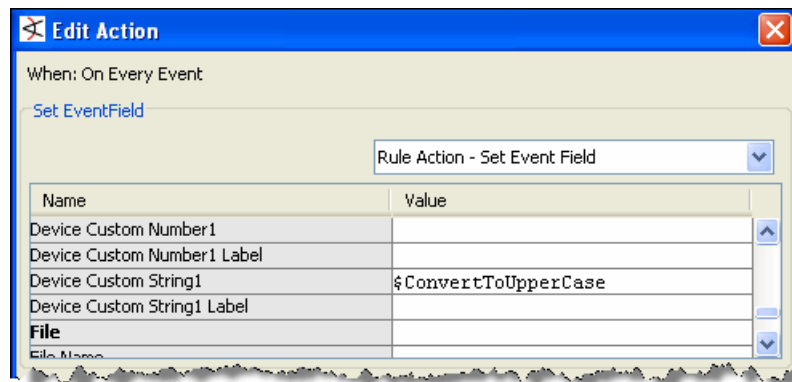
Aggregate only if these fields are identical

```
event1.ConvertToUpperCase
event1.Category Device Group
event1.Device Custom String1
```

Actions

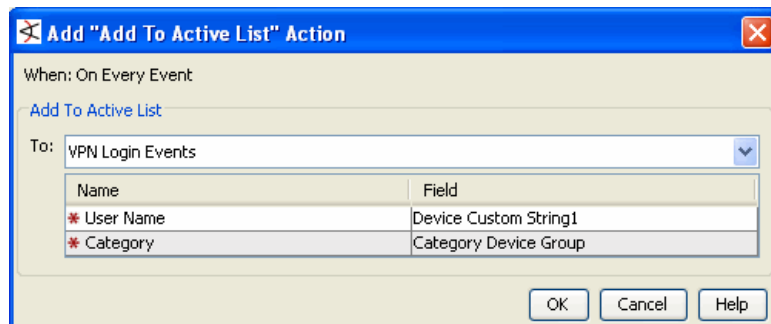
Activate the rule **Actions** option **On Every Event** (de-activate others), and select **Add to Active List**.

- **Insert `ConvertToUpperCase` variable into Active List.** Select **On Every Event**, right-click and choose **Add Set Event Field**. Map `Device Custom String 1` to `$ConvertToUpperCase`. (This is called the velocity template for the function. See "Using Velocity Expressions in Rule Actions" on page 1022.)



- **Add values for User Name and Category to Active List.** Map the fields as follows:

- ◆ User Name: Device Custom String1
- ◆ Category: Category Device Group

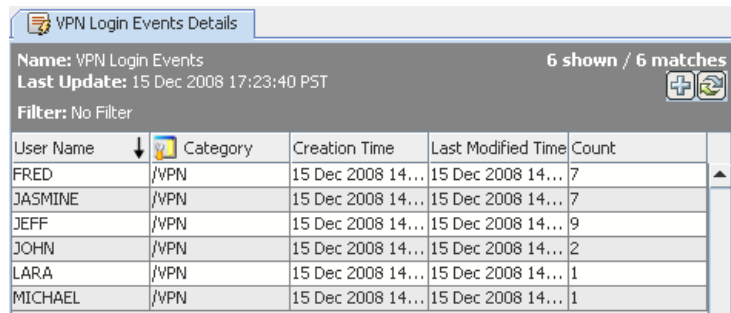


Save and Test

Click **OK** on the Rule Editor to save the rule.

When you are ready to test this; remember to drag-and-drop the rule(s) into the Real-time Rules folder to deploy them. When you do this, you'll get a choice of whether to move, copy, or link them. Linking is often most efficient. (See "Deploying Real-time Rules" on page 473.)

When the VPN Events rule is triggered, user names are added to the VPN Events active list.



The screenshot shows a window titled "VPN Login Events Details". It displays a table with 6 entries. The table has columns: User Name, Category, Creation Time, Last Modified Time, and Count. The entries are for users FRED, JASMINE, JEFF, JOHN, LARA, and MICHAEL, all in the /VPN category. The counts are 7, 7, 9, 2, 1, and 1 respectively. The window also shows the name "VPN Login Events", the last update time "15 Dec 2008 17:23:40 PST", and a filter set to "No Filter".

User Name	Category	Creation Time	Last Modified Time	Count
FRED	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	7
JASMINE	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	7
JEFF	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	9
JOHN	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	2
LARA	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	1
MICHAEL	/VPN	15 Dec 2008 14...	15 Dec 2008 14...	1

A logical next step in this example scenario would be to create another rule that checks to see if certain user names are showing up in the active list, and then takes some action (like sending an e-mail or adding those names to a "suspicious users" list, if appropriate).

Editing Active List Entries

- 1 Right-click an item in the Active List resource tree and choose **Show Entries**.
- 2 In the active list grid view, right-click an entry and choose **Edit**.
- 3 Click the entry's **Source Address** or **Count** to make changes.
- 4 Click **Modify** to change the existing entry or **Add** to post the changed entry as a new one.

Editing an Active List

- 1 In the Active Lists resource tree, right-click an active list and choose **Edit Active List**.
- 2 Make appropriate changes to the properties of the active list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Move or Copy an Active List

- 1 In the Active Lists resource tree, navigate to an active list and drag and drop it into another group.
- 2 Choose **Move** to move the active list, **Copy** to make a separate copy of the active list, or **Link** to create a copy of the active list that is linked to the original active list.

If you choose **Copy**, you create a separate copy of the active list that is not affected when the original active list is edited. If you choose **Link**, you create a copy of the active list that is linked to the original active list. Therefore, if you edit a linked active list, whether the original or the copy, all links are edited as well. When deleting linked active lists, you can either delete the selected active list or all linked active list copies.

Importing an Active List

You can import a comma-separated-value (CSV) file as data. This is useful if you have data from other systems that you want to import; you can use the import to populate your active lists.

- 1 In the Active Lists resource tree, select an active list, right-click, and choose **Import CSV File**. This brings up a file browser.
- 2 Browse to find the CSV file you want to import, select it, and click **Open**.

The Import Preview displays. If this is the file you want to import, click **OK** to add it to the active list.

- 3 Right-click the active list you just populated with the CSV file and choose **Show Entries**. This displays the newly-added data from the CSV file in the Viewer panel as active list details.



The default view limit is 2000 entries. To view more, specify the number of entries in your filter.

Exporting an Active List

In the active list viewer, you can export selected entries from an active list to a CSV file. This is useful if you want to manage active list data external to the ESM Console.

- 1 In the Active Lists resource tree, select an active list, and choose **Show Entries**. The data in the active list is displayed in the Viewer panel as active list details.
- 2 On the active list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting an Active List

- 1 Right-click an active list and choose **Delete Active List**.
- 2 In the dialog box, click **Yes**.

Managing Active List Groups

Active list groups are created to store similar groups or active lists in a single location. Groups can be created within groups to meet enterprise needs.

Groups and active lists can be managed with drag and drop functionality. You can move or copy groups and active lists into other groups in the Active Lists resource tree. If a group is deleted, the active lists within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Navigating to Active Lists

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Active Lists** tab.

Creating an Active List Group

- 1 In the Navigator panel, choose the **Active Lists** resource tree.

- 2 In the Active Lists tree, right-click a group and choose **New Group**.
- 3 A name text field appears under the group you selected.
- 4 In the name text field, type in a name.
- 5 Press **Enter**.

Renaming Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Rename**.
- 2 In the name text field, rename the group.
- 3 Press **Enter**.

Editing Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying Active List Groups

- 1 In the Active Lists resource tree, navigate to a group and drag and drop it into another group.
- 2 Select **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you select **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you select **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting Active List Groups

- 1 In the Active Lists resource tree, right-click a group and choose **Delete Group**.
- 1 In the dialog box, click **Yes**.

Managing Session Lists

While you can manually update session lists, their real value comes when you author automatic, rule-driven lists with dynamic content.

See also [“Understanding Session Correlation” on page 543](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#).



Note

As described in Creating a session list, filters improve session list performance by restricting the number of events that must be evaluated. Filters, such as DHCP IP address ranges, are installation-specific. Therefore, consider adding a filter to pre-defined session lists, such as /All Session Lists/ArcSight Foundation/Network Monitoring/DHCP, to improve performance.

Creating a Session List

Note that session lists are usually defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules are empty or contain only manually added entries that have not timed out. (See [“Understanding Session Correlation” on page 543](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#) for more information.)

- 1 Choose the **Lists** resource tree in the Navigator panel.
- 2 Click the **Session Lists** tab.
- 3 Right-click a session list group and choose **New Session List**.
- 4 In the Session List Editor, in the Inspect/Edit panel, define the following values.

In this field...	...enter this
Name	Enter a name for the session list. This name identifies the session list in ArcSight pick lists. Spaces and special characters are OK.
Overlapping Entries	Check this box to alert the system to allow multiple instances of key pairings, which keeps the previous session with the same key field open. For example, you might check this box if the list is tracking activity for an asset that supports multiple user logins.
In Memory Capacity (x1000)	<p>This setting indicates the maximum number of session entries the system keeps in memory. 10,000 is the default value. For most cases, 10,000 is appropriate, however, you may wish to adjust this setting if the devices you are monitoring for this session list contain a lot of data to ensure you have adequate memory cache available.</p> <p>As a best practice, be sure to set In Memory Capacity higher than the number of live sessions you anticipate. This helps optimize performance and, therefore, keeps results reliable.</p>
Entry Expiration Time	<p>Enter an expiration time for session list entries. This indicates the time after which entries are marked as terminated (if no explicit termination event is received previous to this).</p> <p>The default is 0 seconds, which means the entry will never expire. An entry with no expiry date/time can only be terminated explicitly (through user action on ESM Console, rule actions, or archives).</p>

- 5 Set the **Common** and **Assign** fields as appropriate. Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

- 6 Define columns for session list entries by clicking the row of the lower panel labeled "<Enter Name>." Columns for Start Time, End Time, and Creation Time are pre-defined.

In this field...	...enter this
Name	Enter a name for each session parameter you wish to track; for example, IP address, zone, or MAC address. The name you enter here appears as a label in the session list, and in the Variable pick list. Names can contain spaces, such as "User name."
Type	Type indicates the data type of the entry. Data types can be: <ul style="list-style-type: none"> • Address (IP address or MAC address) • Date • Double • Integer • Long • Resource Reference (with appropriate subtype) • String
Sub-type	There are only two data types that require subtypes: Address and Resource reference. <ul style="list-style-type: none"> • Address – Choose IP address or MAC address. • Resource reference – A Resource reference can refer to any resource, such as Asset, Knowledge Base Article, or Zone.
Key field	Select one or more fields that must be unique to indicate a session start. In most cases, you would select at least two fields to make a key-value pair. For example, in the case of a DHCP login event, when a new IP and zone combination are written to the list, this indicates that a new session has started.

Columns can only be defined when the session list is created. Column definitions cannot be added, removed, or changed once the new session list is saved.

- 7 Click the **Filter** tab in the Session List Editor and define a filter that limits the number of events to consider for the new session list. Session lists without filters must evaluate every event, which can negatively affect performance. The Filter tab presents the familiar [Common Conditions Editor \(CCE\)](#). Although the filter editor is similar, session list filters are not the same as Filter resources. Session list filters use different fields than Filter resources, for one thing.

Session lists are often concerned with logins to specific machines. In this case, you would write a filter that would limit evaluation to IP address ranges of interest. By filtering out all events except those targeting IP addresses in the DHCP server's subnet, for example, you are effectively limiting session list evaluation to inside traffic, reducing the overhead of session list evaluation. Other uses of session lists suggest other installation-specific knowledge that can be used to create session list filters that restrict the number of events matched against the session list.

- 8 Click **Apply** to save and continue editing or **OK** to save and close.

You can use the **Add Entry** button in the Session List Editor to manually create more entries for the current session list.

Using Rules to Populate a Session List

Session lists are usually defined in conjunction with **rules** specifically tailored to interact with and populate the lists dynamically. Lists not driven by rules are empty or contain only manually added entries that have not timed out. See [“Understanding Session Correlation” on page 543](#) and [“Using Session Lists to Correlate Session Data on User Logins \(Example\)” on page 551](#) for more information, including an example walk-through of how to create a session list and rules with which to populate it.

For information about rules, specifically, see [Chapter 16, Rules Authoring, on page 439](#).

Editing a Session List

- 1 In the Session Lists resource tree, right-click a session list and choose **Edit Session List**.
- 2 Make appropriate changes to the properties of the session list.
- 3 Click **Apply** to save and continue editing or **OK** to save and close.

Moving or Copying a Session List

- 1 In the Session Lists resource tree, navigate to a session list and drag and drop it into another group.
- 2 Choose **Move** to move the session list, **Copy** to make a separate copy of the session list, or **Link** to create a copy of the session list that is linked to the original session list.

If you choose **Copy**, you create a separate copy of the session list that is not affected when the original session list is edited. If you choose **Link**, you create a copy of the session list that is linked to the original session list. Therefore, if you edit a linked session list, whether the original or the copy, all links are edited as well. When deleting linked session lists, you can either delete the selected session list or all linked session list copies.

Exporting a Session List

In the session list viewer, you can export selected entries from an session list to a CSV file. This is useful if you want to manage session list data external to the ESM Console.

- 1 In the Session Lists resource tree, select a session list, and choose **Show Entries**. The data in the session list is displayed in the Viewer panel as session list details.
- 2 On the session list detail in the Viewer panel, select one or more entries (typically, rows of events).
- 3 Right-click and choose either **Export CSV - Visible Columns** or **Export CSV - All Columns**. This brings up a file browser.
- 4 Browse to the location where you want to save the exported data, enter a file name in the File Name field, and click **Save**. The entries you selected for export are saved as a CSV file in the chosen location.

Deleting a Session List

- 1 Right-click a session list and choose **Delete Session List**.
- 2 In the dialog box, click **Delete**.

Adding a Session List Entry Based on an Existing Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click an entry that is similar to the entry you would like to add. Choose **Edit**. The Session List Entry editor appears in the Inspect/Edit window.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to post the changed entry as a new one.


Adding a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Edit Session List**. The Session List Entry editor appears in the Inspect/Edit window.
- 2 Click the **Add Entry** button.
- 3 Click a row's **Value** column to make changes. The column type may limit the kind of data that can be entered.
- 4 Click **Add** to save the new entry. The **Reset** button clears all values.

Deleting a Session List Entry

- 1 Right-click an item in the Session List resource tree and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry that you would like to delete. Choose **Delete**. Confirm the deletion by clicking **Delete**.

Terminating a Session List Entry

- 1 In the Session Lists resource tree, right-click a session list and choose **Show Entries**.
- 2 In the session list grid view, right-click the entry you want to terminate and select **Terminate Session Entry**.
- 3 Enter the date and time for the session end time. Click the  button for a context menu containing relative times such as Now, 1 hour ago, 1 day from now, and so on. Click **OK**.

Case Management and Queries

Cases track individual or multiple related events and export event data to third-party products. Cases can stand alone or integrate with a third-party case management system, such as BMC Remedy.

A case contains information about an incident, usually with one or more events attached. Use cases to track, investigate, and resolve events. You can assign cases of interest to analysts, who can investigate and resolve them based on severity and enterprise policies. You can also use rules to automatically open a case when certain conditions are met.

You can assign cases to groups of users who receive a notification with access to the case and its associated data. Those users can take action on the assigned case and specify other actions to be taken, assign it to another user, or resolve the case.

If you have the Remedy Action Request System, you can configure ArcSight to integrate with it using an application called *ArcRemedyClient*. Then you can use Remedy to provide supplemental or alternative ticketing, tracking, and workflow support for ArcSight security event data.

ArcRemedyClient runs in the background as a service, transferring data from ArcSight to Remedy. *ArcRemedyClient* can also be configured to update the ArcSight database with Remedy status. For more about the *ArcRemedyClient*, ask your ArcSight Customer Service representative.

Also refer to the reference guide topic [“Case Editor Tab Fields” on page 829](#) when building and using cases.

[“Managing Cases” on page 585](#)

[“Managing Case Groups” on page 591](#)

[“Running Case Queries” on page 592](#)

Managing Cases

This topic describes the basic tasks necessary to create, manage, and delete cases.

Cases can be created and automatically updated as a rule action when the conditions of the rule are met by incoming events. You can also add an event to a case directly from resources that monitor events, such as active channels and dashboards.

The events added to a case are attached to the case itself, which makes it possible to preserve case event history over time.

See also, [“Collaborating on Events” on page 216](#).

Create a New Case

- 1 Choose the **Cases** resource tree in the Navigator panel.
- 2 Right-click a case group and choose **New Case**. You can also choose the **New Case** option on the File menu.
- 3 In the Case Editor, select the **Initial** tab.
- 4 Select the **Attributes** sub tab.
- 5 Enter a name for this case in the required **Name** field.
Display ID numbers are assigned automatically when you save the case.
- 6 Specify **Ticket** info for the case as described below in the Case Properties table.
- 7 In the Assign section, choose a user on the **Owner** drop-down menu, to assign one or more case owners.
- 8 Also in the Assign section, choose groups on the **Notification Groups** drop-down menu, to notify groups of the new case.
- 9 Click **OK**.

For details on defining case attributes, see [“Case Properties” on page 586](#), [“Editing a Case” on page 587](#) and [“Case Editor Tab Fields” on page 829](#) (a complete reference).

Case Properties

Property	Usage
Ticket Type	The drop-down list includes Internal , Client , and Incident types.
Stage	Selections indicate workflow stage of ticket; default selections include Queued , Initial , Follow-Up , Final , and Closed . (See also “Creating New Stages” on page 218 and “Editing Stages” on page 219 .)
Frequency	Indicates how often reported issue occurs. Values assigned are 0 (never or once), 1 (less than 10 times), 2 (10 to 15 times), 3 (15 times), 4 (more than 15).
Operational Impact	Impact of reported issue. Values assigned are 0 (no impact), 1 (no immediate impact), 2 (low priority impact), 3 (high priority impact), 4 (immediate impact).
Security Classification	Values assigned are 1 (Unclassified), 2 (Confidential), 3 (Secret), 4 (Top Secret).
Consequence Severity	Values assigned are 0 (None), 1 (Insignificant), 2 (Marginal), 3 (Critical), 4 (Catastrophic).
Reporting Level	Calculated based on Ticket info values entered. You can also use entries in all Case Ticket fields to generate reports so you can categorize cases based on specific case information.
Incident Information	Automatically populated based on events included in the case.

For more information on entries in the remaining Initial tabs, and the **Follow-Up**, **Final**, **Events**, and **Notes** tabs, see [“Editing a Case” on page 587](#) and [“Case Editor Tab Fields” on page 829](#) (a complete reference).

Creating a Case from Displayed Events



Caution

Events added to a case are accessible in the context of that case to any user who has permissions to view or edit the case. Even users who do not have permissions on the *events* themselves have permissions to view full events *in the context of a case* on which they have permissions.

As a best practice, please keep this in mind when adding events to a case and setting access control lists (ACLs) on cases. For more information, see [“Granting or Removing Resource Permissions” on page 647](#).

You can also create cases directly from the Viewer panel, while monitoring suspicious events.

1 In an active channel grid view, select one or more events.

2 Right-click and choose **Add to Case > New Case**.

The selected event(s) appears in the Case Editor on the Events tab.

3 In the Case Editor, select the **Initial** tab.

4 Select the **Attributes** tab.

5 Enter text in the required **Name** field.

Display ID numbers are assigned automatically when you save the case.

6 Specify **Ticket** info for the case as described above in the Case Properties table.

7 In the Assign section, choose a user on the **Owner** drop-down menu, to assign one or more case owners.

8 Also in the Assign section, choose groups on the **Notification Groups** drop-down menu, to notify groups of the new case.

9 Click **OK**.



Tip

Events related to a use case are preserved in the case for tracking purposes even after the time period where the events would typically age out of the database.

For more information on entries in the remaining **Initial** tabs, and **Follow-Up**, **Final**, **Events**, and **Notes** tabs, see [“Editing a Case” on page 587](#).

For information on adding events to an existing case, see [“Adding Events to a Case” on page 589](#).

Editing a Case

To be able to edit a case that has already been saved, you first need to lock it by selecting the **Locked by** checkbox. This prevents other users from modifying the case while you're editing it.

1 In the Cases resource tree, right-click a case and choose **Edit Case**.

2 In the Case Editor, select the particular workflow tab you want to edit, as described below.

- 3 Select the tab and add or edit its information. When you are finished with this, click **OK** to save your changes.
- 4 When you are finished with the case, clear the **Locked by** checkbox to release the lock on the case before you click **Close**.

Cases Editor Workflow Tabs

Tab	Usage
Initial	Provides basic case information: case ticket attributes, description and security classification.
Follow-Up	Descriptions of actions taken, planned, or recommended.
Final	Ticket resolution and reporting, including attack mechanism, attack agent, incident information, and vulnerability information.
Events	A list of the events included in the case.
Notes	Miscellaneous case information.

Finding Cases

You can locate a particular ArcSight case by its reference ID if you wish.

- 1 Right-click a group in the Cases resource tree and choose **Edit Case by ID**.
- 2 Enter the ID string in the dialog box and click **OK** to display it in the Case Editor.

When working from cases listed in a Viewer panel channel view, you can locate a particular case's position in the Navigator panel's resource tree.

- 1 Right-click a case in the channel grid view and choose **Find Case in Navigator**.
- 2 Look for the highlighted item in the Navigator panel's Cases resource tree.

Attaching a File to a Case

Make sure that since installing the ESM Console you have logged in at least twice before attaching a file. A second login solves an authentication problem that can prevent you from attaching or uploading a file.

- 1 Open an existing case and click **Lock** to edit it.
- 2 Click **Attachments** and attach by uploading the file.

Field	Description
File Name	The default is the uploaded filename, which you can change.
Attachment Name	A descriptive name for the file. This name can differ from the actual file name, and can include spaces. If you do not provide an alternative name here, the original file name is used.
Attachment Description	Optional description of the file.
Sharing	Click Share this file in Arcsight if you want to make the file available as a shared resource on the ArcSight Manager.

Field	Description
Mime Type	Read-only field that indicates the Multipurpose Internet Mail Extensions (MIME) type of the attached file.
Encoding	Text encoding; for example, you could select Chinese text for internationalization requirements.

3 Click **Attach**.

4 The Attachments list displays. Select a file to view its summary. From the summary view, you can attach, edit, or detach a file.

- ◆ Attach: attaches the file to the case.
- ◆ Edit: enables you to edit the name and description. You can also upload a new file to replace the existing file by selecting **Replace file** and click **Update**.
- ◆ Detach: removes the file from the attachment.

Viewing a Case Attachment

Once a file is attached to a case, anyone viewing the case can view details about the file and download it. To do this, open a case and click the Attachments tab, which lists files attached to the selected case. Right-click a file name and choose **Open** to open the file or **Download** to download the file to your local system.

If you click **Download**, you get a file browser in which to navigate to the local directory where you want to store the file. In the **File Name** field, type the name under which you want to store the file on your local system and click **Save**. The file is saved as specified.

If the case attachment was also added as a shared resource, the file is available in the ArcSight Manager Files resource folders. To access a shared file, choose **Files** in the Navigator and browse the folders, or choose **Edit > Find Resource** from the menus, enter the file name in the **Search query** field, and click **Find**. (See ["Finding Resources" on page 671](#) for more information on this utility.)

Adding Events to a Case



Caution

Events added to a case are accessible in the context of that case to any user who has permissions to view or edit the case. Even users who do not have permissions on the *events* themselves have permissions to view full events *in the context of a case* on which they have permissions.

As a best practice, please keep this in mind when adding events to a case and setting access control lists (ACLs) on cases. For more information, see ["Granting or Removing Resource Permissions" on page 647](#).

There are several ways to add events to a case:

- 1 In the **Cases** resource tree, right-click a case and select **Edit Case**.
- 2 In a Viewer panel grid view, select one or more events.
- 3 Right-click and select **Add To Case**.

Or, if you already have the Case Editor open on the right case, simply select one or more events in the Viewer panel grid, right-click and choose **Add to Case > Case in Editor**.



Note

- If there are multiple Case Editors open when you choose **Add to Case > Case in Editor**, the selected events get added to the Case Editor with focus (showing on top of the others).
- If no Case Editors are currently open but you choose **Add to Case > Case in Editor** option anyway, a new case is created with the selected events added.

To add events to another case (not currently open), select one or more events, right-click and choose **Add to Case > Other**. This brings up the Case Selector dialog. Navigate to the case where you want to add the events, select the case, and click **OK**.

To create a new case from selected events, select one or more events, right-click and choose **Add to Case > New Case**. (Provide a name for the new case, and any other details needed.)

After adding events to a case, click **OK** on the Case Editor to save the case with the events.



Tip

Events related to a use case are preserved in the case for tracking purposes even after the time period where the events would typically age out of the database.

See also, [“Creating a Case from Displayed Events” on page 587](#).

Showing Event Details for Cases in Channels

- 1 In the Cases resource tree, right-click a case and choose **Case Details Channel**. The events associated with the case appear in an active channel grid view in the Viewer panel.
- 2 In the grid view, use any of the Viewer panel's features to further analyze the events.

Deleting Events from a Case

- 1 In the Cases resource tree, right-click a case and choose **Edit Case**.
- 2 In the Case Editor, select the **Events** tab.
- 3 Select one or more events.
- 4 Right-click and choose **Remove from Case**.
- 5 In the dialog box, click **Yes**.

Creating a Channel for a Case

In the Cases resource tree, right-click a case and choose **Case Details Channel**. A new channel is created and displayed in the Viewer. The channel filters for events associated with the selected case.



Note

You can create a channel based on a case only if the case has one or more events associated with it. See [“Adding Events to a Case” on page 589](#).

Exporting a Case to an External System

If you have an integration to an external case management system such as Remedy, you can transfer cases from the Cases resource tree to the external system as XML by doing the following.

- 1 Choose the Cases resource tree in the Navigator panel.
- 2 Right-click a case and choose **Export to External System**.

The Case Editor displays a message informing you of a successful transfer. Exported cases also display a flagged icon indicating the case has been exported.

Moving or Copying a Case

- 1 In the Cases resource tree, navigate to a case and drag and drop it into another group.
- 2 Choose **Move** to move the case, **Copy** to make a separate copy of the case, or **Link** to create a copy of the case that is linked to the original case.

If you choose **Copy**, you create a separate copy of the case that is not affected when the original case is edited. If you choose **Link**, you create a copy of the case that is linked to the original case. Therefore, if you edit a linked case, whether the original or the copy, all links are edited as well. When deleting linked cases, you can either delete the selected case or all linked case copies.

Deleting a Case

- 1 In the Cases resources tree, right-click a case and choose **Delete Case**.
- 2 In the dialog box, click **Yes**.

Managing Case Groups

Case groups are created to store similar groups or cases in a single location. Groups can be created within groups to meet enterprise needs.

Groups and cases can be managed with drag and drop functionality. You can move or copy groups and cases into other groups from the Cases window. If a group is deleted, the cases within that group are also deleted.



Note

To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Case Group

- 1 From the **Navigator Panel** drop-down menu, select **Cases**.

Cases are displayed in different colors based on the assigned "Consequence Severity" in the case. The severity descriptions are Catastrophic (Dark Red), Critical (Red), Marginal (Orange), Insignificant (Green), or None (Gray).



Note

Before being able to edit a case that has already been saved, you need to lock the case by selecting the **Lock Case** checkbox, so other users cannot modify the case while you're editing it.

- 2 In the **Cases** resource tree, right-click a group and choose **New Group**.
- 3 A **Name** text field appears under the group you selected.
- 4 In the name text field, type in a name.
- 5 Press **Enter**.

Renaming a Case Group

In the Cases resource tree, right-click a group and choose **Rename**.

- 1 In the **Name** text field, rename the group.
- 2 Press **Enter**.

Editing a Case Group

- 1 In the Cases resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text field.
- 3 Click **OK**.

Moving or Copying a Case Group

- 1 In the Cases resource tree, navigate to a group and drag and drop it into another group.

The ESM Console displays a dialog box with drag-and-drop options.

- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Case Group

- 1 In the Cases resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Running Case Queries

You can create groups in the Cases resource tree that automatically query every case change that occurs. If a case change results in a state that meets the criteria for such a group, the case is listed in that group.

Setting Up an Automatic Case Query Group

- 1 Choose the **Cases** resource tree in the Navigator panel.
- 2 Right-click a group in the tree and choose **New Group**.
- 3 Give the group a suitable name.
- 4 Select the **Attributes** tab and enter values as you always do when [Editing Groups](#).

- 5 Select the **Conditions** tab and construct query statements as you do when [Creating Filters](#).
- 6 Click **Apply** to save your changes and keep editing, or **OK** to save and close.

Integration Commands

[“What are Integration Commands?” on page 595](#)
[“Planning Checklist and Workflow” on page 598](#)
[“Navigating to Integration Command Resources” on page 599](#)
[“Quick Example” on page 599](#)
[“Defining Commands” on page 602](#)
[“Using Configurations to Group Commands” on page 610](#)
[“Specifying Targets” on page 617](#)
[“Authorization and Authentication Settings” on page 618](#)
[“Running Integration Commands” on page 622](#)
[“Ready-Made ArcSight TRM Commands” on page 623](#)
[“ArcSight Logger Search Commands” on page 630](#)
[“Network Tools as Integration Commands” on page 634](#)

Integration commands leverage the power of security and event management, and broaden its view to show external, snap-in views from applications like ArcSight NSP TRM and ArcSight Logger, as well as third-party applications.

ArcSight ships with standard content (pre-built commands) and a platform for building your own command configurations.

Contact ArcSight Professional Services if you need assistance in authoring tools integrations with ArcSight products or other applications.

What are Integration Commands?

Integration commands enable you to link from the ESM Console to information in other views and applications. You can also build and launch commands locally and on remote servers or appliances, using field values in events as command parameters. You can configure the commands as context-aware, right-click options on different views, resources, and editors on the ESM Console.

Configurations can define valid data types and selections for a set of commands. For example, you could configure a set of URL commands to run as a right-click on a selected cell in an active channel and accept only IP addresses as data types.

The ability to integrate commands for various applications means the ESM Console can serve as a central hub for defining, managing, and launching TRM actions, Logger searches, and third party applications, as well as local ArcSight scripts. You can also configure and manage role permissions and access lists (ACLs) for tools and commands in the ESM Console.

Supported Command Types

You can build these types of context-based, right-click commands into the ESM Console:

Command Type	Output Results	Examples
URL commands link to Web page URLs or URIs	<ul style="list-style-type: none"> ESM Console internal browser External Web browser 	<ul style="list-style-type: none"> Out-of-the-Box NSP TRM URL commands Out-of-the-Box Logger Searches
Script commands run scripts	Script/executable output result (for example, action)	Network Tools
Connector commands are derived from associated nodes or applications (for example, CounterACT configuration XML for a CounterACT connector command)	Structured result based on the SmartConnector and its associated node or application	CounterACT SmartConnector commands

For more information on working with commands, see [“Defining Commands” on page 602](#).



All integration commands are designed as **manual**, right-click options in various contexts in the ESM Console. This enables you to launch commands in ESM Console displays and, access available work flows in other applications (for example, in the NSP TRM Web UI).

To define **rule-driven commands**, configure rule actions to send **SmartConnector commands** (rather than by creating integration commands).

For example, with rule-driven TRM CounterACT commands, you do not need to build integration commands. You can add TRM CounterACT commands as rule actions by having the CounterACT SmartConnector installed and registered with the Manager.

For more information about using SmartConnector commands in rules, see [“Execute Connector Command” on page 456](#) in [Rule Actions Reference](#).

Out-of-the-Box Commands for Logger and NSP TRM

ArcSight ships with pre-built, URL-based commands for the following ArcSight appliances.

- ArcSight Network Synergy Platform (NSP) Threat Response Manager (TRM): A typical command would take an action based on the event. For example, you might select a suspicious login attempt in an intrusion monitoring channel or Hot List, and investigate or quarantine the associated IP address using TRM. (For information on NSP TRM commands, skip to [“Ready-Made ArcSight TRM Commands” on page 623](#).)
- ArcSight Logger: A typical command would be to run a remote search or query on an element in a selected Logger stored event in an active channel. (For information on Logger commands, skip to [“ArcSight Logger Search Commands” on page 630](#).)

Local Scripts and Commands to Other Applications

Typical activities for which you might build and run commands in the ESM Console that connect to other applications and tools include:

- Launch third-party Web interfaces
- Launch scripts
- Run external searches
- View submitted tickets
- Get Asset/Vulnerability information
- Get Payload Information

You can set up context-aware commands to third-party applications and custom scripts. With command configurations, you can make these available in specified ESM Console views and use particular fields as parameters to your commands.

ArcSight ships with standard utilities configured to be available in ESM Console views. For example, the **ping** command is available in grid views such as active channels, lists, and query viewers, and takes as a parameter the *IP address* or *host name* in the selected event.

For information on integrating basic network tools such as Ping, Nslookup, or ArcSight specific “Send Logs”, see [“Using the Network Tools” on page 107](#) and [“Network Tools as Integration Commands” on page 634](#).

How it Works

Integration commands provide resources for tools integration authors to:

- Build context-sensitive commands that you can run locally or on multiple, remote target servers, and you can mix, match, and re-use with configurations.
- Associate parameters with commands to read the resources for which you call the commands. Command parameters make use of Velocity Expressions to pick up values from fields and resources. (See [“Velocity Templates” on page 1019](#).)
- Define configurations sets of commands) for various external applications to specify relevant contexts, commands, rendering formats, and, optionally, remote targets.

Once integration commands and configurations are in place, analysts and operators working with the ESM Console can use your custom-built commands or ArcSight pre-built commands (for Logger or NSP TRM) to manage and monitor networks and assets with an extended reach into other views, toolkits, and servers.

Configure Login credentials for authentication on external applications through integration parameters on the user resource. See [“Setting User Login Parameters” on page 619](#) and [“Setting Logins and Other Parameters to Prompt for Values at Runtime” on page 620](#).)

Define authorization to use or edit commands through access control lists (ACLs) as described in [“Access Control Lists \(ACLs\) on Integration Commands” on page 621](#).

Planning Checklist and Workflow

Plan your command integrations by identifying the utilities or applications to integrate and collecting the necessary information. Here is a checklist of considerations.

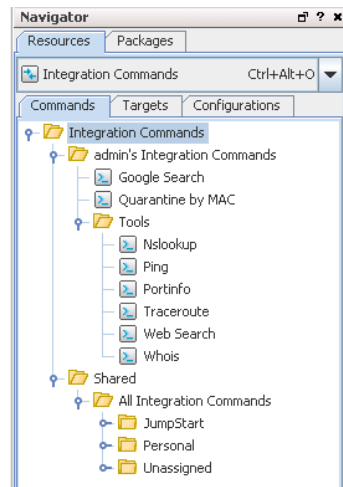
Components	Questions
Commands	<ul style="list-style-type: none"> What commands will you run on the external application? Is there a subset of commands you want to integrate into the ESM Console? What is the command type (Web URL, local executable script, or CounterACT Connector command) and syntax.
Servers, Authentication SmartConnectors	<p>Integrating Logger or NSP URL commands requires an IP address or Host name of the appliance and authentication credentials for users.</p> <p>Integrating a Connector command like NSP CounterACT requires access to the NSP TRM appliance, and a CounterACT connector deployed and registered with the Manager to which your ESM Console is connected.</p>
Configurations	<ul style="list-style-type: none"> How do you want to render (display) output results of commands? This largely depends on the command type; for example, URL commands are rendered in an external or embedded browser. How many integration configurations do you need? Does the application you are integrating have more than one type of interface? (for example, Web and CLI, like TRM) If so, you'll need a configuration for each interface and associated command type.
Users	<ul style="list-style-type: none"> Which users work with these integration tools or applications? Are authentication parameters required on target servers, appliances, or applications? If so, collect or establish user names and passwords for users who run these commands. Plan for configuring integration parameters on user accounts for users who work with the external applications. These users need login credentials for both ArcSight and the target applications. For users with the same authentication parameters for a target server, you can create a target resource with those parameters instead of duplicating the parameters in each user account. Then you can configure the ACL of that target resource so that only those users have access to it. When a command is triggered in the right context, only the target to which that user has access is displayed. Use a similar ACL approach for commands. For example, a single configuration can contain groups of commands, where some commands require special privileges.

Once you have a plan, you might try configuring the commands and testing in this order:

- 1 Add the commands (command name, type, the command itself, and its parameters).
- 2 Specify the targets (remote servers where commands run), if any.
- 3 Create one or more configuration(s), add in the commands you created, choose how command results are rendered (displayed), and define ESM Console UI contexts where these commands are available for use.
- 4 Add Integration Parameters to User Accounts. If authentication is required on target servers, configure login credentials on user accounts for users who run these commands. These users need login credentials for both ArcSight and on the target applications.
- 5 Test the commands. See ["Running Integration Commands" on page 622](#)

Navigating to Integration Command Resources

To create or edit integration commands and configurations, start by navigating to **Integration Commands** resources.



Users can access existing integration commands and configurations through right-click commands on the ESM Console in various contexts. The contexts depend on how the commands are configured.

Quick Example


To experiment with building integration commands, you need one **command** and one **configuration**. Create the command(s) first because the configuration references the commands.

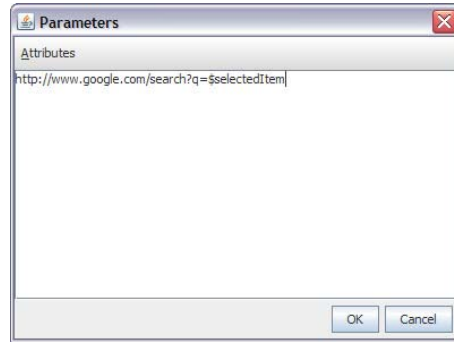
The configuration also defines how command results are rendered, and references **contexts** where your new Integration Commands appear in the ESM Console right-click menus (for example, Viewers, Resource Panel, Editors, and more specifics within those contexts).

To define **targets** (remote servers where commands run), add them to the configuration.

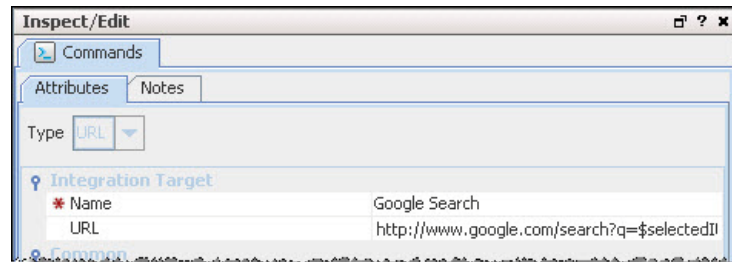
Here is an example of how to set up a command to do a Google Search on a selected cell in the ESM Console. This example does not require a “target,” so just set up a command, add it to a configuration, and run it. The details of this and other types of commands and configurations are discussed further in the topics that follow.

- 1 Start by getting the format of the Google search. Do a Google Search in a Web browser. Copy the first part of the URL (everything *before* or *to the left of* the search term) from the Address bar, so you have it on your clipboard. (You will be using this to paste in to the Parameters dialog in [Step 4.](#))
- 2 Now let's set up the command. In the ESM Console Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Commands** tab.
- 3 Right-click the group (folder) where you want to create the command and select **New Command**.
- 4 On the Commands Editor, fill in these attributes:
 - ◆ For command Type, choose **URL**.

- ◆ For Name, provide a user-friendly name like "Google Search".
- ◆ For URL, click the browse button  to get the Parameters dialog. Paste the Google search prefix (from [Step 1](#)) into the Parameters dialog scratch pad:
`http://www.google.com/search?q=`
- ◆ Click **Attributes** on the Parameters dialog to get a list of Velocity Expressions. Select the option, **Selections** > `$selectedItem`. The expression is added as a parameter to the search:
`http://www.google.com/search?q=$selectedItem`



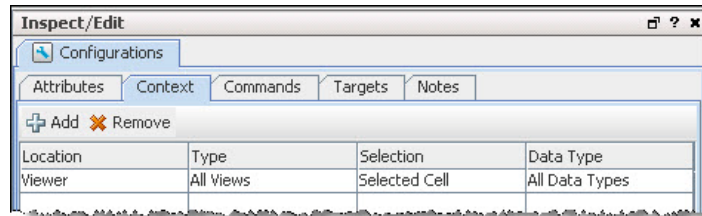
- ◆ Click **OK** to close the Parameters dialog and save your changes.
- ◆ Click **Apply** or **OK** on the Commands editor to save the command.



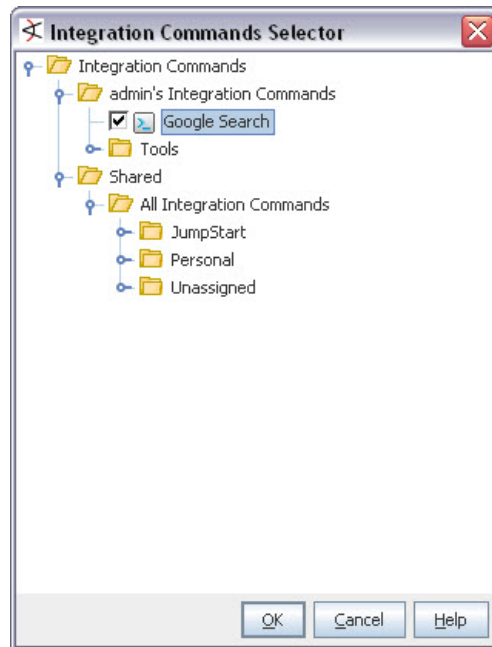
- Now, let's *set up the configuration and add the command to it*. Click the **Configurations** tab.
- Right-click a group and select **New Configuration**.
- On the Configurations Editor, select **URL** as the configuration Type, and fill in these other attributes:
 - ◆ For Name, provide a user-friendly name.
 - ◆ For Renderer, click to select either Internal Browser or External Browser.
- Still on the Configurations Editor, click the **Context** tab. This sets where in the ESM Console the command is available. Click **Add** to get a set of context fields, then click into each field to select a location, type, selection, and data type. (You can add multiple contexts by clicking Add again.) Add one context to show in the Viewer in all "views" and to take the selected cell as the "selection":

Location	Type	Selection	Data Type
Viewer	All Views	Selected Cell	All Data Types

When the search command is deployed as part of this configuration, and run via a right-click command in the context of the ESM Console, it searches on the text in the "cell" (Viewer table cell) the user selects in the ESM Console.



- 9 Finally, add the command to the configuration. On the Configuration Editor, click **Commands**. Click **Add** to get the command selector, select your Google Search command, and click **OK**.



- 10 Click **Apply** or **OK** on the Configurations Editor to save the configuration.

Now run the Search command you just built:

- 11 Open any active channel, list, data monitor, or query viewer with a table style view.
- 12 Right-click any cell in the Viewer that contains a term you would like to search on, and select **Integration Commands > Google Search** (or whatever you named the command).

The command runs a search using the text from the selected cell as the search term, and returns search hits in the browser (either the ESM Console internal browser or an external Web browser, depending on which you selected for the Renderer for the command.)

The following topics provide more information and examples on how to build all types of commands, how to add user authentication, how to use targets for TRM commands, how the standard network tools are implemented as integration commands, and more.

Defining Commands

Use the **commands** feature to configure URL, Script, and Connector commands for custom and third party applications and other ArcSight products. Setting up **commands** is the first step in a multi-part process to providing a set of integration commands. (Other tasks include setting up configurations, targets, and user login parameters). This topic explains how to add and edit the command portion of an integration command solution.

To add a new command, do the following:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Commands** tab.
- 2 Right-click a group (folder) in which to create the command, and select **New Command**. This launches the Command Editor in the Inspect/Edit panel. It is best to create new content in your own folder.
- 3 On the **Command Editor**, select the command **Type** and fill in the fields for command Name, and other attributes.

Command Type	Description
Script	Executable script that runs <i>locally</i> to the ESM Console where the command is launched.
URL	Web URL for which you can define parameters.
Connector	Commands for SmartConnectors



- 4 Click **Apply** or **OK** to add the new command.

Command Types and Attributes

The command attributes vary, depending on the type (Script, URL, or Connector), as described below.

Script Commands


Like other commands, you can make script commands available to multiple users and user groups. Users probably run the ESM Console on many different machines. Integration script commands always run on the same machine as the ESM Console used to launch them. Therefore, the working directory and program path names should reflect where commands are found in ESM Console users' environments

Attribute	Description
Name	User-friendly Name for the command.
Working Directory	<p>Directory containing the executable script.</p> <p>For example, <code>\$systemRoot\system32\</code></p> <p>You can type the directory path in the Program field, or click the Browse Directory button  to get a file browser. Use the file browser to navigate to and select the command.</p> <p>Note: Be sure this path reflects the location of the script on machines used by ESM Console users for whom you are building these commands.</p>
Program	<p>Full path to the executable command.</p> <p>For example, <code>\$systemRoot\system32\ping.exe</code></p> <p>You can type the full path to the command in the Program field, or click the Browse Directory button  to get a file browser. Use the file browser to navigate to and select the command.</p> <p>Note: Be sure this path reflects the location of the script on machines used by Console users for whom you are building these commands.</p>
Parameters	<p>Provide parameters for the command. (See "Adding and Editing Command Parameters" on page 606.)</p> <p>The Attributes list provides Velocity Expressions for all event fields and an option to add <code>\$selectedItem</code> as an attribute.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 684.](#)

URL Commands

Attribute	Description
Name	User-friendly Name for the command.
URL	<p>The URL for the command, along with any parameters provided as arguments to the URL.</p> <p>Click the browse button  to get the Parameters dialog. (See “Adding and Editing Command Parameters” on page 606 for information on how to add the URL along with parameters or <i>arguments</i> to the URL.) You can copy/paste URLs onto the Parameters dialog scratch pad or type them directly. The Attributes link provides Velocity Expressions you can add as parameters (attributes) to the URL.</p> <ul style="list-style-type: none"> Type or paste URL directly in the Parameters dialog scratch pad. Click Attributes to add a Velocity Expression as a URL parameter. <p>Determine the URL by first accessing it from a Web browser address bar. This also shows you where in the URL to add the parameters (if any).</p> <p>Example: Web Search</p> <p>To set up a Google Search on a parameter, do a Google Search in a Web browser. Extract the first part of the URL (everything <i>to the left of</i> the search term) from the Address bar, and paste it into the Parameters dialog scratch pad: http://www.google.com/search?q=</p> <p>Click Attributes on the Parameters dialog to get a list of Velocity Expressions. Select the option, Selections > \$selectedItem. The expression is added as a parameter to the search: http://www.google.com/search?q=\$selectedItem</p> <p>Click OK to close the Parameters dialog and save your changes. Click Apply or OK on the Command Editor when you are satisfied with all settings.)</p> <p>When this search command is deployed as part of an integration configuration, and run via a right-click command in the context of the ESM Console, it searches the text in the cell (Viewer table cell) the user selects in the ESM Console.</p>
Parameters	Parameters for URL commands are <i>added as attributes to the URL</i> as described above in URL .



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

Connector Commands




Prerequisites for Connector Commands

If you plan to build and use **TRM CounterACT Connector commands** you need:

- access to relevant servers such as NSP TRM appliance for TRM CounterACT command)
- One or more of the associated SmartConnectors deployed and registered with the Manager to which your ESM Console is connected. (For example, when you set up the CounterACT connector, it verifies its connection to the TRM appliance and asks for authentication credentials).

Test connectivity and authentication between your local machine, SmartConnector(s), and appliance(s) before setting up Connector integration commands.

Attribute	Description
Name	User-friendly Name for the command.
Group	<p>Choose a group from the Group drop-down menu. Depending on which Group you select, relevant commands are provided in the next field (Command).</p> <p>Note: The Group is filled in for you as <i>CounterACT</i>, and the Group field is not editable. CounterACT is the only SmartConnector for which you can build integration commands (manual commands, launched from the ESM Console). Alternatively, you can create rules that automatically send commands to any SmartConnector. (See “Execute Connector Command” on page 456 in Rule Actions Reference.)</p>
Command	<p>Choose a command from the drop-down menu. Depending on which Group you selected, relevant commands are provided here. Choose a Connector command from the drop-down list.</p> <p>See “TRM CounterACT Connector Command Example” on page 608 for references, examples, and details on TRM commands and parameters.</p> <p>Note: In order to get the list of Connector commands, you need to have the SmartConnector deployed and registered with the Manager to which your ESM Console is connected.</p>
Parameters	<p>To define parameters for the command:</p> <ol style="list-style-type: none"> 1 Click the browse button  to get the Parameters dialog. A table of name-value pairs is provided that represents the valid parameters for the given command. 2 Select the parameters to use, and define values for them with either hard-coded values or <i>Velocity Expressions</i>. For example, you could define the CounterACT command Quarantine Node By IP Address to use three parameters; IP Address, Quarantine Period, and Overwrite Active Quarantine (a yes/no value set to 0 or 1, respectively). You could set the IP address to a Velocity Expression for <i>attacker address</i>, Quarantine Period could be set to 1 hour, and overwrite set to Yes. The Attributes list provides Velocity Expressions for all event fields along with options to add Console selections, dates, and channel start and end times as attributes. 3 Click OK on the Parameters dialog to save your changes. <p>For more information about using Velocity Expressions for parameter values, see “TRM CounterACT Connector Command Example” on page 608.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

Adding and Editing Command Parameters

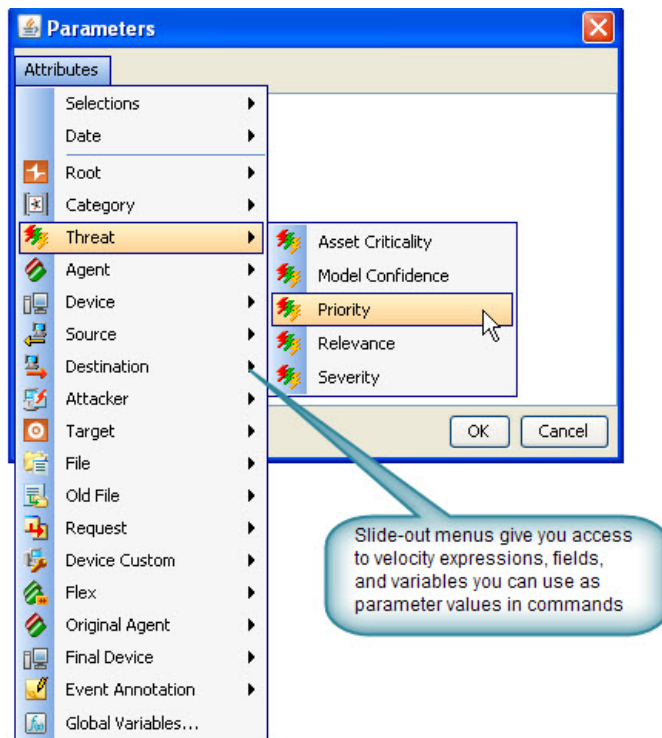
The Attributes list includes Velocity Expressions for all event fields and an option to add user field or item selections, channel start or end time, date/time, and other Velocity Expressions as attributes.



See also [“TRM CounterACT Connector Command Example” on page 608](#) for adding parameters to Connector commands. The Parameters dialog for Connectors is slightly different.

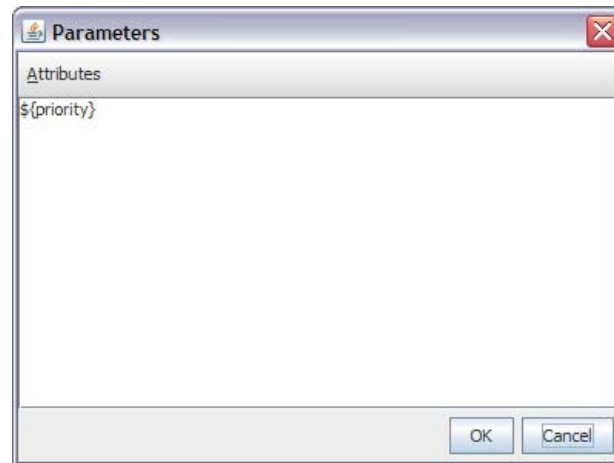
Provide **Parameters** for a command as follows.

- 1 Click the browse button to get the Parameters dialog.
- 2 Click **Attributes** to get a list of variables and Velocity Expressions.



- 3 Select the expression you want to add. The attribute list includes Global Variables. If the global variable to add is composed of a list of fields, expand the global variable displayed in the Parameters dialog and select the field you want.

The expression is added to the Edit Attributes scratch pad as a parameter.



- 4 You can continue adding expressions, which are chained together.

For example, selecting **Threat > Priority** from the Attributes list results in this parameter being placed on the scratch pad:

```
${priority}
```

Subsequently selecting **Attacker > Address**, updates the scratch pad entry with chained-together expression:

```
${priority} ${attackerAddress}
```



The Parameters dialog is an editable scratch pad. In addition to adding Velocity Expressions from the Attributes menu and Templates for Connector command parameters, you can type new expressions directly into the dialog. Also, you can select and edit existing expressions manually. (See also [“Removing a Command Parameter” on page 607](#))

- 5 When the Parameters scratch pad reflects the expressions you want to include as command parameters, click **OK**.


The parameters you added are reflected on the Attributes tab in the Command Editor.



Be sure to click **Apply** or **OK** on the **Command Editor** to save changes to command parameters along with any other changes to the command that you want to retain.

Removing a Command Parameter

To remove a command parameter:

- 1 Click the browse button  to get the Parameters dialog.
- 2 Select the parameter in the scratch pad and hit the Delete key on your keyboard.
- 3 To add a new parameter to replace the one you are deleting, do so by following steps described in [“Adding and Editing Command Parameters” on page 606](#).
- 4 Click **OK** on the Parameters dialog.
- 5 Click **Apply** or **OK** on the **Command Editor** to save your changes.


TRM CounterACT Connector Command Example

Since adding parameters to a Connector type command is slightly different than for URL or Script command types, here is an example of creating a CounterACT Connector command.

To learn more about TRM CounterACT commands, see the *SOAP API Reference Guide for ArcSight NSP*. See also [“Deep Dive into TRM CounterACT Connector XML” on page 609](#).

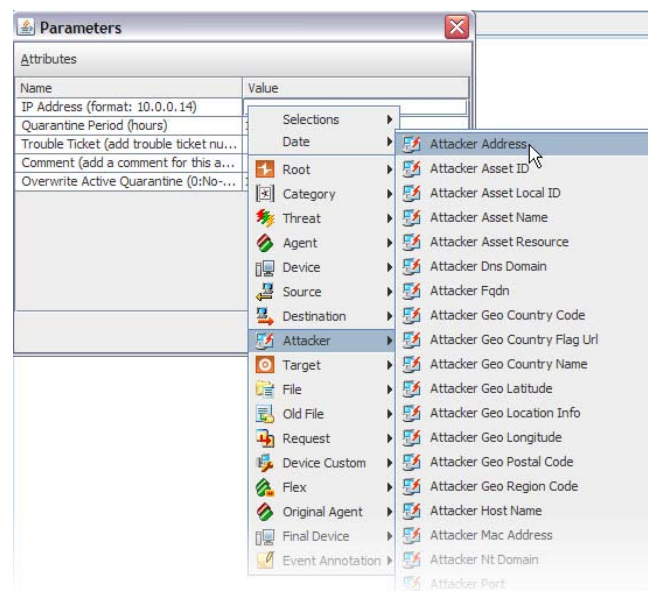
Example of CounterACT Command and Parameters

In this example, you use the TRM CounterACT command “Quarantine Node By IP Address” to quarantine an attacker node. Use three parameters: IP Address, Quarantine Period, and Overwrite Active Quarantine. In the Parameters field for this command, use hard-coded values for length and overwrite, but use a Velocity Expression to let the user derive the attacker address for a selected event on the ESM Console.

- 1 Create a new command of type **Connector** and name it.
- 2 In the Group field, select **CounterACT**.
- 3 In the Command drop-down menu, select **Quarantine Node By IP Address** from the list of CounterACT SmartConnector commands provided.
- 4 In the Parameters field, click the browse button  to get the Parameters dialog.

Right-click the Value field next to IP Address on the Parameters dialog to get the Velocity Expression chooser.

To get the Velocity Expression `${attackerAddress}`, select **Attacker > Attacker Address** on the Parameters dialog.



To quarantine the attacker node for 1 hour and overwrite the value, type in the number **1** for both Quarantine Period and Overwrite Active Quarantine.

Name	Value
IP Address (format: 10.0.0.14)	\${attackerAddress}
Quarantine Period (hours)	1
Trouble Ticket (add trouble ticket nu...)	
Comment (add a comment for this a...)	
Overwrite Active Quarantine (0:No-...)	1

Hit the Enter key after adding each value to be sure it is applied.

After entering the parameter values, the command attributes are defined as follows:

Parameter Name	Value
IP Address	<code>\${attackerAddress}</code>
Quarantine Period	1
Overwrite Active Quarantine	1

Click **OK** to save them.

- Review the parameter values on the Editor Attributes tab. They formatted similar to an XML-formatted TRM CounterACT command:

```
ip=${attackerAddress},length=1,troubleticket=,comment=,overwrite=1
```

You might have to stretch the Editor window to see all the parameters.

Name	Quarantine Node By IP Address
Group	CounterACT
Command	Quarantine Node By IP Address
Parameters	ip=\${attackerAddress},length=1,troubleticket=,comment=,overwrite=1 ...

- Click **Apply** or **OK** to save the command.

Deep Dive into TRM CounterACT Connector XML

If you want to learn more about NSP TRM commands, the best reference is the *SOAP API Reference Guide for ArcSight NSP*. A number of Simple Object Access Protocol (SOAP) calls for TRM actions have been enabled in common event format (CEF), and these are the TRM CounterACT commands currently available in the ESM Console as integration commands.

If you are interested in knowing more about how these commands are constructed, you can look at the CounterACT configuration XML files. This is not necessary; you can use the CounterACT SmartConnector integrations commands without ever looking at the SOAP Guide or the CounterACT XML. We are providing this information in case you are interested in exploring further on the NSP TRM side of things.

To access the CounterACT configuration XML file, select Connectors in the Navigator, right-click the CounterACT SmartConnector and do one of the following:

- Choose **Send Command > Tech Support > Get Configuration XML** and save the file. (This gets a copy of this file directly from the SmartConnector. In some cases, this file might be more up-to-date than the one on the Manager.)

Or

- Choose **Export Connector Configuration As XML** and save the file. (This gets the version of this file that is currently on the Manager.)

Example of CounterACT Command XML

Here is the configuration XML for a CounterACT "Quarantine Node" command:

```
<Command Description="Quarantine Node"
  DisplayName="Quarantine Node" Name="quarantine">
  <Parameters>
    <Parameter ContentType="-1"
      Description="IP to quarantine" Name="ip" Prompt="IP to quarantine"/>
    <Parameter ContentType="-1"
      Description="Time to quarantine" Name="length" Prompt="Time to quarantine"/>
    <Parameter ContentType="-1"
      Description="Overwrite(0:No,1:Yes)" Name="overwrite" Prompt="Overwrite(0:No,1:Yes)"/>
  </Parameters>
</Command>
```

Using Configurations to Group Commands

An integration **configuration** resource represents a family of commands of the same type. Commands in a configuration share the same context, rendering method, and targets.

Configurations provide a way of grouping similar commands and specifying common options for where on the ESM Console UI the commands are available (**contexts**), how command results are displayed (**renderer**), and where commands run (scripts run locally; others, like Connector commands, can have one or more remote **targets**). This is partly a matter of preference (about how you want to group, organize, and present commands to ESM Console users), and partly a matter of which commands belong together.

Typically, each integration maps to a single product; for example, one resource each for ArcSight Threat Response Manager (TRM) and ArcSight Network Configuration Manager (NCM). However, you can distribute sets of commands across multiple configurations, if needed. This is useful when the same product has different types of interfaces. For example, ArcSight TRM-Web takes URL based commands whereas TRM CounterACT requires Connector commands.



Note

Configurations can include only commands of the same type (script, URL, or Connector). Commands that share a configuration use the same renderer, contexts, and (if relevant) targets. You might want to make finer-grained groupings; for example, sub-groups of scripts or Connector commands.

For example, you might group a set of CounterAct TRM commands that deal with quarantine of nodes into a single configuration. Or you might group a set of URL-based commands used for searching and researching on particular types of events (via Google Searches, Knowledge Base articles, and so forth).

Setting up *configurations* is a step in a multi-part process of making a set of integration commands available to ESM Console users. (Other tasks include setting up commands, targets, and user login parameters).

This topic explains how to add and edit the *configuration* portion of an integration command solution. For an overview of the integration commands feature, see [“Integration Commands” on page 595](#). For more details on the relationship between commands, configurations, and targets, see [“How it Works” on page 597](#).

To create a configuration:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Configurations** tab.
- 2 Right-click a group (folder) where you want to create the configuration, and select **New Configuration**. This launches the Configurations Editor in the Inspect/Edit panel.
- 3 Fill in the fields on Attributes, Context, Commands, and Targets tabs as described in:
 - ◆ [“Configurations Attributes” on page 612](#)
 - ◆ [“Configurations Contexts” on page 613](#)
 - ◆ [“Configurations Commands” on page 614](#)
 - ◆ [“Configuration Targets” on page 615](#) (when commands run on remote targets)

The screenshot shows the 'Inspect/Edit' window for a configuration named 'Google Search'. The window has tabs for 'Attributes', 'Context', 'Commands', 'Targets', and 'Notes'. The 'Attributes' tab is selected. Below the tabs, there is a 'Type' dropdown set to 'URL'. The main area contains several sections with expandable/collapsible icons:

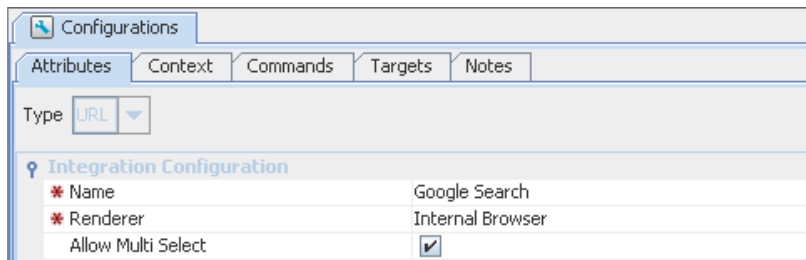
- Configuration** (expanded):
 - Name: Google Search
 - Renderer: Internal Browser
 - Allow Multi Select: ☒
- Common** (expanded):
 - Resource ID: eHZ2J+xsBACE-zxEFPjb0A==
 - External ID:
 - Alias:
 - Description:
 - Version ID:
 - Deprecated: ☐
- Assign** (expanded):
 - Owner:
 - Notification Groups:
- Parent Groups** (expanded):
 - Samantha's Integration Configurations: /All Integration Configurations/Personal/Samanth...
- Creation Information** (expanded):
 - Created By: admin
 - Creation Time: 25 Aug 2008 13:25:03 PDT
 - Time Since Creation: 9 day(s) 5 hour(s) 12 min(s) 21 sec(s)
- Last Update Information** (expanded):
 - Last Updated By: admin
 - Last Update Time: 26 Aug 2008 16:36:31 PDT
 - Time Since Last Update: 8 day(s) 2 hour(s) 53 sec(s)

At the bottom of the window, there are fields for '(Name)' and '(Description)', and buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

- 4 Click **Apply** or **OK** to add the new configuration.

Configurations Attributes

Define the configuration name, renderer and other basic details for the configuration on the Configurations **Attributes** tab.



Attribute	Description
Type	<p>Choose the type of configuration from the drop-down menu:</p> <ul style="list-style-type: none"> • Script • URL • Connector <p>Note: The configuration type must match the command types in the configuration. (See “On the Command Editor, select the command Type and fill in the fields for command Name, and other attributes.” on page 602.) Once the configuration is saved, the type is not editable. This setting influences choices on other options for the configuration, such as the Renderer.</p>
Name	A user-friendly, informative name for the configuration that (preferably, one that indicates the commands contained in it).
Renderer	<p>Select how the output of the command is rendered. The renderers available depends on the configuration Type chosen.</p> <p>For URL commands, you have the choice between using the ESM Console internal browser or an external Web browser to render HTML based command results. For a discussion of features, advantages, and limitations of internal and external browser displays, please see “Web Browsers (Internal and External)” on page 1030 and “Flash Plug-in and Setup Requirements for Internal Browser” on page 1032.</p>
Allow Multi Select	<p>Use this to allow selecting multiple events on which to run a command. It is off by default. A check mark indicates it is on/enabled.</p> <p>When on, users can select multiple events and the commands assign the values to a parameter as a comma-separated list.</p> <p>For example, suppose you have a command with the parameter ip=\$targetAddress.</p> <ul style="list-style-type: none"> • With Multi Select disabled, the command accepts only a single IP address based on a selected event (for example, ip=127.1.0.0). • With Multi Select enabled, a user can also get "ip=127.1.0.0,192.168.1.1" if two rows are selected. <p>In order for this to work: (1) the ESM Console context (for example, active channel) must allow multi-row selection, and (2) the integration target (for example, NSP TRM) must support a comma-separated list of values for the given command and parameter.</p> <p>Note: Multi Select does not affect how individual fields in an event are processed. Event field processing is determined entirely by the definition of command parameters. For example, a command with an Attacker Address parameter always gets that value from the selected event.</p>



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see [“Common Resource Attribute Fields” on page 684](#).

Configurations Contexts

As a part of constructing command configurations, you can configure **contexts** for where in the ESM Console certain commands are available. At the same time, you can define **parameters** for picking up and passing the value in any selected cell, row, or event field.

For example, you could configure a URL command for a Google search as a right-click command on any cell in an ESM Console grid view. By using a parameter as the argument to the search command, you could pick up the text from the selected cell or value from any selected field to use as your search term. (In the Commands editor, all fields, provided as a list of Velocity Expressions, are available for use as command parameters.)

Once configured, integration commands are available on right-click context menus from a variety of contexts including:

- Relevant fields in active channels (for example, IP address, host name, MAC address)
- Relevant resources (for example, assets)
- Active Lists, sessions lists, query viewers and channels

Also, you can configure **user login parameters** on ESM Console users (via a new Integration Parameters tab in the Users resource editor), thereby binding user login information to commands for third-party or ArcSight applications that require secure logins. (See [“Setting User Login Parameters” on page 619](#) for more information.)

You can configure a command to prompt for parameter information, which is often useful for login scenarios and as well as others. (See [“Setting Logins and Other Parameters to Prompt for Values at Runtime” on page 620](#) for more information.)

How to Set Up Command Contexts

Use controls on the Configurations **Context** tab to add, edit, or remove contexts in a configuration.

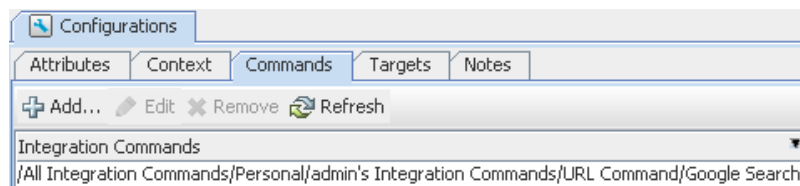
Configurations			
Attributes	Context	Commands	Targets
Notes			
+ Add ✖ Remove			
Location	Type	Selection	Data Type
Editor	All Editors	All Selections	All Data Types
Viewer	All Views	All Selections	All Data Types

Click the fields under Location, Type, Select, and Data Type to get drop-down menus with which to select contexts in the ESM Console UI where the command is available and to which selections it applies.

Attribute	Description
Location	View where in the ESM Console the command is available. For example: <ul style="list-style-type: none"> Viewer, for the Viewer panel where Views of active channels, dashboards, and so on are shown Resource, for the Navigator Panel resource tree Editor, for resource editors
Type	Contexts in the ESM Console panels where the command is available. Available types vary depending on the location you choose. For example, if you choose Viewer for the location, you can specify types of "views" where you want the command to display, such as Grid View, Chart View, various List entries, Dashboards, Query Viewers, and so on.
Selection	User selection or subset of it that is fed into the command. Options can include All Selections, Selected Cell, Selected Row, Selected Attribute.
Data Type	Data type for the parameters fed into the command (derived from the Selection). Options include: <ul style="list-style-type: none"> All Data Types IP Address MAC Address Date Double Integer Long Resource String

Configurations Commands

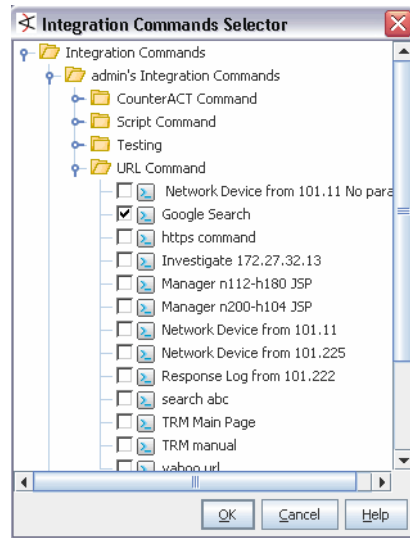
Use controls on the Configurations **Commands** tab to add, edit, or remove commands in a configuration.



Adding a Command to a Configuration

On the Configurations **Commands** tab:

- Click **Add** to bring up the Commands Selector dialog.



- Navigate to and click (checkmark) the commands you want to add, and click **OK**.
The commands are added to the list. (You can add multiple commands to a single configuration.)

Editing Commands in a Configuration

On the Configurations **Commands** tab:

- Select the command you want to edit and click **Edit**.
- This provides a shortcut into the **Command Editor** for the selected command. See [Step 3 on page 602](#) and ["Command Types and Attributes" on page 603](#) for information on editing the command.

Removing Commands from a Configuration

On the Configurations **Commands** tab, select a command in the list and click **Remove**.

Configuration Targets

Targets are not required for all command types, only for those that run on remote servers. Before you can add a target to a Configuration (explained here), you first need to define it as described in ["Specifying Targets" on page 617](#).

Use controls on the Configurations **Targets** tab to add, edit, or remove targets in a configuration.



Note

If you plan to add remote targets to a configuration, you need host information for the remote servers and login credentials if authentication is required.

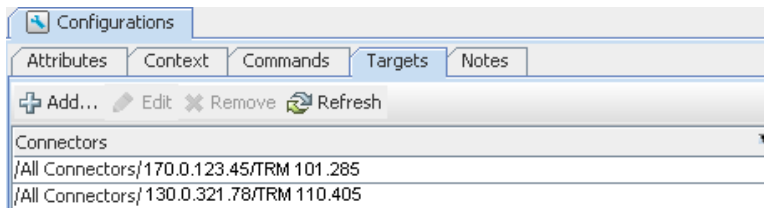
If you plan to add remote NSP TRM targets to a configuration, you need the following:

- Access to deployed TRM appliances
- *If you plan to access TRM via CounterACT commands*, you need one or more CounterACT SmartConnectors installed and configured to connect to your TRM appliances
- *If you plan to access TRM via URL commands*, you need a TRM Web client to derive URL commands. For TRM URL commands, you also need to define a target separately as described in [“Specifying Targets” on page 617](#).
- *If you plan to access TRM via URL commands*, you also need TRM user login credentials for the TRM appliances you plan to use. If you are an administrator configuring TRM commands for multiple users who send TRM commands each using their own TRM logins, you need the TRM login credentials for all those users in order to configure them as integration commands. (See [“Setting User Login Parameters” on page 619](#).)

See also, [“Configuring the SmartConnector” on page 695](#), the *CounterACT SmartConnector User Guide*, and the ArcSight™ NSP documentation.

Adding a Target to a Configuration

Targets are applicable to Connector commands like Threat Response Manager (TRM) commands sent to a TRM appliance via a CounterACT SmartConnector (which is treated as the “target” for TRM commands), and any other commands that you want to send to a remote server.



- Click **Add** to bring up the Connectors Selector dialog.
- Navigate to and click (check mark) the target you want to add, and click **OK**.

Editing Targets in a Configuration

- Select the target you want to edit and click **Edit**.
- This provides a shortcut into the **SmartConnector Configuration** Editor for the selected connector or target. (See [“Configuring the SmartConnector” on page 695](#), and also the *CounterACT SmartConnector User Guide*.)

Removing Commands from a Configuration

On the Configurations **Contexts** tab, select a target in the list and click **Remove**.

Specifying Targets

Optionally, you can specify targets (remote servers where one or more commands run). For example, Threat Response Manager (TRM) commands can be sent to a TRM appliance via a Web URL.

If you have multiple remote servers, you might want to configure multiple targets on which to run a single command with the same or different parameters.

For example, you can configure any of the following as command targets.

- Applications with Web interfaces/clients like...
 - ◆ ArcSight Threat Response Manager (TRM) appliances
 - ◆ ArcSight Logger appliances
 - ◆ Search providers (for example, Google, Yahoo, ask.com)
 - ◆ IT/Security portals
 - ◆ Asset/Vulnerability information
 - ◆ Ticketing Web servers
- CounterACT SmartConnector
 - ◆ TRM CounterACT

Setting up *targets* is a step in a multi-part process of making a set of integration commands available to ESM Console users. (Other tasks include setting up commands, configurations, and user login parameters).

This topic explains how to add and edit the *configuration* portion of an integration command solution. For an overview of the integration commands feature, see [“Integration Commands” on page 595](#).

To add a new target, do the following:

- 1 In the Navigator panel, select the **Integration Commands** resource from the drop-down menu and click the **Targets** tab.
- 2 Right-click a group (folder) where you want to create the target, and select **New Target**. This launches the Command Editor in the Inspect/Edit panel.
- 3 Fill in the fields as described below.
- 4 Click **Apply** or **OK** to add the new target.

Target Attributes

The only target attribute you need to provide is a user-friendly name for the server.

Attribute	Description
Name	Name for the remote server or appliance where the command run.

Target Integration Parameters

Targets are used only for URL configurations, where you parameterize the Web host target of the URL, and sometimes login credentials. Type directly into the fields to define a parameter, as described below.

Parameter	Type	Value
NSPHostIP	Text	xxx.xxx.xx.x

Field	Description
Parameter	Parameter name, as specified in the command definition related to this target. For example: <ul style="list-style-type: none"> NSPHostIP is a parameter for the IP address of the TRM target appliance.
Type	Parameter type. Choose Text or Password from the drop-down menu. Password type parameters are automatically encrypted. Notes: <ul style="list-style-type: none"> Always set login credentials (passwords or authentication tokens) to type "Password" (not "Text"). (Credentials set to "Text" are not masked on the UI and are sent as clear text if the renderer is an external browser.) You can set passwords and authentication credentials on target servers too, but we recommend against it in most cases. Doing so risks opening up a target server to any user who has access to the integration commands (not necessarily an account on the target server). Additionally, it does not give you any tracking information based on user logins to the server.
Value	Hard-coded value, variable, or Velocity Expression for the parameter. For example: <ul style="list-style-type: none"> A host name or IP address as a value for a target server parameter

To add a new parameter, click **Add**. This gives you a new row in which to enter Parameter, Type, and Value information. You can add multiple parameters to a target.



Entering data in the Common and Assign sections is optional, depending on how your environment is configured. For information about the Common and Assign attributes sections, as well as the read-only attribute fields in Parent Groups and Creation Information, see ["Common Resource Attribute Fields" on page 684](#).

Authorization and Authentication Settings

Authentication: You can specify user login behavior for commands designed to run on secure, remote target servers. You can specify login credentials to be used as part of the command, or set parameters that prompt users to enter their user name and password when they run the command.

Authorization: You can set up fine-grained access control lists (ACLs) to specify which ESM Console users have permissions to view, run or edit different commands.

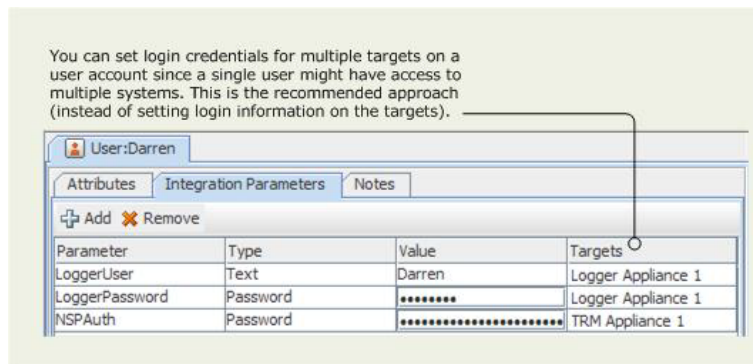
The following topics explain how to set up login details and ACLs in integration commands.

Setting User Login Parameters

You can specify login credentials on user accounts or on remote target servers. It is best to set login credentials on user accounts, but both options are described below. (Login credentials are not required for Connector integration commands because the authentication is handled as part of the SmartConnector setup.)

Setting Login Credentials

For URL commands on remote targets (including TRM commands) and script commands that run locally, you can define login credentials as a part of user configurations. (Choose Navigator > **Users**, select and edit a user or create a new one, then click the **Integration Parameters** tab on the **User Editor**.)



Defining login information as part of user accounts gives you the flexibility to configure multiple users, each with different logins. In this case, login credentials are not tied to the command target, but rather associated with individual users.

A single user account can have login credentials for different servers and scripts. In the example pictured above, the user "Darren" has login credentials for a TRM appliance (via the authentication token defined for the NSPAuth parameter) and also for a Logger appliance (which takes a user name and password as authentication).



For **security best practices**, we recommend that you:

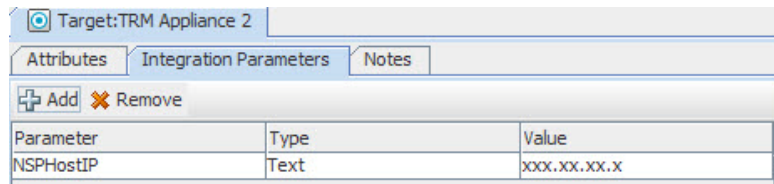
- Always set login credentials (passwords or authentication tokens) to type "Password" (not "Text"). (Credentials set to "Text" are not masked on the UI and are sent as clear text if the renderer is an external browser.)
- Save authentication information only as parameters on user accounts, not on target servers. This strategy binds authentication details to specific users, and gives you tracking information based on user logins (for example, you can tell which users ran which commands and when).

Examples of authentication information are user name and password combinations, and authentication tokens sent in URLs such as in NSP TRM.

Setting Login Credentials on Target Servers

Although not generally recommended, login credentials for URL commands on remote targets also can be defined as part of the Target definition, as described in ["Specifying Targets" on page 617](#). (Choose Navigator > Integration Commands > Targets tab, select

and edit a target or create a new one, then click the **Integration Parameters** tab on the **Targets Editor**.)



If login information is defined here, everyone who uses the command uses the same credentials to log in to the remote target server.



- Do not save authentication information as parameters on target servers. It runs the risk of opening up a remote server to any user who has access to the integration commands. Additionally, it does not give you any tracking information based on user logins to the server.
- Always set login credentials (passwords or authentication tokens) to type "Password" (not "Text"). (Credentials set to "Text" are not masked on the UI and are sent as clear text if the renderer is an external browser.)

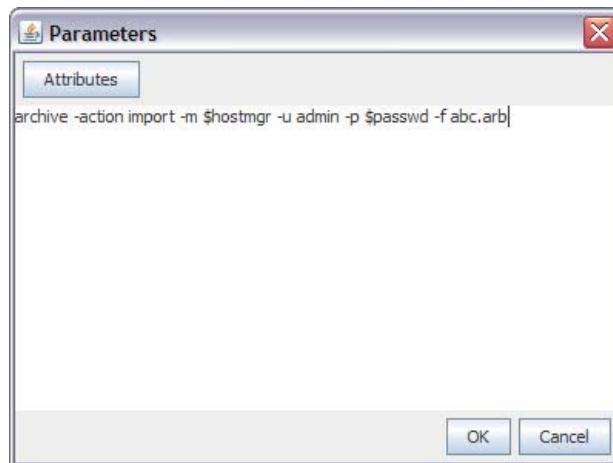
Setting Logins and Other Parameters to Prompt for Values at Runtime

You can set parameters for which you would like to prompt users to specify values at runtime, such as user name and password, host names, IP addresses, and other options.

When an integration command runs (i.e., when a user selects an integration command in some context on the ESM Console), the command first looks for any required parameter values in a variety of sources, including in the command statement itself, in the defined context, on the user account, on the target (if there is one), and so forth. If it doesn't find parameter values in any of these places, the system prompts the user to type in the values.

You can include login and other parameters as flags on a script command that runs against a server, as shown here for the archive command which runs on a Manager. When this command is run, it prompts the user for a Manager host name and administrator password. (It does not prompt for the user name, `admin`, since this already is provided in the command statement.)

```
archive -action import -m $hostmgr -u admin -p $passwd -f abc.arb
```



Please refer to [“Entering/Saving Command Parameters at Runtime” on page 622](#) (in [Running Integration Commands](#)), for an example of the run-time prompts users see when they run this command.

Access Control Lists (ACLs) on Integration Commands

You can configure access control lists (ACLs) on integration commands, since they are resources (and ACLs can be configured on resources). For details on how this works in general, please see [“Granting or Removing Resource Permissions” on page 647](#).

You can grant or limit read/write access to integration commands, integration configurations, and integration targets down to the *grouped resource* level for particular *user groups* by setting the setting ACL permissions on the resource group for any set of commands. Note that both the resources themselves and the users must both be in groups in order to work with them in this way.

For example, suppose you have a group of TRM CounterACT commands. The commands are grouped in a command group called “CounterACT Investigate Commands,” and associated with a configuration called “CounterACT Investigate Configurations.” You have two users (Darren and Larry) in a group called “Analyzers” to whom you want to give permissions to simply *run* these commands (not edit them). To do this, you would choose **Users** in the Navigator, select the Analyzers group, right-click and choose **Edit Access Control**. On the Resources tab, add both the CounterACT Investigate commands and configurations groups, and give read access on both. (Add the resource Integration Command and select the appropriate command group in the selector, and add the resource Integration Configuration and select the appropriate configuration group in the selector, then click the **Read** check boxes for each under Resource Targets and save the ACLs for the user group.)



Tip

- User group ACLs with **read** permissions on the integration command and configuration resources groups can **run** commands.
- User groups with **read and write** permissions on integration command and configuration resource groups can **run and edit** these commands.
- Commands can be configured to prompt for input parameter values when the command runs. If you want to give users permissions to **save the parameter values** required at command runtime, then you also need to give **read and write** permissions to the associated **Integration Targets** groups on the ACL editor for the user group.

You can organize users and the commands, configurations, and targets into various groups to fit with the permissions schemes you want to create. You might, for instance, want to create one set of TRM *Investigate* commands/configurations and give those permissions to one set of users (for example, Darren and Larry in the Analyzers group). Then you could create another set of TRM *Quarantine* commands/configurations and give those permissions to a different group of users (for example, Samantha, Endora, and Arthur in Analyzer Administrators group). It might be appropriate for this second group to have more authority, and therefore you would grant a broader set of permissions to it (for example, both Investigate and Quarantine permissions per the ACL settings on the Analyzer Administrators group).

Running Integration Commands

After commands are configured, they are available in various contexts in the ESM Console.

For example, suppose you have a configuration for a set of commands with the contexts set as follows:

Location	Type	Selection	Data Type
Viewer	All Views	All Selections	IP Address

This means that the given commands are available on right-click context menus on any view (for example, active channels, list views, chart views, dashboards, and so on). The user can select any row, cell, or area on a chart. In this context, only IP addresses can be provided as valid parameters to the command.

If one of the commands in this configuration was a an NSP TRM “Quarantine Node” command (a type of CounterACT Connector command), then to use the command you would do the following:

- 1 Bring up an active channel, session list, active list, dashboard, or other resource in the viewer that shows, for example, a suspicious device, machine, or user that you want to quarantine.
- 2 Find the row on the Viewer display that contains the suspicious entity, and select a cell in that row that contains the source IP address (for example, Attacker Address).
- 3 Right-click over the cell with the source IP address (for example, Attacker Address), and choose **Integration Commands > Quarantine Node**.

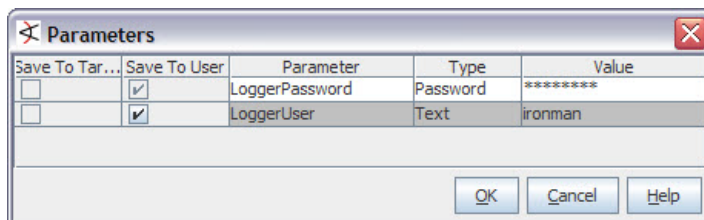
This launches the selected command, using the IP address for the selected cell as the parameter for the command.

In general, a right-click any context in the ESM Console UI for which integration commands have been configured show all integration configurations.

Entering/Saving Command Parameters at Runtime

Commands can be configured to prompt for parameter values at runtime (as described in [“Setting Logins and Other Parameters to Prompt for Values at Runtime” on page 620](#)).

Also, if ready-made commands (such as for Logger or TRM) are not pre-configured, you are prompted for values. For example, parameters might ask for a particular host name as command input, an IP address against which to run a command, or login credentials to a target server.



If you launch a command that prompts for input, enter the appropriate text in the “Value” field for each required parameter.

If you have appropriate permissions, you have the option to save parameter values with the target or with your user account so that you don't have to re-type them each time you run the command.



- In order to save parameter values at runtime, you need to belong to a group with *read and write permissions* to the associated *targets*.

Security Best Practice Recommendations:

- Always set login credentials (passwords or authentication tokens) to type "Password" (not "Text"). Credentials set to "Text" are not masked on the UI and are sent as clear text if the renderer is an external browser.
- Always save login credentials to user (Save to User), not to the target server. This strategy binds authentication details to specific users. This better safeguards access to the remote server to appropriate users. Also, you have tracking information based on logins as to which users entered which commands.

If you save authentication details as parameters on a target, you run the risk of opening up a remote server to any user who has access to the integration commands (but not necessarily an account on the target server). And you have no per-user tracking information.

Examples of authentication information are user name and password combinations, and authentication tokens that are sent in URLs (for example, NSPAuth parameter that holds the authentication token in NSP TRM).

Creating New Configurations On-the-Fly

You can also create a new integration configuration from within a context. To do this, right-click anywhere in the UI, and choose Integration Commands > New Configuration. (See ["Using Configurations to Group Commands" on page 610](#) for next steps.)

Ready-Made ArcSight TRM Commands

ArcSight NSP TRM commands are integrated into the ESM Console and provided as standard content. These commands run on ArcSight NSP TRM appliances.

The TRM commands are fully described in the ArcSight NSP documentation, particularly in the *ArcSight NSP Installation and Administration Guide*.

Options for Up-Front or On-the-Fly Configuration

Configuring these integrated TRM commands involves specifying the target TRM appliances and saving TRM authentication tokens on users who need TRM command access.

You can use either of these approaches for setting up the NSP TRM integrated commands:

- Configure target and authentication details before the commands are run (for example, a single administrator specifies TRM targets, users, and command parameter values). For this workflow, see ["Enabling NSP TRM Commands" on page 625](#).
- Let users configure commands at command runtime (for example, a user launches a command based on an active channel selection and fills in the target appliance IP address, authentication token, and parameter values on-the-fly). For this strategy, users can refer to ["TRM Integration Commands" on page 624](#) and ["Understanding NSP TRM Authentication" on page 627](#).

If the command details aren't pre-configured, users are prompted to enter the right values when they run the commands. Running one of the commands should set up the

target for most commands. Some commands might require further setup that can be done again on-the-fly. Information on how to run integration commands, see [“Running Integration Commands” on page 622](#). (This topic includes information about running commands and entering/saving parameter values at command runtime.)

TRM Integration Commands

The following integration commands are supported in ArcSight NSP v5.0 and newer versions. These are defined in /All Integration Commands/ArcSight Administration/TRM. For all, you need to provide values for the given parameters. At a minimum, these include NSPAuth (user authentication token) and NSPHostIP (target TRM appliance).

The commands execute based on which events you select in the ESM Console to launch the command. This is accomplished with Velocity Expressions, which are built into the commands to get values for some parameters, such as *\$selectedItem*, *\$selectedField*, *\$attackerAddress*, *\$targetAddress*, and so on. For example, “Quarantine Node” would quarantine the node in the selected event.

Commands	Description
Auth Queue	Shows the Authorization queue so you can allow or deny any TRM actions listed in the queue (such as Block IP Traffic or Disable Enterprise Account).
Auth Report	Generates reports for quarantines located in the authorization queue.
Block IP Range	Blocks an IP address range on Layer 3 devices on your network so that traffic from nodes with those IP addresses is not permitted.
Block IP Traffic	Blocks any IP traffic coming from a node on the network to the destination port specified in the event.
Disable Enterprise Account	Disables a user account so that the user cannot log on to your network. The user account needs to belong to the default Enterprise Account Source configured on the TRM appliance.
Investigate Node	Initiates the “investigate” process so you can obtain information about a node’s connectivity to the network, such as its IP address, DNS name, MAC address, and location type (whether the node is on an internal or an external interface in the network topology). You can also see which Layer 3 network device is closest to the node and the Layer 2 network device to which the node connects. You can use this information in a Case.
Network Devices	Lists all the network devices that NSP is managing, such as routers and switches.
Attacker-Target Maps	Displays a map showing network connections for an Attacker-Target scenario (based on the nodes in the event selected in the ESM Console). Note: The map shows Layer 3 logical connectivity (possible routes) not physical connectivity (wires that connect devices). So, the map might not depict the physical topology of the network.

Commands	Description
Quarantine Node	Quarantines a node when you discover a problem that has the potential to spread to other nodes in your network. You can select from these Quarantine actions: Disable Port, Filter MAC, and Move to VLAN.
Response Log - Blocked IP Range	Lists all Block IP Range actions taken by TRM and provides details about each one, such as who performed the action, when the action was taken, and the devices on which the action was taken.
Response Log - Blocked IP Traffic	Lists all the Block IP Traffic actions taken by TRM and provides details about each one, such as who performed the action, the date and time the action was performed, and the devices on which the action was taken.
Response Log - Disabled Account	Lists the Disable Enterprise Account actions taken by TRM and provides details about each one, such as who disabled the account, the date and time the account was disabled, and the status of the disabled account.
Response Log - Quarantined Nodes	Lists the Quarantine Node actions taken by TRM and provides details about each one, such as the IP address of the quarantined node, the date and time the node was quarantined, and the status of the quarantine (active or removed).
Response Report	Generates a response history report that contains a text and graphical representation of the actions performed on the TRM appliance.

Enabling NSP TRM Commands

To enable pre-configured ArcSight NSP TRM commands from the ESM Console, follow these steps.

1. Set up the Command Targets

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Targets**.
- 2 Create an integration target for your TRM Appliance, or edit one of the existing entries.

We recommend that you start by editing the target already provided for you in /All Integration Targets/ArcSight Administration/TRM/:

◆ TRM Appliance 1
- 3 In the Target editor on the **Integration Parameters** tab, add at a minimum, the following parameters.

Parameter	NSPHostIP
Type	Text
Value	<IP address or Host Name of the TRM Appliance>

you are prompted for other parameters needed when you run the commands. If you want to set up more parameters and values now, you can do so. (See [“TRM Integration Commands” on page 624.](#))



Best Practice Recommendation: We recommend saving only the target host information (for example, IP address) on the target server, not the authentication credentials. If you save authentication details as parameters on a target, you run the risk of opening up a remote server to any user with access to integration commands (but not necessarily an NSP TRM account). And you have no per-user tracking information, like you do if you save this information to user accounts.

- 4 If you have more than one TRM Appliance, create an additional integration target for each appliance you want to integrate into the command hub.
- 5 Click **Apply** or **OK** to save your changes to the target.

(For general information about command targets, see [“Specifying Targets” on page 617.](#))

2. Set up the Command Configuration

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Configurations**.

You can find the pre-built NSP TRM command configuration in /All Integration Configurations/ArcSight Administration/TRM/**TRM Commands**.

This configuration includes all the standard content TRM commands.

- 2 Edit the **TRM Commands** integration configuration:
 - ◆ In the Configuration editor, click the **Targets** tab, and then add the integration target(s) you created in the previous steps (for example, if you used the provided target, choose TRM Appliance 1).
- 3 Click **Apply** or **OK** to save your changes to the configuration.

(For general information about command configurations, see [“Using Configurations to Group Commands” on page 610.](#))

3. Set up Users for TRM Access

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Users**.
- 2 Edit the users that have access to the TRM Appliance. In most cases, these users should have administrator privileges.
- 3 Click the **Integration Parameters** tab, and then create an integration parameter for TRM authentication token. (Administrators and users with accounts on the target server can obtain this token from the TRM appliance as described in [“Understanding NSP TRM Authentication” on page 627.](#))

Parameter	NSPAuth
Type	Password
Value	<NSP TRM Authentication Token encrypted login credentials>
Targets	<Select targets for that TRM user>

**Best Practice Recommendations:**

- Always set login credentials (passwords or authentication tokens) to type "Password" (not "Text"). (Credentials set to "Text" are not masked on the UI and are sent as clear text if the renderer is an external browser.)
- Always save login credentials to user account (Save to User), not to the target server. This strategy binds authentication details to specific users and better safeguards target server access. Also, you have tracking information based on logins as to which users entered which commands.

- 4 Click **Apply** or **OK** to save your changes to the user.

(For general information about setting up login credentials and access control lists for integration commands, see ["Authorization and Authentication Settings" on page 618.](#))

Understanding NSP TRM Authentication

Integrated NSP TRM commands require use of an encrypted authentication string (token) to connect to the TRM appliance. (An integrated TRM command sends this token to the target TRM appliance as part of a URL to accomplish user login.)

The authentication token is used to log in to a TRM appliance (instead of a user name and password combo).

Users who want to send TRM commands to an appliance need to have a valid TRM authentication token.

This is used to set up login credentials on users. The token is specified as a value for the NSPAuth parameter for a particular user (in user accounts).

How to Get a TRM Authentication Token

To get a TRM authentication token, you need access to the NSP TRM appliance.

Log in to the TRM appliance, and generate the authentication token based on your login credentials.



Before you can generate an encrypted value as a TRM administrator or view it as a non-admin user, the setting **Allow Encrypted Authentication Credentials in URL** must be enabled (set to Yes). (By default, this setting is disabled.)

So, as a prerequisite, an administrator needs to navigate to **Admin** tab > **Users & Groups** > **Settings** > **Authentication** tab to enable this setting.

- 1 Generate the token.

There are two ways to obtain an encrypted value for an NSP TRM user name and password:

- An NSP admin user can view the encrypted values for all NSP users on the View Encrypted Authentication Credentials page (**Admin** tab > **Users & Groups** > **Settings** > **Authentication** > **View URL Strings**).

The key is displayed after you click View URL Strings.

(Make sure the setting Allow Encrypted Authentication Credentials in URL is set to Yes, otherwise the URL strings do not show up.)

- An NSP user (with non-admin privileges) can view the encrypted value for their user name and password on the **Change Password For <User_Name>** page. To get to this page, click **Options** in the top, right-hand side of any NSP screen. The authentication key is displayed under “Encrypted Authentication Credentials in URL is enabled”.
- 2 Copy the token. On both the administrator and user pages, the authentication token is displayed in this form: `enc_auth=<AuthenticationKey>`



The authentication token is the string that follows `enc_auth=`. Be sure to copy only that string and do not include `enc_auth=`. A common problem with getting the TRM login to work with the integrated commands is not copying the full string, or including `enc_auth=` in the copy.

- 3 After you get the encrypted value, use it as the value for the NSPAuth parameter (paste it into the parameter value field), as described in “3. Set up Users for TRM Access” on page 626.

If you are setting up NSP TRM commands on-the-fly (as you run the commands), you use this token during that process. For more on this, see “Entering/Saving Command Parameters at Runtime” on page 622.



Best Practice Recommendations:

- Always set login credentials (passwords or authentication tokens) to type “Password” (not “Text”). Credentials set to “Text” are not masked on the UI and are sent as clear text if the renderer is an external browser.
- Always save login credentials to user, not to the target server. This binds authentication details to specific users, limits access to the remote server to appropriate users, and provides tracking information based on logins about which users entered which commands.

If you save authentication details as parameters on a target, you run the risk of opening up a remote server to any user who has access to the integrated commands (but not necessarily an account on the target server). And you have no per-user tracking information.

Examples of Running TRM URL Commands

When you have NSP TRM target appliance information and user authentication details, you are ready to run TRM commands from the ESM Console. Here are some examples of what to expect when you run a TRM command.

These examples show the NSP Web client in the ESM Console internal browser rather than on an external Web browser. The ready-made TRM command configurations are set by default to display in an external Web browser. To change the TRM command configuration to display results in the internal browser, go to **Console Navigator > Integration Commands > Configurations > All Integration Configurations ArcSight Administration > TRM Commands**, and edit the selection for the Renderer. (Additional setup is needed for this display choice.)

The *Console internal browser is more secure*, but requires additional setup to display some elements in NSP displays, for example, Adobe Flash plug-ins. Also, the internal browser is not currently supported on Mac OS.

See “Web Browsers (Internal and External)” on page 1030 for information on configuring ActiveX controls on the internal browser, OS platform support, and security considerations.

Attacker-Target Network Map

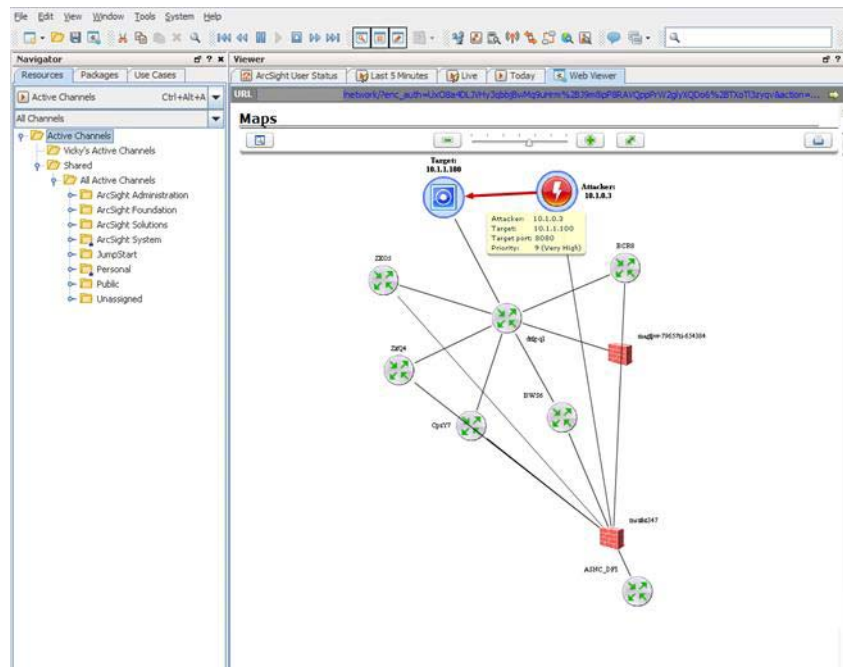
This example shows a network map with an attacker/target scenario and network paths.

Right-click on an event in an active channel, and choose **Integration Commands > TRM Commands**.

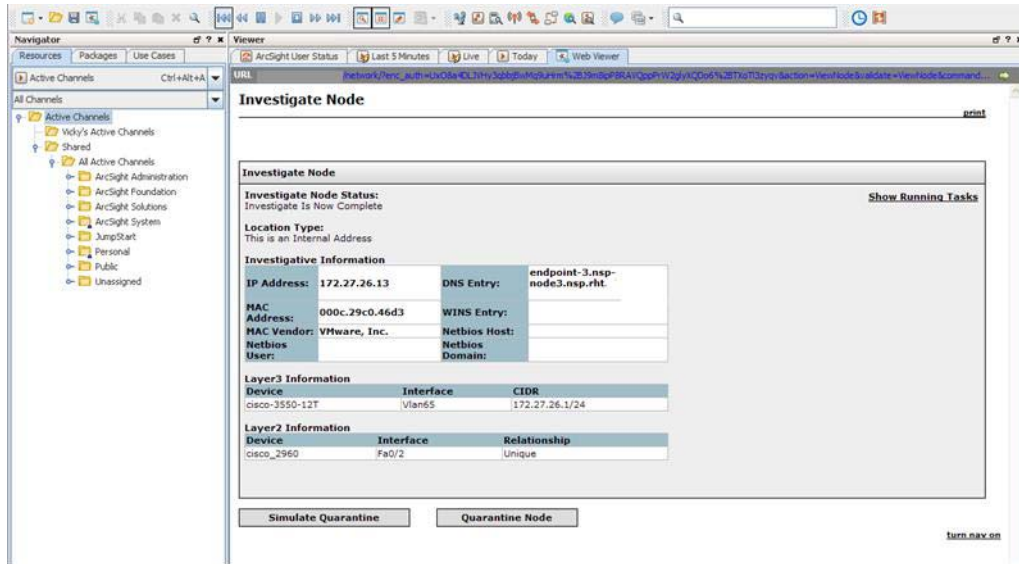
On the TRM Commands dialog, select **Network Maps** and **TRM Appliance 1** as the target appliance, and click **OK**.

This logs you in to the target TRM appliance, and sends the Attacker IP address, Target IP address, and Target Port as parameters on the Attacker-Target Map command.

As a result, we get this map.



This logs us in to the target TRM appliance, and sends the selected node as a parameter on the Investigate command.



Going Further with NSP TRM Command Results

From here, there are a number of ways you could leverage the details you get from the NSP TRM examples.

You can create a case based on the initial event you selected, and feed the NSP details into the case as Notes or an attached file. The drill-down information you get from a TRM Investigate Node command is typically richer. You can copy those details into case notes or into a text file and add it as an attachment.

The Investigate Node display also provides a **Simulate Quarantine** option that lists actions TRM would take to quarantine the node. Running simulations and saving related details is useful where the security operations center (SOC) and network operations center (NOC) need to coordinate authorizations for taking actions. A SOC operator without authorization to quarantine nodes could investigate the node, run the simulation, and send the details to the NOC to take action.

In this scenario, administrators might also use the TRM authorization queue. The operator who runs the TRM commands could quarantine the node, but the command would sit in an authorization queue until an administrator approves it to run.

ArcSight Logger Search Commands

ArcSight Logger Search commands are integrated into the ESM Console and provided as standard content. These commands enable searches on ArcSight Logger appliances and are supported starting with ArcSight Logger v4.0.

Configuring the ready-made integrated Logger commands involves specifying IP addresses for the target Logger appliances and saving login credentials on users who need Logger search access.

Logger Integration Commands

These integrated commands are supported in ArcSight Logger v4.0 and later versions. (These are defined in /All Integration Commands/ArcSight Administration/Logger.)

Command	Description
Logger Search	<p>Allows you to right-click an event in an active channel and run a search for one of the fields presented in a list.</p> <ul style="list-style-type: none"> Displays a pop-up dialog with search options. Allows you to search by: <ul style="list-style-type: none"> Event Name Destination Source Destination and Source User Service Vendor and Product You can select the Logger Appliance on which to search.
Logger Quick Search	<p>Allows you to right-click a field in an active channel to search based on the field and value selected. If there is more than one Logger appliance set up, a pop-up dialog box allows users to choose which appliance to search.</p>

Enabling Integrated Logger Searches

You can use either of these approaches for setting up the Logger searches:

- Configure target and authentication details before the commands are run (for example, a single administrator specifies Logger targets, users, and command parameter values). For this workflow, follow the steps below to:
 1. [Set up Logger Command Targets](#),
 2. [Set up the Logger Command Configuration](#), and
 3. [Set up Users for Logger Access](#).
- Configure commands at command runtime (for example, if you launch a command based on an active channel selection and fill in the target appliance IP address, authentication token, and parameter values on-the-fly).

If you have not pre-configured the command details, you are prompted to enter the right values when you run the commands. Information on how to run integration commands, see [“Running Integration Commands” on page 622](#). (This topic includes information about running commands and entering/saving parameter values at command runtime.)

To enable pre-configured ArcSight Logger searches from the ESM Console, follow these steps.

1. Set up Logger Command Targets

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Targets**.
- 2 Create an integration target for your Logger Appliance, or edit an existing target in /All Integration Targets/ArcSight Administration/Logger/, such as Logger Appliance 1 or Logger Appliance 2.

- 3 In the Target editor on the **Integration Parameters** tab, add these parameters.

Parameter	LoggerHost
Type	Text
Value	<IP address or Host Name of the Logger Appliance>

- 4 If you have more than one Logger Appliance, create an additional integration target for each appliance to be made searchable.
- 5 Click **Apply** or **OK** to save your changes to the target.
- 6 For information about command targets, see [“Specifying Targets” on page 617](#).

2. Set up the Logger Command Configuration

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Integration Commands > Configurations**.

You can find the pre-built Logger command configurations in /All Integration Configurations/ArcSight Administration/Logger/

- 2 Edit the **Logger Search** integration configuration:

In the Configuration editor, click the **Targets** tab and add the integration targets you created earlier.

- 3 Edit the **Logger Quick Search** integration configuration:

In the Configuration editor, click the **Targets** tab and then add one integration target from the list of targets you just created.

- 4 Click **Apply** or **OK** to save your changes to the configuration.

For information about command configurations, see [“Using Configurations to Group Commands” on page 610](#).

3. Set up Users for Logger Access

- 1 In the Navigator, click the **Resources** tab, and then navigate to **Users**.
- 2 Edit the users that have access to the Logger Appliance. In most cases, these users should have administrator privileges.
- 3 Click the **Integration Parameters** tab, and then specify the integration parameters for the Logger search

Parameter	Description
LoggerUser	The Logger account name to use when accessing a Logger target.
LoggerPassword	The password for that Logger account.
LoggerHost	The IP address of the Logger host.
OTPUser	The Logger user account to use with the OTP authentication feature (see note, below).
OTPPassword	The password to use for the OTPUser specified above.
LoggerPort	For OTP, you must specify the port number for the Logger. For a Logger appliance the port number is 443.



The **One-Time Password (OTP)** function requires that you are using Logger 5.1 or later.

If you have an earlier version of Logger, then for Logger searches continue to use the LoggerUser and LoggerPassword as before. Until you install Logger 5.1 or later, searches display a message that it failed to negotiate a single-use session token and is proceeding with regular authentication. Just click **OK** to continue.

For all of these parameters, you can specify a type of “Password” or “Text.” For Text type the password will appear in plain text in the session URL. This is not an issue for any parameter except passwords, so use text for the others but use the Password type for passwords.

Save to Target means that this parameter automatically applies whenever any user is accessing the currently-specified target Logger.

Save to User means this parameter is used automatically whenever the currently-logged-in user accesses any Logger target.

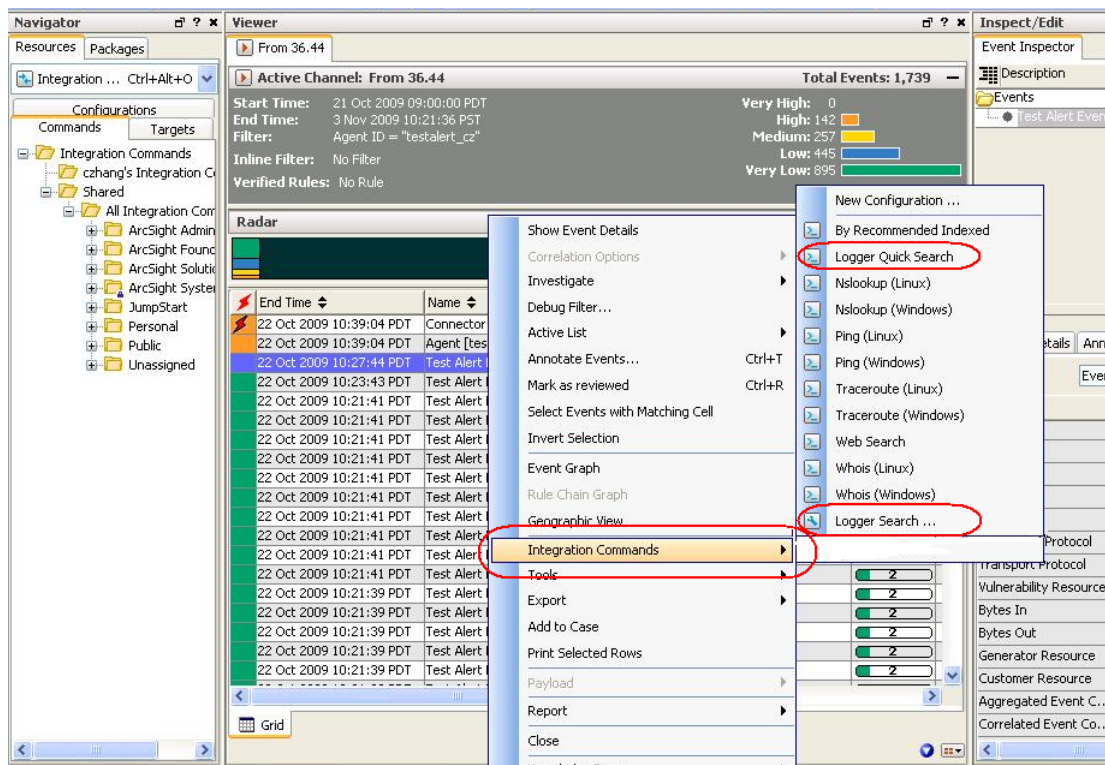
- 4 Click **Apply** or **OK** to save your changes to the user.

For information about setting up login credentials and access control lists for integration commands, see [“Authorization and Authentication Settings” on page 618](#).

Example of Running a Logger Quick Search

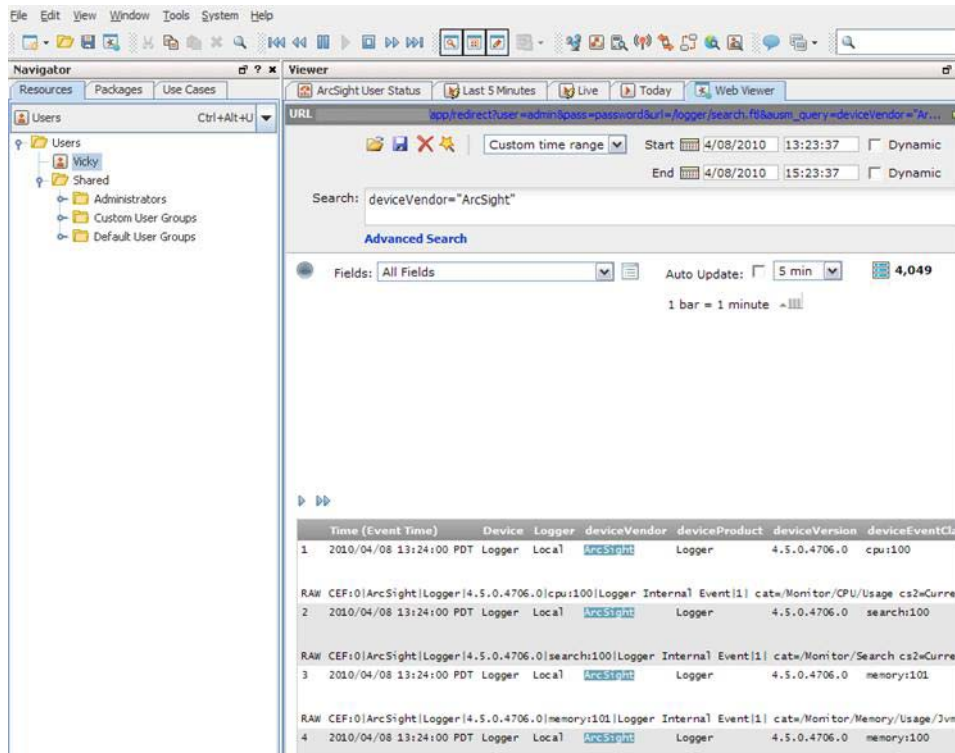
With Logger target appliance information and user authentication details, you are ready to run Logger searches from the ESM Console.

Right-click on an event in an active channel, select a field such as Device Vendor or Device Product, and choose **Integration Commands > Logger Quick Search**.



This logs you into the target Logger appliance (for example, Logger Appliance 1), and sends values for the selected fields as parameters on the search command.

You get the results of the search in the ESM Console internal browser, and are now logged in to the Logger Web client, if you want to take further actions on the appliance.









Network Tools as Integration Commands

The following standard network tools are also provided as integration commands. You can find this toolset in: /Integration Commands/Shared/ArcSight System/Tools/. You can edit these or add new commands, configurations, and contexts as described in [“Defining Commands” on page 602](#) and [“Using Configurations to Group Commands” on page 610](#). (Also see [“Using the Network Tools” on page 107](#))

With network tools integration commands you can:

- **Define contexts for where tools show up on the ESM Console.** You can customize integrated network tools and configure them for all types of views (charts, graphs, tables), and in the navigator, editors, and so on. Legacy network tools are available only on grid views; you cannot define the context.
- **Select and run commands on navigator tree items, all types of views, and editors items.** With integrated network tools, you can select various items in chart and graph views, on the editors, and in the navigator tree. Legacy network tools are limited to running only on the selected cell in a grid view (table) in the Viewer.
- **Configure access control lists (ACLs).** You can grant or limit access to integrated network tools commands for particular user groups by setting the setting ACL permissions on the tools resource group. The integrated network tools reside under /All Integration Configurations/ArcSight System/Tools. You can control access to the tools commands and configurations groups (select the Tools group, right-click, and choose **Edit Access Control**) as described in [“Granting or Removing Resource Permissions” on page 647](#). You can organize users and the tools themselves into various groups to

fit with the permissions scheme you want to create. With the legacy network tools, you do not have this ACL option. See [“Access Control Lists \(ACLs\) on Integration Commands” on page 621](#) for more information.

Tree	Icon	Resource
Nslookup		Resolves an IP address to a host or domain name or vice versa.
Ping		Determines whether a particular IP address is online and/or it tests and debugs a network by sending a packet and waiting for a response.
PortInfo		Lists standard usage such as WWW or FTP, for a specified port number.
Traceroute		Shows the path from the ESM Console to the IP address selected in the grid view, reporting the IP addresses of all routers in between.
WebSearch		Search the Web through Google to find links to the keywords present in currently selected active channel grid view cells.
Whois		Looks up who is behind a given domain name; information might include addresses and telephone numbers.

These are configured with default Velocity Expressions for parameters. You can edit the commands and configurations for these network tools as needed (and add new ones).

To run a network tool, select an IP address in a grid view (for example, active channel, list, data monitor) and select **Integration Commands > <Network Tool>** from the context menu (for example, **Integration Commands > ping**).



Note

- The Send Logs command is not configured as an integrated command. See [“Using the Network Tools” on page 107](#) and [“Send Logs” on page 980](#) for information on that command.
- To add or re-configure the legacy tools, choose **Tools > Local Commands > Configure**, select a tool, and click **Edit**. Keep in mind that they have limitations compared to the new tools.

Chapter 24

Knowledge Base Authoring

These topics explain how to do the basic tasks of managing Knowledge Base articles.

["Managing Knowledge Base Articles" on page 637](#)
["Managing Knowledge Base Article Groups" on page 639](#)
["Getting Knowledge Base Updates" on page 640](#)
["Associating Knowledge Base Articles" on page 640](#)

Managing Knowledge Base Articles

Creating Knowledge Base Articles

- 1 On the Navigator panel's drop-down menu, choose the Knowledge Base resource tree.
- 2 Right-click a group and choose **New Article**.
- 3 In the Knowledge Base Editor, select the **Article** tab.
- 4 On the Article tab, type in the **Name** text field.
- 5 Optionally use the **Summary** field to add a brief description of the article.
- 6 Optionally enter a different name for the information source in the **Author/Credits** field. Your user name is the default.
- 7 The **Origin URL** text field contains the URL or directory path to the page or file that contains the article's information. Use one of these methods to provide this string:
 - a Type the URL or directory path to the page or file, or
 - b Click **Upload File** to select and save an HTML file, with a .htm or .html extension, from your local drive, or
 - c Click **Launch Editor** to use an editor to create a new file. If an editor was not set prior to using the **Launch Editor** button, the Preferences dialog box appears so you can point to one.
 - d In the **Preferred text/HTML Editor** text field, type the path to a text editor or click the **Browse** button to select a text editor.
 - e In the editor, create a new file containing information on the article.
- 8 Choose the **Import** or **Reference** option, depending on how you want the Original URL page or file to appear in the article.

Use **Import** to copy the HTML file into the Knowledge Base. The page or file remains linked to, and continue to be updated from, its original location.



When you select **Import**, only the content between the body tags of the HTML page appear. Therefore, you should use **Reference** when the HTML page uses JavaScript, uses frames, or includes images. Choose **Import** when you use an editor to create a file specified in the **Origin URL** text field.

Choose **Reference** if you want the page or file to remain static. The URL or the directory path to the page or file appears as a link in the article.

9 Enter a summary of the article in the **Summary** text field.

10 Click **Preview** to see the article as it will appear in a browser window.

Use the **Preview** button to assist you in selecting either the **Import** or **Reference** radio button for HTML pages.

11 Click **Apply** to enter the changes and keep editing or click **OK** to save and close.

Showing a Knowledge Base Article

In the Knowledge Base window, right-click an article and choose **Show Article**.

Editing a Knowledge Base Article

1 In the Knowledge Base window, right-click an item and choose **Edit Article**.

2 In the Knowledge Base Editor, select the **Article** tab.

3 On the Article tab, make edits.

For more information, see [“Creating a Knowledge Base Article Group” on page 639](#).

4 Click **Preview** to see how the article will appear in a Web Viewer tab.

5 Click **OK**.

Moving or Copying a Knowledge Base Article

1 In the Knowledge Base window, navigate to an article and drag and drop it into another group.

2 Choose **Move** to move the article, **Copy** to make a separate copy of the article, or **Link** to create a copy of the article that is linked to the original article.

If you choose **Copy**, you create a separate copy of the article that is not affected when the original article is edited. If you choose **Link**, you create a copy of the article that is linked to the original article. Therefore, if you edit a linked article, whether the original or the copy, all links are edited as well. When deleting linked articles, you can either delete the selected article or all linked article copies.

Deleting a Knowledge Base Article

1 In the Knowledge Base window, right-click an item and choose **Delete Article**.

2 In the dialog box, click **Yes**.

Managing Knowledge Base Article Groups

Knowledge Base article groups can be used to organize similar or related articles in a single location. For example, you could create a Denial of Service group to store specific articles about Denial of Service attacks such as a Ping Flood attack.

Groups and articles can be managed with drag and drop functionality. You can move or copy groups and articles into other groups within the Knowledge Base resource tree. If a group is deleted, the articles within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Creating a Knowledge Base Article Group

- 1 In the Navigator panel's drop-down menu, choose the Knowledge Base resource tree.
- 2 In the Knowledge Base window, right-click a group and choose **New Group**.
A name text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Rename**.
- 2 In the name text field, rename the group.
- 3 Press **Enter**.

Editing a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, type in the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Knowledge Base Article Group

- 1 In the Knowledge Base window, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a Knowledge Base Article Group

- 1 In the Knowledge Base resource tree, right-click a group and choose **Delete Group**.

- 2 In the dialog box, click **Yes**.

Getting Knowledge Base Updates

In the Knowledge Base resource tree, the **Refresh** right-click option refreshes the tree from the selected level, showing changes made to the sub-trees below that group. Supposing a group or article name was modified through another ESM Console, or a group or article was deleted, renamed, or moved from another ESM Console, refresh shows those changes.

Refreshing the Knowledge Base Tree

In the Knowledge Base resource tree, right-click the **Knowledge Base** group or article and choose **Refresh**.

Associating Knowledge Base Articles

Knowledge Base groups and articles can be associated with other resources such as cases, reports, or filters.

Associating Resources with Knowledge Base Groups or Articles

- 1 Use the Navigator panel to locate an individual or group target resource, for example, a case or case group.
- 2 Right-click the resource and choose **Knowledge Base > Associate with**.
- 3 Use the Knowledge Base Article Selector to find and select an article to associate with the resource.
- 4 Click **OK**.

Associating Grid View Elements with Knowledge Base Articles

- 1 In a Viewer panel grid view, right-click an event attribute and choose **Knowledge Base > Associate > Cell/Row/Column with**.
- 2 Use the Knowledge Base Article Selector to find and select an article to associate with the grid view's selected cell (data), row (event), or column (attribute).
- 3 Click **OK**.

Managing Users and Permissions

The following topics cover user management, user permissions with regard to specific resources, and system notifications.

[“Managing Users” on page 641](#)

[“Managing Permissions and Resources” on page 646](#)

[“Managing Notifications” on page 658](#)

Managing Users

You manage numbers of users by organizing them into groups based on roles or other logical groupings, setting their permissions and passwords, and enabling or disabling their login functionality. Permissions to access specific ArcSight resources (for example, to create rules or reports) are granted to specific groups by editing the access control lists (ACLs) for those groups.

All ArcSight user group memberships and permissions are stored in the ArcSight Database. When users log in, they are allowed to perform any operations for which they are granted permission through their membership in one or more groups.

Handling Users

When you create an ArcSight user, that person automatically receives access to a set of resource groups. Users can store, create, edit, or delete resources within their groups without jeopardizing other users' resources.

Creating a User

- 1 In the Navigator panel drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click the group in which to place the new user and choose **New User**.
- 3 In the **User Editor**, fill in these fields on the **Attributes** tab in the **Login** section:

User Fields	Description
User ID	User name for login ID. This is a required field.

User Fields	Description
User Type	<p>Choose a user type from the drop-down menu. This is a required field.</p> <p>The currently supported user types are:</p> <ul style="list-style-type: none"> • Normal User: Has full privileges to use the ESM Console or ArcSight Web client, and all tools. Only apply this user type to accounts that actually need access to the ArcSight Manager. • Management Tool: Has only the privileges needed to run certain management tools used in conjunction with network management products. • Forwarding Connector: Has only the privileges needed by the ForwardingConnector. • Archive Utility: Has only the privileges needed to run the archive utility. Access to specific resources is controlled through ACLs. • Connector Installer: A specialized identity used only to add SmartConnectors to the system. • Web User: Has privileges to use the ArcSight Web client or ArcSight Management Console (not the ESM Console or other tools). <p>See also “About the System User” on page 645.</p> <p>For more information, see “Users” on page 1005 and “User Types” on page 1006.</p>
Login Enabled	<ul style="list-style-type: none"> • Select the Login Enabled checkbox to <i>give the user login privileges</i> (a checkmark indicates this feature is on): <p style="text-align: center;">Login Enabled <input checked="" type="checkbox"/></p> <ul style="list-style-type: none"> • Or leave it deselected and off (no checkmark showing) to <i>disable logins</i> for this user: <p style="text-align: center;">Login Enabled <input type="checkbox"/></p> <p>Note: A user account login must be <i>enabled</i> to allow login access to the Console. If you disable a login for a user account, the user cannot log into the Console with the credentials associated with the disabled account.</p>
External User ID	Optionally, provide an alternate, external user ID. (An external user ID might be relevant if you have user accounts from other applications feeding into user database.)
Password	<p>Enter a password for this user. This is a required field.</p> <p>By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.</p> <p>(Passwords can be modified later as a part of editing user information. See “Resetting User Passwords” on page 643.)</p>
Confirm	Re-type the password to confirm it. This is a required field.

4 Fill in these fields on the **Attributes** tab in the **User** section:

User Fields	Description
Last Name	User's last name

User Fields	Description
First Name	User's first name
Title	User's job title
Department	User's department
Phone	User's phone number
Fax	User's fax number
E-mail	User's e-mail address. Use the format user@host.domain. The "@" sign and host domain are required. E-mail addresses are not case-sensitive.
Pager	User's pager number



For phone, fax, and pager numbers, parentheses (), dashes (-), and periods (.) are allowed. Alphabetic characters are not allowed.

- 5 In the **UserID** text field, enter a user login name. This field is required.
- 6 Click **OK**.

Editing a User

- 1 In the **Users** resource tree, right-click the user and choose **Edit User**.
- 2 In the **User Editor**, edit the text fields as described in the table above.
- 3 Grant or withhold login permission by selecting or deselecting the checkbox next to **Login Enabled**.
- 4 In the **Password** and **Confirm** text fields, edit the user password and confirm it by typing it again. These fields are required.

By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. System administrators can set special policies or requirements for their sites via a configuration file.

- 5 Click **OK**.

Resetting User Passwords

Administrators may also reset user passwords; for example, if a user's original password has been compromised or you want to make users update their passwords.

- 1 While logged into the ESM Console as an administrator, choose the **Users** resource in the Navigator panel.
- 2 Right-click the user whose password you want to reset and choose **Reset Password**.

The ArcSight Manager assigns a new random password (8 characters, including numbers and letters) and sends it to the selected user's assigned e-mail address.



Be aware that sending a password by e-mail can be dangerous since e-mails can be intercepted.

Alternatively, the following command on ArcSight Manager can be used to reset a user's password:

```
arcsight resetpwd
```

Moving or Linking a User

- 1 In the **Users** window, navigate to a user and drag and drop it into another group.
- 2 Choose **Move** to move the user or **Link** to create a copy of the user that is linked to the original user.

If you choose **Link**, you create a copy of the user that is linked to the original user. Therefore, if you edit a linked user, whether it is the original or the copy, all links are edited as well. When deleting linked users, you can either delete the selected user or all linked user copies.

Deleting a User

- 1 In the **Users** resource tree, right-click the user and choose **Delete User**.
- 2 In the dialog box, click **Delete** to delete the user and the listed user's resources or click **Disable Login** to disable the user.



By default, only administrators have permissions to delete users in a group. If you want to grant non-Administrator users permission to delete users in a particular group, you first need to provide *Write* access to the group by editing access to **User Groups** in the ACL Editor.

An additional step (providing *Write* access to user Reports) is necessary.

To grant non-Administrator users permissions to delete other users in a group, do the following:

- 1 In the `server.default.properties` file, set the `user.allowmodification=true`.
- 2 Restart the Manager.
- 3 Log into the ESM Console as Administrator, and select the **Users** resource in the Navigator.
- 4 Select the non-administrators group for which you want to provide permissions, right-click, and choose **Edit Access Control** to bring up the ACL Editor.
- 5 On the ACL Editor, click the **Resources** tab.
- 6 Select **Report** in the Resource drop-down menu, and click **Add** to bring up the Reports Selector dialog.
- 7 In the Selector dialog, select all users under `Reports/Shared/Personal/` and click **OK**. All users are shown as Resources targets.
- 8 Click to set **Read (R)** and **Write (W)** permissions as desired. Any user in the group now has Edit access to Report groups showing **Write** access (i.e., where **W** is check-marked), and therefore can delete users in this group.
- 9 Click **Apply** or **OK** to save your changes.

With *Write* permissions enabled on Reports for users you want to delete, members of this group can log into the ESM Console and delete those users.

For more information, see ["Granting or Removing User Group Permissions" on page 651](#).

About the System User

A special user called the system user can lock and unlock ArcSight System Core content. (For more information about System Core content, see [Chapter 3, Standard Content](#), on page 47 and [Chapter 4, ArcSight Express Solution](#), on page 73.)

The system user is configured as 'systemuser' by default. ArcSight recommends that you change this name to a non-standard name. This name can be changed only once. For example, once you change the name to 'coreuser', you cannot change this name again.



Note

ArcSight strongly discourages you from logging in as the system user for regular ArcSight system administration tasks. The purpose of this user is special and its capabilities are limited. For example, the system user cannot use channels or dashboards, install ArcSight SmartConnectors, or log in to ArcSight Web.

Handling User Groups

User groups associate related users or groups of users. When a group is created within a group, the new group inherits the existing group's permissions.

Groups and users can be managed with drag-and-drop functionality. You can move or copy groups and users into other groups from the Users resource tree. If a group is deleted, the users within that group are also deleted, unless they are also contained by other groups.



Note

To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.



Tip

You can grant or block non-administrator user access to deploy or un-deploy data monitors. These permissions are configured at the user group level.

For information on how to set user group permissions to enable or disable data monitors, see ["Controlling Who Has Permissions to Deploy Data Monitors"](#) on page 656.

Creating User Groups

- 1 On the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, right-click a group and choose **New Group**.
A name text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Edit Group**.

- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Linking User Groups

- 1 In the **Users** resource tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group or **Link** to create a copy of the group that is linked to the original group.

If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it is the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting User Groups

- 1 In the **Users** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Setting Startup Views

You can define the set of active channel and dashboard resource groups that members of a given ArcSight user group see by default when they first log in. This includes both ESM Console and ArcSight Web users. These channels and dashboards are initial defaults only: once users begin changing the content of the Viewer panel, the ESM Console and ArcSight Web follow their normal behavior of remembering the most recent state.

The default active channels and dashboards you select for user groups are listed in the User Group Editor on the Startup Views tab.

- 1 Right-click a user group in the Navigator panel's Users resource tree, and choose **Edit Group**.
- 2 In the User Group Editor, click the **Startup Views** tab, then the **Active Channels** or **Dashboards** tabs.
- 3 In either resource tab, click **Add** to open a resource selector dialog box.
- 4 Navigate to and select the appropriate active channels or dashboards to set as users' start-up resources, and click **OK**. Repeat this step to add more resources.
- 5 Click **Refresh** to update the current list of resources, or click **Remove** to take a selected resource off the list. Click **Edit** to change a selected resource in its own editor.
- 6 Click **Apply** to make changes and leave the editor open, or click **OK** to apply your changes and close the editor.

Managing Permissions and Resources

The subject of managing users is largely that of managing their access to and use of resources.

Editing Access Control Lists (ACLs)

The user groups ACL Editor has these tabs for viewing or editing permissions on resources, operations, user groups, events, and sortable field sets:

- Resources tab - Lists all resources available to the user group with either inspect or edit permissions, and lets you add/edit resource permissions.
- Operations tab - Lists operations for which this user group has permissions, and lets you add/edit operations permissions. (For example, a user group can have permissions to enable or disable data monitors.)
- User Groups tab - Lists the user groups with either inspect or edit access to the user group itself, and lets you add user groups.
- Events tab - Lists event filters for which this group has permissions, and lets you add/edit event filter permissions. This user group is permitted to see only events from the filters listed on the Events tab.
- Sortable Field Sets tab - Lists sortable field sets for which this user group has permissions. Lets you add/edit field set permissions.

See also, [“Access Control Lists” on page 787](#).



Always remember to have both ESM Console and ArcSight Web users log out and back in after changing user or resource access permissions, so they can see those changes.



The Resource ACL display shows relationships between users and groups, and how permissions are acquired for each of the user groups. Child groups inherit permissions from parent groups.

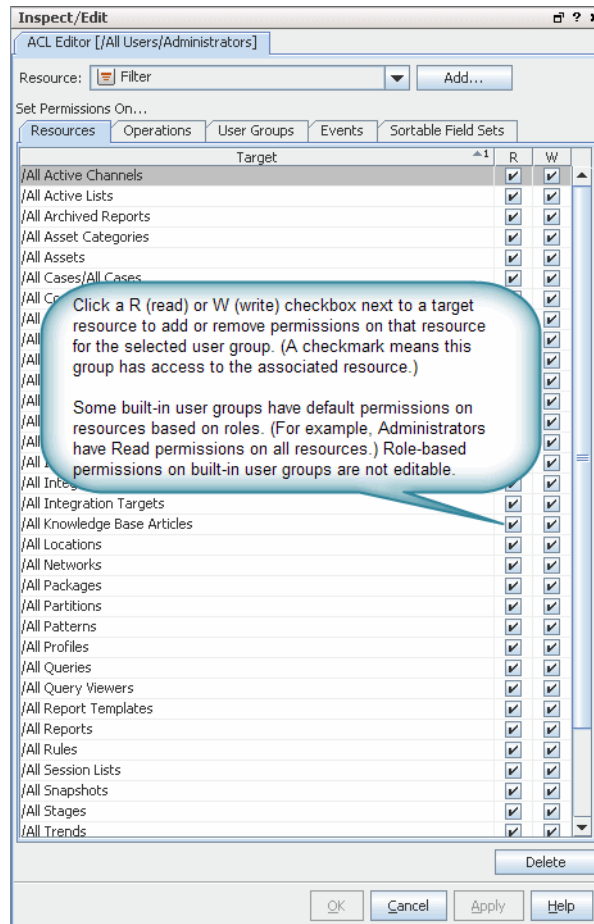
For example, consider the following scenario.

- A user logged in as Administrator (belonging to the group /All Users/Administrators) has read and write permissions by virtue of being in the Administrators group.
- All users have read permissions because they belong to the group /All Users/Default User Groups by default.
- A user logged in as an Analyzer Administrator has both read and write permissions because they inherit read permissions from the parent group (/All Users/Default User Groups) and get write permissions per the Analyzer Administrators child group.

Granting or Removing Resource Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Resources** tab.

The Resources tab lists all resources available to this user group with either inspect (**Read**) or edit (**Write**) permissions, and lets you add/edit resource permissions. Available resources are listed based on *user permissions*, so some might not show.



Be sure to set both permissions on resources and permissions on events appropriately for user groups. Preventing users from viewing groups of resources (as described here) does not necessarily prevent those same users from viewing event data on those resources.

Users with permissions to view certain events (as described in [“Granting or Removing Event Permissions” on page 652](#)), can view *all event fields* for those particular events (in reports, query viewers, etc.) even if they do not have permissions on some *resources* reflected in the event data.

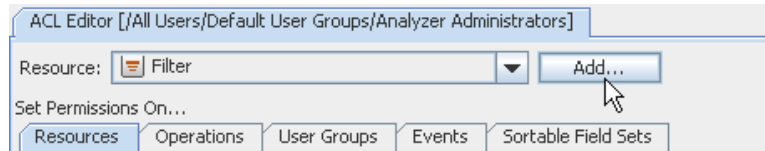
As a best practice, please keep this in mind when granting permissions on events. Otherwise, you might give some users a view into information via event data that you did not intend for them to see. For more information, see [related information on page 653](#) in the Caution note.

- 5 Add or remove permissions on a resource for this user group as follows.
- ◆ **To edit permissions on a resource *shown* in the current list**, click the **(R)** read or **(W)** write checkbox next to a target resource to add or remove permissions on that resource.

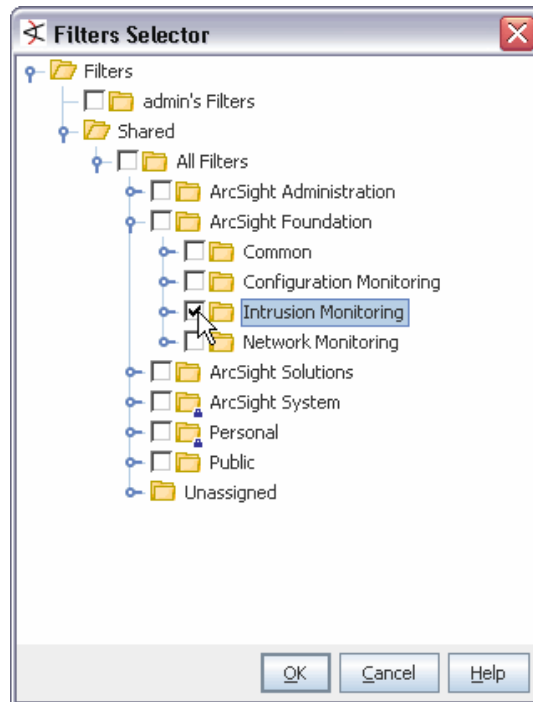
A checkmark means that this user group has access to the associated resource. A blank checkbox means this group does not have access to the resource.

Target	R	W
/All Active Channels	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Active Lists	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ◆ To add permissions for a resource *not shown in the current list*, select a resource from the Resource drop-down menu at the top of the Resources tab and click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the resources you want to add permissions for and click **OK**.



The resource you added is listed as a target on the Resources tab and then you can edit its **Read/Write** permissions as needed.

- ◆ To remove a resource from the list (and **remove all permissions on it** for this group), select the resource in the list and click **Delete**. (The Delete button is at the bottom of the Resources tab).

6 Click **OK** on the User Group ACL Editor to save changes to Resources permissions.

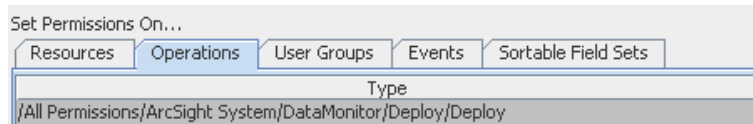
Granting or Removing Operations Permissions

Data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions by setting permissions on this particular “operation”. The only operation available to set permissions on is data monitor deployment. It is likely that fine-grained permissions control is added for

other operations as needed. (See also, [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656.](#))

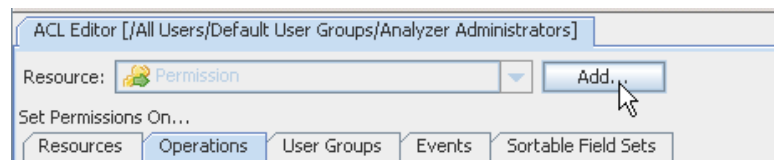
- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Operations** tab.

The operations for which this user group has permissions (if any) are listed.

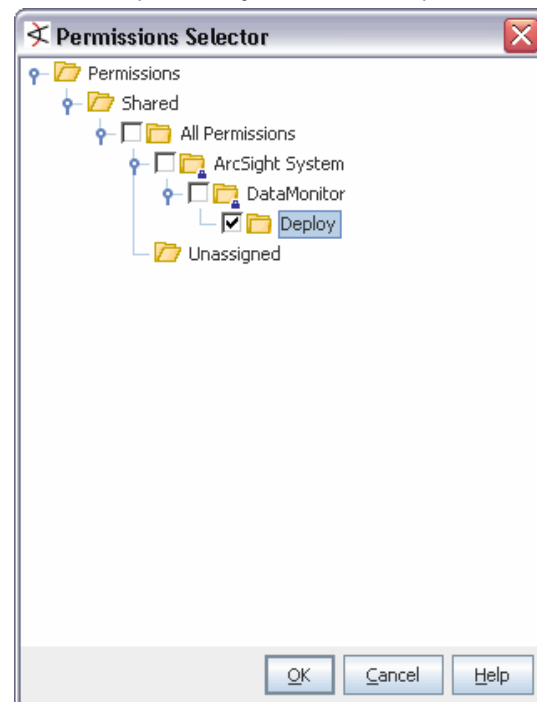


- 5 Add or remove user group permissions to perform an operation as follows.

- ◆ **To add permissions to perform an operation not listed**, click **Add**.



Select the operations you want to add permissions for and click **OK**.



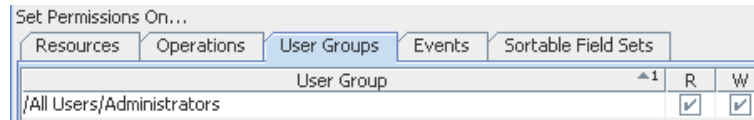
The list of Operations is updated to include the one you added. Operations listed are those this user group has permissions to perform.

- ◆ **To remove permissions to perform an operation**, select the operation in the list and click **Delete**. (The Delete button is at the bottom of the Operations tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

Granting or Removing User Group Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **User Groups** tab.

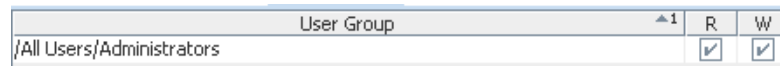
The User Groups tab lists all user groups for which members of the selected group have inspect (**R**) or edit (**W**) permissions, and lets you add/edit group permissions.



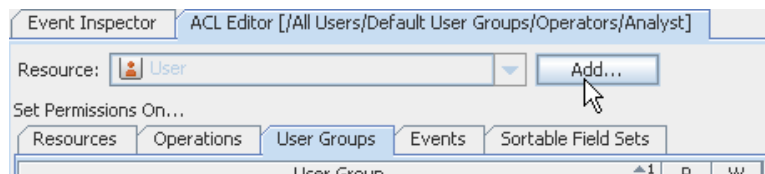
This is where you grant or deny members of the group you are editing permissions to edit their own user groups. Depending on your own user permissions, some user groups may or may not be shown, and Read/Write checkbox options may or may not be editable.

- 5 Add or remove permissions on a user group as follows.
 - ◆ **To edit permissions on a user group *shown in the current list***, click the (**R**) read or (**W**) write checkbox next to a target resource to add or remove edit permissions on that user group.

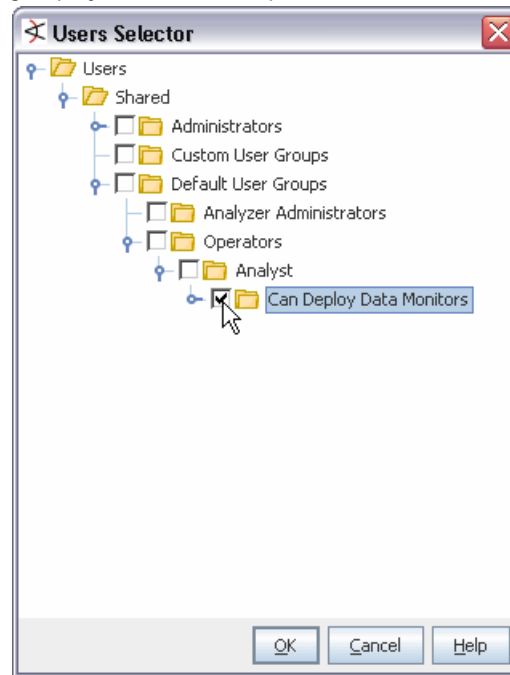
A checkmark means that this user group can edit permissions on the associated group. A blank checkbox means this group does not have edit permissions on it.



- ◆ **To add permissions on a user group *not shown in the current list***, click **Add**.



This brings up the resource selector dialog for the chosen resource. Select the groups you want to add permissions for and click **OK**.



The user group you added is now listed on the User Groups tab and then you can edit its **Read/Write** permissions as needed.

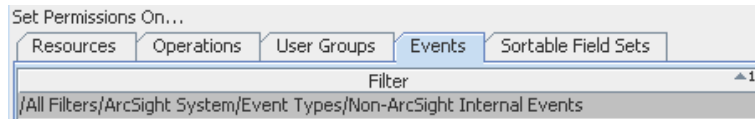
User Group	R	W
/All Users/Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Users/Default User Groups/Operators/Analyst/Can Deploy Data Monitors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- ◆ To remove a user group from the list (and **remove all edit permissions on it**), select the user group in the list and click **Delete**. (The Delete button is at the bottom of the User Groups tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to User Group permissions.

Granting or Removing Event Permissions

- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Events** tab.

The *event filters* that return the types of events for which this user group has permissions are listed.



Tip

User groups are granted permissions to events by means of event *filters* applied to groups. The event filters limit the types of events group members can access through the ESM Console.

For example, members of the administrators group can view all events, as indicated by the event filter assigned to the Administrators group by default: [/All Filters/ArcSight System/Core/All Events](#).

For more information about filters, see [Chapter 11, Filtering Events](#), on page 223. For more information about events, see [“Events”](#) on page 941.



Caution

Be sure to set both permissions on resources and permissions on events appropriately for user groups. Preventing users from viewing groups of resources (as described in [“Granting or Removing Resource Permissions”](#) on page 647) does not necessarily prevent those same users from viewing event data on those resources.

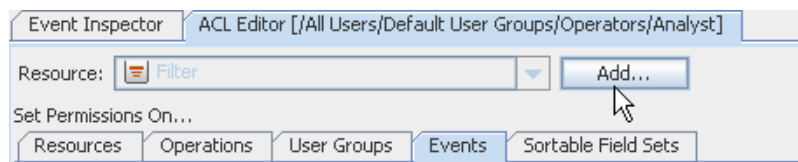
Users with permissions to view certain events (determined by event filters as described here), can view *all event fields* for those particular events (in reports, query viewers, etc.) even if they do not have permissions on some *resources* reflected in the event data.

For example, a user with no read permissions on an asset could still have permissions to view event data related to the asset, and thereby have access to the data contained in the event fields (such as server name, IP address) in the context of that event.

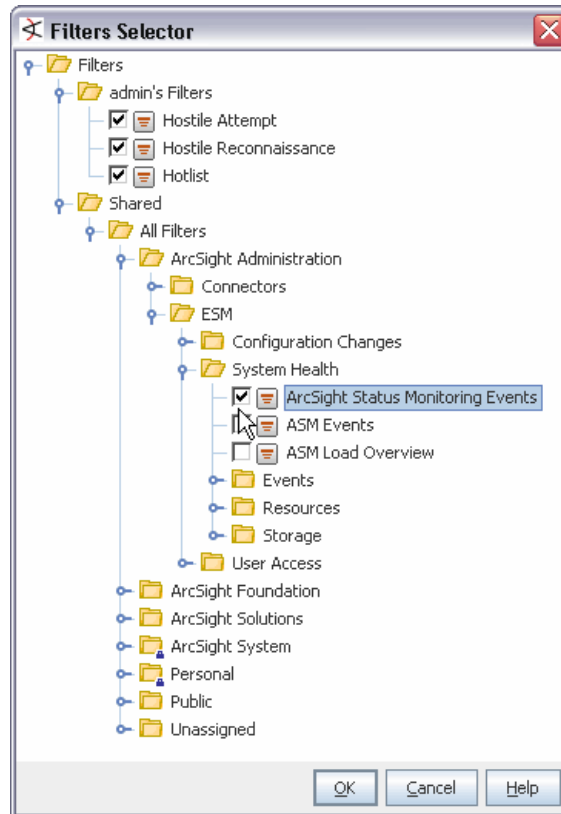
As a best practice, please keep this in mind when granting permissions on events. Otherwise, you might give some users a view into resource information via event data that you did not intend for them to see.

5 Add or remove user group permissions to view events as follows.

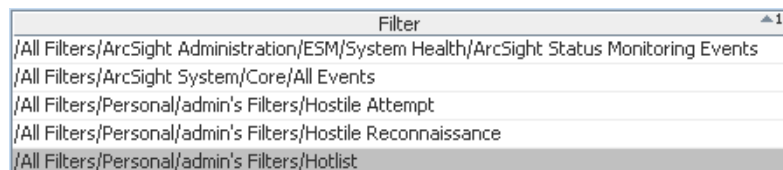
- ◆ **To add permissions to view events** captured by a filter not shown in the current list, click **Add**.



Select the event filters you want to add permissions for and click **OK**.



The list of event filters is updated to include the ones you added. Filters listed capture and allow all event types this user group has permissions to view.

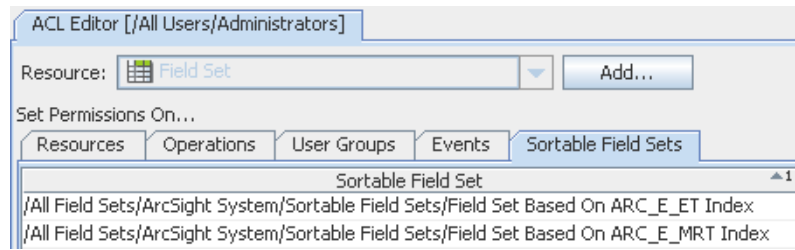


- ◆ **To remove event filters** (permissions to view certain types of events), select a filter in the Events “Filter” list and click **Delete**. (The Delete button is at the bottom of the Events tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Operations permissions.

Granting or Removing Sortable Field Sets Permissions

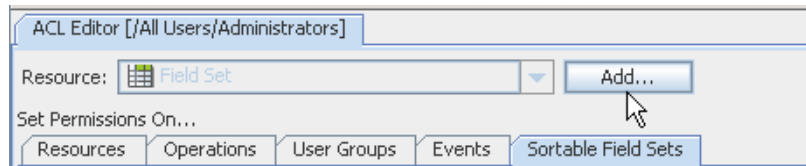
- 1 In the Navigator panel's drop-down menu, choose **Users**.
- 2 In the **Users** resource tree, expand it and select a group.
- 3 Right-click the user group and select **Edit Access Control**.
- 4 In the **ACL Editor**, select the **Sortable Field Sets** tab.

The event field sets for which this user group has access permissions are listed.

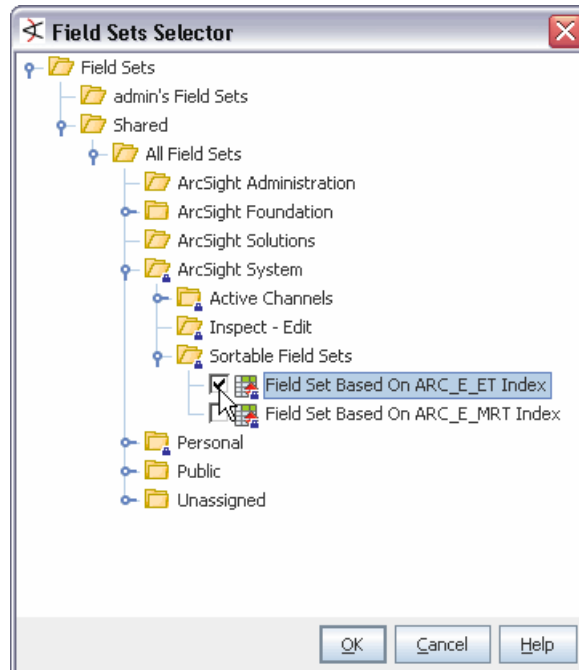


- 5 Add or remove user group permissions on sortable field sets as follows.

- ◆ **To add permissions to use a field set** not shown in the current list, click **Add**.



Select the sortable field sets you want to add permissions for and click **OK**.



The list of sortable field sets is updated to include the ones you added. Field sets listed represent those this user group has permissions to use.

- ◆ **To remove sortable field sets**, select a field set in the list and click **Delete**. (The Delete button is at the bottom of the Sortable Field Sets tab).
- 6 Click **OK** on the User Group ACL Editor to save changes to Sortable Field Sets permissions.

Sharing Resources

You can share your resources with other users by moving, copying, or linking your resource to or into another resource's Public group; for example, to share a filter you would move it into the Public Filters group in the Filters resource tree.

To share a resource

- 1 In a resource tree, drag a resource and drop it into the Public group (this can be a single resource or a resource group).
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the resource that is not affected when the original resource is edited. If you choose **Link**, you create a copy of the resource that is linked to the original resource. Therefore, if you edit a linked resource, whether the original or the copy, all links are edited as well. When deleting linked resources, you can either delete the selected resource or all linked resources.

You can also multiple-select resources with the **Shift** key, and drag-and-drop or keyboard copy-and-paste, to move, copy, or link them in another group.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Note

Controlling Who Has Permissions to Deploy Data Monitors

Data monitor deployment is controlled through User Access Control Lists (ACLs). Administrators can allow or block users for data monitor deployment permissions.

Depending on the permissions associated with the user group to which they belong, users may or may not have options available on their ESM Consoles to **Enable** (*deploy*) or disable (*un-deploy*) data monitors. (See also [“Enabling or Disabling a Data Monitor” on page 161.](#))

Administrators (all users belonging to the [admin](#) user group) have permissions to deploy/undeploy data monitors.

Administrators can grant permissions to deploy/disable data monitors for other non-Administrator through the Users resource Access Control Lists (ACLs) editor, as described in [“Granting or Removing Operations Permissions” on page 649.](#) As with user permissions for other resources, these are applied at a user group level. As an administrator, you can grant all users in a given group permission to deploy data monitors. Once user groups are set up and appropriate permissions applied to those groups, you can add new users to appropriate groups, and change access permissions for existing users by moving them in or out of various groups. If you want to allow or disallow a particular user the option to deploy data monitors, move the user in or out of a group that has that permission.



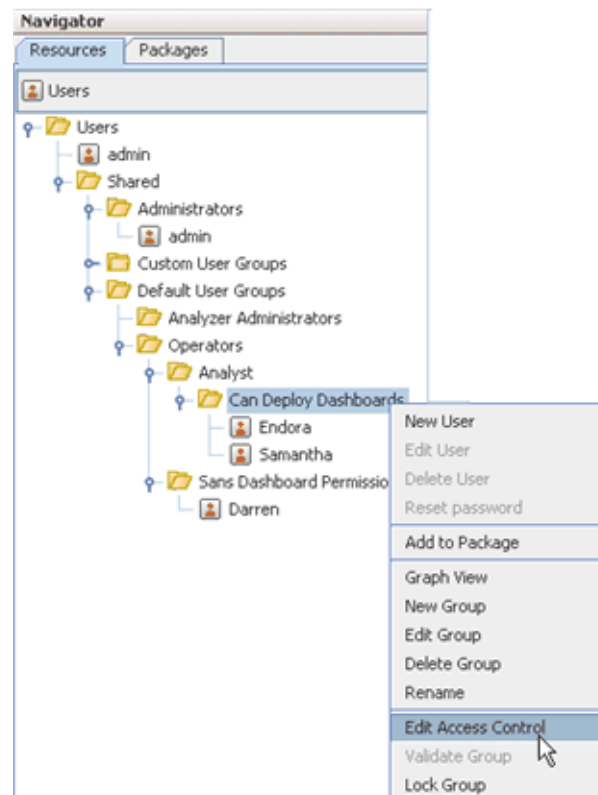
Write and Deploy permissions. Data monitor deployment is an all-or-nothing permission (it applies to all data monitors), while read and write permissions are specific to each data monitor. So, in some cases a user could have read-only access to one data monitor and read-write access to another. To deploy a data monitor, a user needs *both* deployment permissions and write permissions. Users with permissions to deploy data monitors can deploy only those data monitors for which they have write permissions. (Fields in the data monitor editor are grayed out for all users without write permission.)

To configure data monitor deployment permissions:

- 1 If needed, set up one or more user groups for non-admin users to whom you want to control permissions to deploy data monitors. (For example, at the simplest level you might have a group for analysts and operators who are allowed to deploy data monitors and another for those you want to block from this option.)

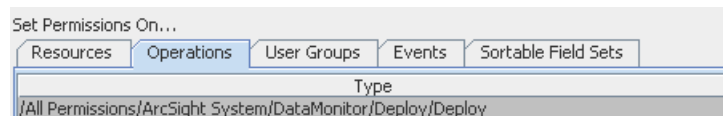
See [“Handling Users” on page 641](#) and [“Handling User Groups” on page 645](#) for information on adding, deleting, and editing users and user groups.

- 2 Follow the instructions provided in [“Granting or Removing Operations Permissions” on page 649](#) to grant or remove permission to deploy data monitors to a particular group. As a part of these instructions, you’ll select the **Users** resource in the navigator, right-click a group and choose **Edit Access Control**.



- 3 In the ACL Editor, click the Operations tab, and click **Add**.
- 4 On the Permissions Selector, select **Deploy** under [Permissions\Shared\All Permissions\ArcSight System\Data Monitor\](#) and click **OK** to save the settings and close the dialog.

The list of Operations is updated to include deployment permissions on data monitors.



(To remove the permission for this group, select the permission and click **Delete**.)

- 5 Click **OK** on the ACL Editor to save your changes.

For information on deploying or disabling data monitors, see [“Enabling or Disabling a Data Monitor” on page 161](#).

For more information on administrator tasks of working with user permissions and ACLs, see [“Managing Permissions and Resources” on page 646](#).

How Upgrades Affect Data Monitor Deploy Permissions

Upon installation and deployment of a different version of software (for example, version or service pack upgrades), only administrators ([admin](#) users) keep permissions to deploy/disable data monitors. Non-[admin](#) users do not have deploy permissions on data monitors even if they had such permissions as part of the previous configuration.

After upgrades, all users have access to already-deployed data monitors. But, initially, non-[admin](#) users do not have permissions to enable/disable data monitors, nor have access to new data monitors unless an administrator enables (deploys) these.

To re-establish data monitor deployment permissions for non-[admin](#) users after an upgrade, administrators can reconfigure fine-grained permissions. They can re-group users and perhaps link non-[admin](#) users into existing or new groups with more permissions (like data monitor deployment), as described in [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).


Deployment Permissions on Imported Data Monitors


If a user without data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import succeeds but the data monitor is disabled. After the import, the user do not have permissions to deploy the data monitor unless an administrator reconfigures permissions for that user.

If a user with data monitor deploy permissions imports a data monitor that was archived in the enabled state, the import succeeds and the data monitor keeps its enabled (*deployed*) setting. After the import, this user can view the data monitor and re-set its deployment state as needed.

Managing Notifications

Managing Received Notifications

When the Notifications button in the ESM Console toolbar indicates that new notifications have arrived (), you click that button to open the Notifications tab in the Viewer panel. This is your central notification repository.

You can open the Notifications manager at any time by clicking the toolbar button, even if no new notifications are present ().

To use the Notifications manager you first choose a category tab for the type of notification received.

Notification Category	Use
Pending	These are notifications that you have not yet handled (reassigned to one of the following categories). Pending notifications older than 24 hours are automatically refiled as Not Acknowledged.

Notification Category	Use
Undelivered	These are notifications that were not delivered.
Acknowledged	These are notifications to which you have replied.
Not Acknowledged	Pending notifications that go unacknowledged or unresolved for more than 24 hours are automatically refiled as Not Acknowledged.
Resolved	These are notifications for which you or a colleague have found a resolution and so have marked the notification accordingly.
Informational	These are notifications that are provided for information purposes only and do not require resolution or intervention.



If you don't see notifications appearing, make sure your ArcSight user identity (not just your e-mail address) is set as a destination in the Notifications Editor.

In a category, click **Acknowledge** to mark a selected notification as acknowledged. Click **View Event** to see the event that triggered a notification. Click **Resolve** to reclassify the notification as Resolved.

For each category of notification there is a common set of columns of information concerning them..

Notification Column	Definition
Priority	This is the same priority set by the SmartConnector and modified by the current threat level formula (and seen in grid views), unless modified by the rule that triggered the notification.
Triggering Event	The event that caused the rule to trigger the notification.
Notification Group	The branch of the Notifications resource tree to which this destination belongs.
Escalation Level	The Escalation Level (and implied destinations) the notification has reached while waiting for resolution.
Create Time	The time at which the notification was created



Also note that you can set a severity threshold for notification pop-ups and sounds in ESM Console Preferences, and also manage your notifications from an ArcSight Web browser client.

Managing Notification Groups and Levels

This chapter describes how to handle the tasks required for managing notification groups and levels.

Creating Notification Groups

- 1 On the Navigator panel drop-down menu, choose the **Notification** resource tree.
- 2 In the Notification panel, right-click **All Destinations** and choose **New Group**.

A "name" text field appears under the group you selected.

- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.



As a user, you can create new groups under **All Destinations**, but not new subgroups under existing system-defined groups.

Renaming Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Deleting Notification Groups

- 1 In the **Notifications** resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Adding Escalation Levels

In the Notifications resource tree, right-click a notification group and choose **Add Escalation Level**.

New escalation levels are added in sequential order. If you want to add a level between two existing levels, add another level then move destinations accordingly. For example, if you have **Level 1** and **Level 2** and you want to add a level between them, add another level, **Level 3**. Then, move all destinations from **Level 2** to the new **Level 3**.

Deleting Escalation Levels

- 1 In the Notifications resource tree, select the last escalation level in a notification group.



All destinations within this escalation level are also be deleted. If you want to save the destinations, make sure you move them to another level **before** deleting.

- 2 Right-click the escalation level and choose **Delete Escalation Level**.

Managing Notification Destinations

The task descriptions in this topic explain how to manage notification destinations.

Creating Destinations

- 1 In the Notification resource tree in the Navigator panel, right-click an escalation level (such as **Level 1**) and choose **Add New Destination**.

- 2 In the Notification Editor, enter a label for the notification in the **Name** field.
- 3 Set a **Start Time** and **End Time** during the day within which the notification is to be active. The default is all day (12:00:00 AM to 11:59:59 PM).
- 4 For destinations other than the ESM Console, select that **Destination Type** and enter the **Address**, **PIN**, or **Provider** for that device.
- 5 For the ESM Console, choose a **User/Group** identity.



Always set the ArcSight **User/Group** identity. If not set, notifications cannot be sent to users' Consoles.

- 6 Click **OK**.

Editing Destinations

- 1 In the Notification resources tree, right-click a notification destination and choose **Edit Destination**.
- 2 In the Notification Editor, edit the Value fields for the necessary destination attributes.
- 3 Click **OK**.

For more information, see ["Changing Notification and Acknowledgement Settings" on page 662](#).

Moving or Copying Destinations

- 1 In the Notification resources tree, find a destination and drag it to a different escalation level. You can drag across groups if needed.
- 2 Right-click the destination and choose **Move** to move it, **Copy** to make a separate copy, or **Link** to create a copy of the destination that is linked to the original destination.

If you choose **Copy**, you create a separate copy of the destination that is not affected when the original destination is edited. If you choose **Link**, you create a copy of the destination that is linked to the original destination. Therefore, if you edit a linked destination, whether the original or the copy, all links are edited as well. When deleting linked destinations, you can either delete the selected destination or all linked destination copies.

Deleting Destinations

- 1 In the Notification resource tree, right-click a notification destination and choose **Delete Destination**.
- 2 In the dialog box, click **Yes**.

Changing Notification and Acknowledgement Settings

Administrators can configure notifications, acknowledgements, and wait-time settings. The escalation time window or wait-time depends on the event's severity.



Note

If notifications and/or acknowledgements were disabled during Manager setup, mail server settings made through the ESM Console do not take effect until you re-run the Manager setup to enable notifications and/or acknowledgements on the Manager side.

To run the Manager setup: (1) stop the ESM Console and Manager, (2) re-run the Manager setup wizard from the Manager's `/bin` directory ([arcsight managersetup](#)). See the *ArcSight ESM Installation and Configuration Guide* for more information.

Changing E-mail Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit E-mail Settings**.
- 2 In the Notification Editor, type in the following text fields:

Notification Fields	Definition
From Address	The e-mail address from where the notification messages are sent. It is important that the "from address" specified is one that is not rejected by the SMTP server, since some SMTP servers reject unknown e-mail addresses. For notifications sent by cell phone, any cell phone must be e-mail enabled.
Outgoing Mail Server	The host name of the local outgoing mail server. This is the SMTP server ArcSight uses to send e-mail. The Outgoing Mail Server must be accessible from the ArcSight Manager for e-mail notifications to be sent. SMTP is used to send e-mail. An SMTP server must be configured either at install time or set here.
Incoming Mail Server	The local incoming mail server host name.
Incoming Mail Protocol	Select either IMAP or POP3 mail protocols.
E-mail Account	The e-mail account name. For notifications sent by e-mail, you need to add an address to the e-mail Address field.



Note

POP3 and IMAP can be used to check for e-mail acknowledgments. You can specify these options at install time, or set them here. For acknowledgements, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

- 3 Type the **E-mail Account** password in the Password text field and confirm it in the Confirm **Password** text field.
- 4 Click **OK**.

Adding New Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then **New Service Provider**.
- 2 In the Notification Editor, type in the following text fields:

Pager Notification Field	Description
Provider Name	The name of the service provider, such as Skytel.
Host	The host name for the service provider's server, such as snpp.skytel.com. SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager provider host and port information.
Port	The port number for the service provider's server.

- 3 Click **OK**.



For notifications sent by pager, firewalls must be configured so that the pager can connect directly to the paging service provider. ArcSight currently supports any provider that supports SNPP.

Editing Pager Service Provider Settings

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, edit the text fields.
- 3 Click **OK**.

Deleting Pager Service Providers

- 1 In the Notification resource tree, right-click a group and choose **Settings, Edit Pager Providers**, then the Provider Name.
- 2 In the Notification Editor, click **Delete**.

Changing Wait Time Settings

The default wait-time values for Very-High severity and High severity are set at 5 minutes, Medium is set for 30 minutes, and Low is set for 2 hours.

- 1 In the Notification resource tree, right-click a group and choose **Settings**, then **Edit Escalation Wait Time**.
- 2 In the Notification Editor, type in the wait time for the hour (**Hr**) and minute (**Min**) text fields for **Very-High**, **High**, **Medium**, or **Low** severity.
- 3 Click **OK**.

Testing Notification Groups and Destinations

This topic describes how to test notification groups and destinations.

Testing Group Notifications

In the Notification resource tree, right-click a populated notification group and choose **Test Group Notification**.

A test notification message is sent to the notification destination. Test notifications are not sent to group notification destinations if the End Time has expired. For example, if you test group notification at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message is not sent to the group.

Testing Destination Notifications

In the Notification resource tree, right-click a notification destination and choose **Test Destination Notification**.

A test notification message is sent to the notification device. Test notifications are not sent to notification destinations if the End Time has expired. For example, if you test a notification destination at 6:00:00 PM and the End Time states 5:00:00 PM, a notification message is not sent to the device.

Managing Resources

This chapter discusses the administrator tasks necessary to manage ArcSight.

- [“Managing File Resources” on page 665](#)
- [“Locking and Unlocking Resources” on page 669](#)
- [“Selecting Resources” on page 670](#)
- [“Finding Resources” on page 671](#)
- [“Visualizing Resources” on page 674](#)
- [“Viewing Resources in Grids” on page 677](#)
- [“Validating Resources” on page 677](#)
- [“Extending Audit Event Logging” on page 683](#)
- [“Saving Copies of Read-Only Resources” on page 684](#)
- [“Common Resource Attribute Fields” on page 684](#)
- [“Managing Packages” on page 686](#)

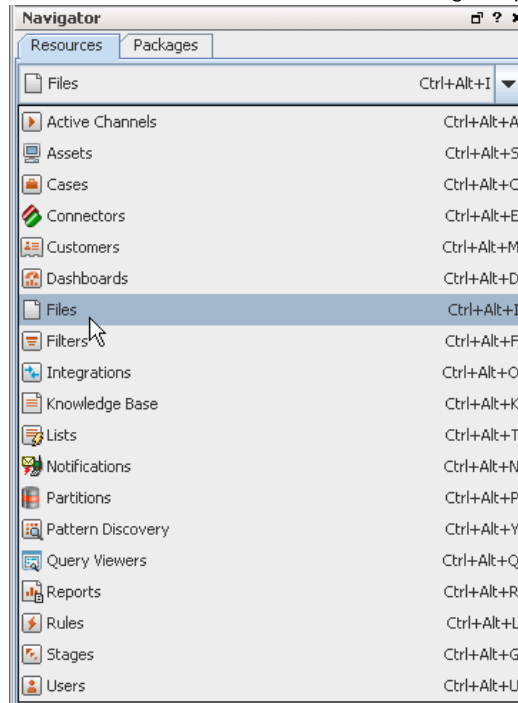
Managing File Resources

The Files resource tree, when populated, lists various files that have been saved as resources so that they are accessible to all users of the system who are authorized for such access. File resources include Case file attachments, templates, and general-purpose shared files.

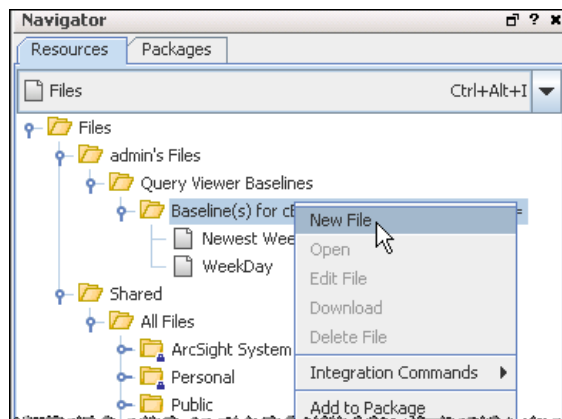
In addition to the tasks detailed below, you can also rename or lock a file, get a Graph View of a file, and so forth. Simply select the file in the Navigator, right-click, and choose a menu option. Operations on groups are also available. Options may vary depending on which file or folder you have selected in the Navigator.

Uploading Files and Creating a File Resource

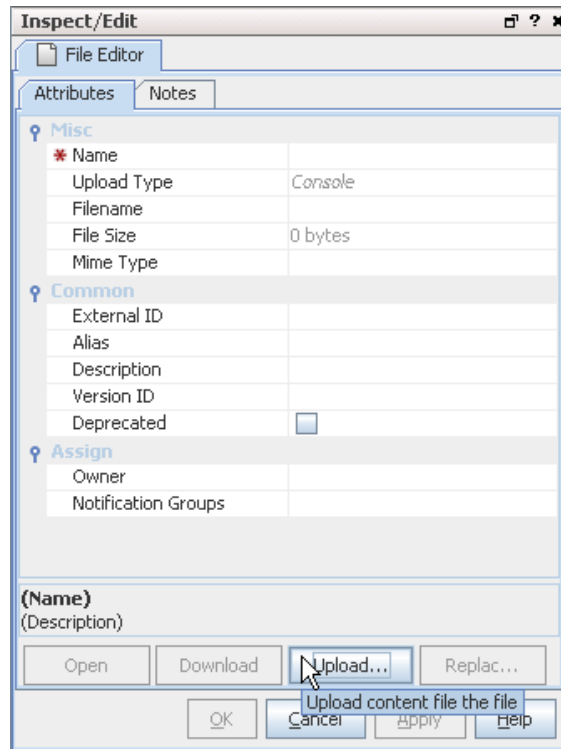
- 1 Choose the **Files** resource tree in the Navigator panel.



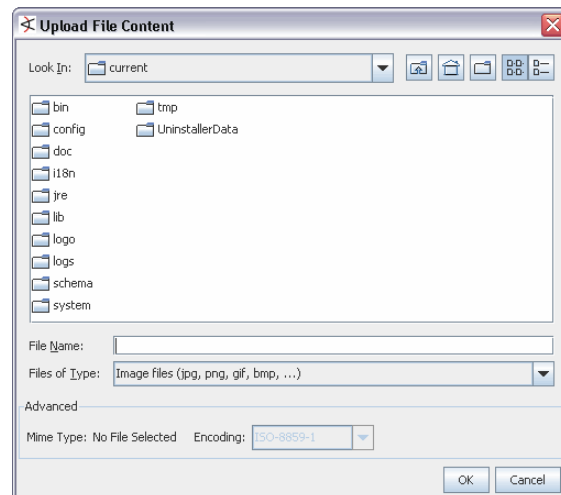
- 2 Right-click a file group and choose **New File**.



This brings up the File Editor in the Inspect/Edit panel.



- 3 Click the **Upload** button on the File Editor and select the local file to add.



- 4 On the File Editor Attributes tab, enter values for the attributes that identify the file.
The Name attribute is initially the same as the Filename attribute, but you can change the Name.
Certain attributes are read-only: Upload type is Console, and Filename, File size, and Mime type are set based on the selected file.
- 5 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Viewing Files

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Open**.
- 3 The file is downloaded to a temporary directory (in a sub-directory called **arcsight-files**) and launches in an appropriate viewer, usually a web browser.

You can also open a file resource from the File Editor by clicking the **Open** button.

Downloading Files Locally

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Download**.
- 3 Specify a location and file name for the new local file.



File resources can be downloaded as often as needed by any console user authorized to access the file resources. Downloading a file does not change the file resource, or the shared file contents on the server.

You can also Download a file resource from the File Editor by clicking the Download button.

Editing File Resource Attributes

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Replacing File Resource Contents

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Edit File**.
- 3 Click **Replace** and select the local file containing the new contents for the file resource. The file resource name changes if the selected local file has a different name.
- 4 Click **Apply** to update the file and leave the editor open, or **OK** to complete editing and close the editor.

Deleting File Resources

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file and choose **Delete File**.
- 3 Click **Yes** to confirm the deletion.

Adding a File or Folder to a Package

From the Files resource Navigator, you can add a file or folder to an existing package or create a new package and add the file to it.

- 1 Choose the **Files** resource tree in the Navigator panel.
- 2 Right-click a file or folder and choose **Add to Package**.

This brings up the Package Selector dialog.

- 3 In the Package Selector dialog, do one of the following:
 - ◆ Navigate to a package to which you want to add the file or folder, and click **OK**. (The file is saved to the selected package.)
 - Or
 - ◆ Navigate to a location where you want to create a new package and click **New Package**. This brings up the Package Editor where you can name and configure the new package. The selected file or folder will be included in the new package.

For more about managing packages, see [“Managing Packages” on page 686](#).

Finding Files

To find files stored on the Manager, choose **Files** in the Navigator and browse the folders or choose **Edit > Search** from the menus, enter a file name in the **Search query** field, and click **Find**. (See [“Finding Resources” on page 671](#) for more information on this utility.)

Locking and Unlocking Resources

The locking and unlocking capability applies to the following ArcSight content:

- System core content
- User created content

System Core Content

A set of predefined content called the System Core content is installed by default. This content provides the foundation building blocks for ArcSight to work.

System Core content is available in the Core group under the ArcSight System sub-tree of each resource tree. For example, core content for the Filters resource is available in [/All Filters/ArcSight System/Core](#).

The modification of System Core content can adversely impact operation, therefore, it is locked by default. ArcSight strongly recommends against unlocking or modifying this content. If there is a need to unlock this content, contact ArcSight Customer Support.



Note

Use the resources available in ArcSight Foundation packages or ArcSight Administration to create content to suit your needs.

User Created Content

ArcSight users can lock any resource or a group of resources to which they have write access privileges. Locking prevents a resource from being modified or deleted. Once locked, such resources or groups can be unlocked only by these users:

- The user who applied the lock—the lock owner.
- Any user who has write permissions to the lock owner. That is, a user who has privileges over the user who applied the lock. For example, the administrator user has write permissions over all users by default. Therefore, if user joe locks a resource, the user administrator can unlock it.
- The system user.



You can make a copy of a locked resource even if you do not have the privileges to unlock it.

You can edit resources in a locked group if you have write access privileges to the resource, however you cannot do the following:

- Delete or remove resources from it.
- Add a new resource to it.

Unlocking a User-locked Resource

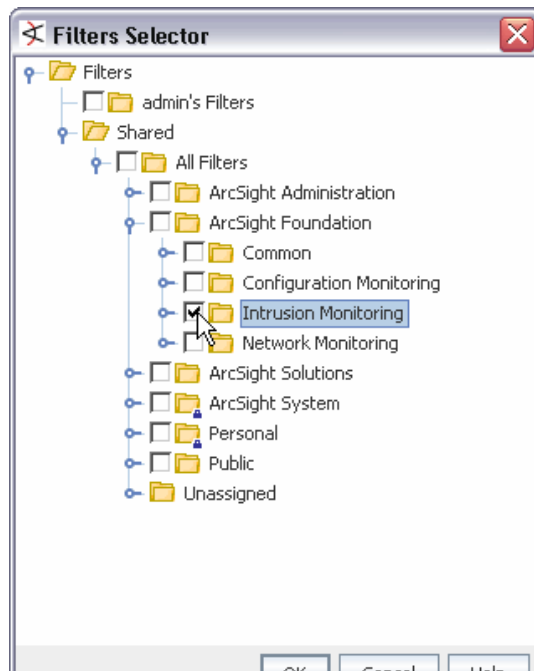
To unlock a resource, right-click the locked resource and select **Unlock** from the drop-down menu. For detailed instructions, see the Console online Help.

Selecting Resources

You often need to select resources to act on or use while authoring or configuring analysis tools. Selecting is often the first step in managing, authoring, or analyzing resources.

While the Navigator panel is your usual means of selecting resources, you can also encounter the Select Resources dialog box any time selection is a necessary part of some

task, such as adding a case group to a rule action or adding user groups to access control lists (ACLs).



For resource groups, click to highlight and select the group you want to choose, then click **OK**. For options that allow multiple selections, select the check boxes next to individual entries in the list under a group, then click **OK**.

This dialog is also displayed for setting user permissions on resources and operations.

For information about setting permissions on resources, see [“Managing Permissions and Resources” on page 646](#).

For information about setting action permissions on who can deploy data monitors, see also [Step 4 on page 657](#) in [“Controlling Who Has Permissions to Deploy Data Monitors” on page 656](#).



Finding Resources

Apart from visually navigating the resources in the Navigator panel, you can also find items in busy resource trees by searching or by locating them.

Searching for System Resources

The search capability uses conventional query elements to search the entire set of system resources, returning a ranked list of qualifying items. Each user sees only those resources for which they have permission, regardless of the query. You can search for a string in All Resources or within a particular resource with both of the following methods.

Search Field on Console Tool Bar

In the Search field  on the Console toolbar type a name or phrase and click the “Find Resource” button (). The Search hits are displayed in the Viewer. Single-click an item to display a preview of its definition in the Details pane on the Viewer, or double-click it to open its definition in an Editor in the Inspect/Edit panel.

To limit a search to a particular resource type, click the **drop-down menu** tab on the Search field and choose a resource type from the menus. Notice that some resource types have sub-types from which you can choose. If you limit the Search to a resource type, an icon representing the resource type you are searching on is displayed in the Search field (instead of the standard looking glass Search icon).

For example, to search for a name or phrase only in Trends, choose **Reports > Trends** from the Search drop-down, enter the search string, and click the **Find Resource** button.

The Search field in the toolbar accepts all the Query Options described below.

The screenshot shows the ArcSight Console 4.0.0.5190.0 interface. The top toolbar contains a search field with a dropdown menu. A callout bubble points to the dropdown menu, stating: "To limit the Search to items of a particular resources, click the Search drop-down button and select a resource type, then enter the Search string and click the Find Resource button. Note that some resource types have sub-types you can select; e.g., Reports > Trends." The dropdown menu is open, showing a hierarchy: All Resources > Active Channels > Assets > Cases > Connectors > Customers > Dashboards > Files > Filters > Knowledge Base Articles > Lists > Notifications > Partitions > Patterns > Reports > Rules > Stages > Users. The 'Reports' folder is expanded, showing 'Report Templates', 'Queries', 'Reports', 'Archived Reports', and 'Trends'. The 'Trends' item is selected. Below the dropdown, the search field contains the text 'VPN Logins' and a 'Find' button. A callout bubble points to the search field, stating: "Type the name or phrase associated with the item you are searching for (you can include spaces in the Search string; e.g., VPN Logins) and click the Find Resource button." The main window is divided into three panels. The left panel is the 'Navigator' showing a tree of resources. The middle panel is the 'Viewer' showing search results for 'VPN Logins'. The right panel is the 'Inspect/Edit' panel showing details for the selected resource. A callout bubble points to the search results in the Viewer panel, stating: "Search results are shown in the Viewer panel on a Find Resource tab. Single-click a found resource to get a Details preview of it. Double-click the item to open it in an Editor." The search results table in the Viewer panel has columns: Score, Type, Name, and Description. The results are sorted by Score. The first result is a 'Trend' named 'VPN Logins' with a score of 35. The second result is a 'Report' named 'VPN Logins' with a score of 34. The third result is a 'Query' named 'VPN Logins' with a score of 33. The fourth result is a 'Query' named 'VPN Logins' with a score of 32. The fifth result is a 'Query' named 'VPN Logins' with a score of 31. The sixth result is a 'Query' named 'VPN Logins' with a score of 30. The seventh result is a 'Query' named 'VPN Logins' with a score of 29. The eighth result is a 'Query' named 'VPN Logins' with a score of 28. The ninth result is a 'Query' named 'VPN Logins' with a score of 27. The tenth result is a 'Query' named 'VPN Logins' with a score of 26. The eleventh result is a 'Query' named 'VPN Logins' with a score of 25. The twelfth result is a 'Query' named 'VPN Logins' with a score of 24. The thirteenth result is a 'Query' named 'VPN Logins' with a score of 23. The fourteenth result is a 'Query' named 'VPN Logins' with a score of 22. The fifteenth result is a 'Query' named 'VPN Logins' with a score of 21. The sixteenth result is a 'Query' named 'VPN Logins' with a score of 20. The seventeenth result is a 'Query' named 'VPN Logins' with a score of 19. The eighteenth result is a 'Query' named 'VPN Logins' with a score of 18. The nineteenth result is a 'Query' named 'VPN Logins' with a score of 17. The twentieth result is a 'Query' named 'VPN Logins' with a score of 16. The twenty-first result is a 'Query' named 'VPN Logins' with a score of 15. The twenty-second result is a 'Query' named 'VPN Logins' with a score of 14. The twenty-third result is a 'Query' named 'VPN Logins' with a score of 13. The twenty-fourth result is a 'Query' named 'VPN Logins' with a score of 12. The twenty-fifth result is a 'Query' named 'VPN Logins' with a score of 11. The twenty-sixth result is a 'Query' named 'VPN Logins' with a score of 10. The twenty-seventh result is a 'Query' named 'VPN Logins' with a score of 9. The twenty-eighth result is a 'Query' named 'VPN Logins' with a score of 8. The twenty-ninth result is a 'Query' named 'VPN Logins' with a score of 7. The thirtieth result is a 'Query' named 'VPN Logins' with a score of 6. The thirty-first result is a 'Query' named 'VPN Logins' with a score of 5. The thirty-second result is a 'Query' named 'VPN Logins' with a score of 4. The thirty-third result is a 'Query' named 'VPN Logins' with a score of 3. The thirty-fourth result is a 'Query' named 'VPN Logins' with a score of 2. The thirty-fifth result is a 'Query' named 'VPN Logins' with a score of 1. The thirty-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The thirty-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The thirty-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The thirty-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The fortieth result is a 'Query' named 'VPN Logins' with a score of 0. The forty-first result is a 'Query' named 'VPN Logins' with a score of 0. The forty-second result is a 'Query' named 'VPN Logins' with a score of 0. The forty-third result is a 'Query' named 'VPN Logins' with a score of 0. The forty-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The forty-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The forty-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The forty-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The forty-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The forty-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The fiftieth result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-first result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-second result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-third result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The fifty-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The sixtieth result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-first result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-second result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-third result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The sixty-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The seventieth result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-first result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-second result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-third result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The seventy-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The eightieth result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-first result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-second result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-third result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The eighty-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The ninetieth result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-first result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-second result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-third result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-fourth result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-fifth result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-sixth result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-seventh result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-eighth result is a 'Query' named 'VPN Logins' with a score of 0. The ninety-ninth result is a 'Query' named 'VPN Logins' with a score of 0. The hundredth result is a 'Query' named 'VPN Logins' with a score of 0.

As an alternative to using the quick Search field option, you can get a full Search panel in the Viewer:

- 1 Choose **Edit > Find Resource** in the Console's menus, or press **Ctrl+F**.
- 2 In the Viewer panel's Resource Search tab, enter a query string in the **Search query** line, set the number of results to allow, and click **Find**. See ["Query Options" on page 673](#).
- 3 When the search returns its results, click any item to see its details or click a result column heading to change the order.

When you click a resource listing in the **Details** panel, it shows you the various pieces of related system information that justified that item's ranking.

Query Options

Pose your queries using these conventions.

Query Elements	Descriptions	Examples
Full or partial strings	Phrases, words, or partial words.	<code>"Attack Notification"</code> <code>notification notif</code>
Wildcards	Question marks (?) for single-character substitutions and asterisks (*) for multi-character substitutions.	<code>attack??</code> (attacker, attacked) <code>notif*</code> (notify, notifier, notification)
Boolean Operators	Use AND and OR to join strings.	<code>attack AND suspicious AND high</code>
Fields	Resource field labels (grid view columns) followed by a colon, with the data expressed as plain strings, Boolean strings, quoted strings, or parenthetical expressions.	<code>type:datamonitor AND name:"event counts"</code> <code>name:"address space"</code> <code>name:(address+space)</code> <code>name:(+address space)</code>
Exclusion	Use NOT, the minus sign (-), and the exclamation point (!) to exclude strings.	<code>at???? - attack at???? NOT attack at???? AND !attack at???? AND !attack AND !type:zone</code>
Proximity	Extend data-field queries' scope with a proximity factor expressed as a numeral following a tilde (~). The numeral sets the maximum number of words allowed between the specified words in the resources found.	<code>name:("top events"~1)</code> (top attack events) <code>name:("top events"~2)</code> (top serious attack events)
Fuzzy	Broaden query results with a relative letter-substitution factor expressed as a decimal fraction following a tilde (~). The values 0.0 to 0.9 apply, with the higher values increasing the substitutions made in the string.	<code>name:mssp~0.2</code>

Result Columns

Click any column heading to toggle between descending and ascending order.

Column	Description
Score	Ranking of resources a query returns, based how frequently the search term appears in each resource.
Type	Top-level categorization of the resource, as shown on the Navigator panel.
Name	The full name of the individual resource.
URI	Full uniform resource identifier for the individual resource.

Locating Specific Resources

The resource trees in the Navigator panel are handy for finding and using the security assets available in your organization and provided by ArcSight. However, when you are working with a particular resource in an editor or grid view, locating that item's position in a heavily populated resource tree can be inconvenient.

You can use two right-click commands to instantly spot resource entries in the Navigator panel, from applicable grid view resource listings or resource editors.

- 1 In an entry in a resources grid view, or in the top tab of a resource editor, right-click and choose **Find <asset type> in Navigator**.
- 2 Look for the highlighted item in the Navigator panel's resource tree.

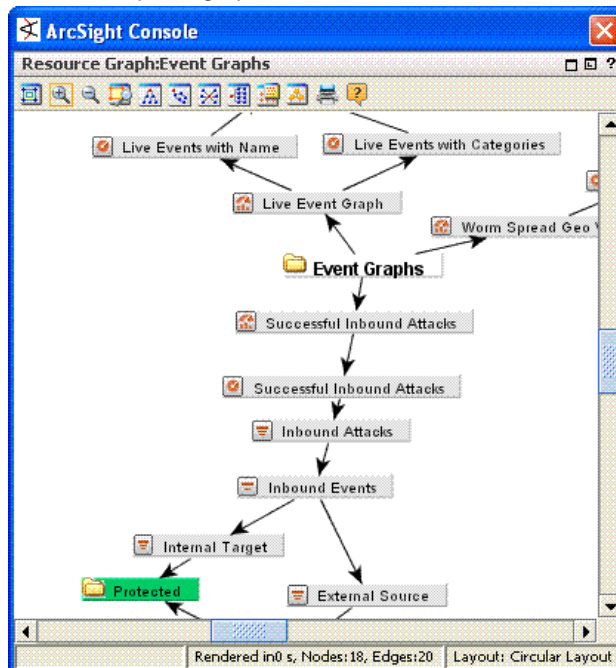
Visualizing Resources

The resources presented in the Navigator panel or graphically in the Viewer panel are organized into hierarchical groups for easy browsing. Among similar types of resources, there can be logical relationships. Graphs can make these relationships readily visible.

Graphing Resources











- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.



The Viewer panel graphs the resources in a new channel.



Using Graphs

Once generated, you can manipulate graphs further. There is a set of command buttons at the top of the view and a parallel set of commands available by right-clicking the graph itself.

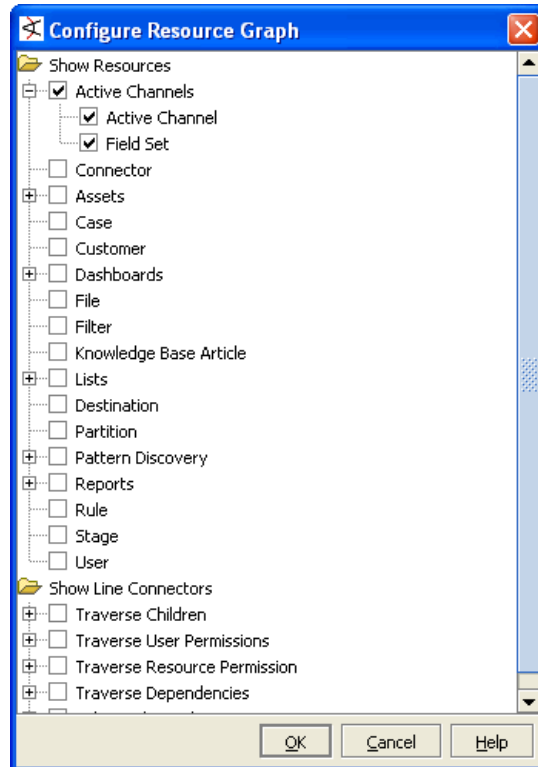
Command	Button	Description
Inspect		Opens a new event-monitoring channel, using the visualization's current timeframe, event and node filters.
Refresh		Updates the graph.
Fit Content		Sizes the graphic to the available display space.
Zoom In / Zoom Out		Increases or decreases the size of the displayed graphic.
Zoom Selected		Zooms in on a selected portion of a graphic.
Hierarchic Layout		Presents nodes in a vertically descending cascade, similar to a family tree. Hierarchic layouts are appropriate when viewing event relationships that have a common root.
Organic Layout		Displays nodes in an arrangement based on minimum edge length, which tends to cluster nodes that relate to a common node. Likewise, node clusters with nodes in common also tend to group together.
Circular Layout		Positions nodes in hub-and-spoke arrangements with each node radiating edges to, or receiving edges from, the nodes with which it interacts. Circular layouts are most useful when multiple roots are present or there are a number of source-target relationships to clarify. If an organic layout is difficult to read because the edges are too dense, try a circular layout instead.
Orthogonal Layout		Arranges nodes on the basis of logical connections, using electrical schematic-style right-angle layouts. These layouts are very useful for clearly tracing connections and identifying node clusters.
Overview		Opens a reduced rendering of the entire graph. You can drag the highlighted section in the reduction to move the displayed area in the main view.
Hierarchy Tree		Opens a complete list of the nodes plotted in graphic layouts. Click a node in the list to scroll to that node in the main view.
Print		Prints the displayed graphic.

Command	Button	Description
Export to JPEG		Create and save a JPEG-format copy of the current image.
Add Graph View to Case		Adds the current graph view to a case you select. Choosing this option opens the Case Selector dialog, where you can browse cases. Select a case to which to add the current graph view and click OK on the Case Selector dialog. The graph view is added to the selected case as an attachment, accessible on the Attachments tab in the case editor for that case.
Help		Display the relevant ESM Console online Help topic.
Snapshot		Creates a new copy of the visualization itself. This graphic is not associated with a dashboard, even when starting from a dashboard viewer.
Snapshot Selection		Opens a new visualization that contains only the selected nodes and their connecting edges.

Configuring Resource Graphs

- 1 Choose any resource tree in the Navigator, with the exception of Notifications and Partitions.
- 2 Select and right-click one or more individual resources or resource groups.
- 3 Choose **Graph View** in the context menu.
- 4 Hover cursor or click anywhere in the Viewer panel, and right-click **Configure Resource Graph** option on the context menu.

This brings up the Configure Resource Graph dialog where you can specify which resources to display in graph views.



5 Select resources to show or hide. (Click checkboxes to toggle show/hide options on resources. Resources with check marks are configured to show for the selected graph view.)

6 Click **OK** to save your changes.

For more information, see [“Selecting Resources” on page 670](#).

Viewing Resources in Grids

While the grids you see in the Viewer panel are most often views of events, these grids can also display organized sets of information about resources in the Navigator panel.

In the Navigator panel, certain resource groups include **Grid View** in their right-click context menus. This command causes the items in the group to display in a grid view, where you can review them using the sorting and column customization features that grid views offer. You can also right-click resource items in grid views and use the same context commands that those resources have in the Navigator panel.



Validating Resources

Resources can break or become invalid because they are improperly built or cannot find other resources they depend on. The following topics describe how to identify valid and invalid resources, show how to troubleshoot and fix broken resources, list requirements for valid resources, and provide tips for manual and automatic resource validation.

Valid and Invalid Resources

Valid resources show up in the Navigator with their associated icons as described in [“Navigating” on page 94](#).

A resource can “break” or become “invalid” either because it is constructed improperly (for example, when an active list schema does not match the underlying table) or because another resource it depends on is missing from the database (for example, when a rule references an unavailable filter). The latter can happen when a resource used in other resources is deleted from the Manager, or not retained during an upgrade, import, or export.

Invalid resources show up in the Navigator as broken or torn. For example, the Navigator displays a valid filter like this: , and an invalid filter like this: . An invalid resource also includes an “Invalid Reason” field under on the Attributes tab of its editor, as described in [Common Resource Attribute Fields](#) under [“Invalid Reason” on page 685](#).



A valid resource is fully available to other resources that reference it, and can participate in the event flow, trends, reports, data monitors, channels, filters, rules, and so forth.

An invalid resource cannot participate in the event flow or other resources in real time. For example, an invalid asset cannot participate in event asset resolution. Correlated events in which the source or target address points to the invalid asset are not generated. Similarly, an invalid rule does not trigger and generate correlation events.

Fixing and Validating Resources

When a resource becomes invalid, its Editor includes a **Validate** button that you can use to test and validate the resource after you fix it. Clicking the **Validate** button on a resource that was previously broken results in a check of the resource logic and dependencies. If the system determines the resource is now valid, the resource icon in the Navigator is updated to reflect a working resource. If the system determines the resource is still broken, it displays an error message describing the problem.

The general flow of steps to fix and validate a resource are:

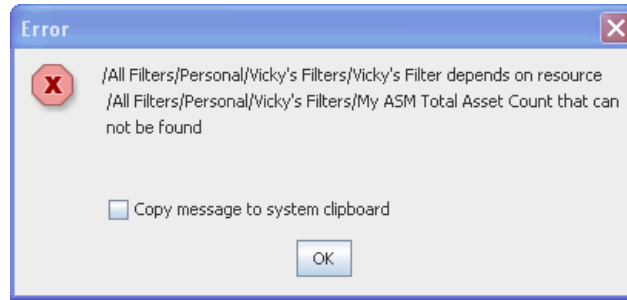
- 1 Identify an invalid resource. Sometimes problems with filters or rules (which are used in many other resources) are a result of broken resources. (A valid resource looks like this: , and an invalid resource looks like this: )

For example, if “My Top Threats” filter depends on “My Hotlist” filter, removing “My Hotlist” filter breaks “MY Top Threats” filter.

A scheduled job (like a scheduled rule group or archived report) can also break if one of the resources it depends on is missing. The broken icon for a scheduled job shows up on the Current Jobs list.

- 2 If you do not already know why a resource is broken, open its editor (double-click the resource in the Navigator panel) and click **Validate** in the resource editor. Validate

gives you an error message that describes the problem. The error dialog includes a Copy button for copying longer messages to an external editor.



- 3 Fix the problems with the resource. This may involve adding back in missing resources or rebuilding the resource to fit various other requirements as described in Troubleshooting Invalid Resources below.

To continue with our example, adding back in the filter "My Hotlist" would fix the problem we mentioned in step 1.

- 4 In the resource editor(s), click **Apply** to save changes to the resources you modified.



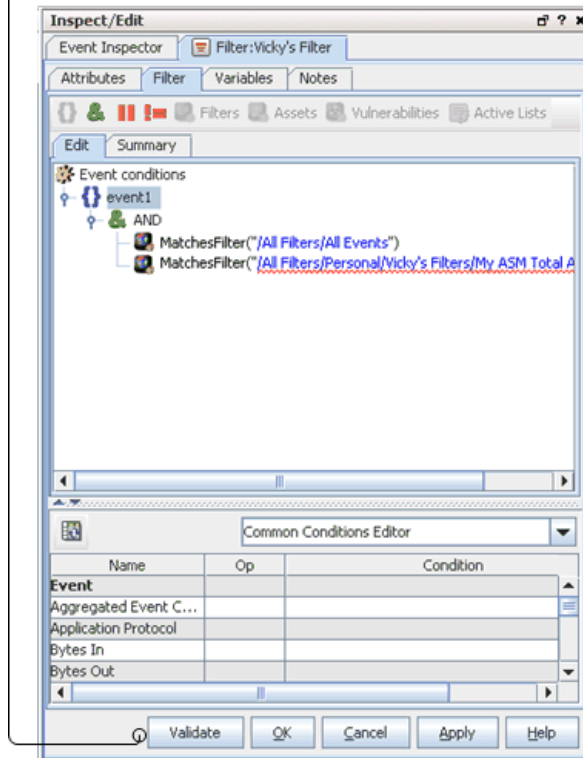
For problems that can be validated on the local client, you can click **Validate** before clicking **Apply** and if the resource is fixed its "working" icon is immediately reflected in the Navigator. However, for other types of problems; you need to **Apply** the changes to the resource before you **Validate** the resource. This is because some types changes must be processed on the Manager to determine dependencies and relationships to other data not available on the local client.

If you think you have fixed a resource but it is still not showing as fixed in the Navigator, make sure you **Apply** all the changes you made to it and then click **Validate** again.

- 5 In the resource editor for the resource that was broken, click **Validate**. If the resource passes validation, its icon in the Navigator updates to reflect a working resource.

In the resource Editor for the resource that was broken, click the **Validate** button. If the resource passes validation, its icon in the Navigator updates to reflect a working resource. Otherwise, the broken icon remains and an error message describes the problems.

Some problems require saving fixes to the Manager, so be sure to click **Apply** and save changes to resources you fix before you click **Validate**.



To validate a scheduled job, click the **Open scheduled jobs list** tool button (🕒) to display scheduled jobs in the Viewer, right-click the job you want to validate, and choose **Validate** from the context menu. If the job passes validation, its icon in the Current Jobs list updates to reflect a valid task.

Troubleshooting (Requirements for Valid Resources)

The most common cause of an invalid resource is a dependency issue; another resource that the broken resource depends on is missing from the database. Some resources have additional requirements or limits that can also affect validity. Following is a summary of requirements for creating valid resources.

If any of these requirements are not met, the resource will break. To fix the resource, edit its definition to be in line with these requirements.

- All Resources - If the definition for a resource references another resource, the referenced resource must be available in the Manager database. This requirement is true for all types of resources.
- Devices and Assets - Each asset address must be unique within a zone, an asset can belong to one zone only, and the asset IP address must fall within the address range of its network zone.

- Device and Asset Ranges - Start addresses must be less than end addresses, asset ranges must be within the address range of the associated network zone, and asset ranges should not overlap another asset range in the same zone.
- Zones - Start addresses must be less than end addresses and network zones should not overlap other zones in the same network.
- Reports - Report templates cannot contain more than 20 charts or more than 15 tables.
- Active Lists - Active List schema must match the underlying table and must not include programming errors.

Resources become invalid when they violate one or more of their constraints. The following table lists the resources that can become invalid:

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Device/Asset	<ul style="list-style-type: none"> Asset address must be unique within a zone. An asset only belongs to one zone. Asset IP address must fall in the address range of its network zone. 	The invalid device/asset cannot participate in the event asset resolution. Therefore, if an event source/target address points to the invalid device it cannot be resolved.
Device/Asset Range	<ul style="list-style-type: none"> Start address must be less than end address. Asset range must be within the address range of its network zone. Asset range should not overlap another asset range in the same zone. 	The invalid device/asset range cannot participate in the event asset resolution. Therefore, if an event has its source/target address fall in an invalid device range its asset resolution cannot be resolved.
Zone	<ul style="list-style-type: none"> Start address must be less than end address. Network zone should not overlap other zones in the same network. 	The assets falling within this invalid zone get invalidated and cannot participate in the event asset resolution.
Filter	Dependency constraint. For example, a filter may depend on other resources, like asset, active list, vulnerability etc.	The invalid filter causes the resources that depend on it to get invalidated.
Rule	Dependency constraint. For example, a rule may depend on other resources, like filter, asset, vulnerability, active list, session list etc.	The invalid rule cannot be triggered, so the corresponding correlation events are missed.
Data Monitor	Dependency constraint. For example, a data monitor may depend on other resources such as a filter.	The invalid data monitor stops fetching live data to feed the dashboard.
Active Channel	Dependency constraint. For example, an active channel may depend on other resources such as a filter, or asset vulnerability.	You cannot attach or open an invalid active channel
Report	Dependency constraint. For example, a report may depend on other resources, such as filter or asset, vulnerability and active list.	You cannot run the invalid report manually from console or as a scheduled task.

This resource becomes invalid...	when it violates one or more of the following constraints...	which results in...
Trend	Dependency constraint. For example, a trend that depends on a query is invalid as soon as a query is changed.	The invalid trend stops generating any trend data.
Scheduled Task	Dependency constraint. For example, a scheduled task may depend on other resources, such as filter.	The invalid scheduled task cannot run.
Report Template	The report template cannot contain more than 20 charts or more than 15 tables.	The invalid template causes the reports that depend on it to be invalid.
Profile	Dependency constraint. The Profile depends on resources such as the filter it uses to determine which events to run discovery on. It also depends on the group where snapshots and patterns are saved. All these resource must exist and the creator should have appropriate permissions for them.	This resource is invalidated and the scheduled runs may be skipped.
Active List	If the Active List schema does not match the underlying table etc, or due to some programming error.	The resources (Rules, reports etc.) that are dependent on the Active List get invalidated
Focused Report	Dependency constraint. For example, a focused report may depend on other resources, such as a report, filter or asset.	The invalid focused report cannot be run either manually from the Console or as a scheduled task.
Query	Dependency constraint. For example, a query may depend on other resources, such as a filter, asset, or active list.	The invalid query causes the resources that depend on it, such as report and trend, to become invalid.

Automatic and Manual Validation

You can validate individual resource manually through the Console with the **Validate** button as described above.

Resource validation takes place automatically during an upgrade, package import or export, or when you insert or update a resource. (Administrators can use a stand-alone, command-line utility on the Manager machine for validating resources and generating validation reports on an off-line Manager. This is often useful after an upgrade.)

You can validate resources manually either through the Console (as described in [“Fixing and Validating Resources” on page 678](#)) or by running the following command from the `<ARCSIGHT_HOME>/bin` directory on the machine where your ArcSight Manager is installed:

```
arcsight resvalidate -persist [true|false] -excludeTypes <list of
comma-delimited resource types>
```



The `resvalidate` is a standalone utility and runs as a batch process. We recommend that you run it only if need be (when there are many database updates that happen offline) after doing a product upgrade only. This utility should not be run while the Manager is running.

After you run this utility, you can find the `validationReport.html` report in the `<ARCSIGHT_HOME>` directory, which lists all the invalid resources.

Resource Validation During Upgrade

If the Manager detects a conflict during an upgrade or import process, it invalidates the conflicting resource, and continues with the upgrade or import process. The dependent resources for the conflicting resource is automatically re-validated and disabled after the resource validation process completes.

After an upgrade process, a report called `validationReport.html` is generated in the `<ARCSIGHT_HOME>/upgrade/out/<time-stamp>` directory. After an import process, you can check the Console to make sure that you do not have any invalid resources. You are expected to fix the invalid resources manually. After you resolve the conflict, the dependent resources for the conflicting resource is automatically re-validated.

An invalid resource cannot participate in the event flow, trends, reports, data monitors, or channels in real time. For example, if an asset is marked invalid, it cannot participate in the event asset resolution. As a result, correlated events in which the source or target address points to the invalid asset are not generated. Similarly, when a rule is marked invalid, it does not trigger, therefore, the corresponding correlation events are not generated.

Extending Audit Event Logging

Updates to existing resources are logged as audit events, as described in “[Resources \(Configuration Events Common to Most Resources\)](#)” on page 812.

If you want to get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property on the Manager to specify which resources should show extended audit event information.

To configure resources for more detailed update auditing, add a URI to the `resource.audit.update.uris` property in the `server.defaults.properties` file. For example:

```
resource.audit.update.uris=/All Users/
```

turns on extended audit logging for all resources under the `/All Users/` subtree.

Leaving this property blank would turn this feature off (and show only default audit information).

To show detailed audit information for multiple resource types, list resource URIs separated by commas (no spaces). For example, to show extended update audit logging for users and system assets, set the property like this:

```
resource.audit.update.uris=/All Users/,/All Assets/ArcSight System
Administration/
```

Extended information on the resource update is logged in two places.

- In the internal audit event generated for the resource update, `Device Custom String5` is set with the update information. The audit event information is shown in the `Device Custom String5` field in this format:

```
<UUID generated for this change>:[<name of attribute>:<old value>:<new value>]+
```

- The update information is also written to a log file, `<ARCSIGHT_HOME>/logs/default/resource_update_audit.log` file. The audit event information is shown in the log in this format:

```
<UUID generated for this change>:<URI of resource>:<ID of resource>:[<name of attribute>:<old value>:<new value>]+
```



- The "+" in the message format examples above is regular expression notation used to indicate that there can be one or more of `<name of attribute>:<old value>:<new value>` triplets shown in the audit event.
- Any ":" character in any attribute name or value is escaped with a backslash to "\:".
- Any "\" character in any attribute name or value is escaped with a backslash to "\\\".

Saving Copies of Read-Only Resources

Although you may be limited to read-only access to certain resources in the Navigator panel, you do have the option to save a copy of such a resource to your own group where you do have write access.

Click the **Save As** button to make a copy of the resource and save it in a specified group.

In the resource group selector dialog, displayed when you click **Save As** in the editor for a read-only resource:

- 1 Select the group in which you want to save a copy of the resource.
- 2 Specify the name you want to assign to your copy of the resource.
- 3 Click **OK**.

The resource copy appears in the resource tree. You have write permission with this copy of the resource.


The Connectors, Users, and Notification editors do not support **Save As** functionality. In these editors, you see the **OK/Cancel/Apply** buttons, but the fields for those resources are read-only.

Common Resource Attribute Fields

The following fields are common to several types of resources. You can find these fields in the resource editor Attributes tabs for the resources in Common, Assign, Parent Groups, Creation Information, and Last Update Information sections. (See also, "[Resource Attributes](#)" on page 970.)

Common

Entering data in the **Common** section is optional, depending your environment setup.

Field	Description
Resource ID	Read-only field that shows the ArcSight system resource ID.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your administrator can advise you on the correct values for this field, if applicable.
Alias	<p>An optional alternate identification string used for referencing resources. If given, this alias appear in place of the resource's name everywhere it may be seen. Your administrator can advise you on the correct values for this field, if applicable.</p> <p>If you use an alternate event naming scheme in your environment, enter an alias for this resource here.</p>
Invalid Reason	<p>If a resource is broken or invalid, an "Invalid Reason" field is included in its Attributes table. An abbreviated explanation is shown in this field. (See also, "Validating Resources" on page 677.)</p> <p>Click the browse button  at the end of this field to get a popup dialog that shows the full text of the explanation.</p>
Description	<p>Description of the resource.</p> <p>You can use this field to communicate the purpose of this resource to other users. For example, if this is a resource that leverages or depends on another resource (for example, a query viewer or trend that uses an SQL query), this is a good place to make note of that relationship.</p>
Version ID	The globally unique version ID for this resource.
Deprecated	Toggle to indicate whether the resource is current or deprecated (obsolete).

Assign

Field	Description
Owner	A user selected from the Users resource tree who should be notified about this resource.
Notification Groups	The user groups selected from the Users resource tree who should be notified about this resource.

Parent Groups

Field	Description
Parent Group	Read-only field that shows the name and path to parent group of this resource.

Creation Information

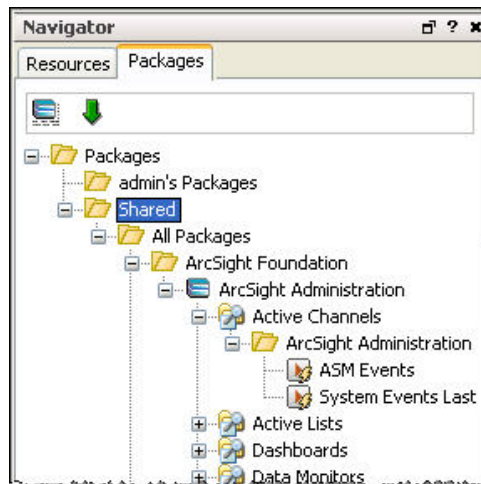
Field	Description
Created By	Read-only field that shows the user who created this resource.
Creation Time	Read-only field that shows the date/time when this resource was created.
Time Since Creation	Read-only field that shows the time elapsed since this resource was created. This value is calculated from Creation Time.


Last Update Information

Field	Description
Last Updated By	Read-only field that shows the user who last updated the resource.
Last Update Time	Read-only field that shows the date/time when this resource was last updated.
Time Since Last Update	Read-only field that shows time elapsed since last update. This value is calculated from Last Update Time.


Managing Packages

Packages are collections of resources that can be installed into the system resource tree.



To access available packages, click the **Packages** tab of the Navigator panel. The tree of all packages is displayed along with the resources within each package. The  button toggles between Normal and Advanced view of the package tree. In the Advanced view, uninstalled packages are visible and package dependencies are shown.


Viewing Installed Packages

Click the **Packages** tab in the Navigator panel. If the  button is highlighted, click it to return to Normal view. The tree view is like the tree view of any other resource except that the resources contained within packages may be of many different types.




The Packages tree view is independent of which resource you have selected in the Navigator. Regardless of which resource is selected, when you click the **Packages** tab, you see the same set of packages. These include the ArcSight stock content packages installed on the Manager along with any custom packages administrators have created on this Manager.

Viewing all Packages (with Dependencies)

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view. In the Advanced view, all packages (including uninstalled packages) and package dependencies are shown.

Showing Package Archive Contents

Click the **Packages** tab in the Navigator panel. If the  button is not highlighted, click it to switch to Advanced view (to show all packages including uninstalled packages). Right-click a package and choose **Show Package Archive Contents** or **Show Current Package Archive Contents** (available only on installed packages). This lists all resources in the package, including details such as resource name, type, and full path to location in the tree.

Creating Packages

- 1 Right-click the **Package Group** in the Packages tree in which you want to put the new Package. Choose **New Package**.
- 2 In the Package Editor that opens in the Inspect/Edit panel, enter the following fields:

In this field...	...enter this
Name	Enter a name for the new package.
Required Packages	Specify the packages that must be installed for this package to function.
Optional Packages	Specify packages that are related to this package, but which are not required for it to function.
Required Features	Enter any features that must be available for this package to function. The pick list of features includes Pattern Discovery, for example.
Installed	(Read-only.) Check this box to indicate that the new package is installed. Unchecking this box is a good way to preview a new package before making its resources visible to all users of the system.
Update Available	(Read-only.) Check this box to indicate to other users that a newer version of the package exists.
Author Name	Enter the name of the author or source for the new package.

In this field...	...enter this
Package Version	The package version can be any string, but by convention, ArcSight recommends a format of 0.0.0.0, with numbers in decreasing importance (major, minor, release, build).
ArcSight Version	(Read-only.) The minimum ArcSight Version needed to support this package.
Format	<p>(Advanced) if you need a specific behavior, choose one of the choices other than default. Otherwise, leave this field set to default.</p> <p>Default - Appropriate format for backing up resources on a Manager. This format captures more information than the other options, including information specific to a Manager installation.</p> <p>Export - A portable format appropriate for packaging resources for transport between systems in which Manager-specific information is excluded from the exported package for resources with attributes that would otherwise retain such information upon a "default" export.</p> <p>For example, a trend packaged in "export" format does not include Start Time or End Time trend attributes nor original table IDs. Instead, the imported trend uses Start and End times that correspond to the time the package is installed on a new system. Also at time of package install, a new trend table is created. (See also, descriptions of Imported Trend Start Time and Imported Trend End Time fields under advanced Trend Attributes in "Building Trends" on page 369.)</p> <p>Similarly, active lists and session lists packaged in "export" format do not include locked by attributes, table IDs, or session/active list entry attributes, respectively. New tables are created when the lists are imported, and the other attributes are tracked starting with launch of these resources on the new system.</p> <p>The package "export" format packages other resources similarly as a means of optimizing portability for content distribution.</p> <p>ArcSight system content is packaged using the "export" format. Also, Managed Security Service Providers (MSSPs) who provide content to ArcSight installations at various customer sites might typically package resources in this format.</p> <p>Exportuser - Highly portable format appropriate only for exporting user accounts with no permissions, personal group information, or relationships to other resources. If you want to export user accounts that include permissions and groups, use the default format instead.</p> <p>Upgrade - For use by Arcsight Professional Services only. This format might be used for ArcSight initiated incremental resource upgrades of older systems in particular circumstances. (In most cases, standard upgrade utilities and processes are used instead.)</p>
Obfuscated	(Advanced) Check this box to scramble the package contents to prevent unauthorized viewing or modification.

In this field...	...enter this
Exclude Reference IDs	(Advanced) Check this box to remove reference IDs from the package when it is exported. Generally, you would exclude reference IDs only when you plan to import the package into a different ArcSight system. Leave the box unchecked to include reference IDs, which improve performance for packages that are imported to the same Manager from which they were exported.

- 3 Click the **Resources** tab in the Package Editor. Click the **Add** drop-down menu to select the resources that this package will contain. You can select groups or individual resources.

Content such as rule or a filter, and so on, does not work if it uses a domain field and the domain field set is missing. If you export and import such content, either include the domain field set in the package, or make sure that the domain field set pre-exists on the import system.

Check the **Children Only** box to include resources below the specified resource in the tree. For example, selecting the group /All Session Lists/ArcSight Administration/User and checking **Children Only** would include only the session list resources in that group, not the group itself.

Check the **Only If Referenced** box to conditionally include resources if they are referenced by other resources without the **Only If Referenced** box checked.


- 4 To exclude resources from the new package by resource type or by specifying actual resources to be removed, use the Removed Resources panel in the lower half of the Resources tab. To exclude resources by type, click the **Excluded Resource Types** tab and select from the list of available types. To exclude specific resources, click the **Removed Resources** tab, click the **Add** drop-down menu, then choose the resource(s) you wish to exclude using the resource picker.



Caution

The only way to exclude Asset Category resources from a package is to specify the Asset Categories explicitly using the Removed Resources tab.

Importing Package Bundles

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Click the  icon to import a bundle.
- 3 Choose an .arb file to import and click **Open**.
- 4 By unchecking the box next to each package, you can choose to import a package without installing it. The default is to install all imported packages.
- 5 Review the Import dialog for any conflicts. Each conflict displays one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window. For more about resolving conflicts, see [“Resolving Package Conflicts” on page 692](#).

- 6 Click **OK** to continue. When the import is done, a Summary Report is displayed describing the packages that were imported.

**Note**

Importing packages created by other users

Packages, like other resources, are always displayed under the user folder in which they were created. Upon import, the Summary Report shows the URI or full path into which the package was imported (for example, [Packages Imported: /All Packages/Personal/Vicky's Packages/VPN Logins Reporting](#)). The import location is not configurable.

- If you log in with a different user name and import a package, you may or may not have write access to the package (depending on permissions).
- If you import the package with a different user name on a Manager that does not include an account for the package originator, you cannot see the imported package.
- If you recreate an account on the Manager with the same user name as the package originator, the imported package reappears.

**Tip**

Importing content from an older package into an existing newer package

If you import the content of an older package into an existing newer package with the same name, the contents from the two packages are merged. The resulting package consists of contents from both packages. The relationships are merged, but the attributes are picked up from the old package.

For best results, export the new package to a bundle file so that you can recover if needed. Then delete the new package before importing the old one.


Exporting Packages

- 1 Click the **Packages** tab in the Navigator panel and click to select one or more packages to export.
- 2 Right-click and choose **Export Package to Bundle**.
- 3 Enter a name and folder for the local bundle file. The default extension is [.arb](#).

The exported bundle has reference IDs if that box was checked in the Package Editor, and it is obfuscated if that box was checked in the editor.

Installing Packages

If you chose not to install a package when its bundle was imported, or if you left the Installed checkbox unchecked when you created a package, it will be uninstalled. Uninstalled packages are not shown in the Normal view of the package tree.

- 1 Click the **Packages** tab in the Navigator panel. If the  icon is not highlighted, click it to switch to the Advanced view.
- 2 Right-click the uninstalled package (shown with a gray icon) that you would like to install and choose **Install Package**.
- 3 Review the dialog for any conflicts. Each conflict displays one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window.

For more information, see [“Resolving Package Conflicts” on page 692](#).

Uninstalling Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be uninstalled. Choose **Uninstall Package**. (This command is disabled if the package is already uninstalled or if it is locked.)

Uninstalling a package removes its resources from the system and hides the package in Normal view, but it remains in the system and can easily be installed again.

Dependent resources are deleted automatically unless they are contained in another package.

For more information, see [“Resolving Package Conflicts” on page 692](#).

Editing Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Change the package name or other properties on the Attributes tab. For more information on package fields, see [“Creating Packages” on page 687](#).
- 4 Click the **Resources** tab to add or remove resources from the package.

Adding Resources to Packages

You can add a resource to an existing package by using the right-click menu on a selected resource in the Navigator tree.

- 1 Click the **Resources** tab in the Navigator panel.
- 2 Choose the resource type you want to add (for example, Reports).
- 3 Navigate to and right-click the particular resource you want to add (for example, My Report), and choose **Add to Package**. The system displays the Package Selector dialog.
- 4 Select a package to which to add the selected resource and click **OK**.

Removing Resources from Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be edited and choose **Edit Package**. The Package Editor opens in the Inspect/Edit panel.
- 3 Click the **Resources** tab in the Package Editor.
- 4 In the upper half of the Resources tab, select the resource you want to remove. (A gray highlight on the entire row indicates the resource is selected.)
- 5 Click **Remove**.

Deleting Packages

- 1 Click the **Packages** tab in the Navigator panel.
- 2 Right-click the package to be deleted and choose **Delete Package**.

- 3 Confirm that you want to delete the specified package.
- 4 Choose **Remove Resources in Package** or **Leave Resources**. If you **Leave Resources**, only the package itself is deleted. The resource that it contained remains in the system resource tree. If you **Remove Resources**, all resources that the package contained are deleted from the system resource tree.



Deleting a package that contains resources that maintain state—active lists with values, session lists, or trends—deletes the state information as well.

Caution

For more information, see [“Resolving Package Conflicts” on page 692](#).

Resolving Package Conflicts

Package conflicts can occur during install, uninstall, delete, or import of packages. Most package conflicts are resolved internally by the ArcSight Manager without the need for user intervention. However, some package conflicts prompt the administrator for an appropriate course of action from among several options. This section describes two of these scenarios as examples.

If the ArcSight Manager detects package conflicts for a pending package **uninstall**, the Console provides choices for resolving the conflict and proceeding, or aborting the uninstall operation. The options provided depend on the type of conflict detected.

For example, if you attempt to uninstall a package that changed since it was installed, the conflict is indicated and you are asked to choose from the following **Resolution Options**.

Option	Description
Create a new archive for package	Creates a new archive for the modified package (and retains original).
Create new archive for remaining changed packages	Creates new archives for all changed packages before uninstall (retains all originals).
Continue without saving changes	Uninstalls this package without saving changes.
Uninstalls this and remaining packages without saving changes	Uninstalls all selected packages without saving changes.
Abort	Abandons the uninstall process and keeps the package(s) as is.

If the ArcSight Manager detects package conflicts for a pending package import or install, the Console provides choices for resolving the conflict and proceeding, or aborting the import operation. The options provided depend on the type of conflict detected.

For example if you attempt to import a package with content that is older than the currently imported package, the conflict is indicated and you are asked to choose from the following Resolution Options:

Option	Description
Leave newer packages	Leaves the newer packages installed.
Never override newer packages	Completes the import but imports only packages that are newer than those currently installed.
Update packages	Imports the selected packages, and prompts for package conflict resolutions on a per-package basis.
Always update packages	Imports the selected packages, and overwrites newer packages if they exist.
Abort	Abandons the uninstall process and keeps the package(s) as is.

See the *Administrator's Guide* for more information on working with the archive command and other utilities.

Managing SmartConnectors

ArcSight SmartConnectors can be configured to optimize their performance and increase their functionality. You can configure SmartConnectors to enable aggregation, batching, and time filter correction functionality. You can also send control commands, from the ESM Console, to SmartConnectors to manage the flow of events.

[“Selecting and Setting SmartConnector Parameters” on page 695](#)

[“Managing SmartConnector Filter Conditions” on page 712](#)

[“Setting Special Severity Levels” on page 713](#)

[“Sending Model Mappings to SmartConnectors” on page 715](#)

[“Sending Control Commands to SmartConnectors” on page 715](#)

[“Managing SmartConnector Groups” on page 722](#)

[“Managing SmartConnector Resources” on page 723](#)

[“Importing and Exporting SmartConnector Configurations” on page 724](#)

[“Upgrading SmartConnectors” on page 726](#)

Selecting and Setting SmartConnector Parameters

From the ESM Console, use the Connector Editor to control SmartConnectors.

Configuring the SmartConnector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to manage and choose **Configure**. This opens the **Inspect/Edit** panel for the **Connector Editor**. On the Connector tab, the Name field is automatically populated with the name assigned during SmartConnector Installation.
- 3 Type in the **Connector Location** and the **Device Location**. All events are tagged with these fields by the ArcSight SmartConnector. Creation date and other information is automatically populated.
- 4 On the Default tab, change any additional Batching, Time Correction or other parameters as desired, using the configuration fields explanations provided below.
- 5 Click **Apply** to add your changes and to keep the Connector Editor open. To apply your changes and close the Connector Editor click **OK**, or, if applicable, click **Add Alternate** to save your changes as an alternate configuration you can select and apply later.

The description entry associated with the setting provides tool tip information. These parameters are not localized since they come directly from the connector and the connector may contain new resources (since it may be a newer version).

The framework for connector commands operates in a similar way. Configuration of the connector command menu is achieved by sending the list of commands that are supported on the connector at registration time.

There are several controls you can adjust in the Connector Editor. The variety of options are best summarized by briefly describing what's available at each of the editor's tabs or sub-tabs.

Connector Editor Option Tabs

The Connector Editor Option Tabs are listed in the following table:

Connector Tabs	Options
Connector Tab Configuration Fields	Basic identification, ownership, and date/time parameters.
Networks	The ArcSight network(s) to which the connector is or can be assigned.
Default Content Tab Configuration Fields	Includes options for report batching, aggregation, and time corrections.
Default: Filters	A filter condition editor for constraining what the connector reports. (Please see “Managing SmartConnector Filter Conditions” on page 712 and “Common Conditions Editor (CCE)” on page 846 for details on how to define filters for connectors.)
Alternate: Content	A set of options identical to those under Default, which you can use to create alternate configurations.
Alternate: Filters	A filter condition editor for constraining what the connector reports, in an alternate configuration.
Notes: Table	A text editor for, and tabular list of, configuration notes.
Notes: List	A text editor for, and text presentation of, configuration notes.

Connector Tab Configuration Fields

You do basic configuration through the Connector and Default: Content tabs. Many of these fields correspond to resource editor fields. See also [“Common Resource Attribute Fields” on page 684](#).

Name Field	Value Field
Name	The Name text field is automatically populated with the name assigned during SmartConnector installation.

Name Field	Value Field
ID	The identification string assigned during SmartConnector installation.
Status	The SmartConnector's current mode of operation.
Connector Location	A description of the (usually) physical location of the SmartConnector. This appears in all the events issued from the connector.
Device Location	A description of the (usually) physical location of the device the SmartConnector is monitoring. This appears in all the events issued from the connector.
Version	The connector's software version number.
External ID	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. If your system interfaces with a third-party incident tracking system, such as Remedy, enter an ID that corresponds to that system. Your administrator can advise you on the correct values for this field, if applicable.
Alias	An optional alternate identification string used for referencing resources. If given, this alias appear in place of the resource's name everywhere it may be seen. Your administrator can advise you on the correct values for this field, if applicable.
Description	A text description of the configuration or other related information.
Owner	A user selected from the Users resource tree who should be notified about this connector.
Notification Groups	The user groups selected from the Users resource tree who should be notified about this connector.
Created By	A user identity provided at SmartConnector installation.
Creation Time	The time of SmartConnector installation.
Time Since Creation	A value calculated from Creation Time.
Last Updated By	The user who made the last configuration change.
Last Update Time	The time of the last configuration change.
Time Since Last Update	A value calculated from Last Update Time.

Default Content Tab Configuration Fields

SmartConnector configuration options available may vary depending on which version of SmartConnectors you are using. SmartConnector configuration options come directly from the connector, and newer versions of connectors might contain new or different resources than previous versions.

The following table shows the Default Content Tab Configuration Fields

Name Field	Value Field
Batching	SmartConnectors can batch events to increase performance and optimize network bandwidth. When activated, SmartConnectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires. You can also prioritize batches by severity, forcing the SmartConnector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, 100 events).
Enable Batching (in seconds)	The SmartConnector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is Time Based if the SmartConnector should send batches as they arrive (the default) or Severity Based if the SmartConnector should send batches based on severity (batches of Highest Severity events sent first).
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the SmartConnector to automatically correct the time reported by the device.
Use Connector Time as Device Time	(No Yes) Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector is more likely to report the correct time. The default is No .
Enable Device Time Correction (in seconds)	The SmartConnector can adjust the time reported by the device Detect Time , using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol.
Enable Connector Time Correction (in seconds)	The SmartConnector can also adjust the time reported by the Connector Time SmartConnector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the SmartConnector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and SmartConnectors is the NTP protocol.
Set Device Time Zone To	(Disabled <TimeZone>)(Default is Disabled) Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the SmartConnector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported.

Name Field	Value Field
Device Time Auto-correction	
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by Past Threshold seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by Past Threshold seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, (ALL) means all devices.
Time Checking	
	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking.
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is 1 hour (3,600 seconds).
Frequency	The SmartConnector checks its future and past thresholds at intervals specified by this number of seconds. Default is 1 minute (60 seconds).
Cache	
	Changing these settings does not affect the events cached, it only affects new events sent to the cache.
Cache Size	SmartConnectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the SmartConnector receives bursts of events. This parameter specifies the disk space to use. The default is 1 GB which, depending on the connector, can hold about 15 million events, but it also can go down to 5 MB . When this disk space is full, the SmartConnector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is 10,000.
Notification Frequency	How often to send notifications once the Notification Threshold is reached. (1 min, 5 min, 10 min, 30 min, 60 min.)
Payload Cache	If the represented SmartConnector supports it, setting this to True causes the connector to automatically create and populate a cache for device payload data. The payload data is retrieved from the original device or retained from the received event data, depending on how it operates. The default setting is False . Consult a SmartConnector's Configuration Guide to find out whether it supports this capability. Changes to this setting take effect after you restart the SmartConnector.

Name Field	Value Field
Payload Cache Size	If Payload Cache is True , these choices determine the maximum size of the cache. The cache operates on a last-in-first-out (LIFO) basis.
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the ArcSight Manager. The default is 10 seconds , but it can go from 5 seconds to 10 minutes . Note that the heartbeat is also used to communicate with the SmartConnector; therefore, if its frequency is set to 10 minutes , then it could take as much as 10 minutes to send any configuration information or commands back to the SmartConnector.
Enable Name Resolution	(Enabled Disabled) The SmartConnector tries to resolve IP addresses to host names, and host names to IP addresses, if the event rate allows it and if required. This setting controls this functionality. The Source, Target and Device IP addresses and Hostnames may also be affected by this setting. (Default is Enabled)
Name Resolution TTL (secs)	This is the amount of time (Time to Live) the name resolution is to be in effect. The name resolution entries are cached for this time. (Default is 3600)
Wait For Name Resolution	(Yes No) If set to Yes, the SmartConnector waits for name resolution to be completed. (Default is No)
Name Resolution Host Name Only	(Yes No) If set to Yes, for reverse resolution (IP Address to Host name), only the host name field is set. If set to No, the host name is split up and put into both the DNS domain and the host name fields. This affects the source, destination, device and SmartConnector name fields. (Default is Yes)
Name Resolution Domain from Email	(Yes No) If set to Yes, the host name and DNS domain fields are empty, and the corresponding user name field appears as an e-mail address, then the domain from the e-mail address is put in the DNS domain field. This only affects the source and destination fields. (Default is Yes)
Clear Host Names Same as IP Address	(Yes No) If set to Yes and the host name field is set to an IP Address that matches the corresponding IP Address field, then the host name field is cleared. This affects the source, destination, and device fields. (Default is Yes)
Set Host Names to IP Addresses When Unknown	(Yes No) If set to Yes, host names that remain unresolved are set to IP addresses. (Default is No)
Don't Resolve Host Names Matching	By default, host names are resolved to their IP addresses. You have the option to specify a regular expression for all or part of a host name <i>for which you do not want the system to attempt host name resolution to an IP address.</i> When this option is configured, the system cannot resolve host names matching this expression.

Name Field	Value Field
Don't Reverse-Resolve IP Ranges	<p>By default, IP addresses are resolved to their domain names. You have the option to specify IP address ranges <i>for which you do not want the system to attempt reverse-resolution to domain names</i>.</p> <p>When this option is configured, the system cannot reverse-resolve IP addresses that fall within any of the specified ranges.</p>
Remove Unresolvable Names/IPs from Cache	<p>(Yes No) If set to Yes, unresolvable host names or IP addresses continue to be in the cache. (Default is No)</p>
Limit Bandwidth To	<p>A list of bandwidth options you can use to constrain the connector's output over the network. (Disabled, 1 kbit/sec to 10 Mbits/sec.)</p>
Transport Mode	<p>You can configure the SmartConnector to cache to disk all the processed events it receives. This is equivalent to pausing the SmartConnector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (Normal Cache Cache (but send Very High severity events)).</p>
Cache Mode	<p>(Normal Drop if Dest Down) This option is meant to be used on a primary destination to control the caching behavior of the primary destination when it is down, and the connector starts sending events to the failover destination. In the Normal mode, events are cached and sent to the primary destination when it comes back up. In the Drop if Dest Down mode, the events are not cached and dropped and therefore not sent to the primary destination when it becomes available again. (Default is Normal)</p>
Address-based Zone Population Defaults Enabled	<p>This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 or newer versions because the system has integral zone mapping.</p>
Address-based Zone Population	<p>This field applies to v3.0 ArcSight Managers, as discussed in the Zones section of the SmartConnectors topic. This field is not relevant in v3.5 because the system has integral zone mapping.</p>
Zone Population Mode	<p>(Normal Rezone (override) No Zoning (clear)) Setting to Normal means zones are computed and assigned, if not already set. Rezone (override) re-computes and re-assigns already populated zones. No Zoning (clear) clears the zones, if already populated. (Default is Normal)</p>

Name Field	Value Field
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's source address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Source Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated source address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Destination Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's destination address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Destination Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated destination address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Connector Zone UR	When populated, this field shows the URI of the zone associated with the SmartConnector's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Connector Translated Zone URI	When populated, this field shows the URI of the zone associated with the SmartConnector's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.

Name Field	Value Field
Device Zone URI	When populated, this field shows the URI of the zone associated with the device's address. How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 or newer versions because of integral zone mapping.
Device Translated Zone URI	When populated, this field shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT (network address translation). How this field gets populated is discussed in the Zones section of the SmartConnectors topic. This field is present for v3.0 compatibility. It is not relevant in v3.5 because of integral zone mapping.
Field Based Aggregation	<p>This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, the fields of the two events are the same per the fields listed in the description of "Enable Aggregation (in secs)" on page 707. However, field-based aggregation implements a more flexible aggregation mechanism; two events are aggregated if only the <i>selected</i> fields are the same for both events. (Note: Field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored, unless "Preserve Common Fields" is set to "Yes".)</p> <p>Field-based aggregation offers several advantages over basic aggregation, including:</p> <ul style="list-style-type: none"> • Control over what fields to aggregate on • Start and end time set to the earliest start time and latest end time, respectively (instead of taking the values from the first event in the group, like basic aggregation) • Option to preserve common fields • Option to sum one or more numeric fields <p>SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate "accepts" and "rejects" in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.</p> <p>Note: The legacy, basic aggregation feature is described in the field description for Enable Aggregation (in secs).</p>
Time Interval	<p>Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. Aggregation time interval and threshold settings need to both be set in order for the aggregation to be enabled.</p> <p>(Disabled, 1 sec, 5 sec, and so on, up to 1 hour.)</p>

Name Field	Value Field
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Field Names	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. Use Ctrl+click to select multiple fields. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-host names. You can use any of the event fields displayed in the event inspector; the name can contain no spaces and the first letter should not be capitalized.
Fields to Sum	Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. If specified, this set of numeric fields is summed rather than aggregated, preserved, or discarded. The most common fields to sum are bytesIn and bytesOut . Note that if any of the fields listed here are also in the list of field names to aggregate, they are aggregated and not summed.
Preserve Common Fields	(Yes No) Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing No , the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events). SmartConnector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.
Time Interval	Choose a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)

Name Field	Value Field
Event Threshold	Choose a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (i.e., contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Fields to Sum	(Optional) Choose one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Processing	
Preserve Raw Event	<p>(Yes No) Some devices contain a raw event that can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field in the event inspector. This feature is disabled, by default, since using raw data increases the event size and therefore requires more database storage space.</p> <p>You can enable this by changing the Preserve Raw Event setting. If you choose Yes, the serialized representation of the "Raw Event" is sent to the ArcSight Manager and preserved in the Raw Event field.</p>

Name Field	Value Field
Turbo Mode	<p>If your configuration, reporting, and analytic usage permits, you can greatly accelerate the transfer of a sensor's event information through SmartConnectors by choosing one of two "turbo" (narrower data bandwidth) modes. The default transfer mode is called Complete, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).</p> <p>Complete mode does indeed use all the database performance advances of ArcSight v3.x.</p> <p>The first level of Turbo acceleration is called Faster and drops just additional data, while retaining all other information. The Fastest mode eliminates all but a core set of event attributes, in order to achieve the best throughput. Consider the possible effects such a restricted data set might have from a given device (for example, on reports, rules, threat resolution) before selecting it.</p> <p>The specific event attributes that apply to these modes in your enterprise are defined in the self-documented \$ARCSIGHT_HOME/config/connector/agent.properties file for the ArcSight Manager. Because these properties may have been adjusted for your needs, you should refer to this file for definitive lists.</p> <p>Only scanner SmartConnectors must run in Complete mode, to capture the additional data.</p> <p>Note: SmartConnector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to Faster cannot pass all the data possible for a SmartConnector that is set for the default of Complete.</p>

Name Field	Value Field
Enable Aggregation (in secs)	<p>Note: If you have already used this feature for setting up previous SmartConnectors, you can continue to do so. However, ArcSight recommends that you use the new Field Based Aggregation feature as a more flexible option. (Please see "Field Based Aggregation" on page 703.)</p> <p>Here is the description of the legacy "Enable Aggregation" feature, for those of you who are still using it:</p> <p>When enabled, Enable Aggregation (in seconds) aggregates two or more events on the basis of the selected time value. (Disabled, 1, 2, 3, 4, 5, 10, 30, 60)</p> <p>The aggregation is performed on one or more matches for a fixed subset of fields:</p> <ul style="list-style-type: none"> • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) <p>The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.</p>
Limit Event Processing Rate	<p>You can moderate the SmartConnector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts.</p> <p>The choices range from Disabled (no limitation on CPU demand) to 1 eps (pass just one event per second, making the smallest demand on the CPU).</p> <p>Be sure to note that this option's effect varies with the category of SmartConnector in use, as described in the SmartConnector Processing Categories table below.</p>

Name Field	Value Field
Fields to Obfuscate	Using MD5 hashing, this option allows you to specify a list of fields for obfuscation in a security event.
Store Original Time In	This parameter allows you to move the original device receipt time to a specified field if altered by the time correction.
Enable Port-Service Mapping	<p>(Disabled Enabled)</p> <p>If Enabled and one of the two fields destination port and application protocol is set, and the other is not, the one that is set is used to set the other. For example, if the destination port is 22 and application protocol is not set, then the application protocol is set to ssh.</p> <p>Default is Disabled.</p>
Uppercase User Names	<p>(Disabled Enabled)</p> <p>Default is Disabled. If set to any of the <i>enabled</i> settings, the two user name fields are automatically changed to uppercase.</p> <p>The original values are saved as follows:</p> <ul style="list-style-type: none"> • Enabled (orig to ID) saves the original values to the sourceUserID and destinationUserID fields, respectively, overwriting any values that may have been there previously. • Enabled (orig to ID or Flex) saves the original values in the same fields if they do not already contain values, or to the <code>flexString1</code> (source) and <code>flexString2</code> (destination) fields if the ID fields do contain values. • Enabled (orig to Add. Data) saves the original values to additional data fields called <code>OrigSrcUserName</code> and <code>OrigDstUserName</code>, respectively. <p>Note: The uppercase operation is typically done using the default Locale for the chosen platform. You can set this to a particular Locale by setting the <code>connector.uppercase.user.name.locale</code> property in <code>agent.properties</code> to the desired Locale (using "en_US" for U.S. English, for example).</p>
Enable User Name Splitting	<p>(Yes No) If this is set to yes and the destination user name contains commas in the event, this parameter duplicates that event. Each user name in the list is placed in one of the events.</p> <p>For example, if the destination user name in an event is "User 123, User 456", then that event is sent twice, with the destination user name set to "User 123" in the first and "User 456" in the second.</p> <p>Default is No</p>

Name Field	Value Field
Split File Name into Path and Name	<p>(Yes No) If this is set to <i>yes</i> and an event's file name field is set but its file path field is not, this parameter splits the file name into a path and a name, placing each part into appropriate fields.</p> <p>For example, if the file name field is set to <code>C:\dir\file.ext</code> and the file path is not set, then the file path is set to <code>C:\dir</code> and the file name to <code>file.ext</code>. The separator character can be either <code>\</code> or <code>/</code> as the system looks to the SmartConnector to determine its platform.</p> <p>Default is No</p>
Event Integrity Algorithm	<p>(Disabled SHA-256 SHA-1 MD5 SHA-512)</p> <p>If this is set to one of the algorithms (such as SHA-256), <i>and</i> the Preserve Raw Event parameter is Enabled, then additional event integrity internal events are generated, normally at a rate of about 1 per 50 normal events.</p> <p>The crypto signature field is <i>also</i> set in each event in the format: "<code>#seq(<i>alg</i>):digest</code>", where <i>seq</i> is a persistent event sequence number, <i>alg</i> is the message digest algorithm, and <i>digest</i> is the hexadecimal message digest.</p> <p>These extra events and the crypto signature field values can be used to verify that no events were tampered with after generation.</p> <p>Supported algorithms are: SHA-256, SHA-1, MD5, and SHA-512.</p> <p>Default is Disabled (i.e., no algorithm is applied)</p>
Generate Unparsed Events	<p>(Yes No) If set to <i>yes</i> and some incoming event data cannot be parsed (perhaps because a device has been upgraded since the SmartConnector parser was written), then a special event named "Unparsed Event" is generated. The raw event appears in the event message field.</p> <p>If set to No, the SmartConnector log files indicate the unparsed events.</p> <p>Default is No</p>
Preserve System Health Events	<p>(Yes No) If set to <i>yes</i>, internal system health events are preserved.</p> <p>SmartConnectors generate system health events that provide information about the systems on which they are installed (for example, disk usage, network memory, JVM memory, percentage of processing of CPU memory usage, and so forth). By default, these events are not retained or passed on to ArcSight destinations and, therefore, not available for viewing. Setting this option to <i>yes</i> makes them available in the Console.</p>

Name Field	Value Field
Enable Device Status Monitoring (in millisec)	<p>(<NumberOfMilliseconds> -1 (disabled))</p> <p>If set to a <NumberOfMilliseconds>, the selected SmartConnector generates internal events periodically 1 minute (60000 milliseconds) or greater with the status of the devices for which the connector is receiving normal events. These events have the name "Connector Device Status."</p> <p>Enabling periodic device status monitoring events helps monitor both the SmartConnector and device uptime.</p> <p>Device status monitoring events include this information, if available:</p> <ul style="list-style-type: none"> • Event name (Connector Device Status) • Vendor and Product information • Source Address and Host Name • Zone • Last event received • Total number of events for the device since the connector started • Event count since last call <p>Device status monitoring events can be set to generate every 1 minute (60000 milliseconds), or less frequently (i.e., a greater number of milliseconds than the minimum).</p> <p>If you specify less than 60000, you get a warning in the log that the minimum is 60000 milliseconds (1 minute) and the system uses the minimum.</p> <p>If you enter a non-number in the field, it generates an error in the log that the value could not be parsed. In this case, the feature is disabled (and logged as such).</p> <p>In such cases, there is no indication on the Console that anything went wrong because there is no way for the Connector to convey that error.</p>
Payload Sampling (when available)	<p>Some SmartConnectors use Payload sampling to send a portion of packet payload (as opposed to the complete payload) along with the original event. This portion is retrieved using the on-demand payload retrieval in the event inspector.</p>
Maximum Length	<p>You can configure the maximum length of the payload sample using the following values:</p> <ul style="list-style-type: none"> • Discard • 128 bytes • 256 bytes • 512 bytes • 1 Kbyte <p>When the Discard option is chosen, no payload sample is sent inside the original event.</p>
Mask Non-printable Characters	<p>This feature allows you to mask the non-printable characters in the payload sample.</p>

SmartConnector Processing Categories

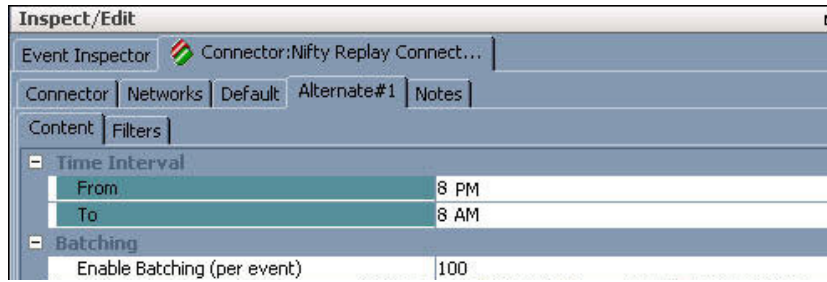
The following table shows the SmartConnector Processing Categories

SmartConnector Type	Effects of Limited Usage
Syslog connectors	Due to the nature of UDP (the transport protocol used by Syslog), these connectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache may fill and the operating system drop UDP messages. Note that ArcSight does not recommend using the Limit CPU Usage option with these connectors because of this possibility of event loss.
SNMP connectors	Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they potentially lose events. SNMP is also UDP-based and has the same issues as Syslog.
Database connectors	Since connectors "follow" the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. On the other hand, note that no events are lost, unless the database tables are truncated. After the event burst is over, the connector may eventually catch up with the database if the event rate does not exceed the configured limit.
File connectors	Similar to database connectors, file-based connectors "follow" files, so limiting their event rates also causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. Similarly, the connectors may catch up if the event rate does not exceed the configured rate.
Proprietary API connectors	These connectors' behavior depends on the particular API, (for example, OPSEC behaves differently than PostOffice and RDEP). But in most cases, there is no event loss unless the internal buffers and queues of the API implementation fill up. Therefore, these connectors work much like database or file connectors.

SmartConnector Time Interval Options

This time interval applies to the Alternate Settings and it specifies when the alternate settings must be used by the SmartConnector. For example, if you want to cache the events during the day and send everything at night, you can configure the Transport Mode

to cache in the default configuration and configure the Transport Mode to normal in the Alternate Settings, then you would set the time interval from 8PM to 8AM (next day).



- **"From:"** Specifies the starting time to apply the Alternate settings.
- **"To:"** Specifies the ending time for the Alternate settings, when it reverts to the default settings). If this is less than the From setting, the value is interpreted as the next day. For example, a setting from 8PM to 8AM is interpreted as starting at 8PM and ending at 8AM the following day.

To save configuration changes to the SmartConnector, click **OK**.

Managing SmartConnector Filter Conditions

SmartConnector can function as a filtering tool between devices and the ArcSight Manager, using filtering conditions. Filtering conditions are set with a combination of AND or OR statements and data field values. Extraneous events are filtered out to minimize the number of events sent to the ArcSight Manager and analyzed in the ESM Console.

Creating SmartConnector Filters

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the Default | Filter tab, right-click and choose **Add new condition**.
- 4 In the Filter Condition dialog box, select a data field from the drop-down menu. (See ["Using Field Sets" on page 855](#) under ["Common Conditions Editor \(CCE\)" on page 846](#), especially ["Condition Tree Command Buttons" on page 848](#) and ["Condition Tree Context Menu Commands" on page 850](#).)
- 5 Choose logic operators from the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

Adding SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click an ArcSight SmartConnector and choose **Configure**.
- 3 In the **Default: Filters** tab, right-click the **if** folder and choose **Add OR** condition to create an OR condition, or right-click the existing filter condition and choose **Add AND condition** to create an AND condition.
- 4 In the Filter Condition dialog box, choose a data field on the drop-down menu.

- 5 Choose logic operators on the drop-down menu.
- 6 Type a value in the last text field.
- 7 Click **OK**.

Deleting SmartConnector Filter Conditions

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector and choose **Configure**.
- 3 In the Filtering section on the Advanced tab, right-click a condition and choose **Delete condition**.

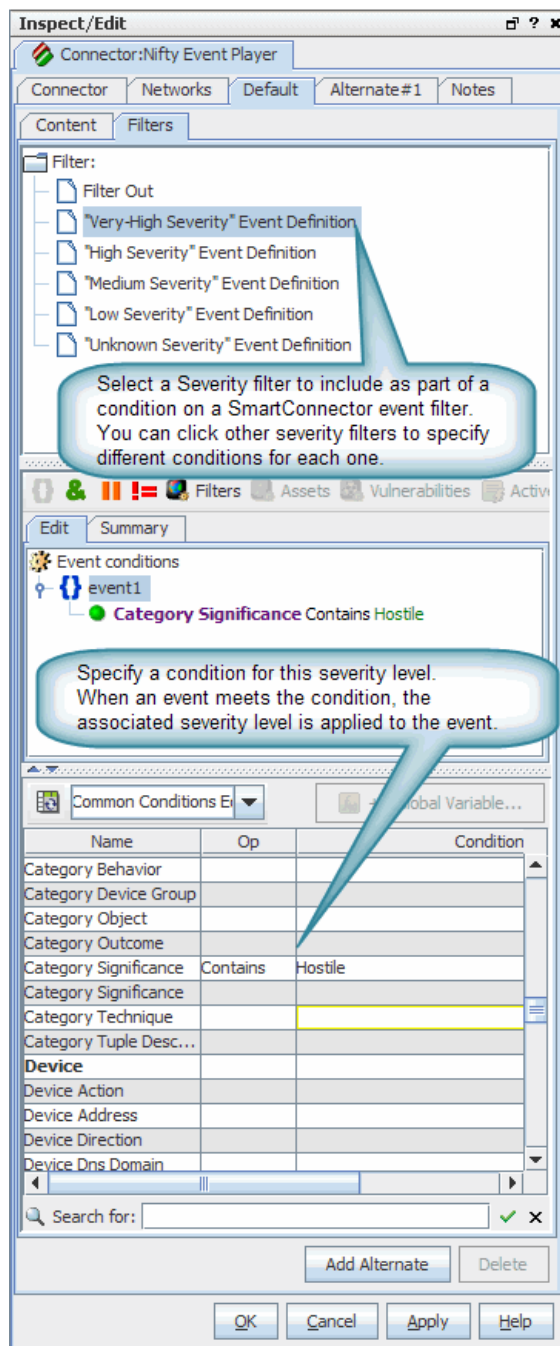
Setting Special Severity Levels

You can customize or conditionalize the event-severity levels reported by SmartConnectors. Customizing means pre-setting a given SmartConnector's filter to one specific severity level; conditionalizing is essentially the same, but with the addition of a filter condition to determine when the pre-set severity level is reported.

Configuring a Conditional or Custom Severity Level

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the appropriate SmartConnector and choose **Configure**.
- 3 In the Connector Configuration Editor, select the **Connector: Default: Filters** tab.
- 4 In the Filters tab, select a severity level.

- 5 In the Filter Condition dialog box choose a field, a logical operator, and enter a value for the condition.



- 6 Click **OK** in the Filter Condition dialog box and **Apply** or **OK** in the Connector Configuration Editor.

In the example pictured here, we selected the "Very-High Severity" filter and defined a condition in which Category Significance contains "Hostile". When this condition is met, the severity of the event becomes "Very-High."

For more information, see ["Managing SmartConnector Filter Conditions"](#) on page 712.

Sending Model Mappings to SmartConnectors

Updates to network model mappings are sent automatically from the ArcSight Manager to SmartConnectors within heartbeat messages. The heartbeat messages themselves are sent on an interval which can be anywhere from every 5 seconds to every 10 minutes, but network model mappings are included in the messages only when there are updates to the model.



The interval on which information is exchanged between the Manager and SmartConnectors is determined by the Heartbeat Frequency setting on each Connector. (See information on [“Heartbeat Frequency” on page 700](#) in default content tab configuration fields under [“Selecting and Setting SmartConnector Parameters” on page 695](#).)

If you have made several configuration updates to the network model on the Manager and would like these changes to take effect immediately on the SmartConnectors without waiting for the next automatic refresh, you can use the following command to send the update information to a selected Connector.

Sending Model Mappings to a Connector

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to update and choose **Send Model mappings now**.

This sends information about the current network model mappings from the Manager to the selected Connector. It forces a comprehensive refresh of the zone mappings and network model information on the Connector.

Sending Control Commands to SmartConnectors

From the Console you can issue basic event-flow-control commands to SmartConnectors, get the operational status of a SmartConnector, or issue control commands to network devices through their SmartConnectors. This topic discusses the first two points. To author rule-driven device-command responses to events, please see [“Creating Rule Actions” on page 451](#).

Getting Status Reports

You can see a SmartConnector's current operational state at any time.

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command>Status>Get Status**.
- 3 In the Connector Status window you can see a readout of all the connector's current parameters.

Sending Flow-Control Commands

- 1 Choose the **Connectors** resource tree in the Navigator panel.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector, choose **Send Command**, and one of the following menu options described below.


- 3 The Console's status bar shows a confirmation message when the flow control option takes effect.



Note

- Commands available on this menu vary depending on which SmartConnectors you are using. The standard set of commands is described here.
- Because there is no local cache, events that occur while a connector is stopped or paused are not retained.
- If a SmartConnector runs out of disk space, it can lose its ability to track events.
- The **Terminate** command should only be used in very special circumstances as it **kills all** SmartConnector processes.
- See [“Creating Rule Actions” on page 451](#) for a description of the rule-based automated alternative for giving SmartConnector commands.

Command	Description
Status Category	
Get Status	Provides a full report on the selected SmartConnector's current operational state.
Get Device Status	Provides the status of the device that reports to the SmartConnector. (Currently only available for the CiscoIDS/IPS SmartConnector.)
Connector Process Category	
Restart	Restarts a running SmartConnector. Caution: Once a connector is terminated, Console commands cannot access it. Therefore, a "restart" works only on a connector that is currently running. Sending a restart command to a running connector terminates and restarts the connector.
Terminate	Shuts down the SmartConnector and all processes the SmartConnector started. Caution: Once a connector is terminated, Console commands (including Connector Process > Restart) cannot access it. The connector must be restarted manually from the machine on which it is installed.
Event Flow Category	
Pause	Stops the SmartConnector from sending events to the ArcSight Manager. Note: Events received from the target device are saved in the connector cache (even though the connector is in Pause state).
Stop	Stops the SmartConnector from sending events to the ArcSight Manager. Caution: A Stop command causes the SmartConnector to drop all events, including events stored in the connector cache.
Start	Prompts the SmartConnector (previously in Stop or Pause state) to start sending events to the ArcSight Manager.

Command	Description
Network Category	
Flush Name Resolver Cache	Clears cache for Network name resolver.
Upgrade Category	
Upgrade	<p>Launches a Command Parameters dialog for remote upgrade to newer versions of ArcSight SmartConnectors for managed assets.</p> <p>Provide the version number of the connector to which you want to upgrade and a wait time to verify that the upgrade completed successfully. (If the upgrade is not successful, the system performs an automatic rollback to the previous version of the connector.)</p> <p>Click OK to start the upgrade.</p> <p>See "Upgrading SmartConnectors" on page 726 for prerequisites for the upgrade process and detailed information on how to upgrade Connectors.</p>
Rollback Upgrade	<p>Launches a Command Parameters dialog for remote rollback of connector version to a specified previous version. See "Upgrading SmartConnectors" on page 726 for complete information.</p>
Adjust Category	
Rename Mismatched Override Files	<p>Enables you to remotely rename an connector parser override file whose version stamp no longer matches the parser that it was intended to override. Renaming it appends ".1" (or 2, or 3, if earlier numbers are in use), which stops the file from being used.</p> <p>The first parameter is a regular expression you can specify to match specific override files (or blank, the default, for all). The second parameter is a boolean where true, the default, means restart the connector if any files are renamed.</p>
 <p>Tech Support commands are provided for use primarily by ArcSight Customer Support. Brief descriptions of these Tech Support commands are provided for informational purposes, but these commands are not intended for use by ArcSight customers except as instructed by ArcSight Customer Support.</p>	

Command	Description
Tech Support Category	
Get Support Info	Gets logs and other feedback on connectors.
Get 'agent.properties'	Shows the list of properties for the selected connector.
Get Upgrade Logs	Get upgrade logs on connectors.
Get 'agent.wrapper.conf'	Shows the wrapper configuration for the selected connector.
Get Configuration XML File	Shows the XML configuration file for the selected connector.
Get Thread Dump	Gets one thread dump for the selected connector.

Command	Description
Get Two Thread Dumps...	Gets two thread dumps for the selected connector spaced by the time interval specified. By comparing both thread dumps, ArcSight Customer Support can troubleshoot connectors with threads that are hanging for unknown reasons.
Get Heap Dump	This generates a heap dump, if possible, which can be useful to ArcSight in some situations to analyze problems. The destination ID is used as part of the file name, the file is placed in the same directory as the connector's logs, and normally only 10 such files are kept.
Get last N lines of 'agent.log'...	Shows an excerpt from the connector log file based on the number of lines you specify. The default is 500 lines.
Get System Properties	Shows system properties for the selected connector, including details on variables such as Java runtime name, Java virtual machine (VM) version, operating system name, paths for various Java components, paths for ArcSight Home, user directories, user home, and so forth.
Enable Event Flow Tracing...	Allows you to specify a component and fields to log for initiating an event flow trace. Component and field names must be provided per appropriate syntax. The component should be chosen from the components listed in the Get Status results.
Disable Event Flow Tracing...	Disables event flow tracing on the selected component.
Get Event Flow Tracing Log	When tracing is enabled on the selected connector, the connector logs data about events it receives.
DNS Test	This command takes one parameter, which is either a host name to resolve or an IP address to reverse resolve. This is useful to see what results would normally be expected for the name resolver component of the connector, since it uses the same mechanism to do the lookup as the name resolver uses.
Enable Map File Logging	Directs the AgentNATProcessor component, which processes map files for each event, to log what it is doing for each event. By default the last 100 events are logged.
Disable Map File Logging	Directs the AgentNATProcessor to stop logging.
Get Collected Map File Logging	Gets the collected log messages for the most recent events (100, by default), which may help debug problems with why a map file is not operating as expected.



The following commands provide access to SmartConnector component mapping and event categorization for advanced users.

Command	Description
Mapping Category	

Command	Description
Get Additional Data Names	<p>Returns a list of additional data names seen for each device vendor/product combination since the connector started running. For example:</p> <pre>Additional Data Names Seen: Generic (no vendor/product): test1 [3 times] test11 test13 [2 times] Vendor/product [vend/prod]: test1 test10 [6 times]</pre> <p>By default, the command limits the list to show only the most recent 100 device vendor/product combinations and the most recent 100 names for each.</p> <p>Tip: You can change this limit by editing the SmartConnector property <code>agent.additionaldata.mapper.track.max.names</code> in the file <code>\$ARCSIGHT_HOME/ArcSightSmartAgents/current/user/agent/agent.properties</code> on the machine where the connector is installed. In most cases we recommend keeping the defaults. If you change a property setting such as this, restart the connector.</p> <p>If a data name is not a string, its data type is displayed in the list. If the connector saw an additional data name more than once, the command output indicates the number of times the name was seen.</p>
Map Additional Data Name...	Brings up a dialog where you can map an additional data name for the selected connector.

Name	Value
Device vendor	
Device product	
Additional data name	
ArcSight field	

Command	Description
	<p>For a generic mapping, you can leave the Device vendor and Device product fields blank. For a specific mapping, fill in these fields with the appropriate vendor and product names.</p> <p>Typically, the Additional data name is one of the names shown in the Get Additional Data Names output (but can be another name not on that list).</p> <p>The ArcSight field must be a valid ArcSight event field.</p> <p>Click OK to create the mapping.</p> <p>Here is an example of the command output for a successful generic mapping:</p> <pre>Successfully mapped additional data name [test11] to event field [message] for vendor/product []</pre> <p>A successful device vendor/product-specific mapping returns output similar to this:</p> <pre>Successfully mapped additional data name [test10] to event field [message] for vendor/product [vend/prod]</pre> <p>If the additional data name has not been seen, the name is still mapped, but with a warning like this:</p> <pre>Successfully mapped additional data name [foo] to event field [deviceCustomString1] for vendor/product [vend/prod] (note that additional data name [foo] has not been seen for vendor/product [vend/prod])</pre> <p>If the ArcSight field is not valid, the error returned is similar to this:</p> <pre>Failed to map additional data name [bar] to event field [messages] for vendor/product [vend/prod] (event field [messages] is unknown)</pre>
Unmap Additional Data Name...	Brings up a dialog where you can unmap an additional data name for the selected connector.

Name	Value
Device vendor	
Device product	
Additional data name	

Command	Description
	<p>To remove a generic mapping, you can leave the Device vendor and Device product fields blank. To remove a specific mapping, fill in these fields with the appropriate vendor and product names. The additional data name should be one that was previously mapped for the specified device vendor and product combination.</p> <p>Click OK to unmap the data name.</p> <p>Here is an example of the command output for a successful generic unmapping:</p> <pre>Successfully unmapped additional data name [test11] for vendor/product []</pre> <p>A successful device vendor/product-specific unmapping returns output similar to this:</p> <pre>Successfully unmapped additional data name [foo] for vendor/product [vend/prod]</pre> <p>If the specified additional data name was not previously mapped, the output looks like this:</p> <pre>Failed to unmap additional data name [foo] for vendor/product [vend/prod] (not previously mapped)</pre> <p>Notes:</p> <ul style="list-style-type: none"> • One additional data name can be mapped to more than one ArcSight field for the same device vendor/product combination, and in this case unmapping it unmaps it from all ArcSight fields for that device vendor/product. This is an unlikely scenario, however. • The converse case, where multiple additional data names are mapped to the same ArcSight field for the same device vendor/product combination, results in the last mapping taking precedence over any previous mappings to that ArcSight field for that device vendor/product. No warning is generated in this case.
Categorizer mapper Category	
Reload custom categorizations	<p>There are several ways to set event category information for events. The least common of these is to store custom categorization files (organized by vendor and product) on the connector machine in the <code>user/agent/aup/acp/categorizer/current directory</code> (or the <code>user/agent/acp/categorizer/current directory</code>).</p> <p>If such categorization files exist and have been changed, this command reloads them without restarting the connector.</p>

Command	Description
Reload custom map files	<p>Rescans and reloads map files in user/agent/map directory on the machine where the connector is installed.</p> <p>The map files are named in the form <code>map.n.properties</code>, where <code>n</code> is a number starting with 0. Use this command to immediately apply the latest changes. Not all connector setups include custom map files.</p> <p>Caution: Map files are created on some connector machines to fulfill specific needs. If you are not familiar with the categorizer/mapping setup of an environment, we recommend that you do not use these commands.</p>
Reload external map files	<p>Re-scans and reloads external map files in the <code>user/agent/extmap</code> directory on the machine where the connector is installed.</p> <p>The map files are named in the form <code>extmap.n.properties</code>, where <code>n</code> is a number starting with 0. Use this command to immediately apply the latest changes. Not all connector setups include custom external map files.</p> <p>Caution: External map files are created on some connector machines to fulfill specific needs. If you are not familiar with them, we recommend that you do not use Reload commands.</p>

Managing SmartConnector Groups

You can best manage ArcSight SmartConnectors when you organize them into groups. You'll find all uncategorized SmartConnectors in the Unassigned group.

You can move or copy groups and SmartConnectors into other groups in the Connectors resource tree by using drag-and-drop. If a group is deleted, the SmartConnectors within that group are also deleted.

You should not delete a Connector resource at the ESM Console, unless the corresponding SmartConnector is first stopped. If the SmartConnector on the device is running and its Connector resource is deleted, the SmartConnector cannot send events to the ArcSight Manager, causing the SmartConnector to start caching events and eventually dropping these events.

Creating SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

Renaming SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Rename**.

- 3 In the "name" text field, rename the group.
- 4 Press **Enter**.

Editing SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Edit Group**.
- 3 In the Group Editor, edit the **Name** and **Description** text field.
- 4 Click **OK**.

Moving or Copying SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting SmartConnector Groups

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

Managing SmartConnector Resources

This topic describes how to do basic resource management for SmartConnectors.

Moving or Copying a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, navigate to a group and drag and drop it into another group.
- 3 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether it be the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting a SmartConnector Group

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click a group and choose **Delete Group**.
- 3 In the dialog box, click **Yes**.

The SmartConnector's resource is deleted from the ArcSight database and the ArcSight Manager no longer recognizes this resource.

Importing and Exporting SmartConnector Configurations

As a part of Managing SmartConnectors, you may want to share configurations among several instances of the same or a similar connector.

You can import and export SmartConnector configurations as a means of sharing custom configurations among several connectors on the same or multiple Managers. Rather than redefining a complex configuration on each connector, you can export the configuration as an XML file and then import it into connectors that share some or all of its configuration settings. An override feature allows you to make changes to any of the parameter values upon import.

Importing a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector into which you want to import a new configuration and choose **Import Connector Configuration...**

This brings up a file browser where you can select the file to import.

- 3 In the file browser, navigate to and select the **.xml** file that contains the connector configuration, and click **Open**.



SmartConnector configurations must be saved and imported as XML files.

This brings up a dialog showing original and proposed new configuration settings for the selected connector, with an option to override any of the proposed new values. (Click **Show** to show the details of the import or **Hide** to hide them.)

- On the Import Connector Configuration dialog, review the import information and override any values that you do not want to import.

This dialog shows original values for the selected connector configuration and new values applied upon import. You can override any of the settings you do not want to import by either keeping the parameter value in the original configuration or defining a new value.

For example, you even can limit the import to only filters by keeping all values in the original configuration and choosing to override only the filter values with the imported

values as is detailed in SmartConnector Filters. (Scroll down to the Filters section at the end of the Import dialog to see the filters.)

Before Import, the Import Connector Configuration dialog shows current value, new value, and override option for each aspect of SmartConnector configuration.

You can accept all new values or override the import by keeping some of the original values.

Name	Current Value	New Value	Override
Batching			
Enable Batching...	100	100	---
Enable Batching...	5	5	---
Batch By	Time Based	Time Based	---
Time Correction			
Use Connector ...	No	No	---
Enable Device T...	0	0	---
Enable Connect...	0	0	---
Set Device Time...	Disabled	Disabled	---
Device Time Auto-Correction			
Future Threshold	-1	-1	---
Past Threshold	-1	-1	---
Device List	(ALL)	(ALL)	---
Time Checking			
Future Threshold	300	300	---
Past Threshold	3600	3600	---
Frequency	60	60	---
Cache			
Cache Size	1GB	1GB	---
Notification Thr...	10000	10000	---
Notification Fre...	10 min	10 min	---
Network			
Heartbeat Freq...	10 sec	10 sec	---
Enable Name R...	Yes	Yes	---
Name Resolutio...	Yes	Yes	---
Name Resolutio...	Yes	Yes	---
Clear Host Nam...	Yes	Yes	---
Limit Bandwidth...	Disabled	Disabled	---
Transport Mode	Normal	Normal	---
Address-Based ...	Yes	Yes	---
Address-Based ...			

- When you are satisfied with the settings to import and overrides (if any), click **OK** to import the configuration.

Exporting a SmartConnector Configuration

- 1 In the Navigator panel, choose the **Connectors** resource tree.
- 2 In the Connectors resource tree, right-click the ArcSight SmartConnector you want to export, and choose **Export Connector Configuration As...**

This brings up a file browser where you can navigate to the location where you want to save the configuration as an XML file.

- 3 In the file browser, navigate to and select the location where you want to save the configuration, provide a name for the file, and click **Save**.



Tip

SmartConnector configurations must be saved as XML files.

SmartConnector Filters

You can import and export only the filters associated with SmartConnectors as a part of an import or export on a SmartConnector.

- To export a SmartConnector filter, export the connector that uses the filter (as described in the previous topic on exporting a SmartConnector configuration).
- To import a SmartConnector filter into another connector, start by selecting in the Navigator the SmartConnector to which you want to add a new filter. Follow the steps to import the connector that includes the filter you want to import (as described in the topic on importing a SmartConnector configuration). On the Import Connector Configuration dialog, limit the import to only the filter(s) you want by keeping all values in the original configuration and choosing to override only the filter values with the import. (Scroll down to the Filters section at the end of the Import dialog to see the SmartConnector Filters.) When you have the new, imported filter values selected to override those in the original connector, complete the import by clicking **OK** on the Import Connector Configuration dialog. This adds the imported filter(s) to the original SmartConnector.

Upgrading SmartConnectors

You can centrally manage and configure SmartConnectors and update them remotely. Use the Upgrade command on the ESM Console to upgrade to newer versions of ArcSight SmartConnector software for managed devices. Use the Rollback command to revert to a previous version on an upgraded connector.

The Upgrade command lets you launch, manage, and review the status of upgrades for all SmartConnectors. A fail-over mechanism launches SmartConnectors with previous versions if upgrades fail. All communication and upgrade processes between components (Console, Manager, connectors) take place over secure connections.

The ESM Console reflects current version information for all of your SmartConnectors.



For this release, SmartConnector remote upgrade is supported for connectors installed on Linux, Solaris, and Windows platforms only.

Overview of the Upgrade Process

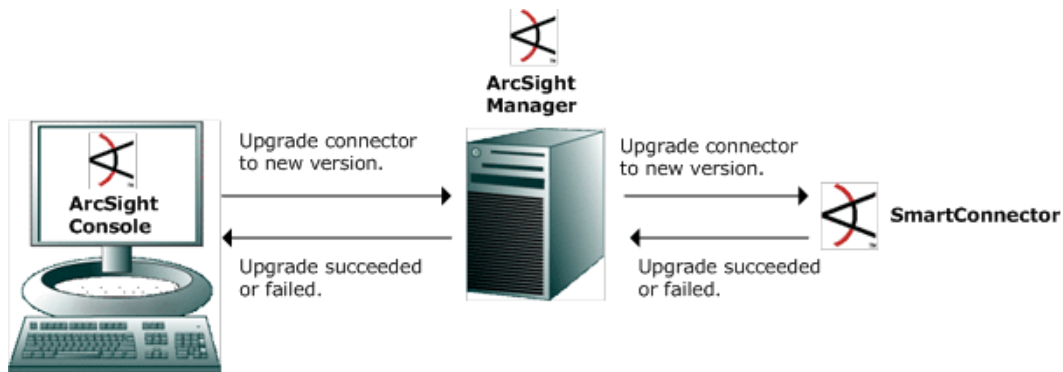
- 1 As an ArcSight customer, you receive e-mail notifications about new connector releases from ArcSight Customer Support.
- 2 ArcSight administrators download the latest releases to the ArcSight Manager where they are available for SmartConnector upgrades.



SmartConnector "upgrade" version files are delivered as ArcSight Update packs (**.aup**) files. (ArcSight update packs are compressed file sets, similar to **.zips**.) The administrator copies the **.aup** file to ARCSIGHT_HOME/updates/ onto a running Arcsight Manager. The Manager automatically unzips the **.aup** file and copies its contents to ARCSIGHT_HOME/repository/.

- 3 From the ESM Console, administrators select connectors to be upgraded (one at a time) and launch the upgrade command for each of them.

- 4 Upon receipt of the upgrade command, the selected connectors upgrade themselves, restart, and send upgrade results (success or failure) back to the ESM Console through the ArcSight Manager.
 - ◆ If the upgrade is successful, the new connector starts and reports on successful upgrade status. (The upgraded connector runs in the same home directory as the old connector.)
 - ◆ If the upgraded connector fails to start, the original connector restarts automatically as a fail-over measure. (This is essentially an automatic rollback, and re-start.)



Tip

Tips on Monitoring SmartConnector Upgrade Status

SmartConnectors automatically determine their upgrade status when they start.

- When a connector starts up, it determines whether it is upgraded.
- If so, it waits for a configurable time interval for events from the monitored device to be processed.
- If, after that time interval, events have been processed, the SmartConnector is deemed up and running. The ESM Console indicates that the upgrade for that connector is a success and the newer connector version is reflected.



Note

Notes on SmartConnector Upgrade Procedure

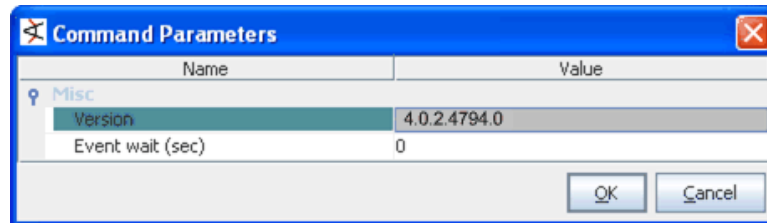
- When upgrading SmartConnectors, be sure to download current versions of the connector Configuration Guides from the ArcSight Customer Support Web site. New or revised information is provided in these guides as appropriate per each release of SmartConnectors. (To check version numbers on your current connectors, see ["Getting Status and Versions on Installed SmartConnectors"](#) on page 729.)
- You need administrative permissions to upgrade connectors.
- Newer versions of the connectors you want must be available on the Manager to which you are connected.
- The option for remote upgrade is available only on SmartConnectors of version 4.0.2.xxxx.0 or newer. Earlier versions of Connectors (or Agents) must be upgraded manually by installing a newer version of the connector.
- As a prerequisite to upgrading connectors, both the ArcSight Manager and the connector must be running.

The **Upgrade** SmartConnectors command is available as one of several SmartConnector control commands.

Upgrading SmartConnectors

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Upgrade**.

This launches a Command Parameters dialog.



- 3 Provide the following information in the dialog.
 - **Version** - The Version field provides a drop-down menu showing the connector versions available on this Manager. Choose the Version number of the connector to which you want to upgrade.
 - **Event wait (sec)** - Number of seconds the upgrade process waits for the first event from the device after the new, upgraded connector is started. If no events are received from the device within the specified time frame, the upgrade is considered "failed" and the old connector is launched.

This optional check is an additional safeguard against upgrade failures. For example, the connector binaries may have been upgraded successfully, but the new version may have problems communicating with the device. In that case, this check assumes that the upgrade failed and bring back the old connector.

If the **Event wait (sec)** value is **0** (the default), then the upgrade does not perform this check.

- 4 Click **OK** to close the dialog and start the upgrade.

As the upgrade proceeds, the connector shows as "down" and then "running" again in the resource tree. Status messages on the ESM Console indicate whether the upgrade succeeds or fails. You can check the logs for the connector to determine if the upgrade succeeded. (**Send Command > Tech Support > Get 'agent.properties' and Get Upgrade Logs.**)

Rolling back to a Previous Version



Notes on SmartConnector Rollback Procedure

- You need administrative permissions to roll back Connectors.
- The option for SmartConnector rollback is available only on SmartConnectors of version 4.0.2.xxxx.0 or newer that have been previously upgraded.
- Rollback automatically reinstates the most recent version prior to the currently installed version. You cannot do a remote rollback on a connector to other than the previously installed version. (For example, if you start with a connector of version 4.0.2.4793, upgrade to 4.0.2.4794, then upgrade again to 4.0.2.4795, a remote rollback at this point re-installs/starts connector version 4.0.2.4794. If you want to roll back to an earlier version, do it manually.)

You can roll back an upgraded connector to the previous version with the Rollback command.

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Upgrade > Rollback**.

As the rollback proceeds, the connector shows as "down" and then "running" again in the resource tree. You can check the logs for the connector to determine if the rollback succeeded. (**Send Command > Tech Support > Get 'agent.properties'** and **Get Upgrade Logs**.)

Troubleshooting

If an upgrade or rollback fails, you can review the related logs. Choose **Send Command > Tech Support > Get Upgrade Logs** from the ESM Console menus.

You can also use the Send Logs wizard to collect and compress logs, which you can then attach to an email, if desired.

Getting Status and Versions on Installed SmartConnectors

Before or after you upgrade a SmartConnectors, you may want to check version numbers of currently installed connectors or get other status information. There are several ways to get information on currently installed connectors (including various control commands, channels, dashboards). Two of these are highlighted here as easy ways to get connector version information.

Getting Status on a SmartConnector

- 1 Choose the **Connectors** resource in the Navigator panel.
- 2 In the Connectors resource tree, select the connector you want to upgrade, right-click to bring up the context menu, and choose **Send Command > Status > Get Status**.

The Status information on a connector includes "Agent Version" near the top of the message window. Here is an example snip-it of the Get Status command results for a Test Alert connector, Version 4.0.2.4793.0:

```
Status Generated: Wed Mar 07 13:20:09 PST 2007
Memory Usage: 65Mb out of 253Mb
```

```
Agent Content Version.....2007-03-01-09-02-05_4793
Agent Type.....testalertng
Agent Version.....4.0.2.4793.0
CommandResponses Processed.....1097
Current Max Rate.....22
Event rate LTC.....Wed Mar 07 13:18:42 PST 2007
Events Processed.....24003
```

SmartConnector Dashboards

Choose **Dashboards** from the Navigator panel, and expand the folders to find various dashboards. To view a dashboard, right-click it and choose **Show Dashboard**.

You can find some these SmartConnector dashboards in /Dashboards/Shared/All Dashboards/ArcSight Administration/Connector/:

- Connector and Device - Heads Up Display
- Connector Status

Modeling the Network

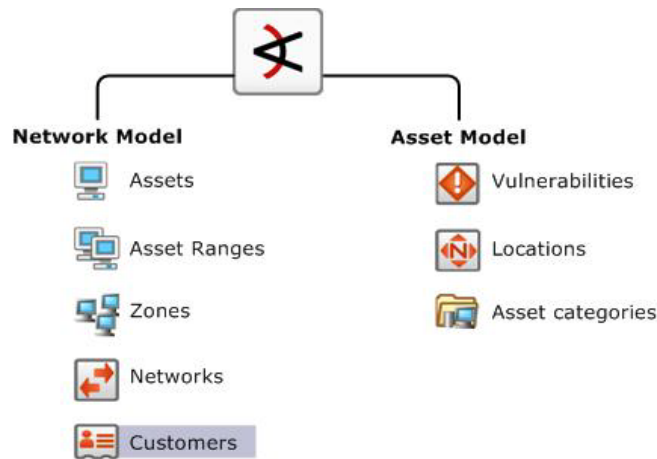
The following topics explain how to model your network and configure various aspects of the network model (assets, locations, zones, and so on), and how to manage customer accounts (if applicable).

- [“About the Network Model” on page 731](#)
- [“Populating the Network Model with Assets” on page 740](#)
- [“Populating the Network Model Using the Wizard” on page 744](#)
- [“Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories” on page 753](#)
- [“Managing Assets” on page 754](#)
- [“Managing Vulnerabilities” on page 758](#)
- [“Managing Zones” on page 763](#)
- [“Managing Networks” on page 764](#)
- [“Managing Asset Categories” on page 764](#)
- [“Managing Locations” on page 765](#)
- [“Managing Customers” on page 766](#)

About the Network Model

ArcSight operates on a data model that enables you to build a business-oriented view of data derived from physical information systems. These distinctions help to clearly identify the events in your network, and provide more layers of detail to correlation capabilities.

Modeling your network and the assets it includes is part of setup and ongoing maintenance.



The network model consists of the asset model and the network model, which, combined, facilitate building detailed correlation criteria. All of the Network Modeling resources, except Customers, are available as part of the Assets resource.

- The [“Network Model” on page 732](#) is a representation of the nodes on your network and certain characteristics of the network itself.
- The [“Asset Model” on page 738](#) describes attributes of the assets themselves for different purposes.

The following topics provide a conceptual overview of network modeling, and describe how to configure, update, and maintain a network model.



- For a description of techniques for dealing with hundreds of thousands of assets, see [“Asset Scalability” on page 757](#).
- For a more detailed conceptual overview, information about configuring each type of asset and modeling your network, refer to the *ESM 101* chapter on the “Network Model.”

Network Model

The network model is a representation of the nodes on your network and certain characteristics of the network itself.

Before you can make an informed decision about what to do about a particular event, it helps to know something about the event's source and destination. Is the source a previous attacker, does it come from a hostile region of the world, or is it a trusted server that has suddenly become the source of a hostile attack? Does the destination expose relevant vulnerabilities, does it host critical applications, or is it a known server of forbidden services?

This kind of information is captured by modeling the assets on your network and particular pertinent attributes of the network. The network model represents information for individual assets and whole zones.

For critical assets on the protected network, network modeling captures important facts that help inform your decisions, such as:

- All open ports

- The operating system running on that host
- Known vulnerabilities that might be exposed
- Applications present
- The missions these applications support and their criticality to your operation

For less critical assets, such as a particular block of addresses on the Internet, it may be sufficient to just know general information about them, such as the country in which those assets reside.

The Network Model consists of the following resources. All of these resources, except Customers, are part of the Assets resource.

- [“Assets” on page 733](#) represent individual nodes on the network, such as servers, routers, and laptops.
- [“Asset Ranges” on page 736](#) represent a set of network nodes addressable as a contiguous block of IP addresses.
- [“Zones” on page 736](#) represent portions of the network itself that are characterized by a contiguous block of addresses.
- [“Networks” on page 737](#) provide an additional distinction to differentiate between two private address spaces with overlapping IP address ranges.
- **Customers** describe the internal or external cost centers or separate business units associated with networks, if applicable to your business environment. Customer tagging is a feature developed mainly to support Managed Security Service Provider (MSSP) environments, although it can also be used by private organizations to denote cost centers, internal groups, or subdivisions. The Customer designation keeps event traffic from multiple cost centers and/or business units clearly identified and separate. A customer can be thought of as the “owner” of an event, rather than the source or target of an event. For more about Customers, see [“Managing Customers” on page 766](#).

Assets

An asset is any network endpoint with an IP address, MAC address, host name, or external ID. For network modeling purposes, an asset is any endpoint you consider significant enough to characterize with details that make correlation and reporting more meaningful.





Auto-Created Assets

ESM automatically creates assets to model the network nodes that host ArcSight components (Managers, Databases, Consoles, and SmartConnectors). It also automatically creates assets for events received from device endpoints on your network that do not already have assets modeled in ArcSight, and, if applicable, for assets arriving from scan reports sent by vulnerability scanners via scanner SmartConnectors. This auto-asset creation feature could require configuration, depending on the assets reporting to the Manager.

As a configuration option, you can also configure it to create assets for devices reporting through SmartConnectors.

Auto-Created Assets for Components

The system automatically creates assets to model the network nodes that host components. These assets do not contain vulnerability information, and are used for system administration.

Component		
Manager		An asset for the Manager is added (if needed) every time the Manager service starts.
ESM database		An asset for the ESM database is added (if needed) every time the Manager starts.
ESM Consoles		An asset is added for each ESM Console the first time it connects with the Manager.
SmartConnectors		<p>An asset is created for SmartConnectors only when the SmartConnector begins reporting base events from the device it represents. A Connector can be successfully added to the Manager, but until it starts reporting events from the device it represents, an asset cannot be created for it in the Asset Model.</p> <p>It creates assets differently for SmartConnectors in static zones and those in dynamic zones. For more about static and dynamic zones, see “Dynamic and Static Zones” on page 736.</p> <p>For details about creating assets for SmartConnectors, see “Creating Assets for SmartConnectors” on page 803.</p>

Devices Discovered by a Vulnerability Scanner

The system also imports asset and vulnerability information from vulnerability scanner reports generated by products such as Nessus, FoundStone, and ISS Internet Scanner. Asset information is passed to the Manager via the scanner SmartConnector appropriate for your vulnerability scanner product based on IP address, MAC address, and host name.

Updated vulnerability information is added to existing assets with matching identifiers. If a matching asset does not already exist, the system creates one.

The system creates assets from vulnerability scan reports differently for dynamic and static zones. For more about dynamic and static zones, see [“Dynamic and Static Zones”](#) on page 736.

For details about how the system creates assets from vulnerability scans, see [“Creating Assets from a Vulnerability Scan Report”](#) on page 802.



Scanner reports list only information received through the scanner, whereas Asset Editors include the full list of both scanner data and vulnerability mappings stored in the system. So, the Editors might show more or different information than that shown in scanner reports.

Devices Reporting Through SmartConnectors

The administrator can configure creating an asset for each device that reports to that SmartConnector based on IP address, MAC address, and host name when the Manager receives events from SmartConnectors.

This feature makes it possible to add assets to the network model that may not be part of a regular asset scanning report without having to create them individually. Assets created using this method do not contain vulnerability information, although once they are added to the network model, they can be supplemented with matching data that arrives from a scanner report or that you add individually using the ESM Console.

Administrators can enable the option to create assets for network devices in the Manager Configuration Wizard. For more about running the Manager Configuration Wizard, see the topic “Reconfiguring ArcSight Manager” in the *Administrator's Guide*.

The system creates assets differently for devices in static zones and those in dynamic zones. For more about static and dynamic zones, see [“Dynamic and Static Zones” on page 736](#).

For details about how the system creates assets for devices reporting through SmartConnectors, see [“Creating Assets for Network Devices” on page 805](#).

For more about how to tune asset auto creation from the ESM Console, see the following topics:

- **For ESM:** [“Configure Asset Auto-Creation Filters” on page 56](#) .
- **For ArcSight Express:** [“Configure Asset Auto-Creation Filters” on page 79](#).

It is also possible to customize how the asset auto-creation function works by modifying settings in the `server.properties` file. For details, see [“Asset Auto-Creation Advanced Configuration Options” on page 808](#).

For an overview of the ways by which the network model can be populated with assets, see [“Populating the Network Model with Assets” on page 740](#).

Asset Aging and Model Confidence

The asset aging function keeps track of the last time an asset was scanned, and incrementally diminishes an asset's model confidence in the priority formula over time to 0 if it hasn't been scanned in over 120 days (the time range can be configured).

Asset's age is tracked by default. You can opt to automatically disable an asset that exceeds the configured age limit. This process is described in [“Asset Aging” on page 88](#) in the *Administrator's Guide*.



Resolving zone information on disabled assets

To ensure that events get sorted properly, the system continues to resolve an asset's zone information and add it to the event even when the asset is inactive (disabled).

To see why an asset was disabled:

- 1 In the Navigator panel, go to the Assets tab in the Assets tree. The disabled asset appears with a grey icon.
- 2 Right-click the disabled asset and select **Show Disabled Reason**. The message displayed indicates how many days it has been since the asset's last scan.

To re-enable a disabled asset:

If an asset has been automatically disabled, you can manually re-enable it.

In the Navigator panel in the Assets tab of the Assets tree, right-click the disabled icon and select **Enable**.

For more about the priority formula, see [“Priority Calculations and Ratings” on page 957](#).

Asset Ranges

An asset range is a group of assets attached to a network that use a contiguous block of IP addresses. An asset range is useful if you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as desktop PCs and laptops.

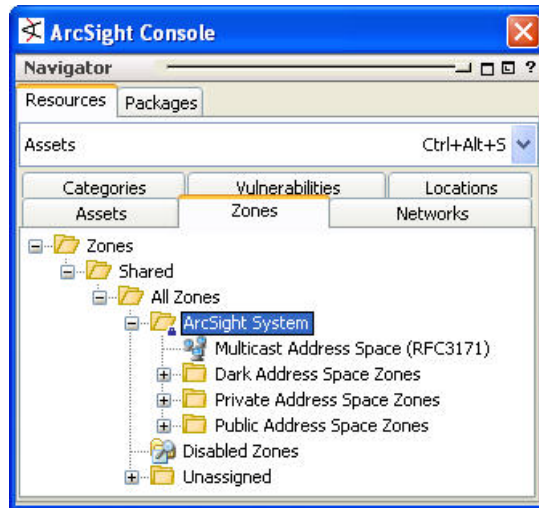
When an event is processed by the SmartConnector, the Manager, or the correlation engine, its endpoints are either identified as a single asset or as an asset belonging to a particular asset range. A reference to the asset or asset range identifier is populated in the event schema.

Zones

Zones are ArcSight resources that represent a functional part of the network with contiguous IP addresses, such as DMZ, VPN, wireless LAN, or DHCP.

With ArcSight v4.0, every asset or address range is associated with a zone. ArcSight comes configured with the standard global IP address ranges already represented as zones, so if your network uses only these public IP addresses, ArcSight can resolve them without setting up any additional zones.

The following zones are standard:



You would need to create your own zones if you have overlapping private networks. Private networks usually model a functional group within your network or a subnet, such as a wireless LAN, the engineering network, the VPN or the DMZ.

For details about using the zone editor, see [“Managing Zones” on page 763](#) in [“Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories” on page 753](#).

Dynamic and Static Zones

Zones are created to model functional portions of the network that share a contiguous block of IP addresses.

The asset auto-creation feature (see [“Auto-Created Assets” on page 733](#)) relies on zones that are already in place before device discovery occurs, either customer-created zones, or the default zones. When you add a SmartConnector, you assign one or more existing

Networks to that Connector. All assets reported by that Connector are then associated with that Network and the zones the Network represents.

The system differentiates between dynamic zones and static zones to classify the types of assets they represent.

Static Zones

Devices in a static zone use static (constant) IP addresses. This represents devices that stay on the network and use the same IP address for all traffic. In order to identify assets classified in static zones, the assets must have either a unique IP address, a unique host name, or both.

Dynamic Zones

Devices in a dynamic zone use dynamic addressing (such as DHCP). Dynamic zones represent assets that come and go from the network, such as laptops. By default, the system requires either a MAC address or a host name to identify assets in dynamic zones. The system first looks for a MAC address; if one is not present, it uses the host name.



Caution

Classifying Zones as Static and Dynamic

It is important that zones are classified properly as dynamic or static.

If a zone is classified as static, but hosts assets that come and go from the network, the system may not be able to update the network model properly. For example:

- The updated network might have duplicate and disabled assets
- Other information, such as vulnerability information and open ports, may not get updated properly

Static Assets in Dynamic Zones

If an asset is classified as static, but belongs to a dynamic zone, the system treats the asset as if it was in a static zone. See the description and links above for how the asset auto-creation feature works for static zones.

Networks

Networks are ArcSight resources that are used to differentiate between zones whose IP ranges overlap, such as when branch locations assign the same private address spaces to resources used in other corporate locations.

The system comes configured with two standard networks: Local and Global. The Local network is where you add your custom zones. Zone mappings in the Local network override the default zone mappings provided by the Global network.

The Global network provides default zone mapping if no local networks are defined, and automatically provides the correct addressing information to ArcSight SmartConnectors when they are installed.

Custom Networks are also used to compartmentalize Customer designations in MSSP situations.

When you associate a customer or a location with a network in the Network Editor, zones automatically access this information. (See [“Managing Networks” on page 764](#) in [“Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories” on page 753](#).)

Asset Model

The resources that make up the asset model are part of the overall network modeling process. The asset model resources describe attributes of the assets themselves for different purposes. *Locations* and *Vulnerabilities* are part of the Assets resource.

Locations

The system provides a location database that maps an IP address to the owning body for the block of IP addresses to which it belongs. Your organization may have finer-grained detail, such as the physical location of all of your networks or networks outside your control, or corrections to the database that the system supplies. The Location resource is the way you can override the default location mappings with location information relevant to your network.

Location is an attribute you can set if the asset you are modeling resides in a geographic location that differs from the location set by the mapping database that associates IP addresses with location information.

Vulnerabilities

The asset vulnerabilities on your network are normally discovered and updated automatically by scanners. The most common manual change to a vulnerability resource is to associate it with a Knowledge Base article. You can associate assets with vulnerabilities from either the Vulnerabilities or Assets editors. (See [“Vulnerability Editor” on page 759](#) in [“Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories” on page 753.](#))

Asset Categories

Asset categories are ArcSight resources that describe the properties of an asset in terms of how it is used. Asset categories are one of the key ways to add differentiation, relevance, and context to the millions of events passing through your network.

Asset categories establish identity, ownership, and criticality of the assets on your network. Asset categories present an extensible schema that adds value to the business properties of your assets. The root of a particular category (for example, **Criticality** in the group [/All Asset Categories/System Asset Categories/Criticality](#)) defines the property itself, whereas the members of the category (for example, the criticality levels [Very High](#), [High](#), and so on) define the possible values for that property.

You can create new asset categories as a right-click option in the navigation panel, and associate categories with assets through the Asset Editor. Most of the methods for populating the network model described in [“Populating the Network Model with Assets” on page 740](#) include a way to add asset categories to your assets, asset ranges, asset groups, and zones.

Asset Categories Assigned to Assets, Asset Ranges, and Asset Groups

Categories assigned to individual assets and asset ranges apply only to those individual assets. This is the most granular level to which you can apply asset categories. If an individual asset falls into an asset range, the asset also inherits the asset categories assigned to the asset range.

Asset Groups are a folder in which one or more Asset resources are stored. Asset Groups are hierarchical, which means that properties assigned to an Asset Group apply to all the assets contained within that group.

Categories assigned to asset groups apply to all assets and asset ranges contained within that group. Individual assets and asset categories within a group inherit the categories assigned to the group, if any, in addition to the asset categories assigned to them individually.

Asset Categories Assigned to Zones

Categories assigned to zones describe the network itself rather than the assets contained within it. This is a way you can categorize traffic on a network where the assets themselves are not constant, such as a wireless or VPN network. For example, the categories might describe whether or not the network is wireless, encrypted, or a VPN network. You may be characterizing the network itself or the traffic on the network (wireless describes the network; encrypted describes the traffic) rather than the particular assets involved.

Asset categories assigned to zones do not get passed on to any assets contained within that zone.

For more about asset modeling, see the topic “Asset Model” in *ESM 101*.

For instructions about how to set asset categories, see the following topics:

- [“Populating the Network Model with Assets” on page 740](#)
- [“Populating the Network Model Using the Wizard” on page 744](#)

- [“Managing Asset Categories” on page 764](#) in [“Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories” on page 753](#).



Always exercise caution when deleting or changing existing asset categories. Changing an asset category can break existing conditions that use that category. As a best practice, create new categories in new groups.

Populating the Network Model with Assets

There are several ways to populate the network model with the assets that represent your monitored network. Most enterprises use a combination of these methods:

ESM Console-Based Methods:

- [“Individually Using Network Modeling Resources” on page 741](#)
- [“In a Batch Using the Network Modeling Wizard” on page 741](#)

SmartConnector-Based Methods:

- [“In a Batch Using the Asset Import FlexConnector” on page 742](#)
- [“Automatically From a Vulnerability Scanner Report” on page 743](#)

ArcSight-Assisted Method:

- [“As an Archive File From an Existing Configuration Database” on page 743](#)



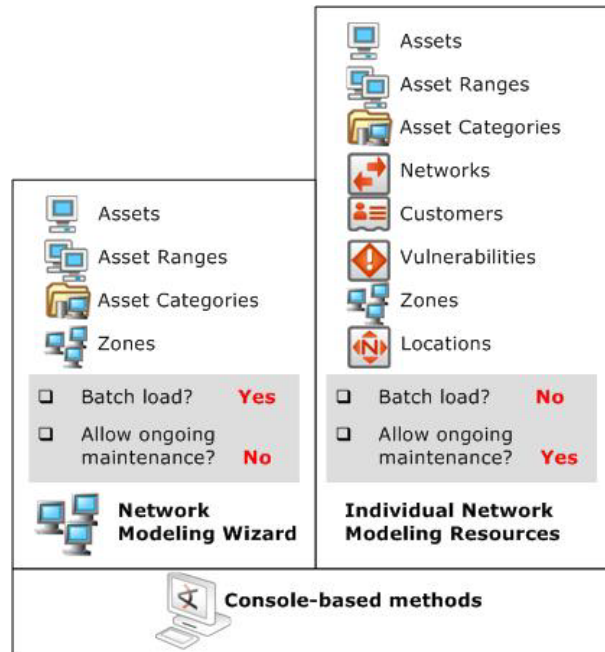
Do not import assets that contain an ampersand (&) in the name. The ArcSight resource framework does not support that character in asset and zone names.

When importing assets using a scanner import connector, the automatically-created asset group name is based on the new asset's zone name. If that name already exists in the same folder, then instead of importing the asset there, as you expect, it imports the asset into either a standard System Asset Group or a higher level custom Asset Group, so as to avoid the folder name-clash.

To avoid this, ensure that when you manually create asset range names, they do not match the Zone names of assets that you intend to import using a asset scanner connector.

ESM Console-Based Methods

The ESM Console provides two ways to populate the network model: individual network modeling resources, and a Network Modeling wizard.



All the individual tools for modeling the network are available in the ESM Console. The Network Modeling Wizard provides a quick way to add basic assets to your Network Model at setup time.

Individually Using Network Modeling Resources

Set every parameter for every asset individually using the network modeling resources (Assets, Asset Ranges, Zones, Networks, and Customers) and asset modeling resources (Asset Categories, Vulnerabilities, and Locations).

You can also use these tools in conjunction with the other batch-loading methods that only offer limited distinctions. As long as primary identifiers, such as IP address, host name, and MAC address, remain the same, the automatic update methods only update fields with new information, so the Network Model remains stable.

For more about network and asset modeling tools, see the topic “ArcSight Network Model” in *ESM 101*.

In a Batch Using the Network Modeling Wizard

The ESM Console provides a Network Modeling wizard as a set-up and configuration tool (menu option **Tools > Network Model**). The Network Modeling wizard enables you to load Assets, Asset Ranges, and Zones along with Asset Category information. If you also add a vulnerability scanner as described in [“SmartConnector-Based Methods” on page 742](#), the existing assets in the model are updated with the vulnerability scan report data.

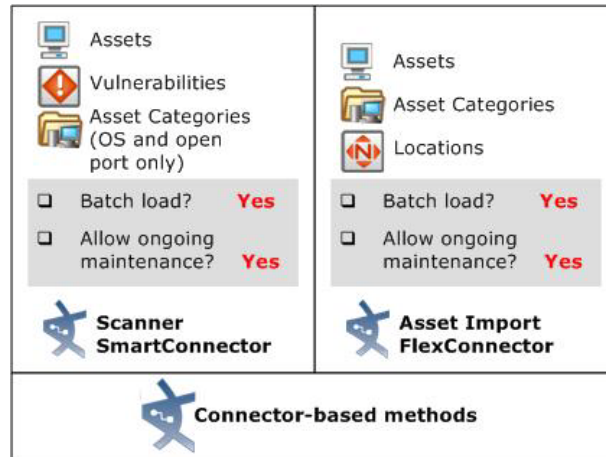
The Network Modeling Wizard is flexible, in that it can take output from any device type in CSV format. The CSV file can be extended to include as many new or pre-existing asset categories as are relevant to the device(s) without having to add asset category information one by one later using the Asset Category resource in the ESM Console. This

tool is appropriate for initial set-up and configuration, not as a method for maintaining the network model.

For more about the Network Modeling Wizard, see [“Populating the Network Model Using the Wizard” on page 744](#).

SmartConnector-Based Methods

Both of these methods enable batch loading and automatic ongoing maintenance. Both methods offer limited distinctions. Both of these methods are described in more detail below.



In a Batch Using the Asset Import FlexConnector

The system offers an Asset Import file FlexConnector that enables you to save Asset, Location, and Asset Category information in a CSV file, which is then automatically pulled into the Manager as part of the SmartConnector heartbeat. Existing assets in the model are updated with any new details discovered by the Asset Import FlexConnector, so the Network Model remains stable.

This method does not create asset ranges, and assumes that Zones and Networks are already created. You can add Customer and Location distinctions to the assets individually. You can find details about how vulnerability information arriving from a scanner report are added to the Network Model in the tech note *“ESM Asset Auto-Creation.”*

This method also takes output from any device type in CSV format. The CSV file for this method can be extended to include as many new or pre-existing asset categories as are relevant to the device(s) without having to add asset category information one by one later using the Asset Category resource in the ESM Console. For details about how to use the ESM Console to import an existing network model as a .csv file, see [“Uploading Files and Creating a File Resource” on page 666](#).

This method is appropriate for updating and maintaining your network model. Updated CSV files are automatically uploaded to the Manager. New data is added to existing assets with matching identifiers. If an existing asset is not present, the system creates one.

For more about the Asset Import File Connector, see the *ArcSight Asset Import SmartConnector Configuration Guide*.

Automatically From a Vulnerability Scanner Report

Set up a scanner SmartConnector (such as FoundStone, ISS Internet Scanner, or Nessus) to use the output of a vulnerability scan to convert device information into Assets along with Vulnerability information, and basic Asset Categories, such as operating system and open ports. The scanner connector that corresponds with your vulnerability scanning product sets up a directory that to regularly scan for updated reports. It then converts the scanner report output into internal scanner meta-events, which the Manager converts into Assets, open port and OS Asset Categories, and Vulnerabilities. For more about the architecture of how this works, see the topic “How Vulnerability Scans Populate and Update the Network Model” in *ESM 101*.

You can also set the scanner SmartConnector to save network model data as a CSV file, which you can then upload into the Manager using the Files resource during your initial network model setup.

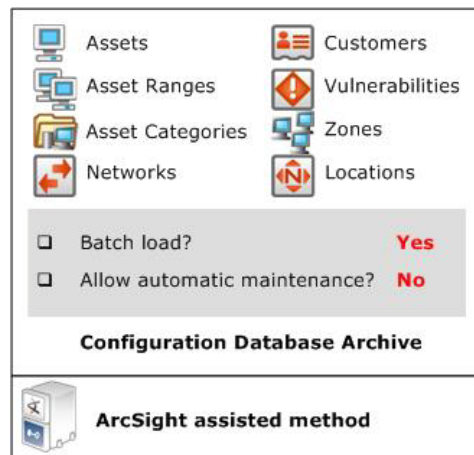
Data derived from vulnerability scanner reports does not create asset ranges, and assumes that Zones and Networks are already created. Once scanner data is imported, you can add Customer and Location distinctions to the assets individually. For details about how the system adds updated vulnerability information arriving from a new scanner report, see the tech note “*ESM Asset Auto Creation*.”

This method is appropriate for updating and maintaining your network model. Subsequent scans update the basic Asset, Asset Category, and Vulnerability information without overwriting the other network modeling settings you add individually.

For more information about the scanner SmartConnector for your vulnerability scanning product, see the SmartConnector Configuration Guide that corresponds with your vulnerability scanning equipment.

ArcSight-Assisted Methods

ArcSight Professional Services can help you populate the Network Model from an existing configuration database.



As an Archive File From an Existing Configuration Database

Many enterprise networks have third-party systems that already model the properties of the assets on your network. With the help of ArcSight Professional Services, you can export these network models, translate the format into the schema using an ArcSight resource-generating utility, and import it to the Manager as a resource archive with the help of ArcSight Professional Services.

The tools ArcSight Professional Services use can generate any type of resource, so using this method, you can have a fully populated network model without having to do any individual configuration.

Populating the Network Model Using the Wizard

The Network Model wizard (menu option **Tools > Network Model**) makes it possible to quickly populate the network model by batch loading asset and zone information from Comma Separated Values (CSV) files.



- The Network Model Wizard is available to users with Administrator privileges.
- Also, do not import assets that contain an ampersand (&) in the name. The ArcSight resource framework does not support that character in asset and zone names.

The following data can be imported into the Manager from CSV files:

- **Zones** define functional parts of a network, such as a wireless LAN, an engineering network, a VPN or a DMZ. For the column types of the zones CSV file, see [“Zones CSV File Format” on page 747](#).
- **Assets** represent individual nodes on the network, such as servers and routers. For the column types of the assets CSV file, see [“Assets CSV File Format” on page 748](#).
- **Asset ranges** represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have many network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. Asset ranges should be a subset of the IP address ranges defined for zones. For the column types of the asset ranges CSV file, see [“Asset Ranges CSV File Format” on page 750](#).

You can import combinations of input CSV files at one time using the Network Model wizard but only one file of each type can be imported during a single import. For example, if you only have assets to import, you can import only an assets CSV file. If you have a zones CSV file, an assets CSV file, and an asset ranges CSV file to import, you can import all three at once using the Network Model wizard.

Specifying CSV Column Types

Each CSV file type defines a set of required column(s) and optional columns. In addition, the CSV file can contain columns that are not used by the Network Model wizard. The columns can be in any order but the Network Model wizard requires that you specify the types of each column so the wizard knows how to interpret each column. You can specify the column type using one of the following methods:

- Specify the column type in the header of the CSV file itself, prior to launching the Network Model wizard. For instructions, see [“Specify the Column Type Using a Header” on page 745](#).
- While running the Network Model wizard, assign the appropriate column type for each column in the Select Column Headers panel. For instructions, see [“Assign the Column Type in the Wizard” on page 745](#).

Columns not used by the Network Model wizard must be assigned the column type [Ignore](#). Only columns of type [Ignore](#) and [Category URI](#) can be repeated in the CSV file. For all other column types, only one instance of the column type can be assigned in the file. For example in a zones CSV file, only one column should be assigned the [Name](#)

column type. If duplicate columns of a non-repeatable column type exist in the CSV file, one of the columns should be assigned the **Ignore** column type. For example if two name columns appear in the CSV file, one should be assigned the **Name** column type and the other should be assigned the **Ignore** column type.

Specify the Column Type Using a Header

In this method, you specify the column type in the first row (header) of the CSV file itself before importing the CSV file using the wizard. The column name in the header must match the column type specified in:

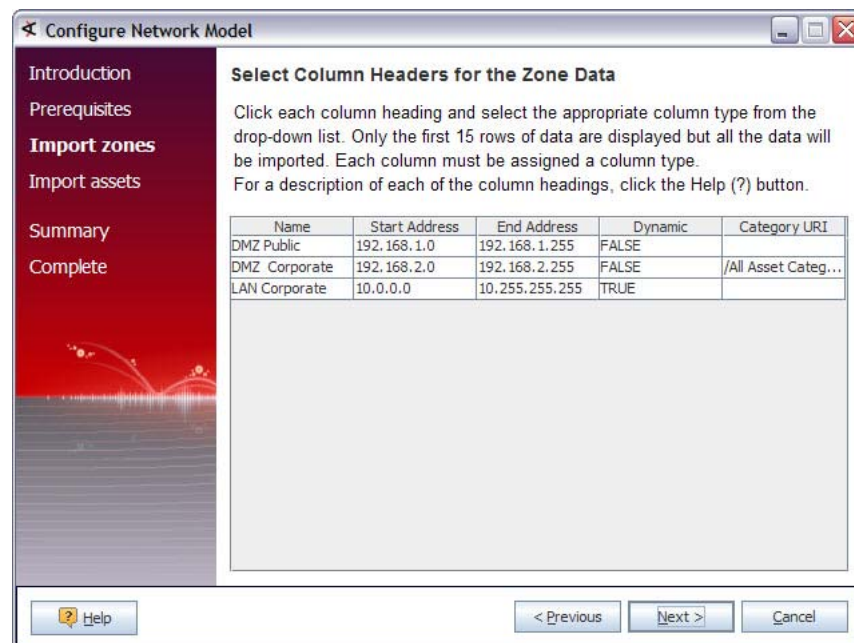
- “Zones CSV File Format” on page 747
- “Assets CSV File Format” on page 748
- “Asset Ranges CSV File Format” on page 750

As shown in following sample zones CSV file, the column names in the first row (highlighted in **bold**) match the column types specified in “Zones CSV File Format” on page 747. The wizard determines how to interpret each column using the column type specified in the header.

Name,Start Address,End Address,Dynamic,Category URI

```
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```

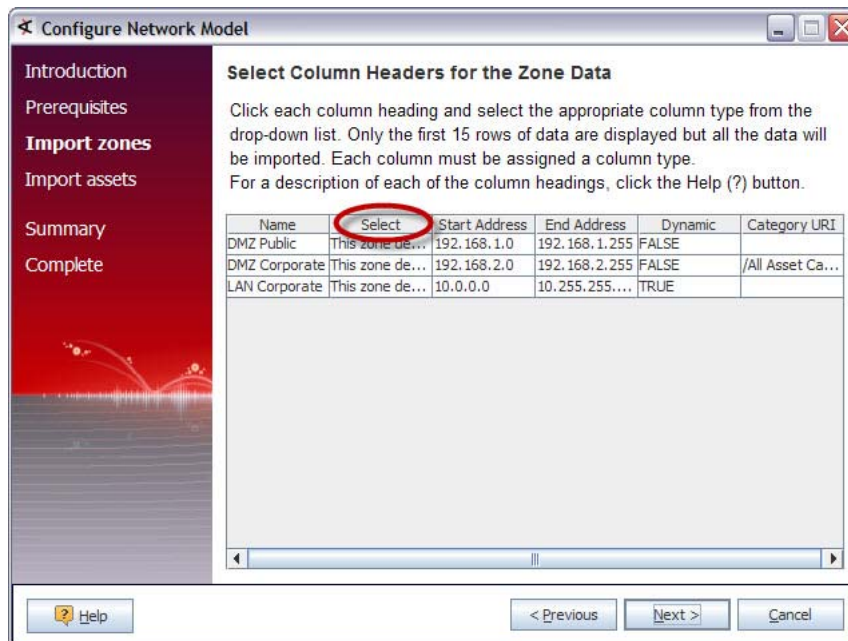
When this zones CSV file is imported into the wizard, the wizard correctly matches the column types because the column types have been correctly specified in the header, as shown below.



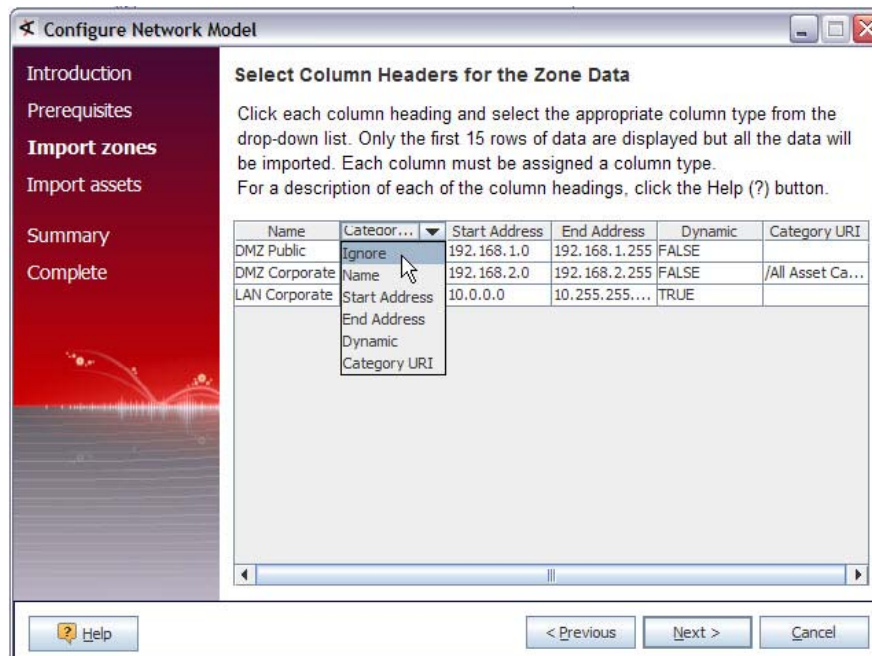
Assign the Column Type in the Wizard

In this method, you assign the column type in the Select Column Headers panels while running the wizard. When the following sample zones CSV file (which does not contain a header row) is imported, the wizard does not know how to interpret all the columns as shown below.

```
DMZ Public,192.168.1.0,192.168.1.255,FALSE,
DMZ Corporate,192.168.2.0,192.168.2.255,FALSE,/All Asset Categories/Site
Asset Categories/Business Impact Analysis/Network Domains/Email/
LAN Corporate,10.0.0.0,10.255.255.255,TRUE,
```



By default, when this sample data is imported into the wizard, the second column is automatically assigned to the **Select** column type but the second column is a description of the zone and should be assigned the **Ignore** column type. To change the column type, click the title of the column and from the drop-down menu select the appropriate column type as shown below.



Zones CSV File Format

Zones define functional parts of a network, such as a wireless LAN, private networks, or subnets. For example, the following network areas could be identified as a zone: the VPN, the DMZ, or an engineering network. Zones are identified with a contiguous block of addresses.



Each zone should specify a unique range of IP addresses. The IP addresses specified by zones should not overlap. If you import a zone that overlaps with a zone already specified on the ArcSight ESM Manager and the new zone has a different name than the existing zone, the following occurs:

- the new zone is created
- the existing zone is invalid and is displayed with the broken zone icon in the ESM Console

You can define a set of zones in ArcSight ESM by batch loading zone definitions from a zones CSV file. Zone CSV files contain the columns listed in the table below. When a zones CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Zone Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see [“Increasing the Number of Rows Displayed” on page 752](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 744](#).

When the Next button is clicked in the Summary of Data to Import panel, the zone data is imported into the ArcSight ESM Manager. The new zones are created in the [/All Zones/Site Zones](#) group. For example, if a zone called [DMZPublic](#) was specified in the imported zones CSV file, a new zone is created at the following URI: [/All Zones/Site Zones/DMZ Public](#). The new zones are assigned to the default network called [Local](#).

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the zone such as the purpose or geographical location.	Yes	No	DMZ Public
Start Address	The start of the range of IP addresses that defines the zone.	Yes	No	192.168.1.0
End Address	The end of the range of IP addresses that defines the zone.	Yes	No	192.168.1.255
Dynamic	Determines whether the devices defined in the zone use dynamic addressing: <ul style="list-style-type: none"> • true—devices in the zone use dynamic addressing (DHCP) • false—devices in the zone use static IP addressing 	No Default is false	No	false

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Category URI	<p>The asset category to assign to zone.</p> <p>NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.</p>	No	<p>Yes</p> <p>This column can be repeated because a zone can be categorized into more than one asset category.</p>	<p>/All Asset Categories/All Site Asset Categories/Business Impact Analysis/Business Role/Service/Web/</p>
Ignore	The column contains data that is not used by the Network Model wizard when creating zones. For example, this column could contain a description of the zone.	No	Yes	<p>This zone defines the public subnetwork of the DMZ.</p>

An Example of a Zones CSV File

Here is an example of the Zones CSV file:

```
HRZoneA,<Starting-IP-address>,<Ending-IP-address>,FALSE,/All Asset Categories/ArcSight System Administration/Databases/
```

```
IT Zone,<Starting-IP-address>,<Ending-IP-address>,TRUE,/All Asset Categories/ArcSight System Administration/Databases/
```

Assets CSV File Format

Assets represent individual nodes on the network, such as servers and routers. For more information, see ["Network Model" on page 732](#).

You can define a set of assets in ArcSight ESM by batch loading asset definitions from an Assets CSV file. Asset CSV files contain the columns listed in the table, below.

When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported. For more information, see ["Increasing the Number of Rows Displayed" on page 752](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see ["Specifying CSV Column Types" on page 744](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset data is imported into the ArcSight ESM Manager. The new assets are created in the [/All Assets/Site Assets](#) group. For example, if an asset called [DMZCorpEmailServer](#) was specified in the imported assets CSV file, a new asset is created at the following URI: [/All](#)

[Assets/Site Assets/DMZCorpEmailServer](#). When imported, the new assets are auto-zoned. For more information, see [“Auto-Zoning of Imported Assets” on page 753](#).

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the asset. This name must be unique. It is recommended to specify a name. However, if a name is not specified, a unique name is generated using the other fields.	No	No	DMZ Corp Email Server 1
Host Name	The host name of the network device represented by the asset.	No	No	dmz_corp_email
IP Address	The IP address of the network device represented by the asset. NOTE: If no value is specified for this column (,,) the asset is created with an IP address of 0.0.0.0.	Yes	No	192.168.2.1
MAC Address	The MAC address of the network device represented by the asset. The MAC address is made up of six groups of two hexadecimal digits can be separated by colons (:) or hyphens (-).	No	No	21-4D-5B-2A-3B-FF
Static Addressing	Defines if the network device is statically addressed even though the IP address of the asset is in a dynamic zone: <ul style="list-style-type: none"> true—asset uses static IP addressing false—device uses dynamic addressing (DHCP) For more information, see “Static Addressing in a Dynamic Zone” on page 750 .	No Default is false	No	false
Category URI	The asset category to assign to network device. NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes This column can be repeated because a network device can be categorized into more than one asset category.	/All Asset Categories/Site Asset Categories/Business Impact Analysis/Network Domains/Email/

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Ignore	The column contains data that is not used by the Network Model wizard when creating assets. For example, this column could contain a description of the asset.	No	Yes	This asset defines the Corporate Email Server in the DMZ.

An Example of an Assets CSV File

Here is an example of the Assets CSV file:

```
Lab Test machine,lab-111,<IP-address>,<Mac-address>,true,/All Asset
Categories/ArcSight System Administration/Consoles/,/All Asset
Categories/ArcSight System Administration/Databases/
```

```
Oracle Server,server-oracle,<IP-address>,<Mac-address>,false,/All
Asset Categories/ArcSight System Administration/Consoles/,/All
Asset Categories/ArcSight System Administration/Databases/
```

Static Addressing in a Dynamic Zone

Set the **Static Addressing** column to `true` if the network device is statically addressed even though the IP address of the asset is in a dynamic zone. For example, set this column to `true`, for the following conditions:

- A dynamic zone is defined with the following IP range: `192.168.2.1 - 192.168.2.255`.
- A network device with an IP address of `192.168.2.15` is statically addressed even though it is defined in the dynamic zone.

For more about static and dynamic zones, see ["Dynamic and Static Zones" on page 736](#).

Asset Ranges CSV File Format

Asset ranges represent sets of network nodes addressable as a contiguous block of IP addresses. Asset ranges are useful when you have a number of network nodes that would be impractical to track individually, or that may come and go from the network, such as laptops. An asset range can define a group of assets that are not addressed individually. Asset ranges should be a subset of the IP address ranges defined for zones.



Caution

Each asset range should specify a unique range of IP addresses. The IP addresses specified by asset ranges should not overlap. If you import an asset range that overlaps with an asset range already specified on the ArcSight ESM Manager and the new asset range has a different name than the existing asset range, the following occurs:

- the new asset range is created
- the existing asset range is invalid and displays with the broken asset range icon in the ESM Console

You can define a set of asset ranges in ArcSight ESM by batch loading asset range definitions from an asset range CSV file. Asset range CSV files contain the columns listed in the table, below. When an assets CSV file is selected for import, by default only the first fifteen rows of data are displayed in Select Column Headers for the Asset Ranges Data panel. However, when the data is imported into the ArcSight ESM Manager, all the rows are

imported. For more information, see [“Increasing the Number of Rows Displayed” on page 752](#).

For the wizard to determine how to process the imported data, the type of each column must be specified. For more information, see [“Specifying CSV Column Types” on page 744](#).

When the Next button is clicked in the Summary of Data to Import panel, the asset range data is imported into the ArcSight ESM Manager. The new asset ranges are created in the [/All Assets/Site Assets](#) group. For example, if an asset range called `DMZCorpHR` was specified in the imported asset range CSV file, a new asset range is created at the following URI: [/All Assets/Site Assets/DMZCorpHR](#).

Column Type	Description	Required Column?	Repeatable Column?	Example Value
Name	A descriptive name for the asset range. This name must be unique.	Yes	No	<code>DMZ Corp HR</code>
Start Address	The start of the range of IP addresses that defines the asset range.	Yes	No	<code>192.168.2.11</code>
End Address	The end of the range of IP addresses that defines the asset range.	Yes	No	<code>192.168.2.20</code>
Category URI	The asset category to assign to asset range. NOTE: The wizard does not create new categories. For the category to be assigned, it must already exist.	No	Yes This column can be repeated because an asset range can be categorized into more than one asset category.	<code>/All Asset Categories/Site Asset Categories/Business Impact Analysis/Data Role/HR Data/</code>
Ignore	The column contains data that is not used by the Network Model wizard when creating asset ranges. For example, this column could contain a description of the asset range.	No	Yes	<code>This asset range defines the all the corporate human resources assets.</code>

An Example of an Asset Ranges CSV File

Here is an example of the Asset Ranges CSV file:

```
HRRangeA,<Starting-IP-address>,<Ending-IP-address>,/All Asset
Categories/ArcSight System Administration/Databases/
```

```
IT Range X,<Starting-IP-address>,<Ending-IP-address>,/All Asset
Categories/ArcSight System Administration/Databases/
```

Increasing the Number of Rows Displayed

By default, only the first fifteen rows of data are displayed in Select Column Headers for the <Resource Type> Data panels. However, when the data is imported into the ArcSight ESM Manager, all the rows are imported.

To increase the number of rows displayed, add the property `usecase.networkmodeling.maxrowfortable` to the `<ARCSIGHT_HOME>/config/console.properties` file and set the value of the property to a number greater than fifteen. Restart the ESM Console.

Summary of Data to Import

In the Summary of Data to Import panel, a summary of the network modeling data ready to import into the ArcSight ESM Manager is displayed. If you click **Cancel** in this panel or any of the preceding panels, no data is imported into the Manager.

- 1 Click **Next** to start the import process.

A temporary Archive Resource Bundle (ARB) file with the import data is created and the Install Packages dialog displays.

- 2 To install the data from the temporary ARB file, in the Update Packages dialog, click **OK**.

The network modeling data is imported into the ArcSight ESM Manager and the Data Imported pane displays. In addition, the Installing Packages and the Importing Packages dialogs display.

- 3 Close the open dialogs:

- a In the Installing Packages dialog, click **OK**.

- b In the Importing Packages dialog, click **OK**.

Network Data Imported into Manager

When network modeling data is imported from the network modeling data CSV files, new resources are created in the following groups on the ArcSight ESM Manager:

- New **zones** are created in the `/All Zones/Site Zones` group. For example, if a zone called `DMZPublic` was specified in the imported zones CSV file, a new zone is created at the following URI: `/All Zones/Site Zones/DMZ Public`.
The new zones are assigned to the default network called `Local`.
- New **assets** are created in the `/All Assets/Site Assets` group. For example, if an asset called `DMZCorpEmailServer` was specified in the imported assets CSV file, a new asset is created at the following URI: `/All Assets/Site Assets/DMZCorpEmailServer`. When imported, the new assets are auto-zoned. For more information, see [“Auto-Zoning of Imported Assets” on page 753](#).
- New **asset ranges** are created in the `/All Assets/Site Assets` group. For example, if an asset range called `DMZCorpHR` was specified in the imported asset range CSV file, a new asset range is created at the following URI: `/All Assets/Site Assets/DMZCorpHR`.

In the Data Imported dialog, click **Finish** to close the wizard.

Auto-Zoning of Imported Assets

When new assets are imported into the ArcSight ESM Manager using the Network Model wizard, an attempt is made to assign the assets to the appropriate zone from the default network called *Local*. This process is called auto-zoning.

When the asset is imported, if a zone is found with an address range that includes the imported asset and that zone is located in the *Local* network, the matching zone is assigned to the asset. For the asset to find the matching zone, the matching zone must either:

- Already exist on the ArcSight ESM Manager prior to the import.
- Be imported with the asset as part of the same import process—part of the same transaction. Zones are created before assets in the import process.

If no matching zone is found in the network, no zone is assigned.

The following example illustrates the auto-zone process. A zone called *DMZCorporate* is defined in the *Local* network on the ArcSight ESM Manager with a starting address of *192.168.2.0* and an ending address of *192.168.2.225*. If an asset called *DMZCorpDatabase* with an IP address of *192.168.2.11* is imported by the wizard, the *DMZCorporate* zone is assigned to *DMZCorpDatabase* asset because the IP address of the *DMZCorpDatabase* asset is in the range of addresses specified in the *DMZCorporate* zone and the *DMZCorporate* zone is located in the *Local* network.



Note

Only one asset with a given host name is allowed in a given zone on a network. When two assets with the same host name are imported, and if the ArcSight ESM Manager assigns them to the same zone in the same network, both assets are imported but one of the assets is disabled and displays with the broken-asset icon in the ESM Console.

Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories

The Assets resource provides tools for managing assets and asset ranges (see [“Assets” on page 733](#) and [“Asset Ranges” on page 736](#)), and tools for managing the other network and asset modeling features associated with assets:

- Networks
- Zones
- Locations
- Vulnerabilities
- Asset Categories

Networks and *Zones* describe characteristics of how the asset is represented in the network itself; *Locations*, *Vulnerabilities*, and *Asset Categories* describe attributes of the assets that can be used for prioritization and correlation.

You can organize any of these distinctions into groups upon which you can set up user access controls.

You can also create a channel based on any of these distinctions to get additional monitoring views into the events happening on your network.

This section describes how to manage these resources, and the context actions you can take from right-click menus.

Managing Assets

This topic explains how to create, edit, move, add to, and delete assets, and how to select them in the Common Conditions Editor. For an overview of what assets are, the resources that comprise them, how they fit into the network model, and the ways to populate the network model, see [“Network Model” on page 732](#).

Creating an Asset

This topic describes how to create an asset manually through the ESM Console.



You can create assets manually using the ESM Console (as described in this topic), using the Network Model wizard, or dynamically from scanner data. See also, [“Network Model” on page 732](#) and [“Populating the Network Model Using the Wizard” on page 744](#).

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 Right-click a group and choose **New Asset**.
- 3 Select the **Attributes** tab and enter values in the fields described below.
- 4 Click **OK**.

Asset Attributes	Description
Name	The asset's friendly name. This field can default to the asset's host name or IP address.
IP Address	The asset's IP address, in dotted-decimal notation.
MAC Address	The unique hardware ID for the network device.
Host Name	The asset's DNS name.
Location	As described in Assets and Changing Assets .
Zone	As described in Assets and Changing Assets .

After you fill in the attribute fields, use the other tabs in the Asset Editor as necessary to add resources.

Asset View	Contents
Categories	Use the Add button on this tab to select network categories with which to associate the asset.
Alternate Interfaces	Use the Add button on this tab to select a second asset ID if this asset has an additional ID on another network. Alternate interfaces usually apply only to network boundary devices, such as bridges, that have two MACs.
Vulnerabilities	Use the Add button on this tab to select certain vulnerabilities with which to associate the asset.
Notes	Use the text box and Save button on this tab to write and file additional information concerning the asset.

Editing an Asset

- 1 In the Assets resource tree, right-click an asset and choose **Edit Asset**.
- 2 On the **Attributes** tab, edit the text fields as described above.
- 3 On the other tabs, add or delete information as necessary.
- 4 Click **OK**.

Moving or Copying an Asset

- 1 In the Assets resource tree, navigate to an asset and drag and drop it into another group.
- 2 Choose **Move** to move the asset, **Copy** to make a separate copy of the asset, or **Link** to create a copy of the asset that is linked to the original asset.

If you choose **Copy**, you create a separate copy of the asset that is not affected when the original asset is edited. If you choose **Link**, you create a copy of the asset that is linked to the original asset. Therefore, if you edit a linked asset, whether the original or the copy, all links are edited as well. When deleting linked assets, you can either delete the selected asset or all linked asset copies.

Deleting an Asset



Caution

Take care when deleting assets. Asset groups required for correct operation are locked, however, depending on your permissions, it is possible to delete the individual assets in those groups, such as the assets automatically created to track ArcSight components.

Do not delete ArcSight System Administration assets without consulting an ArcSight administrator.

- 1 In the Assets resource tree, right-click an asset and choose **Delete Asset**.
- 2 In the dialog box, click **Yes**.

Showing Assets in a Channel

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Show Assets**.

The asset(s) are displayed in an active channel grid view.

- 2 If applicable, you can also show assets recursively. To do so, right-click an asset group, and choose **Show Assets Recursively**. This shows assets not only in the selected group but also all children in an active channel.

Auto Zoning an Asset

- 1 In the Assets resource tree, right-click an asset or group of assets and choose **Auto Zone**.

The Network Selector dialog displays.

- 2 Browse for the network that contains the zone with an IP address range that includes the asset.
- 3 Select the network and click **OK**.

If a matching zone with an address range that includes the selected asset can be found in the network, the zone is assigned to the asset.

For example, a zone called **DMZCorporate** is defined in the **Local** network on the ArcSight ESM Manager with a starting address of **192.168.2.0** and an ending address of **192.168.2.225**. If an asset called **DMZCorpDatabase** with an IP address of **192.168.2.11** is selected for auto zoning in the **Local** network, the **DMZCorporate** zone is assigned to **DMZCorpDatabase** asset because the IP address of the **DMZCorpDatabase** asset is in the range of addresses specified in the **DMZCorporate** zone.

If no matching zone is found in the network, no zone is assigned.

An asset can be selected for auto zoning manually by right-clicking and choosing the **Auto Zone** option as described above. In addition, auto zoning can automatically occur when assets are imported using the Network Model wizard. For more information, see [“Auto-Zoning of Imported Assets” on page 753](#).

Managing Asset Groups

Asset groups are created to store similar groups or assets in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's permissions. If a group is deleted, the assets within that group are also deleted. ArcSight provides these groups:

- **Shared:** this group lists assets to which the user has permission.
- **Unassigned:** this group lists assets not assigned to a group.

If you have Administrator access you also see another group named "All Assets" that contains all asset groups and assets.

Creating an Asset Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**.
- 2 In the Assets resource tree, right-click a group and choose **New Group**. A "name" text field appears under the group you selected.
- 3 In the name text field, type in a name.
- 4 Press **Enter**.

Renaming an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Edit Group**.
- 2 In the **Group Editor**, edit the Name and Description text fields.
- 3 Click **OK**.

Moving or Copying an Asset Group

- 1 In the Assets resource tree, navigate to a group and drag and drop it into another group.

- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

Deleting an Asset Group

- 1 In the Assets resource tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Asset Scalability

ArcSight stores information about hosts and network devices in resources called Assets. These resources can be automatically created by vulnerability scanner SmartConnectors. Asset Scalability refers to ArcSight's ability to manage hundreds of thousands of assets or more without adversely affecting security event throughput.

Viewing Assets in Active Channels

The ESM Console shows assets, vulnerabilities, asset categories, scanner reports, and cases in active channels (rather than static grid views, as in previous releases). Now you can leverage the power of channels for asset management, including use of filters, field sets, better sorting capabilities, and dynamic display of an unlimited number of items (continually updated).

To start working with assets in active channels, choose **Assets** in the Navigator, and see [“About the Network Model” on page 731](#).

Note also that you can create an “asset channel”. For more information on active channels, see [“Monitoring Active Channels” on page 129](#).

Finding Assets

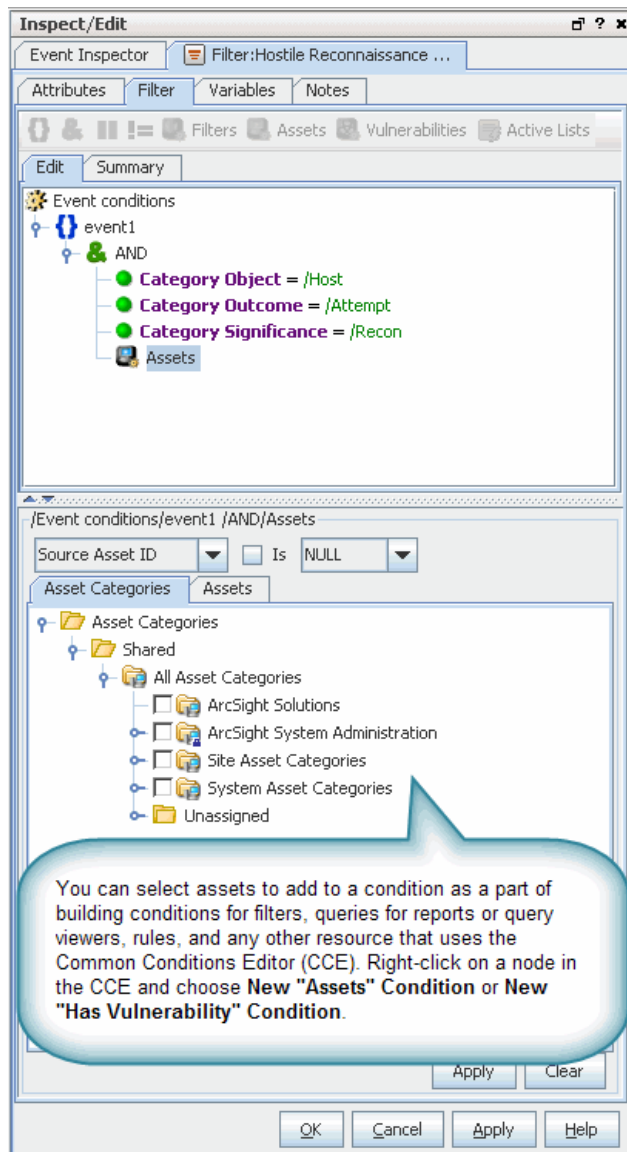
Resource search helps you find one asset in a potentially large set, avoiding the resource tree in the Navigator.

Selecting Assets in the Common Conditions Editor

Once assets are added to your network model, you can select them in order to write conditions that help you analyze their role in the event traffic they process.

The Asset Selector appears in the Query Editor (in Reports), Rules Editor, Filters Editor, and in the Filter Settings panel, when creating an asset condition. In the Asset Selector, select the assets to add as a new condition.

Right-click a node in the Common Conditions Editor (CCE) and choose **New "Assets" Condition**. (For more about using the CCE, see ["Common Conditions Editor \(CCE\)"](#) on page 846.)



Managing Vulnerabilities

This topic describes how to perform the authoring and management tasks for vulnerabilities. See also ["About the Network Model"](#) on page 731.

Note also that you can create a "vulnerability channel". For more information on active channels, see ["Monitoring Active Channels"](#) on page 129.

Vulnerability Editor

Vulnerability Attribute	Description
Name	A descriptive name for the vulnerable asset (required)
Knowledge Base Article	Optionally, provide a link to a relevant knowledge base article.
External ID	Provide an alternate identifier for the vulnerability.

In addition to vulnerability **Attributes** (described above), the Vulnerability Editor includes a subtab for selecting and adding assets as **vulnerabilities**.

Creating a Vulnerability

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.
- 2 Right-click a group and choose **New Vulnerability**.
- 3 On the Vulnerabilities Attributes tab, type in the following text fields:

Vulnerability Attribute	Description
Name	The vulnerability's name. It can be generated by the ArcSight Manager in response to vulnerability scanners. If so, this field is identical to the External ID field except that the pipe () is replaced with a dash (-), such as CVE - CVE-1999-200.
Knowledge Base Article	A Knowledge Base article that further describes the vulnerability.
External ID	An ID of the format <standards body> <id>, such as CVE CVE-1999-200.
Owners	ArcSight users who are interested in the vulnerability.
Notification Groups	ArcSight users who are notified of events involving the vulnerability.

- 4 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 5 Click **OK**.

Editing a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 On the Attributes tab, type in the text fields as described above.
- 3 On the Vulnerable Assets tab, click the **Add New** button, if you've defined assets that include this vulnerability.
- 4 Click **OK**.


Moving or Copying a Vulnerability

- 1 In the Vulnerabilities tree, navigate to a vulnerability and drag and drop it into another group.
- 2 Choose **Move** to move the vulnerability, **Copy** to make a separate copy of the vulnerability, or **Link** to create a copy of the vulnerability that is linked to the original vulnerability.


If you choose **Copy**, you create a separate copy of the vulnerability that is not affected when the original vulnerability is edited. If you choose **Link**, you create a copy of the vulnerability that is linked to the original vulnerability. Therefore, if you edit a linked vulnerability, whether it be the original or the copy, all links are edited as well. When deleting linked vulnerabilities, you can either delete the selected vulnerability or all linked vulnerability copies.

Retrieving Vulnerable Assets


- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 Select the **Vulnerable Assets** tab.

If you used a vulnerability scanner, all vulnerable asset discovered by the scanner are listed on this tab.
- 3 To refresh the vulnerabilities list, click the **Refresh** button (.

Adding an Asset to a Vulnerability

- 1 In the Vulnerabilities resource tree, right-click a vulnerability and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Click the **Add** button (.
- 4 Select an asset in the Assets Selector and click **OK**.
- 5 In the Vulnerability Editor, click **OK**.

Deleting an Asset From a Vulnerability

- 1 In the Vulnerabilities tree, right-click an asset and choose **Edit Vulnerability**.
- 2 In the Vulnerability Editor, select the **Vulnerable Assets** tab.
- 3 Select an asset and click the **Delete** button (.
- 4 In the dialog box, click **Yes**.
- 5 In the Vulnerability Editor, click **OK**.

Deleting a Vulnerability

- 1 In the Vulnerabilities tree, right-click a vulnerability and choose **Delete Vulnerability**.
- 2 In the dialog box, click **Yes**.

Managing Vulnerability Groups

This topic describes the tasks involved in managing vulnerability groups.

Creating a Vulnerability Group

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then the **Vulnerabilities** tab.
- 2 In the Vulnerabilities resource tree, right-click a group and choose **New Group**.
A "name" text field appears under the group you selected.
- 3 In the "name" text field, type in a name.
- 4 Press **Enter**.

Renaming a Vulnerability Group

- 1 In the Vulnerabilities resource tree, under Assets, right-click a group and choose **Rename**.
- 2 In the "name" text field, rename the group.
- 3 Press **Enter**.

Editing a Vulnerability Group

- 1 In the Asset resource tree's Vulnerabilities tab, right-click a group and choose **Edit Group**.
- 2 In the Group Editor, edit the **Name** and **Description** text fields.
- 3 Click **OK**.

Moving or Copying a Vulnerability Group

- 1 In the Vulnerabilities tree, navigate to a group and drag and drop it into another group.
- 2 Choose **Move** to move the group, **Copy** to make a separate copy of the group, or **Link** to create a copy of the group that is linked to the original group.

If you choose **Copy**, you create a separate copy of the group that is not affected when the original group is edited. If you choose **Link**, you create a copy of the group that is linked to the original group. Therefore, if you edit a linked group, whether the original or the copy, all links are edited as well. When deleting linked groups, you can either delete the selected group or all linked groups.

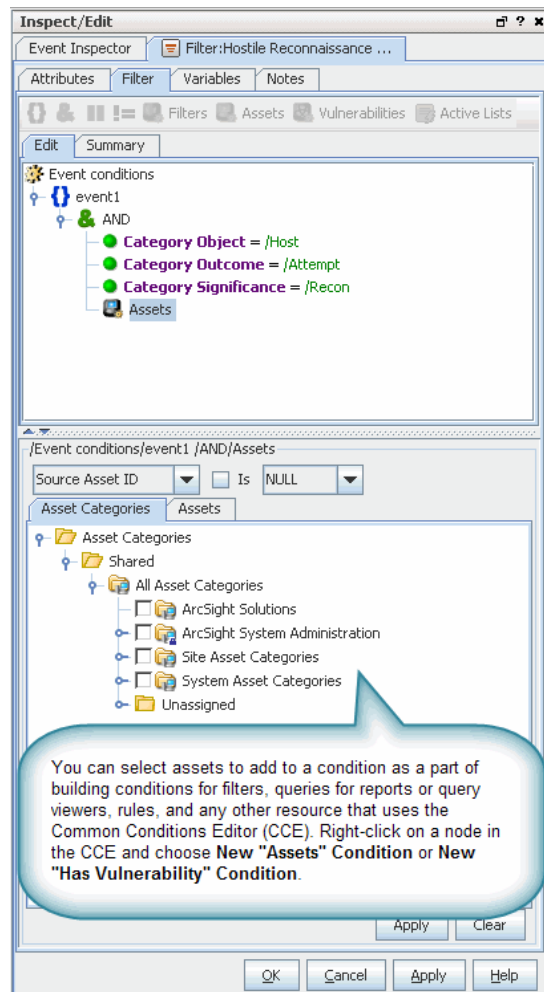
Deleting a Vulnerability Group

- 1 In the Vulnerabilities tree, right-click a group and choose **Delete Group**.
- 2 In the dialog box, click **Yes**.

Selecting Vulnerabilities in the Common Conditions Editor

You can open the Vulnerability Selector from the Reports Query Editor, Rules Editor, Filters Editor, and in the Filter Settings panel. In the Vulnerability Selector, you select vulnerabilities to add to reports, rules, or filters as a new condition.

Right-click a node in the Common Conditions Editor (CCE) and choose **New "Has Vulnerability" Condition**. (For more about using the CCE, see ["Common Conditions Editor \(CCE\)" on page 846](#).)



You use the Vulnerability Selector when performing these tasks:

- Adding a vulnerability condition to a report query (see ["Query Conditions" on page 366](#))
- Specifying rule conditions (see ["Adding Vulnerability Conditions" on page 445](#))
- Using filters (see [Chapter 11, Filtering Events, on page 223](#))

Reporting on Output from Vulnerability Scanners

You can review the output of asset-vulnerability scanners in active channels and in the Vulnerabilities tab of the Asset Editor.

- 1 Choose the Assets resource tree in the Navigator panel.
- 2 In the Assets tab of the Assets tree, right-click an individual asset and choose **Scanner Reports**. If scanner asset-vulnerability reports are available for the selected asset, they appear in a Viewer panel grid view as an active channel.

- 3 You can use the standard controls described in Using Grids and Active Channels to review the reports collectively.
- 4 Also in the channel view, you can double-click vulnerability scanner events to open them in the Asset Editor, where the Vulnerabilities tab lists the vulnerability details.

For information on creating and editing assets, see [“About the Network Model” on page 731](#).

You can create an active channel for selected scanner reports. For information on using active channels, see [“Monitoring Active Channels” on page 129](#).

Reporting on Asset Vulnerabilities

You can create reports to show which assets are vulnerable to particular vulnerabilities or threats. ArcSight also provides Asset Reports that can be run from the Reports resource tree in the Navigator panel. For more information, see [“Using Report Templates” on page 335](#).

- 1 In the Navigator panel's drop-down menu, choose **Assets**, then click the **Vulnerabilities** tab.
- 2 In the Vulnerabilities tree, right-click a vulnerability and choose **Vulnerable Assets Report**.
- 3 In the Report Parameters dialog box, accept the vulnerability listed in the **Vulnerability URL** text field or click the **Vulnerability** button to run the report on another vulnerability.
- 4 Choose a Report File Format from the drop-down menu and click **OK**.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and look different. In addition, Excel format is more memory intensive than PDF.

Managing Zones

For an overview of zones and how they fit into the network model, see [“Zones” on page 736](#).



Note

Shrinking or Splitting Zones

The Zone Editor cannot be used to shrink a zone if there are assets that fall outside the range of the new zone. For example, if you have a zone with an address range of 1.1.1.1 to 1.1.1.100 and an asset in that zone with an IP address of 1.1.1.86, you cannot change the upper end of the zone range to 1.1.1.80 but you can change it to 1.1.1.90.

For shrinking or splitting zones that might encounter such issues, we suggest using a package export and import operation. You can export the asset resources and then import them back in. Package import and install automatically assigns assets to appropriate zones similar to the *auto-zoning* used by the Network Model Wizard. See [“Managing Packages” on page 686](#), [“Populating the Network Model Using the Wizard” on page 744](#), and [“Auto-Zoning of Imported Assets” on page 753](#).

Zone Attribute	Description
Name	A descriptive name for the geographical location (required)

Zone Attribute	Description
Start Address	Provide an IP address that identifies the start of the network scope.
End Address	Provide an IP address that identifies the end of the network scope.
Dynamic Addressing	Click this option on or off to indicate whether this network uses dynamic addressing <ul style="list-style-type: none"> Checkmark (toggle on) this option to indicate that the network you are describing uses dynamic addressing (Dynamic Host Configuration Protocol or DHCP server) Leave this option unchecked (toggle off), if the network you are describing does not use dynamic addressing (but, rather, uses static IP addresses)
Location	Select a location for this zone.
Network	Select the network in which this zone resides.

In addition to zone **Attributes** (described above), the Zone Editor includes subtabs for adding **Assets** and **Categories** into the **zone** you are configuring.

Managing Networks

For an overview of networks and how they fit into the network model, see [“Networks” on page 737](#).

Network Attribute	Description
Name	A descriptive name for the network (required)
Customer	Customer name This option is typically used if configuring assets for a customer on behalf of a managed security service provider (MSSP) or similar scenario.
Location	This is an optional field for a descriptive name of the geographical location of the network.

In addition to network **Attributes** (described above), the Network Editor includes subtabs for adding **Connectors** and **Zones** into the selected **network** you are configuring.

Managing Asset Categories

The Asset Categories subtab in the Navigator provides options to organize assets into groups based on *categories*. From the Navigator right-click menu on Asset Categories, you have several views and tools to help manage and monitor assets. For example, from this menu, you can:

- Create channels to show asset categories and assets
- Move assets into and out of category groups
- Create new category groups
- Configure access control lists (ACLs) to limit or allow user access to groups of assets (see [“Managing Permissions and Resources” on page 646](#))

One asset can be categorized in more than one asset category. You can also assign asset categories to groups of resources. This transfers the asset category onto all the members of the group and its sub-groups. To assign an asset category:

- 1 In the Navigator drop-down menu, go to **Assets**. Select the **Assets** tab. Go to [ArcSight System Administration/Agents](#), to find the SmartConnectors installed for your environment.
- 2 Right-click the asset or asset group you wish to categorize and select **Edit Asset** (or **Edit Group**).
- 3 In the Inspect/Edit panel, click the **Categories** tab. Click the add icon (+) at the top of the screen.
- 4 In the Asset Categories Selector pop-up window, select the asset categories that apply to this asset and click **OK**. For example:
 - a The usage category that applies to the asset (for example, [/All Asset Categories/Site Asset Categories/Business Impact Analysis/Business Role/Revenue Generation](#))
 - b The criticality level that applies to the asset (for example, [/All Asset Categories/System Asset Categories/Criticality/Very High](#))
- 5 Repeat steps 3 and 4 for every asset or group of assets you wish to classify in one of the asset categories.

For an overview of asset categories and how they fit into the network model, see [“Asset Categories” on page 739](#).

Managing Locations

For an overview of locations and how they fit into the network model, see [“Locations” on page 738](#).

Location Attribute	Description
Name	A descriptive name for the geographical location (required)
Latitude	Latitude for the location. The format for this measurement is a preference setting for the ESM Console (menu option Edit > Preferences , click Latitude and Longitude). For more information, see “Latitude and Longitude Options” on page 777 in “Changing User Preferences” on page 772 .
Longitude	Longitude for the location The format for this measurement is a preference setting for the ESM Console (menu option Edit > Preferences , click Latitude and Longitude). For more information, see “Latitude and Longitude Options” on page 777 in “Changing User Preferences” on page 772 .
Address	Provide details for City , Region Code , Postal Code , and Country

Managing Customers

Customer tagging is a feature developed mainly to support Managed Security Services Provider (MSSP) environments, although it can also be used by private organizations to denote cost centers, internal groups, or subdivisions. The Customer designation keeps event traffic from multiple cost centers and/or business units clearly identified and separate. For more general information about this feature, see *ESM 101*.

The Customers resource tree, when populated, maps out the various external or internal customer accounts your enterprise tracks for cost, security analysis, or administrative reasons. These accounts, if present, are usually set up as part of the ArcSight deployment process. If the Customers resource tree is abbreviated or empty, your organization is probably not using this feature.

When the Customers resource tree is populated, you primarily use its branches as references in analysis filters that exclude or include certain customers.

Apart from analysis, the activities necessary to maintain the Customers resource tree include creating new customer references, editing existing references, and occasionally deleting references.

Creating Customers

When you create a customer, remember that the branch you add to the resource tree has to **match** the Customer URI attribute configured for that branch in the relevant SmartConnectors. In other words, you create customer-tracking resources only for those customers that have parallel URI values set in the SmartConnectors that monitor their devices.

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer group and choose **New Customer**.
- 3 In the Customer Editor, enter values for the properties that identify the customer. Note that the **Name** value has to complete the correct Customer URI for this account as found in its related SmartConnectors.
- 4 Click **Apply** to update the customer and leave the editor open, or OK to complete editing and close the editor.

Editing Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Edit Customer**.
- 3 Change the values, as appropriate.
- 4 Click **Apply** to update the customer and leave the editor open, or **OK** to complete editing and close the editor.

Deleting Customers

- 1 Choose the **Customers** resource tree in the Navigator panel.
- 2 Right-click a customer and choose **Delete Customer**.
- 3 Click **Yes** to confirm the deletion.

Chapter 29

Managing Partitions

While the Partition Manager operates automatically, and follows the parameters set for it through the ArcSight Database Configuration Wizard during installation, you can use the Partition features of the Console to review activity and to change partitions' active, inactive, or reactivated status.

["Getting Partition Information" on page 767](#)

["Seeing a Partition Schedule" on page 767](#)

["Archiving Partitions" on page 768](#)

["Reactivating Archived Partitions" on page 768](#)

["Reactivating Zipped or Large Archived Partitions" on page 769](#)

["Deactivating Archived Partitions" on page 769](#)

["Running Scheduled Tasks Right Away" on page 769](#)

["Partition Properties" on page 770](#)

Getting Partition Information

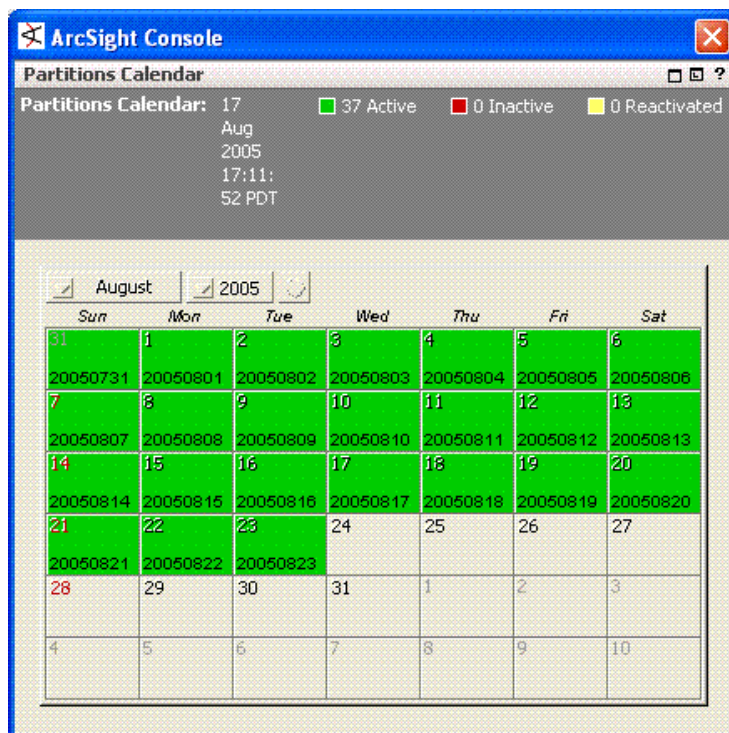
- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a particular partition.
- 2 Choose **Partition Information**.
- 3 Review the partition's properties as displayed in the Partitions Editor, which are described below.

Seeing a Partition Schedule

Partition scheduling applies only to the **System Partitions>Active Partitions** branch of the resource tree. The Partitions Calendar graphically shows the partitioning schedule for a group in the Partitions resource tree. This view can help clarify relationships not readily visible in a resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and right-click a partition group.
- 2 Choose **Partitions Calendar**.

- 3 View the current schedule or click the **Month** or **Year** selectors to change the time period.



Archiving Partitions

Archiving a partition removes it from the database and compresses it for long-term storage. Although it may still be stored online, it is offline relative to the database until you reactivate it. Archiving applies only to the System Partitions>Active Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Archive Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to archive and click **OK**.

Reactivating Archived Partitions

Reactivating a partition restores it to the database, making it available to ArcSight features such as active channels and reports. Reactivation applies only to the System Partitions>Archived Partitions>Inactive Partitions branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Reactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

Reactivating Zipped or Large Archived Partitions

Although you can reactivate most partitions from the Console, follow the process below to reactivate these partitions if

- **Archive Type** was configured as **ZIP** when the partition was archived.
- the partition's **Data Size** field in the Partition Information section of the Partition Editor shows a value of **4000** or greater.

If these conditions are true, do the following:

- 1 Manually unzip the partition with an unzipping tool.
- 2 Ensure that the `arc_event_PartitionName` directory contains the files:

- ◆ `arc_event_data_PartitionName.dmp`
- ◆ `arc_event_data_PartitionName_01.dbf`

If either of these files is missing, the partition archive is invalid and cannot be reactivated. Contact ArcSight Customer Support for assistance.

- 3 On the database machine, enter this in `ARCSIGHT_HOME/bin` to get an SQL interface:

```
arcdbutil sql <username/password>@tnsname
```

- 4 At the SQL prompt, run this script to update the partition's status:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType
<partition_name>
```

Example:

```
@../utilities/database/oracle/common/sql/SetPartitionArchiveType 20060101
```

- 5 Check the log `SetPartitionArchiveType.partition_name.log` to ensure that the script ran successfully. The log shows the before and after values for the row corresponding to the partition in the `ARC_PARTITION_SHADOW` table.
- 6 Reactivate the partition from the Console as described above.

Deactivating Archived Partitions

Deactivating takes a formerly reactivated partition back out of the database. Deactivation applies only to the **System Partitions>Archived Partitions>Reactivated Partitions** branch of the resource tree.

- 1 Choose the **Partitions** resource tree in the Navigator panel and select one or more partitions.
- 2 Right-click the selected partitions and choose **Deactivate Partition(s)**.
- 3 In the Select Partitions dialog box, select the partitions to reactivate and click **OK**.

Running Scheduled Tasks Right Away

You can manually start certain scheduled tasks to cause them to run immediately, rather than wait for the scheduled occurrence. Currently this option covers partition and archive maintenance tasks the system performs automatically.

- 1 Choose the **Partitions** resource tree in the Navigator panel.

- 2 Right-click in the panel and choose **Run scheduled task now**, then **Partition maintenance or Archive maintenance**.
- 3 Depending on the task, timing, and context, the system reports the degree of success or result of the command.

If you schedule a task to run during a transition to or from standard time, see [“Standard Time Transitions” on page 436](#).

Partition Properties

Partition Property	Description
Name	The partition's name, usually by date.
Description	A description of the partition.
Lower Bound	The beginning timestamp for the partition.
Upper Bound	The ending timestamp for the partition.
Fully Valid	Indicates whether or not the partitions for all five tables that make up this logical partition checked as valid. These tables are individually validated in the Table Status section below.
Usable	Indicates whether the most important table, Events, is valid.
Active	Indicates whether the partition is accessible to the database (in contrast to "archived").
Archived	Indicates whether the partition has been removed from the database (in contrast to "active").
Event Count	The number of events recorded in the partition.
Data Size (MB)	The number of megabytes of disk space occupied by event data (not indexes).
Index Size (MB)	The number of megabytes of disk space occupied by indexes (not event data).
Index Type	Either default or custom.
Table Status	These five items show the validity status of the partitions for the tables that make up the logical partition. This is summarized in the Fully Valid field above.

Personalizing the ESM Console

The ESM Console has displays and settings that you use to monitor an enterprise using various windows, panels, views, controls, and tool bars. You can change these displays and settings based on your monitoring needs.

[“Changing the Console Display” on page 771](#)

[“Changing User Preferences” on page 772](#)

[“Saving and Sending Settings” on page 785](#)

Changing the Console Display

You can change the look and feel of the ESM Console to better display information, focus on particular panels, or hide information not of interest. You can resize the ESM Console, float or dock Console panels, apply translucency to a floating panel, and show or hide the menu bars, tool bars, and various displays.

Resizing the Console


To expand the ESM Console to the whole screen, click the **Maximize** icon at the top-right corner of the window. To collapse the ESM Console, click the **Minimize** button or drag the corners of the ESM Console to resize it.

You can also drag and drop any dividers between panels to resize them.


Showing or Hiding Menu Bars and Tools

You can show or hide the ESM Console menu bar, and all the other individual components of the ESM Console interface (apart from the main panels). Right-click the **Menu bar** area of the ESM Console and use the context menu to enable (check) or disable (clear) each component.


Showing or Hiding the Status Bar

Click the **Status Bar** button () on the toolbar, or on the Window menu, choose **Status Bar**.


Showing or Hiding the Navigator Panel

Click the **Navigator** button () on the toolbar, or on the Window menu, choose **Navigator Panel**.


Showing or Hiding the Viewer Panel

Click the **Viewer** button () on the toolbar, or on the Window menu, choose **Viewer Panel**.

Showing or Hiding the Inspect/Edit Panel

Click the **Inspector** button () on the toolbar, or on the Window menu, choose **Inspect/Edit Panel**.

Floating a Console Panel

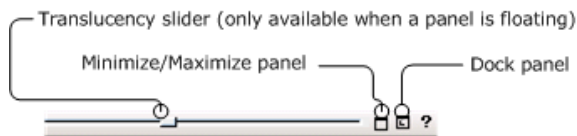
Click the **Float/Dock** button () on the panel header, or right-click the panel header and choose **Float Panel**.

Applying Translucency to a Console Panel


Move the **Translucency** slider on the panel header.




A panel must be floating before you can apply translucency to it. You cannot apply translucency to docked panels.



Docking a Console Panel

Click the **Float/Dock** button () on the panel header, or right-click the panel header and choose **Dock Panel**.

Closing a Console Panel

Click the **Close** button () on the panel header, or right-click the panel header and choose **Close Panel**.

Changing User Preferences

You can change several ESM Console characteristics to suit your security needs, working style, or personal preferences. You reach the Preferences dialog box through the **Edit>Preferences** menu command.

The display on the Preferences dialog changes depending on which Preference button you select.

Changing Your Password

A temporary password is created for you during your first ArcSight session. When you first log in, you should change to a permanent or more personal password. After changing it, be sure to keep it confidential.



You can change your password only if your ArcSight installation is configured to use built-in password authentication. Contact your system administrator for instructions on how to change passwords on ArcSight systems that use RADIUS SecurID or SSL authentication.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Password**.
- 3 Enter your old password, new password, and confirm the new password.
- 4 Click **OK**.

By default, passwords require a minimum of 6 characters, can contain a maximum of 20 characters, and can contain numbers and/or letters. Ask your system administrator about any special requirements for your site.

Changing Other Users' Passwords

Administrators may also reset user passwords; for example, if a user's original password has been compromised or you want to make users update their passwords. For information on how to do this, see [Resetting User Passwords](#) in [Chapter 25, Managing Users and Permissions](#), on page 641.

Setting Program Preferences

You can set the default editors and viewers to use for text, HTML, and packet payloads. For example, you'll use the HTML editor when editing the Knowledge Base and the Web browser for reports.


Program Preference	Value
Preferred Text/HTML Editor	Type the complete path to your preferred text or HTML editor or click the Browse button to locate one.
Preferred Web Browser	<p>You can choose to use your preferred external web browser for all HTML display functions (e.g., reports, documentation indexes) or to use the ESM Console's built-in web viewer, which is Microsoft Internet Explorer by default, for all but exceptionally large, numerous, or insecure HTML files. To use the internal viewer as your primary display, select Use the web browser embedded in ArcSight Console. The external web browser always needs to be specified. Type the complete path or click Browse to locate one. The newest versions of IE and Firefox browsers are preferable.</p> <p>For more information on HTML displays in internal and external Web browsers from the ESM Console, see "Web Browsers (Internal and External)" on page 1030.</p>
Preferred Payload Viewer	Type the complete path to your preferred packet-payload viewer or click the Browse button to locate one.

Program Preference	Value
Text to PCAP Converter	Type the complete path to your preferred packet-payload PCAP converter or click the Browse button to locate one.

Changing Global Options Like Panel and Editor Characteristics

You can make the Inspect/Edit panel open as a docked window inside, or as a floating window outside, the ESM Console. You can do the same with all child windows as a class. You can also choose how informational and error messages are displayed from the ESM Console.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Global Options**.
- 3 Select the checkboxes next to options you want to enable.
- 4 Click **OK**.

Global Option	Description
Font	<p>Set global preference for font face, size, and style used throughout the ESM Console, except on windows or views where you can set fonts specific to those ESM Console elements. (For example, you can set fonts specific to Grid views as detailed in the next topic.)</p> <p>Click into the Font field to get the drop-down menu arrow.</p> <div> <div>Font</div> <div>Tahoma, Plain, 11</div> </div> <p>Click the arrow to bring up the Fonts dialog. Set the Font, Size and Style.</p>
Launch editors in a floating window	Open all editors in a floating window. If deselected, all editors appear in the Inspect/Edit panel. If you select this option, you can still float or dock the windows.
Allow multiple editors of the same type	Permit more than one resource editor to be opened simultaneously for a given resource type (e.g., opening three instances of the Filter Editor at once). Enabling this option is very useful for analysts and persons implementing security solutions, but may inappropriate for operators or other persons who should have less-extensive editing access.
Show error messages in a pop-up dialog	Display all errors in a pop-up dialog.
Show informational messages in a pop-up dialog	Display all information messages in a pop-up dialog.
Create independent floating windows	<p>Independently float new windows that are children of another window such as the Viewer panel. This is the default. When enabled, you can choose a window's name from the list at the</p> <p>Window>Floating command, or toolbar button (), to bring it forward.</p>

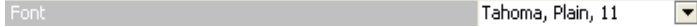
Global Option	Description
Auto Relogin	Automatically log in again after logging out of the Console.
Use system defaults for dashboard background	When this option is selected, your system defaults are used for all Dashboard backgrounds.
Launch Help in external Web browser	<p>When this option is de-selected, the ESM Console Online Help is displayed in an embedded Web browser (the ESM Console internal browser). This is the default.</p> <p>Launch Help in external web browser <input type="checkbox"/></p> <p>When this option is de-selected, the Online Help is displayed in your default Web browser (not embedded).</p> <p>You can access ESM Console Online Help from the Help menu on the ESM Console, right-click Help options on the Navigator and Grid displays, Help buttons on dialogs, and so on. For more about the Help, see “About the Online Help” on page xxxvii.</p> <p>Note: The ESM Console uses Web browsers to display various charts, graphs, reports, and data monitor output (not just Online Help). On Windows systems, the ESM Console defaults to using Internet Explorer Web browser even if you have a different browser set as your personal default browser. So if you enable “Launch Help on web browser” and want the Help to launch in a browser other than IE, also re-set the ESM Console preference for its “External Browser”. On Preferences dialog, click Programs for “External Browser” preference setting. (See also “Setting Program Preferences” on page 773.)</p>
Set Help dialog size (Width,Height)	<p>The Help display window defaults to width of 910 x length of 650 pixels.</p> <p>Set Help dialog size (Width,Height) 910,650</p> <p>You can specify a different default Help window display size here. To do this, enter a new window size (for example: 750,900) and hit keyboard Enter or Return.</p> <p>Note: You need to hit keyboard Enter or Return after entering the new display size, and then <i>also</i> click Apply or OK to save all preference settings. If you do not press Enter or Return, the new window size setting cannot be saved even if you click Apply or OK.</p>

Setting Grid View Options

You can change several characteristics of the Viewer panel's grid views.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Grid View Options**.
- 3 Select the checkboxes of the options you want to enable.

- 4 Click **Apply** to put your changes into effect and leave the Preferences dialog box open, or **OK** to save your changes and close the dialog box.

Grid View Option	Description
Font	<p>Set global preference for font face, size, and style used in Grid views.</p> <p>Click into the Font field to get the drop-down menu arrow.</p>  <p>Click the arrow to bring up the Fonts dialog. Set the Font, Size and Style.</p>
Color text by priority in grid	<p>Apply distinguishing colors to the event rows in Viewer panel grid displays, based on their threat-priority levels. Note that this option can be overridden by the Color text by filter in grid option if conflicts occur. When these options are not selected, the text in grid rows defaults to black.</p>
Color text by filter in grid	<p>Apply distinguishing colors to the event rows in Viewer panel grid displays, based on the filters that selected them. You set these colors through the Configure button, described below. Note that this option, when selected, overrides the Color text by priority in grid option if conflicts occur. When these options are not selected, the text in grid rows defaults to black.</p>
Pause the current channel on event selection	<p>By default, selecting an event pauses the event flow to avoid scrolling. Clear this checkbox to allow the flow to continue regardless of a selection.</p>
Do not prompt on verifying rule channel's timestamp change	<p>Toggles on or off the option to have the system generate a prompt when the timestamp changes on an active channel populated by correlation events.</p>
Do not prompt on channel restart	<p>Toggles on or off the option to have the system generate a prompt when an active channel is restarted.</p>
Check available database partitions on Active Channel start	<p>When selected, this option causes the ArcSight Manager to recheck the status of available database partitions before starting an active channel. This does have a performance effect and is used only for certain forensic purposes.</p>
Filter Coloring Preferences	<p>Click Configure to assign identifying colors to as many as five filters in the Configure Filter Colors dialog box.</p>
Print Column Flip Limit	<p>Determines the print format for Grid Views (channels, lists, and so forth). Grid views with the same or fewer columns than the Column Flip Limit print as a table, the same as is shown in the UI on the ESM Console grid view. Grid views with the more columns than the Column Flip Limit print details per row rather in a normal table like that shown on the ESM Console grid view.</p> <p>The default setting for Column Flip Limit is "10" columns. (Tables with more than 10 columns print details per row.)</p> <p>See also "Printing from the Console" on page 120.</p>

Setting Date and Time Formats

Use the Date/Time option to choose a formatting style for the date and time strings displayed throughout the ESM Console. You can also customize the details of any style you pick.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Date & Time**.
- 3 Click the **Formats** buttons and choose a date/time style from the lists for **Date & Time** Format and **Short Date & Time** Format options. Select **Express all times as GMT** to universally show time values in GMT rather than local times.
- 4 Click **Apply** to put your changes into effect and leave the Preferences dialog box open, or **OK** to save your changes and close the dialog box.

If you wish, you can customize the selected format. Edit the **Format** string using the Java-style date options described in the **Format Help** window, and the information in **Timestamp Variables**.

Configuring Event Graphs

You can modify the way graphs plot events, choosing to keep the source-event-target visual relationships compact, or to emphasize unique sources, targets, or both in order to more easily clarify the nature of attacks or situations.

- 1 On the Edit menu, choose **Preferences**.
- 2 In the Preferences dialog, click **Event Graph**.
- 3 Click the **Value** fields of the graph attributes to choose appropriate options, as described below.
- 4 Click **OK**.

Latitude and Longitude Options

Set the Latitude and Longitude preferences here . . .

Latitude & Longitude Entry Format

☒ DMS: Degree Minute Second (-49°30'00")

☐ DM: Degree Minute (-49°30.0')

☐ DD: Decimal Degree (-49.5000°)

☒ Show compass direction (49.5000° S).

. . . to control which measurement entry format is used for **Asset Locations** descriptions in the Assets Location Editor. (Choose **Assets** in the Navigator, click **Locations**, and edit or create new location to bring up the **Location Editor**.)

Inspect/Edit

Location Editor

Inspect/Edit

Attributes Notes

Location

* Name

Latitude 0° 0' 0" N

Longitude 0° 0' 0" W

City

Region Code

Postal Code

Country N/A

(See ["Managing Locations" on page 765](#). This is a part of [Working with Assets, Locations, Zones, Networks, Vulnerabilities, and Categories](#) in [About the Network Model](#).)

The options for latitude and longitude format vary from more exact to less so. Latitude and longitude can be shown in degrees, minutes, and seconds; degrees and minutes; or decimal degrees only. Additionally, an indicator of compass direction for the specified location can be shown or hidden in the editor.

Event Graph Options

- **Show Event Nodes:** Choose a basis for visually expanding or aggregating event nodes, relative to their source and target node instances.

Choice	Description
Once per common event	Graph only one instance of a given event node, regardless of the number of unique sources and targets that have it in common. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there may be visual instances for each source and target, but only one of the event node.
Once per unique source	Graph one instance of a given event node per unique source, regardless of the commonality of associated targets. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there are two visual instances of the event in support of the two distinct sources.
Once per unique target	Graph one instance of a given event node per unique target, regardless of the commonality of associated sources. For example, if sources 1 and 2 are directing the same event at targets 1, 2, and 3, there are three visual instances of the event in support of the three distinct targets.
Once per unique source-target pair	Graph one instance of a given event node per unique source-target pair, regardless of the commonality of the events involved. For example, if sources 1 and 2 are directing a given event at targets 1, 2, and 3; and as a chain, targets 1, 2, and 3 are sourcing the same events on to targets 4, 5, and 6; then there are six visual instances of the event in support of six distinct targets.

- **Show Source/Target IP Addresses as:** In cases where one source-event-target chains to another, you can choose to graph a source/target IP address as a single node, or to graph both the source and target instances of such an IP address.

Choice	Description
Distinct nodes	Visually plot both the source and target instances of a chained IP address.
Simple nodes	Visually plot a single node for an IP address that represents both source and target.

- **Source Node Identifier:** Choose a different event attribute to use as the identifier for source nodes. The default attribute is Source Address. Note that while all attributes are available, not all are appropriate choices for this purpose.
- **Event Node Identifier:** Choose a different event attribute to use as the identifier for event nodes. The default attribute is **ArcSight Category**. Note that while all attributes are available, not all are appropriate choices for this purpose.

- **Target Node Identifier:** Choose a different event attribute to use as the identifier for target nodes. The default attribute is **Target Address**. Note that while all attributes are available, not all are appropriate choices for this purpose.

Setting Notification Popups

You can manage received notifications from within the ESM Console. In the Preferences dialog box, you can set a severity threshold for notification popups and optionally play a sound when notifications arrive.

For **Severity threshold for notification popup**, raise or lower the integer value to a priority value that is appropriate for the level at which you want to be alerted.

Select **Play a sound when a notification message is received** to also emit a sound when the alert threshold is met.

Managing Hot Keys

The ESM Console provides schemas for configuring keyboard shortcuts to common actions. These schemas come with the ESM Console:

- \$default
- Schemas for users (such as **admin** and other users)



- Schemas for users other than admin are listed only for users who have set up custom shortcuts on this ESM Console under their login.
- Custom shortcuts are available locally only. (See [“Sharing Custom Shortcut Schemas” on page 785](#) for more information.)

Schemas for users are all based on the \$default schema. That is, user schemas inherit all \$default schema shortcuts. The \$default schema.

On the Edit > Preferences > Manage Hot Keys dialog, under “Available shortcut schemas”, the schema currently in use shows as “**(active)**” next to its name.

You can define a keyboard shortcut for each command listed. Each command can have a different (or the same) keyboard shortcut depending on which schema is selected.

Keyboard shortcuts are pre-defined for common commands. For example, the pre-defined keyboard shortcut for the Select All command (`edit.selectAll`) is Ctrl+A.

Commands shown in red on Preferences dialog are not editable (e.g., `edit.delete`, `edit.redo`, `edit.cut`, `edit.copy`, `edit.paste`, and so forth). The flyover tooltips on these commands also indicates they are not editable.

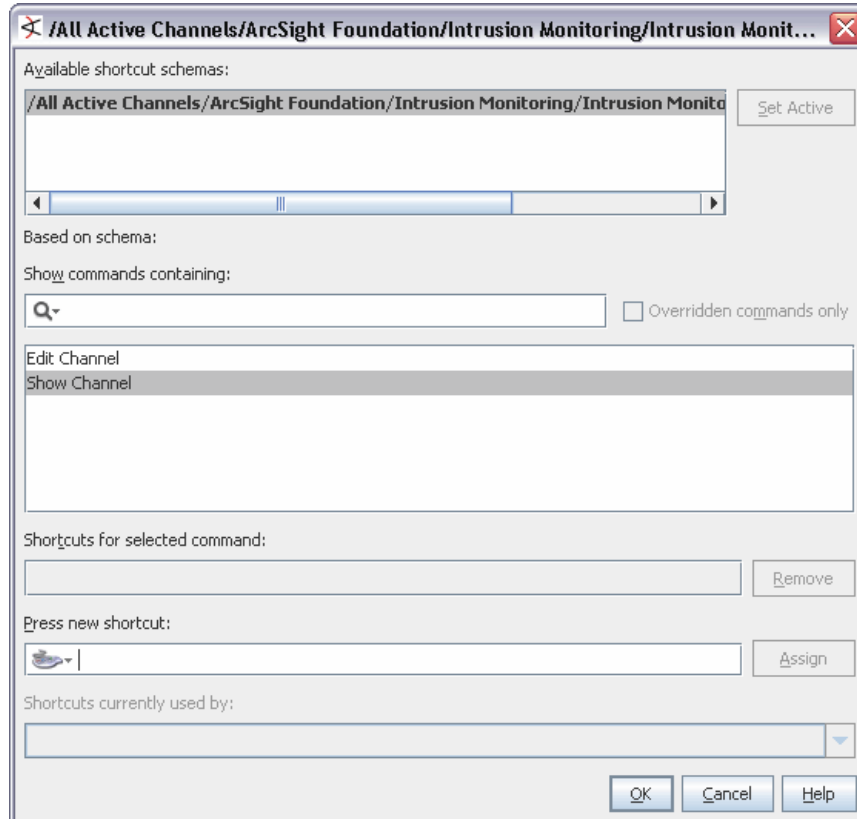
There are many commands listed for which no shortcut is provided (e.g., `file.new.Report`, `file.new.Rule`, `navigator.reports`, `navigator.queryViewers`, etc.)


Adding Shortcuts for Frequently Used Resources

This first task is not initiated on the Edit > Preferences dialog, but rather from various resource contexts in the ESM Console. But the results of setting up Hot Keys on selected resources are shown on the Edit > Preferences > Managing Hot Keys dialog, as described below.

To add a shortcut to a resource:

- 1 Navigate to and select the resource for which you want to add a shortcut.
(For example, choose **Active Channels** in the Navigator, and select an active channel such as [/All Active Channels/ArcSight Foundation/Intrusion Monitoring/Intrusion Monitoring - Significant Events](#).)
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.



- 3 Select the action you want to take with regard to the resource (e.g., Edit or Show).
- 4 In the **Press new shortcut** field:
 - ◆ Optionally, press the button () to get a drop-down menu where you can set the type of shortcut to add (mouse, tab, etc.) and limits on keystrokes. (For example, if you want to set the shortcut on this channel to Ctrl+C+H, this requires first changing the keystroke limit from the default of 1, to 2 keystrokes.)
 - ◆ Type the keyboard sequence you want to associate with the command.
 If there the keyboard sequence you typed is not in use, a light gray "no conflicts" message is shown in the "Shortcuts currently used by" field. (For example, if you select [navigator.rules](#), place the cursor in the "Press new shortcut field", and type Ctrl+Alt+X, you get the "no conflicts" message.)

 If you type a sequence that is already used by another shortcut, you get a message in the "Shortcuts currently used by" field telling you which resource is currently using the shortcut. (For example, the default shortcut for [navigator.rules](#) is Ctrl+Alt+L. If you type Ctrl+Alt+R in the "Press new

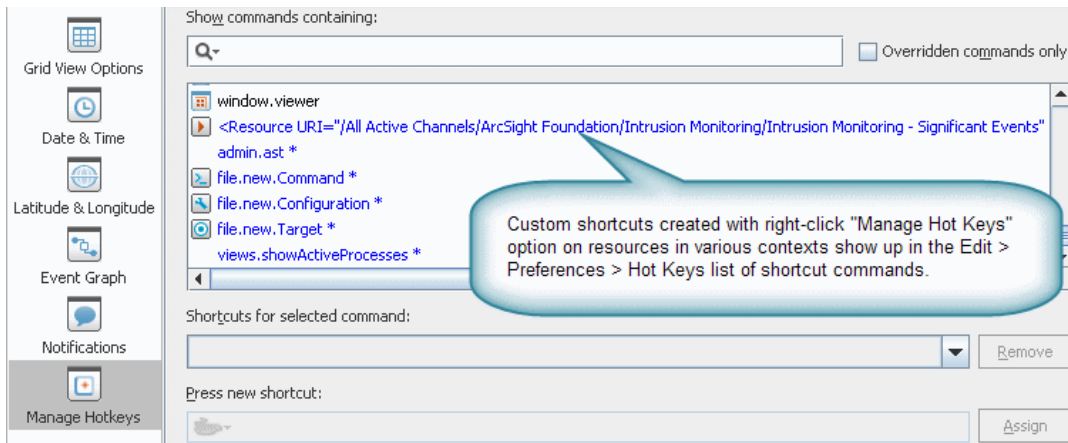
shortcut" field, you get a message noting that this sequence is already in use for `navigator.reports`.)

If you continue with the assignment, you get a prompt asking whether you want to remove the shortcut from the other resource and add it to this new one.

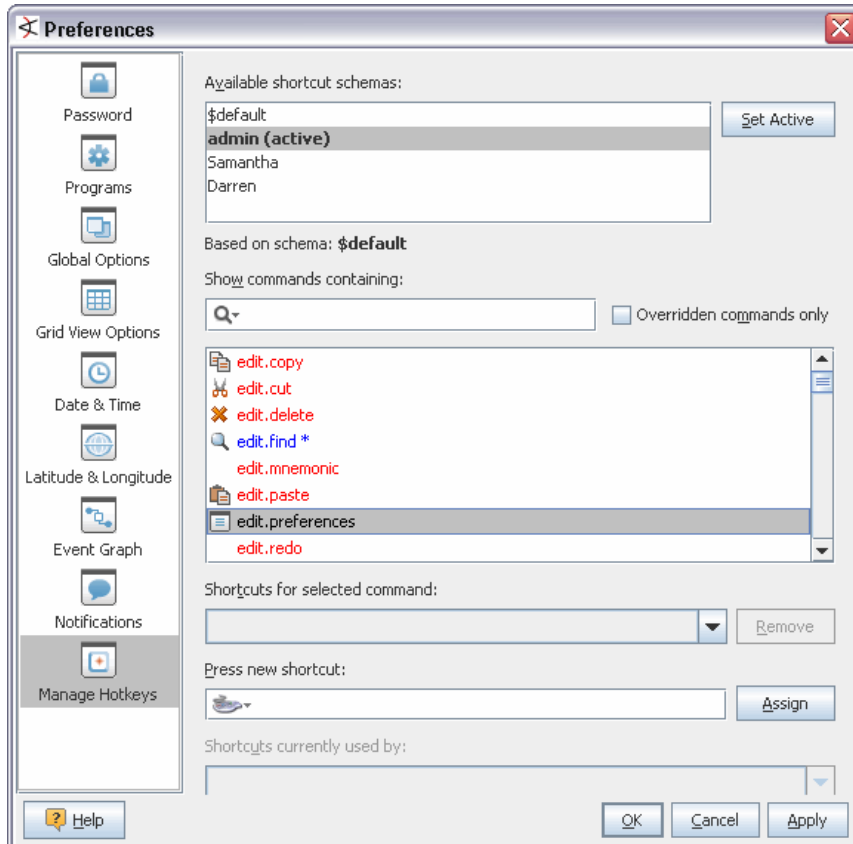
5 Click **Assign** to associate the shortcut with the resource.

6 Click **OK** to save your changes and close the dialog.

Custom shortcuts added to resources are listed on the **Edit > Preferences > Managing Hot Keys** dialog.



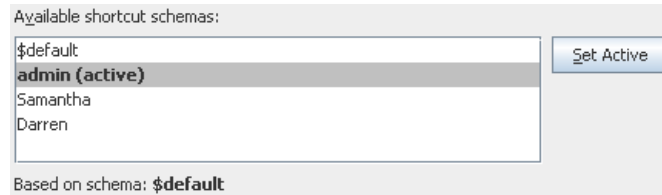
Modifying a Custom Shortcut



To modify a custom shortcut:

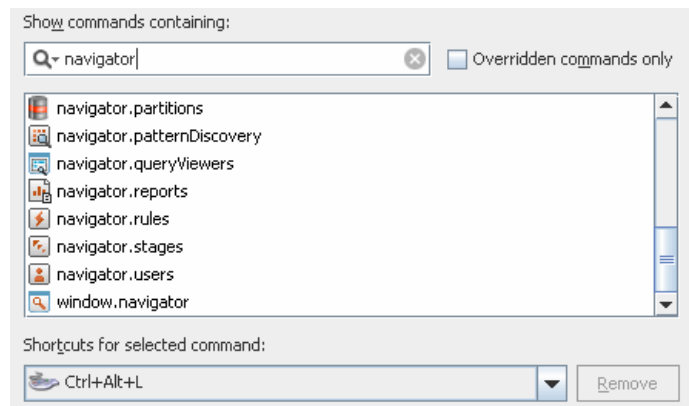
- 1 Select the schema in which you want to modify shortcuts for commands.

In this example, the **admin** schema is selected. Note, however, that the schema selected for modifying a hot key need not be the “active” schema; as it happens to be in this example.




- 2 Select the command for which you want to modify the hot key(s).

You can filter for commands containing a given string (e.g., “navigator” to find all navigator commands).



- 3 In the **Press new shortcut** field:

- ◆ Optionally, press the button () to get a drop-down menu where you can set the type of shortcut to add (mouse, tab, etc.) and limits on keystrokes. (The default keystroke limit is one. If you set it to 2 or 3, you have more combinations of keystrokes available to use for custom settings.)

- ◆ Type the keyboard sequence you want to associate with the command.

If there the keyboard sequence you typed is not in use, a light gray “no conflicts” message is shown in the “Shortcuts currently used by” field. (For example, if you select [navigator.rules](#), place the cursor in the “Press new shortcut field”, and type Ctrl+Alt+X, you get the “no conflicts” message.)

If you type a sequence that is already used by another shortcut, you get a message in the “Shortcuts currently used by” field telling you which resource is currently using the shortcut. (For example, the default shortcut for [navigator.rules](#) is Ctrl+Alt+L. If you type Ctrl+Alt+R in the “Press new shortcut” field, you get a message noting that this sequence is already in use for [navigator.reports](#).)

If you continue with the assignment, you get a prompt asking whether you want to remove the shortcut from the other resource and add it to this new one.

- 4 Click **Assign** to apply the new shortcut to the command.



An asterisk is displayed next to commands for which the pre-defined shortcuts have been modified or overwritten. These customized commands are also displayed in blue text, rather than the usual black.

```

navigator.queryViewers
navigator.reports
navigator.rules *
navigator.stages
  
```

- 5 Click **Apply** to save/apply the new shortcut, or click **OK** to save/apply the new shortcut and close the Preferences dialog.

Modifying Custom Shortcuts for Resources

You can modify a custom shortcut for a resource in either of these ways:

- Directly from the right-click Manage Hot Keys dialog on that resource
- From the Edit > Preferences > Manage Hot Keys dialog as described above in [“Modifying a Custom Shortcut” on page 781](#).

To remove a custom shortcut directly from the resource:

- 1 Navigate to and select the resource from which you want to remove the shortcut.
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.
- 3 Select the action (e.g., Show or Edit) associated with the shortcut.
The shortcut is shown in the “Press new shortcut” field.
- 4 Modify it as needed. (See [“Modifying a Custom Shortcut” on page 781](#).)
- 5 Click **OK** to save your changes and close the dialog.

Removing a Custom Shortcut

To remove a custom shortcut (key sequence) for any command:

- 1 Select the schema in which you want to modify the command.
- 2 Select the command for which you want to modify the hot key(s).
- 3 Select one of the customized commands (blue, with an asterisk).

```

navigator.queryViewers
navigator.reports
navigator.rules *
navigator.stages
  
```

The current key sequence associated with this command is shown in the **Shortcuts for selected command** field.

- 4 Click the **Remove** button next to the “Shortcuts for selected command field”.

The custom shortcut (key sequence) is removed, and replaced by the default key sequence (if there was one).



As soon as you remove the shortcut by clicking **Remove**, the changes are saved. Even if you click Cancel to close the Preferences dialog at this point, *the shortcut is not saved* for when you return.

For example, if `navigator.rules` was modified to be associated with Ctrl+Alt+X, then when you remove this shortcut `navigator.rules` would again be associated with its default shortcut of Ctrl+Alt+L.



Only custom shortcuts can be removed. Default shortcuts cannot be deleted.

Removing Custom Shortcuts for Resources

You can remove a custom shortcut for a resource in either of these ways:

- Directly from the right-click Manage Hot Keys dialog on that resource
- From the Edit > Preferences > Manage Hot Keys dialog as described above in [“Removing a Custom Shortcut” on page 783](#).

To remove a custom shortcut directly from the resource:

- 1 Navigate to and select the resource from which you want to remove the shortcut.
- 2 With the appropriate resource selected, right-click and choose **Manage Hot Keys** from the context menu to bring up the shortcut setup dialog for this resource.
- 3 Select the action (e.g., Show or Edit) associated with the shortcut.

The shortcut, if any, is shown in the “Press new shortcut” field.

- 4 Click **Remove**.
- 5 Click **OK** or **Cancel** to close the dialog.



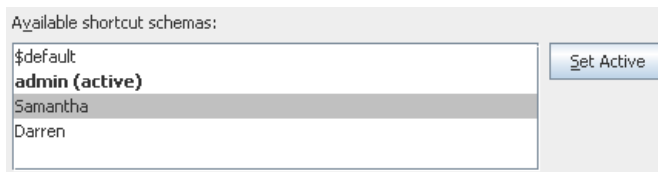
As soon as you remove the shortcut by clicking **Remove**, the changes are saved. Even if you click Cancel to close the dialog at this point, *the shortcut is not saved* for when you return.

Activating a New Shortcut Schema

For more information on schemas, see the introduction to the hot key management at [“Managing Hot Keys” on page 779](#).

To activate a new schema:

- 1 Select the schema you want to activate.

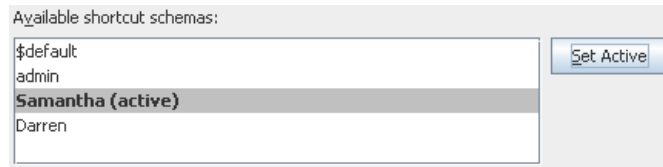


- 2 Click **Set Active**.



To get an enabled Set Active button, select a schema that is not currently applied. If you select a schema that is already active, the Set Active button is disabled.

- 3 Click **Apply** to apply the new schema, or click **OK** to apply the new schema and close the Preferences dialog.



Sharing Custom Shortcut Schemas

Shortcut schemas are made available local to the ESM Console only. That is, if schemas for several different users are configured on an ESM Console running on a particular machine, those shortcut setups (schemas) are not available from the same user logins on other machines.

For example, suppose you customize shortcuts for **admin** user, and two other users (e.g., Samantha and Darren) on laptop A. All three of those users can log in and use their shortcuts on the ESM Console running on laptop A. But if the same users log in on another machine (laptop B) and log in as admin, Samantha, or Darren, none of the custom shortcuts are available on laptop B (unless the same shortcuts were set up manually here also).

Saving and Sending Settings

The **File Save** and **Save As** options allow you to save ESM Console settings (.ast files) locally. You can also save and load your own personal settings from the ArcSight Manager by using the **File Save to Manager** and **File Load from Manager** options. That way, for example, you can quickly restore ESM Console settings when you move to an ESM Console running on a different computer.

Saving a File

- 1 On the File menu, choose **Save** or **Save As**.
- 2 In the Save dialog box, navigate to a directory and enter a file name.
- 3 Click **Save**.

The ESM Console saves your settings in the file you specified, on the local computer. Later, you can restore those settings to return the ESM Console to that configuration, using the **File>Open** command.

Saving a File to the ArcSight Manager

On the File menu, choose **Save to Manager**.

Your ESM Console settings (based on your login user name) are saved to a file and maintained by the ArcSight Manager. To restore your ESM Console to those settings, choose **File>Load from Manager**.

Loading a File From the ArcSight Manager

On the **File** menu, choose **Load from Manager**. The ESM Console loads the saved settings (.ast) file and asks whether you want to apply them to your current session. If you say **Yes**, the Console restarts and refreshes the display.

Sending a File by E-mail

- 1 Choose **File>Send To**.
- 2 In the Send To dialog box, enter the **E-mail Address** and click **OK**.

Chapter 31

Reference Guide

The topics that follow provide information on resources, components, and terms used throughout the guide. Topics are organized alphabetically, and introduced and defined in a style meant to help you get more drill-down information about a term quickly and easily. Unlike a standard “glossary,” however, many of these topics present quite a bit of in-depth information including conceptual and reference material. These topics are cross-referenced (linked) extensively with the rest of the Help topics and vice versa.

Access Control Lists

ArcSight uses Access Control Lists (ACLs) to manage user group permissions. ACLs define which user groups have permissions to which resources, and to which components such as rules, reports, and filters. (See also [“Editing Access Control Lists \(ACLs\)” on page 646.](#))

User groups can have inspect (read) permissions, edit (write) permissions, or both. If a user group has inspect permissions, they can read the resource. For example, the users in the group can see the resource and related information through the ESM Console. If the group has edit permissions, they can write to or change the resource, such as writing or editing a rule or report resource.

Resources, too, can have inspect (read) permissions, or edit (write) permissions. Resources, like user groups, are managed as groups and not as individual resources. Therefore, a resource can only be accessed if a user group has access to the resource's group. Permission to inspect or edit resources is granted when the user logs in, and the resource only appears in the ESM Console if the logged in user has inspect permissions.



Note

Best practice: Log out and log back in again for permission changes to take effect

As a best practice whenever an Admin changes another user's permissions, the other user should log out and log back in again. This ensures that the new permissions are registered with the Manager, and the user can see the changes.

Resource ACLs

Resources have ACLs to help you manage user permissions based on the resource. You can use the resource ACL to determine which user group can access it. You can control which user group has access to inspect or to edit any resource, such as rules, cases, and reports. (See also [“Editing Access Control Lists \(ACLs\)” on page 646.](#))

Events are also available to user groups based on resource ACLs. For example, you can control which user group has access to a filter by adding the group to the filter's ACL and giving them inspect or edit permissions. If you no longer want the group to have

permissions to that filter, you can edit the group's permissions or remove the group from the filter ACL. In this example, the user group listed on the filter ACL with inspect permissions can see events from that filter in the ESM Console. Those without permissions cannot see any events from that filter.

Events are also extracted from the ArcSight Database based on ACLs. For example, when users generate reports, events extracted from the database are based on ACLs. Therefore, only data that users have access to is retrieved and all data may not be included in the report. Report ACLs can only provide events if the user generating the event has the permissions to view those events. For example, if user group A has permissions to view events from filter A and user group B does not, user group B cannot be able to extract event values from filter A when running a report; the report comes back empty. However, since user group A does have permissions to filter A, user group A's report comes back with the values from filter A.



The Resource ACL display shows relationships between users and groups, and how permissions are acquired for each of the user groups. Child groups inherit permissions from parent groups.

For example, consider the following set of ACLs for assets.

Resource	R	W
/All Users/Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
/All Users/Default User Groups	<input checked="" type="checkbox"/>	<input type="checkbox"/>
/All Users/Default User Groups/Analyzer Administrators	<input type="checkbox"/>	<input checked="" type="checkbox"/>

In this scenario, the following permissions apply:

- A user logged in as Administrator (belonging to the group /All Users/Administrators) has read and write permissions by virtue of being in the Administrators group.
- All users have read permissions because they belong to the group /All Users/Default User Groups by default.
- A user logged in as an Analyzer Administrator has both read and write permissions because they inherit read permissions from the parent group (/All Users/Default User Groups) and get write permissions per the Analyzer Administrators child group

Actions

Actions are automatic procedures that occur when all rule conditions and threshold settings have been met. You can choose to be notified of a triggered rule at the ESM Console or through the Notifier, have information about the events that triggered the rule sent to a case or an active list, or automatically execute a command line function. You can also assign more than one rule action to any rule. See also [“Rule Actions” on page 972](#).

Active Channels

Almost all event-related views are **active channels**. Also, several types of resources related to assets and cases are shown as active channels.

Rather than simply flowing events through as received, or capturing a fixed set of events for replay, a channel is in effect a live, on-going event query. Because it is continually re-evaluated, the set of events collected in a channel can continue to change (due to reporting latency), even when defined with a fixed time-bracket.

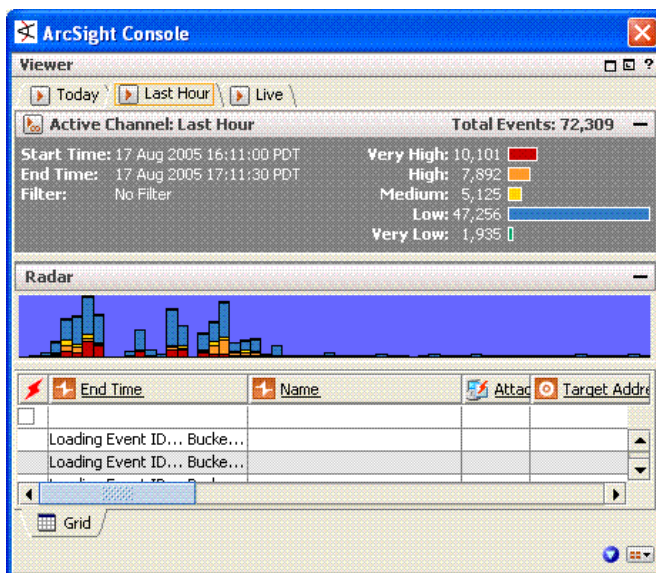
In other words, active channels are definitions for collections of events; definitions that are always freshly re-evaluated so the resulting sets are as valid as the data received up to that moment.

The queries that define active channels are composed, at a minimum, of time parameters; other filter conditions of the usual sorts can also apply. You find and use these queries in the Navigator panel's Active Channels resource tree. You create these definitions through the **File>New>Active Channel** command and can refine them using inline filters and the Active Channel Editor. Once defined and displayed, you can manipulate the order, format, and content of these views with all the familiar features of the ESM Console.

Query viewers are provided as a quick alternative to active channels, better suited to some scenarios. See [“Query Viewers” on page 287](#) for more information.

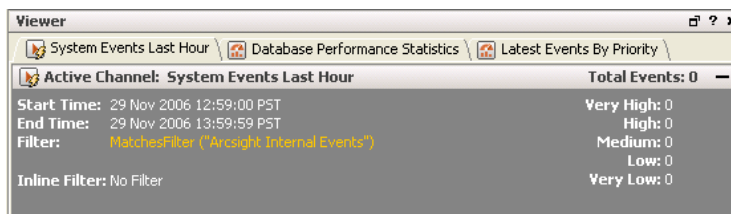
Active Channel Views

Each individual view is one **rendering** of an active channel, whether it is a grid view or chart view. Individual views are represented by the tabs you see at the bottom edge of the Viewer panel. Channels are represented by the tabs at the top of the Viewer panel, that group together individual views.



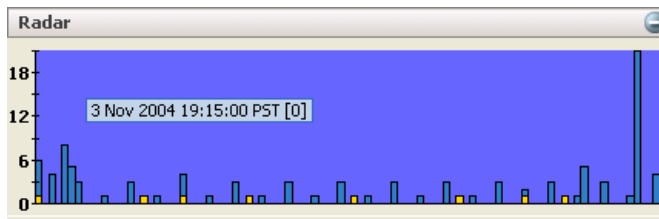
Active Channel Headers

The channel name and statistics line appears at the top of active channel views. These statistics are event-severity indicators for the view. The indicators show the current number of events in the view for each of the priority categories. You can click these indicators to instantly filter the channel to show only the selected priority.



The **Filter** status line describes the filter conditions the channel is currently using.

The Radar display in active channel headers indicates the activity taking place in the channel, in graphics that represent units of time horizontally, and numbers of events in vertical bars segmented by Priority attribute-value counts. The time and quantity scales in the graphic automatically adjust to accommodate the scope of the channel. The broader the scope, the smaller the graphical units become.



You can open and close the Radar display with the **Plus (+)** and **Minus (-)** button at the right end of the Filter line.

With simple gestures, you can control the contents of a grid view using its Radar display. **Click**, **Shift+click**, **Ctrl+click**, or drag to select one or more contiguous or non-contiguous bars in the display. You can also drag selection borders left or right to adjust a span further. The grid then shows just the events the selection represents.

Comparisons

You may want to note that the Manager handles active channel traffic through its database. This means that the content is persisted, but may involve processing delays that cause an active channel to show information later than a more direct method such as the data monitors in dashboards. Conversely, data monitor traffic resides only in memory and is subject to loss or abbreviation by server restarts.

See the topic [“Viewing and Using Channels” on page 130](#) to learn more about active channel tasks. You may also want to compare active channels to active lists as analysis tools.

Active Channel Views for Assets and Cases

The ESM Console shows assets, vulnerabilities, asset categories, scanner reports, and cases in **active channels** (rather than static grid views, as in previous releases). Now you can leverage the power of channels for asset management, including use of filters, field sets, better sorting capabilities, and dynamic display of an unlimited number of items (continually updated).

Active Lists

You can use **active lists** to create a configurable data store that can hold information derived from events, or other sources.

Active lists can monitor activity based on any rule-driven combination of event attributes or set of custom fields. For example, active lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised.

You can populate active lists manually when necessary (adding entries from grid views or the Active List Editor), or use active lists in conjunction with rules specifically tailored to work with them. Rules can dynamically add and remove entries on active lists, thereby making them a flexible information-gathering tool.

You can now open and edit active lists in grid views.

Active lists function differently than active channels. Active lists are not continuously re-evaluated and are not time-window constrained. Active lists draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them.

You can use active lists as filters in other resources that are not based on active channels, such as reports.

In addition to their integral definitions, you can apply temporary (not saved) filters to active list grid views. Click the status description in the **Filter** line in the view header to use the Common Condition Editor.

Use the default items in the Active Lists resource tree for templates or for operational monitoring with minor modifications. For example, use the Trusted List to watch activity from known-to-be-safe IP sources and the Untrusted List to do the same for known unsafe sources.

If you have Administrator access you can have another group named All Active Lists that contains all active list groups and lists.

Uses of Active Lists

The main uses of active lists are to:

- Maintain information, such as in the system content provided "Hostile List" or "Trusted List" which maintain information on hostile and trusted IP addresses (and corresponding zones)
- Check for the existence of particular information in lists using the InActiveList condition (see ["Condition Tree Command Buttons"](#) on page 848).



InActiveList operator does not parse multi-value attributes

The InActiveList operator only evaluates single-value attributes, and treats multi-value attributes, such as Actor Account ID and Role, as single-value attributes.

For example, when a system is compromised (such as in a security breach), it can be added to the compromise list using rule actions. The information in the active list can then be used to collect all the events that occur on the asset while it is compromised. This can be used for tracking and further investigation on other systems that have come into contact with the compromised system

Active Lists for Long-Term State Retention

Active lists can store data over a longer period of time than rules or data monitors are capable of retaining. For example, rules can hold a state that describes the very recent past, normally few minutes. Data monitors may contain up to a day's worth of data, but data monitors usually contain aggregated data.

For example, Active Lists can answer the following question, which cannot be addressed directly by rules or data monitors: "Has the source IP of the current event attacked one of my systems in the last 30 days?"

Optimize Data with Hash-Based Active Lists

A **hash-based active list** uses a hash function to map a set of data to a single number (a hash value).

To create a hash-based active list, enable the Optimize Data option on the Active Lists **Attributes** tab. (See [“Managing Active Lists” on page 571](#).)

The main advantage of using the hash-based active list (via the Optimize Data option) is to reduce memory usage. Instead of storing the complete active list entry in memory, only the hash code (a number), count, and last modified time are stored. The complete entry is available in the database. Therefore, the size of each entry in memory is constant, regardless of the number of fields and corresponding data types in the active list schema.

In terms of performance, there is little or no difference between hash-based and regular active lists.

The Optimize Data option is useful for active lists that contains a large number of entries (for example, more than 100,000 entries) or a large amount of information per entry.



Note

There is a possibility of getting an inaccurate result from an active list that uses the Optimize Data option due to hash collisions. When two active list entries map to the same hash code, the result of the InActiveList condition can be inaccurate in some cases. However, the chances of two entries evaluating to same hash code are quite rare. In the current scheme, for an active list with 1 million entries, the chances of hash code contention are about 1 in 4,000,000.

Active Lists can be switched between optimized (hashing) and non-optimized (non-hashing) after they are created.

Active List Audit Events

Audit events are sent on the following Active List Activity.

- Adding an entry (DEC: /ActiveList/Add)
- Removing an entry (DEC: /ActiveList/Delete)
- Updating an entry (DEC: /ActiveList/Update)
- Expiration of an entry (DEC: /ActiveList/Expire)
- Eviction of an entry (DEC: /ActiveList/Evict)



Tip

DEC stands for *device event category*, an event field. For example, when an active list entry is added, an audit event is generated with a DEC string of /ActiveList/Add.

You can use audit events in rules, filters, and other analytical or administrative resources. For more information, see [“Audit Events” on page 811](#).

Active List Monitor Events

The following monitor events include Active List Usage statistics. (See [“Status Monitor Events” on page 988](#) for more information.)

- Open Active Lists count (DEC: /Monitor/ActiveLists/ListCount)

- Active List entry count (DEC: /Monitor/ActiveLists/EntryCount)
- Active List entry capacity (DEC: /Monitor/ActiveLists/EntryCapacity)
- Active List entry usage (% of capacity used) (DEC: /Monitor/ActiveLists/EntryPercentUsed)
- Active List entry look-ups per second (DEC: /Monitor/ActiveLists/QueriesPerSecond)
- Active List entry updates per second (DEC: /Monitor/ActiveLists/ChangesPerSecond)
- Temporary Active Lists count (DEC: /Monitor/ActiveLists/TemporaryListCount)
- Temporary List entry count (DEC: /Monitor/ActiveLists/TemporaryEntryCount)
- Temporary Active List entry capacity (DEC: /Monitor/ActiveLists/TemporaryCapacity)
- Temporary Active List entry usage (% of capacity used) (DEC: /Monitor/ActiveLists/TemporaryPercentUsed)

Active Lists with Values

An active list with values divides the set of fields into key fields and value fields. Active lists with values provide the following functionality:

- Use an `InActiveList` condition to check the existence of an entry (using only keys, or keys along with values). See [“Condition Tree Command Buttons” on page 848](#) for more about applying an `InActiveList` condition.



InActiveList operator does not parse multi-value attributes

The `InActiveList` operator only evaluates single-value attributes, and treats multi-value attributes, such as Actor Account ID and Role, as single-value attributes.

- Look up value fields for given key field values. Keys and values can consist of one or more columns.

A single key can map to a single value; for example, user name (key) to badge ID (value).

Also, a single key can map to multiple values (in a *multi-map* active list); for example, user name (key) to badge ID, first name, last name (three values). The actors resource is a typical use case for multi-map active lists. For example, you might map a single actor (key) to multiple roles (values).

Variables are used to retrieve the value portion of the active list entry.

To create an active list with values, select the **Fields-based** data option on the Active List editor Attributes tab, check **Key Fields** to enable a per-field Key option, and then select one or more data fields that must be unique. (For the complete procedure, see the topic on [“Creating an Active List” on page 571](#).)

Using Variables to Retrieve Data from Active Lists with Values

To add a list field in a condition, use the following variable functions, which can yield list values:

- `ConvertListToString`
- `GetSessionData` (on overlapping session lists)
- `GetActiveListValue` (on multi-map active lists)
- `GetGroupsOfAsset`

- [GetGroupsofNetworkZone](#)
- [AliasField](#)

When defining a variable to retrieve value information from active lists with values, be sure to specify these attributes for the variable:

- Name of the variable
- The active list to be used to retrieve values for the key
- Field mappings (mapping of the event fields to key fields in the active list)

For more about working with variables, see [“Variables” on page 1006](#).

Example: Active List with Values to Store Directory Information

As an example, suppose we want to create an active list with values to store directory information.

Create an Active List

We follow the basic procedure to create a new active list shown in [“Managing Active Lists” on page 571](#). For the example, we create the active list with these options.

- Specify **Fields-based** data using **Key** fields
- The **Key** is the **Username**.
- The values contain various information corresponding to the given user name. For simplicity, you can store only user role information. (The user role usually determines the type of actions a user can take, and on what type of resources.) If desired, you can store additional information such as the user's First Name, Last Name, Phone Number, Email Address, and so on.

The screenshot shows the 'ArcSight Console' window with the 'Active List: User Roles' configuration. The 'Active List' tab is selected, showing a table of attributes and a 'Common' section for defining the data source and key fields.

Active List	
* Name	User Roles
Optimize Data	<input type="checkbox"/>
* Capacity (x1000)	1
* TTL Days	1
* TTL Hours	0
* TTL Minutes	0

Common

(Name)
(Description)

* Data: ☐ Event-based ☒ Fields-based ☒ Key Fields

Name	Type	Sub-type	Key-field
Username	String		<input checked="" type="checkbox"/>
User Roles	String		<input type="checkbox"/>

OK Cancel Apply Help

Populate the Active List

We can populate the list in any of various ways:

- Manual data entry
- Export required information from Active Directory into a CSV file, and then import entries to the active list from the CSV file
- Use Active Directory User Group Puller tool
- Use event-based integration or other tools

Correlate Information Stored in UserRoles List

Once the Active Directory information is populated to an active list with values, we can access and correlate the user information using reports, rules, active channels, data monitors, and so on. The details of the correlation logic are as follows.

Create a Rule

For this example, we choose a rule that does the following:

- Looks for events that update some critical database information
- Checks if the target user had privilege to perform the operation using the Active Directory User Role information, maintained in the active list

(For more information on creating rules, see [“Creating Rules” on page 440](#) and [Chapter 16, Rules Authoring, on page 439](#).)

Use Variable to Get Role Information

For the database update events, we can get the corresponding Active Directory role information using the **GetActiveListValue** variable.

Edit Variable

Name:

Function:

Retrieve ActiveList value

Arguments

List:

Field Mapping

For each key field, select a matching event field.

Name	Field	Key
Username	Target User Name	<input checked="" type="checkbox"/>

Preview

Set a value for each key field.

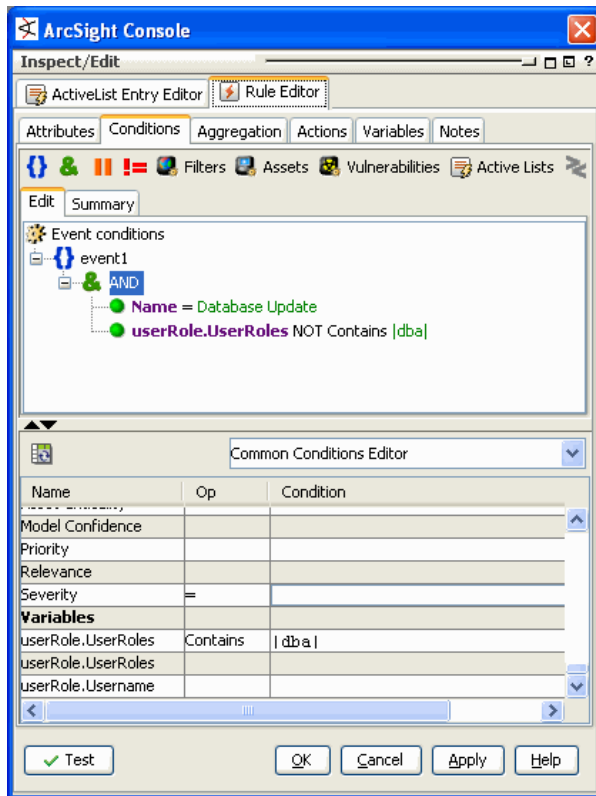
Name	Value
Key Fields	
Username	

Calculate

OK Cancel Help

Set Conditions to Check Role Permissions

Once the role information is retrieved, we can check if the user has the role required to perform this operation. If the user does not have the required role, then the rule is triggered to alert the administrator to the unauthorized access.



Take Action Based on Results of Permissions Check

If the user does not have required role, then rule can trigger and alarm the administrator regarding this unauthorized access. (This is configured via the Actions tab.)

Working with Active Lists

For procedural information about working with active lists (including how to create, edit, delete, import, and export them), see [“Managing Active Lists” on page 571](#).

Administrator

An administrator is a person who has the rights to administer ArcSight and manage users, groups, and their permissions.

See also [“Users” on page 1005](#), [“User Types” on page 1006](#), [Chapter 25, Managing Users and Permissions, on page 641](#).

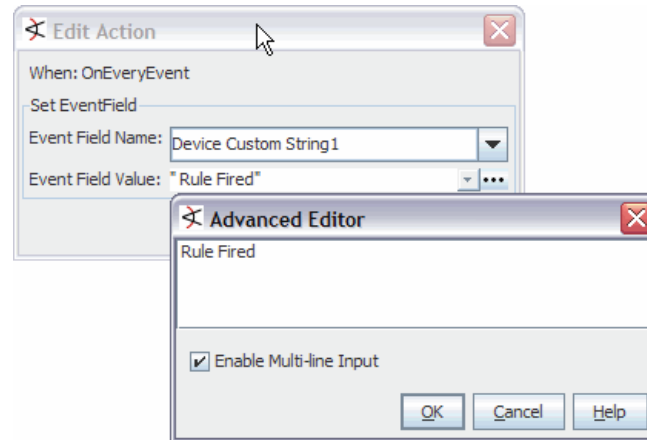
Advanced Editor

An Advanced Editor is available to accommodate special requirements based on context for providing input to various fields, conditions, or other values. The Advanced Editor provides different features, depending on the context in which it is called or used in the ESM Console.

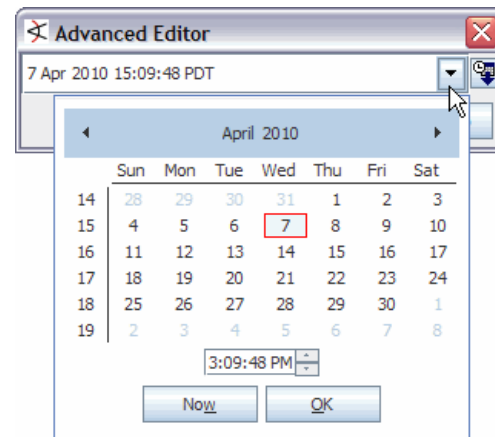
Typically, the Advanced Editor shows up during edit operations in the [Common Conditions Editor \(CCE\)](#), [Rules Editor](#) (for example, editing rule actions), and [Variables](#) editors, but it might show up in other contexts also.

Here are just a few examples of some of the contexts and features the Advanced Editor provides.

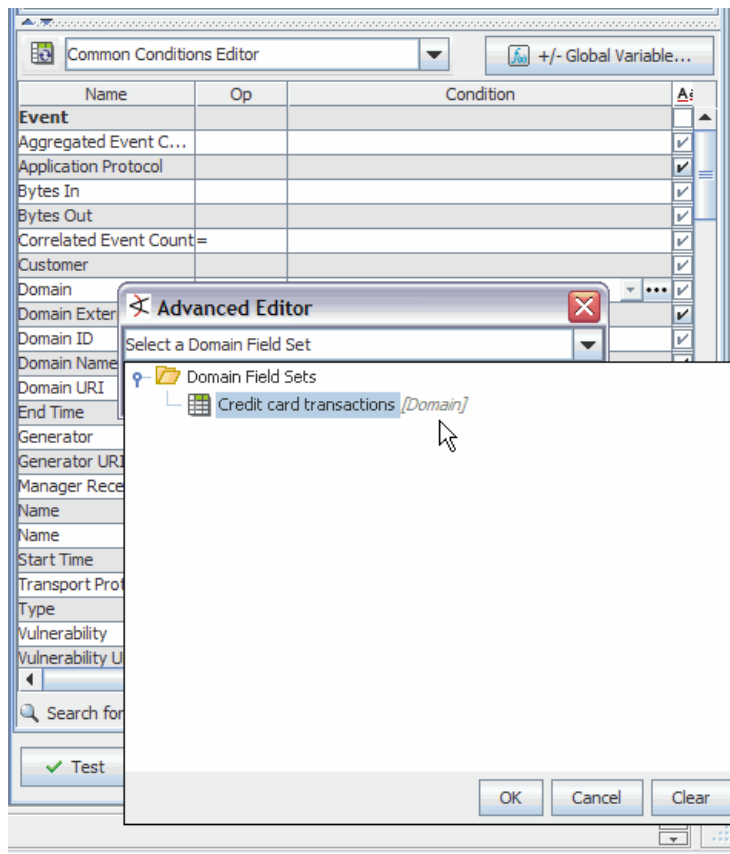
- Enable multi-line input. Advanced editors provide an option to enter multi-line input for rule action triggers, event field values in the common conditions editor (CCE), and so forth.



- Provide calendars and times.



- Choose a field set from a list.



Aggregation

Aggregation is a composition technique for building a new event from one or more existing events that support some or all of the new event's conditions.

You use aggregation to group occurrences of matching conditions based on incoming event field data values, and optionally count only distinct occurrences of those events. To support that, the ESM Console provides Group By aggregation, in which you can group (aggregate) correlated events by field values. You can also optionally include distinct-value event processing combined with either join conditions and/or event grouping, to provide further constraints on when rules should fire.

Rules always run subject to their associated aggregation parameters, even if only the defaults. For more information, see [“Specifying Rule Thresholds and Aggregation” on page 449](#).

The *aggregated event count* (see [related information on page 882](#)) is a derived event field available in the [Event Inspector](#), the [Common Conditions Editor \(CCE\)](#), and shows up in various data monitors (for example, [Moving Average Data Monitor](#)).

ArcSight Web

ArcSight Web provides access to the ArcSight [Manager](#) from a Web-based client.

- ArcSight Web offers a subset of the features found in the ArcSight [ESM Console](#), including full event monitoring and drill-down capabilities.

- For ArcSight Express users, the streamlined ArcSight Web client fitted with ArcSight Express specific content is the primary user interface for monitoring and analysis.

ArcSight Web features include monitoring [Events](#), managing [Cases](#), acknowledging and resolving [Notifications](#), running [Reports](#), and reading [Knowledge Base](#) articles. You can open ArcSight Web with the **File > Launch ArcSight Web** command in the ESM Console, or use a bookmark that points to a URL similar to:

<https://<ArcSightWebHost>:9443/>

Because it can be installed at a location remote from the Manager, ArcSight Web can operate outside a firewall that protects the Manager. It also offers opportunities for custom branding and styling.

To learn more about ArcSight Web, use its online Help system.

ArcSight Web uses the Macromedia Flash player, version 6.0 or later. While most browsers for most operating systems include Flash, some do not. If not, download it from <http://www.macromedia.com>.

See the instructions in the **ArcSight Installation and Configuration Guide** to install, set up, and begin using ArcSight Web.



When installing ArcSight Web, it is important to ensure that its version number matches the Manager. Because a mismatch could cause unpredictable results, the web server prevents users from logging in. During setup, you specify the ArcSight Web server. There is an option not to setup this server, but doing so de-activates ArcSight Web.

Assets

Assets are network devices, installed throughout your enterprise, that you monitor for vulnerability or attack. Once asset information is stored, ESM tracks your assets and notifies you if they are exposed to a threat or vulnerability, or if they are attacked.

Within the Navigator panel's Assets resource tree there are a number of views of associated information. The Assets, Networks, Zones, Locations, Categories, and Vulnerabilities tabs each show different aspects of the devices in question.

When, how, and why you might need to modify the resources in the Assets tabs is described in Managing Assets and Associated Resources, and particularly in Changing Assets. Help for managing hundreds of thousands of assets is described in [“Asset Scalability” on page 757](#). What the Assets tabs contain is described below.

Assets Tab

This view shows the population of your network as discreet entities with specific IP addresses and unique MAC and host names. You often use this view to pinpoint a particular asset, then double-click it to change its characteristics and associations in the Asset Editor. The presentation is hierarchical and shows only the assets to which you have access through the Asset Editor. Note that you can also identify mobile assets by MAC address.

Because the usage (Zones) and descriptive (Categories) views are separate, the Assets view is free to accurately describe the access restrictions that apply to a given user.

The Internet Address Range asset category has its own Asset Range Editor. The address range groups are standard spans of IP addresses provided as a convenience for your use in

rules. You can also collectively reference these ranges using the named networks on the Zones tab. For example, a rule could reference the Dark Address Space item under System Zones to identify a category of source IP addresses from which traffic should not legitimately originate.

The Asset, Zone, and Asset Range Editors all include Categories and Zones tabs for editing these attributes.

The Asset Editor has an Alternate Interfaces tab. When a single device has multiple network interfaces, you can define each interface as an independent asset. Common examples of multiple interface devices are network connection points such as routers and bridges. To use this editor from an appropriate asset in the tree, right-click it and choose **View Asset Alternate Interfaces**.

An asset or asset range (or its group) can belong to only one zone or location.

Zones Tab

The **Zones** tab shows the hierarchy of network-related logical (usage) groups into which assets are collected, and on which you can act through the Zone Editor.

You can also think of zones as aliases for portions of your network that are dedicated to certain organizational groups or functions. The Zones view can help disambiguate multiple private networks that might have overlapping address spaces.

When the zones in your enterprise are referencing multiple global or local zones, ArcSight networks can help disambiguate erroneous address space overlaps or gaps, especially for SmartConnectors. A zone or zone group can belong to only one network or location, and expresses a single contiguous address range.

Networks Tab

Here you can view the hierarchical collection of network entities recognized within your system. In this context, a network is an enterprise-level registry of ArcSight zones. Networks are used to reconcile overlapping or missing asset ranges among zones (if they should erroneously occur). When networks are present, SmartConnectors use them to find their correct zone assignments. Note that networks apply only in enterprises that have networks broad enough to require multiple local or global maps. If your enterprise maps only its own address space (meaning that overlaps and gaps aren't likely) the Networks tab won't be populated.

Each Network resource can relate to only one Customer resource, but to multiple Zones, provided address ranges do not overlap.

Categories Tab

The hierarchy of asset categories provides a way to reference assets by means of their application or context. A given asset can be associated with multiple categories.

Asset categories are a cross-referencing capability that supports numerous business objectives. By making it possible to track network activity with certain assets on the basis of their business significance, data collection becomes possible; but just as importantly, other ArcSight analytical tools can also be brought to bear to derive many kinds of information. Finally, reporting capabilities can further analyze and permanently record the results.

The categories for a given enterprise are often quite specialized, but certain categories are usually present, even if customized.

Typical high-level asset categories often include:

- **ArcSight System Administration:** These assets include its Console, Databases, SmartConnectors, and Managers. ESM automatically detects its own administrative assets and creates these entries in their respective groups.
- **Site Asset Categories:** These can be general monitoring categories such as Address Spaces, Applications, or Open Ports, but may include asset-tracking categories that are specific to issues such as business impacts and regulatory compliance. Business impacts might analyze the activity of a server that supports a particular product line. Regulatory compliance could monitor groups of workstations for HIPAA conformity.
- **System Asset Categories:** These can be any of a number of categorizations of assets such as Criticality (low, medium, high, very high), which would monitor by a classification of how crucial assets are to the enterprise.



SmartConnector configuration also affects the ability to automatically create the assets that represent network devices. Each SmartConnector needs to report an IP address or hostname for its sensor so its events can be identified on the network. See the configuration guides for your SmartConnectors to ensure they are reporting this information.

Vulnerabilities Tab

The **Vulnerabilities** tab presents known vulnerabilities associated with the devices identified through the Assets tab.

Device vulnerabilities are presented as closely as possible with device descriptions to facilitate useful comparisons and easy reference

Locations Tab

The **Locations** tab shows the hierarchy of names your enterprise uses for its physical or geographical domains.

Similar to zones, you can think of locations as another type of alias. You use this alias for portions of your network that are referenced by where they are rather than by organizational group or function. A given asset or asset range can be associated with only one location, but a given location can be associated with any number of appropriate assets, zones, or their groups.

Asset Auto-Creation

As described in [“Auto-Created Assets” on page 733](#), ESM automatically creates assets for components and, if applicable, for assets arriving from scan reports sent by vulnerability scanners via scanner SmartConnectors.

As a configuration option, you can also configure the creation of assets for devices reporting through SmartConnectors.

This section describes in detail how assets are automatically created from vulnerability scan reports and, if so configured, for devices reporting through SmartConnectors. All of the default behaviors described in this section can be customized by changing settings the `server.properties` file. For details, see [“Asset Auto-Creation Advanced Configuration Options” on page 808](#).

Creating Assets from a Vulnerability Scan Report

Assets are created from vulnerability scan reports differently for dynamic and static zones (for more about dynamic and static zones, see [“Dynamic and Static Zones” on page 736](#)).



Scanner reports list only information received through the scanner, whereas Asset Editors include the full list of both scanner data and vulnerability mappings stored in the system. So, the Editors might show more or different information than that shown in scanner reports.

Creating Assets from a Vulnerability Scan Report for Static Zones

For assets in static zones, you need at least an IP address or a host name to create an asset. Asset identifiers are looked up in the following order in a static zone:

- **MAC address > IP address > host name**

The table below describes the action taken based on available IP and host name information.

Table 31-1 Vulnerability Assets in Static Zones

Example	Action taken if no conflicts	Action taken if previous asset with similar information
IP=1.1.1.1 hostname=myhost	Asset created	Previous asset updated
IP=1.1.1.1 hostname=null	Asset created	Previous asset updated
IP=null hostname=myhost	Asset created	Previous asset updated
IP=null hostname=null	Asset not created. Either IP or host name is required.	No action taken. Either IP or host name is required.

Creating Assets from a Vulnerability Scan Report for Dynamic Zones

For assets in dynamic zones, assets are identified by IP address and host name and/or MAC address. Asset identifiers are looked up in the following order in a dynamic zone is:

- **MAC address > host name > IP address**

By default, assets are not created in a dynamic zone if there is no host name present. The property set by default is:

```
scanner-event.dynamiczone.asset.nonidentifiable.create=false
```

Also by default, previous assets with similar information are discarded. This ensures that the network model is kept up to date with devices that are actively reporting events. The default property is set like this:

```
scanner-event.dynamiczone.asset.ipconflict.preserve=false
```

Below are the actions taken by default.

Table 31-2 Vulnerability Assets in Dynamic Zones

Example	Action taken if no conflicts	Action taken if previous asset with similar information
IP=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created	Previous asset deleted
ip=1.1.1.1 hostname=myhost mac=null	Asset created	Previous asset deleted
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created	Previous asset deleted
ip=1.1.1.1 hostname=null mac=null	Asset not created. Either host name or MAC address is required.	Asset not created. Either host name or MAC address required. Previous asset deleted.
ip=null hostname=myhost mac=null	Asset created	Previous asset deleted
ip=null hostname=null mac=0123456789AB	Asset created	Previous asset deleted
ip=null hostname=myhost mac=0123456789AB	Asset created	Previous asset deleted

You can configure the system to create an asset if the asset has either an IP address or a host name, or to preserve previous assets with similar information by customizing settings in `server.properties`. For details, see [“Asset Auto-Creation Advanced Configuration Options” on page 808](#).

Creating Assets for SmartConnectors

ESM auto-creates assets for the ArcSight SmartConnectors connected to it. Creating assets for SmartConnectors is affected by the following conditions:

- ESM does not create an asset if there is no Network defined for the SmartConnector. This could happen if a SmartConnector is added incorrectly, or if an unforeseen condition occurs, such as a database corruption. If you do not specify a Network for the Connector during setup, ESM uses the default RFC1918 system zones.
- ESM does not create an asset unless the event is a base event: that is, an event generated by the device whose events the SmartConnector represents. For example, ESM creates an asset for the SmartConnector if the event is a firewall event, but it does not create an asset for the SmartConnector if the event is an ArcSight internal event, such as heartbeat events with the Manager.

- ESM does not create an asset for the SmartConnector if the Connector Asset Auto Creation Controller filter (at [/All Filters/ArcSight System/Asset Auto Creation/Connector Asset Auto Creation Controller](#)) is specially configured to exclude traffic from assets in this zone.

If the Connector Asset Auto Creation Controller filter is configured to exclude Connectors in a certain zone, such as a zone designated for VPN traffic that comes and goes from the network, then ESM does not create an asset for that Connector every time VPN traffic comes in from that Connector. This ensures that assets are not created unnecessarily.

For more about the Asset Auto Creation Auto Controller filter and how to configure it, see [“Configure Device Asset Auto Creation Controller Filter” on page 59](#).

Creating Assets for SmartConnectors in Static Zones

By default, the SmartConnector auto-create function is enabled. For static zones, ESM needs both the IP address and host name to positively identify the SmartConnector asset. The table below shows the action taken when base events come in from devices involving that SmartConnector.

Table 31-3 SmartConnector Assets in Static Zones

Example	Action taken if no previous SmartConnector	If a SINGLE enabled SmartConnector with the same IP address exists in the same zone	If multiple previous SmartConnectors with the same name exist in the zone
ip=1.1.1.1 hostname=myhost	Asset created	Existing asset is relocated to the zone assigned to the Connector. If there's an asset with the same name in the group, the new asset is renamed by adding '_#', for example, asset_1 .	No asset created.
ip=1.1.1.1 hostname=null	Asset not created. Both the IP address and host name are required.	Existing asset is relocated to the zone assigned to the Connector. If there's an asset with the same name in the group, it gets renamed.	No asset created.
ip=null hostname=myhost	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.	No asset created.
ip=null hostname=null	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.	No asset created.

Creating Assets for SmartConnectors in Dynamic Zones

By default, the SmartConnector auto-create function is enabled. For dynamic zones, it first looks for a MAC address, then a host name to positively identify the SmartConnector asset. The table below shows the action taken when base events come in involving that SmartConnector. (If multiple previous assets with the same name exist in the zone, no asset is created.)

Table 31-4 SmartConnector Assets in Dynamic Zones

Example	Action taken if no previous SmartConnector	If a SINGLE enabled asset with the same IP address exists in the same zone
ip=1.1.1.1 hostname=myhost mac=0123456789 AB	Asset created.	Existing asset is relocated to the zone assigned to the Connector. If there's an asset with the same name in the group, the new asset is renamed by adding '_#', for example, <code>asset_1</code> .
ip=1.1.1.1 hostname=myhost mac=null	Asset created.	Existing asset is relocated to the zone assigned to the Connector. If there's an asset with the same name in the group, it gets renamed.
ip=1.1.1.1 hostname=null mac=0123456789 AB	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.
ip=1.1.1.1 hostname=null mac=null	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.
ip=null hostname=myhost mac=null	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.
ip=null hostname=null mac=0123456789 AB	Asset not created. Both the IP address and host name are required.	Asset not created. Both the IP address and host name are required.

Creating Assets for Network Devices

By default, the Manager also auto-creates assets for the network devices that originate the events. This feature can be configured during Manager setup using the Manager Setup Wizard.

Creating assets for devices is affected by the following conditions:

- The Manager does not create an asset if there is no Network defined for the SmartConnector. This could happen if a SmartConnector is added incorrectly, or if an unforeseen condition occurs, such as a database corruption. If you do not specify a Network for the Connector during setup, ESM uses the default RFC1918 system zones.
- The Manager does not create an asset unless the event is a base event: that is, an event generated by the device whose events the SmartConnector represents. For example, the Manager creates an asset for the device if the event is a firewall event,

but it cannot create an asset for the device if the event is an ArcSight internal event, such as heartbeat events with the Manager.

- The Manager does not create an asset for the device if the Connector Asset Auto Creation Controller filter (at [/All Filters/ArcSight System/Asset Auto Creation/Device Asset Auto Creation Controller](#)) is specially configured to exclude traffic from assets in this zone.

If the Connector Asset Auto Creation Controller filter is configured to exclude events from Connectors in a certain zone, such as a zone designated for VPN traffic that comes and goes from the network, then the Manager does not create an asset for the device the Connector represents every time VPN traffic comes in from that Connector. This ensures that The Manager does not create unnecessary assets.

For more about the Connector Asset Auto Creation Auto Controller filter and how to configure it, see ["Configure Connector Asset Auto-Creation Controller Filter"](#) on page 57.

Creating Assets for Network Devices in Static Zones

If you configured Manager setup to auto-creates assets for the network devices generating assets, it takes the following actions based on IP address and host name in static zones.

Table 31-5 Network Device Assets in Static Zones

Example	Action taken if no previous device	Asset with same information exists on any zone related to SmartConnector
IP=1.1.1.1 hostname=myhost	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.
ip=1.1.1.1 hostname=null	Asset not created. Both IP address and host name are required.	Asset not created. Both IP address and host name are required.
ip=null hostname=myhost	Asset not created. Both IP address and host name are required.	Asset not created. Both IP address and host name are required.
ip=null hostname=null	Asset not created. Both IP address and host name are required.	Asset not created. Both IP address and host name are required.

Creating Assets for Network Devices in Dynamic Zones

If you configured Manager setup to auto-create assets for the network devices generating assets, it takes the following actions based on IP address, host name, and MAC address in dynamic zones.

Table 31-6 Network Device Assets in Dynamic Zones

Example	Action taken if no previous device	Asset with same information exists on any zone related to SmartConnector
ip=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.
ip=1.1.1.1 hostname=myhost mac=null	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.
ip=1.1.1.1 hostname=null mac=null	Asset not created. Host name or MAC address is required.	Asset not created. Host name or MAC address is required.
ip=null hostname=myhost mac=null	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.
ip=null hostname=null mac=0123456789AB	Asset created.	Move asset to a new group. If there is already an asset with the same name, the previous one is renamed.

Asset Names

The Manager names the auto-created assets using the following templates. The creation rules work differently depending on how the events are arrive, by Connector or by scanner, and whether they belong to a dynamic or static zone.

Naming Assets from Scanner Events

By default, assets that come from scanners use the naming scheme outlined below, depending on whether the assets came from a static or dynamic zone. This scheme controls how asset names appear in channels and labels in the user interface.

Table 31-7 Asset Names from Scanner Events

	Static Zone	Dynamic Zone
Property:	scanner-event.auto-create.asset.name.template	scanner-event.auto-create.dynamiczone.asset.name.template

Table 31-7 Asset Names from Scanner Events

	Static Zone	Dynamic Zone
Value:	\$destinationAddress - \$!destinationHostName	\$destinationHostName
Example:	1.1.1.1 - myhost	myhost

You can reconfigure this default naming scheme the `server.properties` file, for example, if you want to show the host name first, or use an underscore to separate the elements. For details, see [“Changing the Default Naming Scheme” on page 810](#).

Naming SmartConnector and Device Assets

SmartConnector and device assets are given the host name of the system that hosts them:

```
name = hostname
```

Asset Auto-Creation Advanced Configuration Options

If the profile of events in your network causes the asset auto creation feature to create assets in your network model inefficiently, you can modify the asset auto creation default settings in the user configuration file, `server.properties`.

The `server.properties` file is located at
`$ARCSIGHT_HOME/config/server.properties`.

For more about working with properties files, see the topic “Managing and Changing Properties File Settings” in the *Administrator’s Guide*.

Asset Auto-Creation from Scanners in Dynamic Zones

The following properties relate to how the Manager creates assets from a vulnerability scan report for dynamic zones.

Create Asset if either IP Address or Host Name

By default, the Manager does not create an asset in a dynamic zone if there is no host name present, as described in [“Creating Assets from a Vulnerability Scan Report for Dynamic Zones” on page 802](#). The property set by default is:

```
scanner-event.dynamiczone.asset.nonidentifiable.create=false
```

You can configure the Manager to create the asset as long as it has either an IP address or a host name. In `server.properties`, change `scanner-event.dynamiczone.asset.nonidentifiable.create` from **false** to **true**. The Manager discards conflicts between an IP address and host name (similar IP address, but different host name and/or MAC address).



Caution

Creating an asset if no host name is present can result in an inaccurate asset model.

Setting `scanner-event.dynamiczone.asset.nonidentifiable.create` to **true** means that assets are created if the asset has either an IP address or a host name.

This could lead to disabled assets or duplicated assets being created. Change this configuration only if you are using a dynamic zone to host ostensibly static assets, such as long-lived DHCP addresses.

When this property is set to **true**, the Manager takes the following actions.

Table 31-8 Asset Creation with IP Address Only or Hostname Only

Example	Action taken if no conflicts	Action taken if previous asset with similar information
IP=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=myhost mac=null	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created	Asset created, previous asset is deleted.
ip=1.1.1.1 hostname=null mac=null	Asset created	Asset created, previous asset is deleted.
ip=null hostname=myhost mac=null	Asset created	Asset created, previous asset is deleted.
ip=null hostname=null mac=0123456789AB	Asset not created. Either host name or IP address is required.	Asset not created. Either host name or IP address is required.
ip=null hostname=myhost mac=0123456789AB	Asset not created. Either host name or IP address is required.	Asset not created. Either host name or IP address is required.

Preserve Previous Assets

This setting applies when the Manager creates assets from a vulnerability scan report for dynamic zones. By default, if a previous asset with similar information already exists in the asset model, the Manager creates a new asset and delete the old one, as described in [“Creating Assets from a Vulnerability Scan Report for Dynamic Zones” on page 802](#).

If you want to preserve the previous asset rather than delete it when a scan finds a new asset with similar information, you can configure the Manager to rename the previous asset. In `server.properties`, change `scanner-event.dynamiczone.asset.ipconflict.preserve` from **false** to **true**.



Preserving previous assets results in a larger asset model.

Setting `event.dynamiczone.asset.ipconflict.preserve` to true means that assets are continually added to the asset model and not removed. Use this option only if you know you must preserve all assets added to the asset model.

When you configure the Manager with `scanner-event.dynamiczone.asset.nonidentifiable.create=false` and

`scanner-event.dynamiczone.asset.ipconflict.preserve=true`,
it takes the following actions:

Table 31-9 ESM Actions for Preserved Previous Assets

Example	Action taken if previous asset with similar information and preserve = true
IP=1.1.1.1 hostname=myhost mac=0123456789AB	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=myhost mac=null	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=null mac=0123456789AB	Asset created, previous asset is renamed.
ip=1.1.1.1 hostname=null mac=null	No action taken. Either host name or MAC address is required.
ip=null hostname=myhost mac=null	Asset created, previous asset is renamed.
ip=null hostname=null mac=0123456789AB	Asset created, previous asset is renamed.
ip=null hostname='myhost' mac=0123456789AB	Asset created, previous asset is renamed.

Changing the Default Naming Scheme

By default, the Manager names assets that come from scanners using the naming scheme outlined in [“Asset Names” on page 807](#).

Table 31-10 Asset Default Names

	Static Zone	Dynamic Zone
Property:	scanner-event.auto-create.asset.name.template	scanner-event.auto-create.dynamiczone.asset.name.template
Value:	\$destinationAddress - \$!destinationHostName	\$destinationHostName
Example:	1.1.1.1 - myhost	myhost

You can reconfigure this default naming scheme, for example, if you want to show the host name first, or use an underscore to separate the elements.

For example, you want the asset name for an asset in a static zone to appear this way in the user interface:

```
myhost_1.1.1.1
```

In this case, change the default

```
$destinationAddress - $!destinationHostName
```

to

```
$!destinationHostName_$destinationAddress
```

Attack

An exploited threat or an attempt to bypass security controls on a computer. The attack may alter, release, or deny data. Whether an attack succeeds depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

Audit Events

Audit events are events generated within the Manager to mark a wide variety of routine actions that can occur manually or automatically, such as adding an event to a case or when a Moving Average data monitor detects a rapidly rising moving average. Audit events have many applications, which can include notifications, task validation, compliance tracking, automated housekeeping, and system administration.

This topic lists the ArcSight audit events you can use in rules, filters, and other analytical or administrative resources. Observe the way these events are used in the standard system-related content for examples of how to apply them.

In the table below, use the **Audit Event Category** to locate events. Use the Device Event Class (DEC) ID string in rules and filters. The **Audit Event Description** reflects the resource name you see in active channel grids. Additional details, when necessary, appear in the **Notes** column.

Compare audit events, which report on *system activity*, with [Status Monitor Events](#) events, which provide information about a wide variety of *system states*.

All resources (except actors, groups, and users) use the general audit events described in [“Resources \(Configuration Events Common to Most Resources\)”](#) on page 812 when a resource is added, deleted, updated, locked, or unlocked. Actors, groups, and users each use their own unique set of audit events. Other resources present unique audit events that are listed in this section in alphabetical order by resource.



To get *additional* details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property called `resource.audit.update.uris` in the file `server.defaults.properties` on the Manager to specify which resources should show extended audit event information.

For more information, see [“Extending Audit Event Logging”](#) on page 683.

Audit Event Categories

["Resources \(Configuration Events Common to Most Resources\)" on page 812](#)
["Active Channel" on page 813](#)
["Active List" on page 814](#)
["Actor" on page 814](#)
["Authorization" on page 815](#)
["Connectors" on page 816](#)
["Dashboard" on page 817](#)
["Data Monitors" on page 818](#)
["Domains \(for Domain Fields\)" on page 819](#)
["Global Variables" on page 819](#)
["Group Management" on page 820](#)
["License Audit" on page 820](#)
["Manager Activation" on page 821](#)
["Manager Database Error Conditions" on page 821](#)
["Manager External Event Flow Interruption" on page 821](#)
["Notifications" on page 822](#)
["Partition Archiver" on page 823](#)
["Partition Manager" on page 823](#)
["Reports" on page 824](#)
["Resource Quota" on page 824](#)
["Rules" on page 824](#)
["Scheduler" on page 826](#)
["Stress" on page 827](#)
["Trends" on page 828](#)
["User Login" on page 828](#)
["User Management" on page 829](#)

Resources (Configuration Events Common to Most Resources)

These audit events are generated in response to creation events and configuration updates to most resources, except users, actors, and groups, which use different audit events. When a resource is added, deleted, updated, locked, or unlocked, the Manager generates one audit event with the following attributes:

- Device Event Class ID = `resource:100` (deleted) or `resource:101` (updated) or `resource:102`, and so on.
- Event Name = `<resource type> deleted/updated/added`.
- File Name = `<Resource Name>` (for example, John's Filter)
- File Path = `<Resource URI>` (for example, /All Filters/admin's Filter/John's Filter)

- File Type = <Resource Type> (for example, Filter)



To get additional details within the “update resource” audit events (beyond what is provided by default), you can enable a resource audit property called `resource.audit.update.uris` in the file `server.defaults.properties` on the Manager to specify which resources should show extended audit event information.

For more information, see “Extending Audit Event Logging” on page 683.

Table 31-11 Audit Events on Resources

Audit Event Category	Device Event Class ID	Audit Event Description
Resource (Delete)	<code>resource:100</code>	Resource deleted. The Event Name describes the action and resource type (<code><ResourceName> deleted</code>); for example, deleting a filter results in an event named <code>Filter deleted</code> .
Resource (Update)	<code>resource:101</code>	Resource updated. This audit event is generated when an existing resource is modified or added. See also Resource (Add) . The Event Name describes the action (update) and resource type (<code><ResourceName> updated</code>); for example, modifying a report, results in an event name of <code>Report updated</code> .
Resource (Add)	<code>resource:102</code>	Resource added (inserted). The Event Name describes the action (insert) and resource type (<code><ResourceName> inserted</code>); for example, adding a case, results in an event name of <code>Case inserted</code> . Adding a Case group results in an event name of <code>Group [Case] inserted</code> .
Resource (Lock)	<code>resource:103</code>	Resource locked <code><ResourceName> locked</code> .
Resource (Unlock)	<code>resource:104</code>	Resource unlocked <code><ResourceName> unlocked</code> .
Resource	<code>resourcereference:100</code>	Could not locate a resource through the supplied universal resource identifier (URI).

Active Channel

Table 31-12 Audit Events on Active Channel Category

Device Event Class ID	Audit Event Message
<code>channel:001</code>	An active channel [Channel Name] was opened/started.
<code>channel:002</code>	The channel [Channel Name] is empty; that is, there are no matching events for the built-in channel filter.
<code>channel:003</code>	The channel [Channel Name] query completed.
<code>channel:004</code>	The channel [Channel Name] query is slow.

Active List

Table 31-13 Audit Events on Active List Category

Device Event Class ID	Audit Event Message
<code>activelist:101</code>	An entry was added to an active list.
<code>activelist:102</code>	An entry was removed from an active list.
<code>activelist:103</code>	An entry was changed in an active list.
<code>activelist:104</code>	An entry has expired in an active list.
<code>activelist:105</code>	An entry has been evicted from an active list. The active list is full and an entry is dropped.

Actor

Table 31-14 Audit Events on Actor Category

Device Event Class ID	Audit Event Message
<code>actor:100</code>	An actor was deleted.
<code>actor:102</code>	An actor was created.
<code>actor:110</code>	One or more Actor Attributes were updated.
<code>actor:111</code>	A Multi-Valued Actor Attribute was added to an actor.
<code>actor:112</code>	A Multi-Valued Actor Attribute was removed from an actor.

Authentication

Table 31-15 Audit Events on Authentication Categories

Audit Event Category	Device Event Class ID	Audit Event Message
Authentication	authentication:100	A client authenticated with the Manager.
Authentication	authentication:101	A client authentication login failed.
Authentication	authentication:102	An authenticated client logged out of the Manager.
Authentication	authentication:103	Authentication logout time.
Authentication	authentication:104	A client made several unsuccessful attempts to log in to the Manager, resulting in an excessive number of failed logins.
Authentication	authentication:105	<p>A non-FIPS client authenticated with the Manager via login.</p> <p>(A valid login by a non-FIPS ESM Console authenticating itself to the Manager triggers this audit event.)</p> <p>For information on how to configure a non-FIPS client (such as ESM Console) to log in to a FIPS-enabled Manager, see the <i>Administrator's Guide</i>.</p>
Connector Login	authentication:200	Successful connector authentication.
Connector Login	authentication:201	Connector authentication failed.
Authentication	authentication:202	<p>A non-FIPS connector authenticated with the Manager via login.</p> <p>(A valid login by a non-FIPS SmartConnector authenticating itself to the Manager triggers this audit event.)</p> <p>For information on how to configure a non-FIPS SmartConnector to connect to a FIPS-enabled Manager, see the <i>Administrator's Guide</i>.</p>



Looking for User Login and User Management audit events? See ["User Login" on page 828](#), ["Group Management" on page 820](#), and ["User Management" on page 829](#).

Authorization

Table 31-16 Audit Event on Authorization Category

Device Event Class ID	Audit Event Description
authorization:100	Manager refused to authorize client.



Looking for User Login and User Management audit events? See [“User Login” on page 828](#), [“Group Management” on page 820](#), and [“User Management” on page 829](#).

Connectors

Audit events related to SmartConnectors are described in the following tables.

Connector Connection

Table 31-17 Audit Events on Connector Connections Category

Device Event Class ID	Audit Event Description
agent:009	Manager rejected a connection attempt from a connector for reasons other than authentication failure.
agent:030	Connector started.
agent:031	Connector shutting down.
agent:101	Connector has just connected to Manager.
agent:102	Connector is sending events but no heartbeats.
agent:103	Connector is sending neither events nor heartbeats.
agent:104	An unknown connector attempted to connect to the Manager.
agent:105	A connector presented an incorrect shared secret when authenticating.

Connector Exceptions

Table 31-18 Audit Events on Connector Exceptions Category

Device Event Class ID	Audit Event Description
agent:012	Connector detected source events from a sensor device containing incorrect time stamps.
agent:013	Connector noted that a new sensor device is sending events.
agent:014	Connector could not find a base event referenced in a syslog aggregate event.
agent:015	connector connection device failure.
agent:016	connector connection device success.
agent:017	Connector successfully executed a command.
agent:018	Connector could not execute a command.
agent:019	Connector is caching events because they could not be immediately transmitted to the Manager.
agent:020	Connector has emptied its cache of events.

Table 31-18 Audit Events on Connector Exceptions Category (Continued)

Device Event Class ID	Audit Event Description
agent:021	Connector could not communicate with an NT collector sensor.
agent:023	Connector could not communicate with a CheckPoint sensor.
agent:024	Connector is having difficulty communicating with CheckPoint.
agent:028	Connector experienced an unexpected problem.
agent:029	Connector was forced to drop its cached data.

Connector Login

Table 31-19 Audit Events on Connector Login Category

Device Event Class ID	Audit Event Description
authentication:200	Successful connector authentication.
authentication:201	Connector authentication failed.

Connector Registration and Configuration

Table 31-20 Audit Events on Connector Registration and Configuration Category

Device Event Class ID	Audit Event Description
agent:007	Connector successfully registered with Manager.
agent:008	Connector did not successfully register with Manager.
agent:010	Connector upgrade succeeded. This is currently in the context of an installer upgrade.
agent:011	Connector upgrade failed. This event is not currently being generated.
agent:022	Connector could not process a reconfiguration request.
agent:025	Connector content was successfully updated.
agent:026	Connector content update failed.
agent:032	Connector configuration was successfully changed.

Dashboard

Table 31-21 Audit Events on Dashboard Category

Device Event Class ID	Audit Event Description
dashboard:001	A data monitor on a dashboard was newly accessed after not having been accessed for some time (for example, the dashboard had been closed). This audit event is generated on a per-user, per-Console-session basis.

Table 31-21 Audit Events on Dashboard Category (Continued)

Device Event Class ID	Audit Event Description
<code>dashboard:100</code>	Dashboard has opened.

Data Monitors

Audit events related to data monitors are described in the following tables, categorized by data monitor type. (See also the [Dashboard](#) audit events topic.)

Last State Data Monitors

Table 31-22 Audit Events for Last State Data Monitors

Audit Event Category: Statistical Data Monitor	
Device Event Class ID	Audit Event Description
<code>datamonitor:400</code>	A Last State data monitor entry has exceeded its time-out period and was automatically removed.
<code>datamonitor:401</code>	A Last State data monitor entry value was manually changed by the user.
<code>datamonitor:402</code>	A Last State data monitor entry was manually removed by the user.

Moving Average Data Monitor

Table 31-23 Audit Events for Moving Average Data Monitor Category

Device Event Class ID	Audit Event Description
<code>datamonitor:101</code>	Moving average threshold.
<code>datamonitor:102</code>	Moving Average data monitor detected a rapidly falling moving average
<code>datamonitor:103</code>	Moving Average data monitor detected a rapidly rising moving average.
<code>datamonitor:104</code>	Moving Average data monitor reporting the current moving average.
<code>datamonitor:105</code>	A value was added to a Moving Average data monitor, which is now monitoring a new Group-By set of values.
<code>datamonitor:106</code>	A value was removed from a Moving Average data monitor. The data monitor is no longer monitoring a particular Group-By set of values.

Reconciliation Data Monitor

Table 31-24 Audit Event for Reconciliation Data Monitor Category

Device Event Class ID	Audit Event Description
<code>datamonitor:300</code>	Correlation data monitor reporting a correlated or non-correlated event.

Statistical Data Monitor

Table 31-25 Audit Events for Statistical Data Monitor Category

Device Event Class ID	Audit Event Description
<code>datamonitor:200</code>	Statistical Data Monitor reported a change in status.
<code>datamonitor:201</code>	A value was added to a Statistical Data Monitor, which is now monitoring a new Group-By set of values.
<code>datamonitor:202</code>	A value was removed from a Statistical Data Monitor. The data monitor is no longer monitoring a particular Group-By set of values.

Top Value Counts Data Monitor

Table 31-26 Audit Events for Top Value Counts

Audit Event Category: Moving Average Data Monitor	
Device Event Class ID	Audit Event Description
<code>datamonitor:500</code>	For a Top Value Counts Data Monitor, the top <i>N</i> counts (<i>N</i> events).
<code>datamonitor:501</code>	Counts that were most recently added to the data monitor (from 0 ... <i>N</i> events).
<code>datamonitor:502</code>	Counts that were most recently removed from the data monitor (from 0 ... <i>N</i> events).

Domains (for Domain Fields)

<jm> This addresses ESM-45409 (TTP 62583). The other three audit events used by domains are added here, but commented out, since the functionality to support them is not included as part of v5.0. </jm>

Audit Event Category	Device Event Class ID	Audit Event Description
Domain	<code>domain:100</code>	All out of underlying database columns of type <x>, delete a Domain Field of the same type to free up a column.

Global Variables

Table 31-27 Audit Events for Global Variables Category

Device Event Class ID	Audit Event Description
<code>resource:100</code>	Global variable deleted.
<code>resource:101</code>	Global variable updated.
<code>resource:102</code>	Global variable inserted.

Table 31-27 Audit Events for Global Variables Category (Continued)

Device Event Class ID	Audit Event Description
resource:103	Global variable locked.
resource:104	Global variable unlocked.

Group Management

The following audit events are generated for any group add, update, or delete, including user groups. The details of the which type of resource was configured or modified are provided in the event name. (For more information on user management audit events, see ["User Management" on page 829](#).)

Table 31-28 Audit Events for Group Management

Audit Event Category	Device Event Class ID	Audit Event Description
Group Delete	group:100	A group was deleted.
Group Update	group:101	A group was updated. This audit event is generated when an existing group is modified or added.
Group Add	group:102	A group was added (group inserted). When a new group is added, two audit events are generated: this event (group:102), and a Group Update audit event (group:101).

License Audit

Each of these events is reported every 24 hours, beginning 24 hours after you start the Manager.

Table 31-29 Audit Events for License Audit Category

Device Event Class ID	Audit Event Description
license:100	The number of assets you have at this time.
license:101	The number of devices you have at this time.
license:102	The number of actors you have at this time.
license:103	The number of ESM Console users you have at this time.
license:104	The number of web users you have at this time.
license:105	The average number of incoming events per second (EPS) over the last 24 hours and whether it exceeds your license.
license:106	The number of times that event-105 threshold breaches have occurred since the Manager started, and the license limit.

Table 31-29 Audit Events for License Audit Category (Continued)

Device Event Class ID	Audit Event Description
license:107	The number of times that EPS violations have breached the threshold over the number of days specified in your license. This is a serious license violation. For more information look at the License:105 and License:106 events.

Manager Activation

Table 31-30 Audit Events for Manager Activation Category

Device Event Class ID	Audit Event Description
manager:100	Manager has started.
manager:101	A clean Manager shutdown has been requested.

Manager Database Error Conditions

Table 31-31 Audit Events for Manager Database Error Conditions Category

Device Event Class ID	Audit Event Description
database:100	Database tablespace is low and is deactivated.
database:101	Database has generated a fatal error and is deactivated.
database:102	Database has been reactivated.
database:103	Database has more tablespace available after detecting a low tablespace condition.
database:104	Database event discarded.

Manager External Event Flow Interruption

Table 31-32 Audit Events for Manager External Event Flow Interruption Category

Device Event Class ID	Audit Event Description
manager:200	Manager has stopped the event flow.
manager:201	Manager has allowed the event flow to resume.

Notifications

Audit events related to notifications are described in the following tables.

Notification

Table 31-33 Audit Events for Notification Category

Device Event Class ID	Audit Event Description
<code>notification:100</code>	Notification has been disabled.
<code>notification:101</code>	Notification has been disabled because the queue of notifications to be sent is too large.
<code>notification:102</code>	Notification has been enabled.
<code>notification:103</code>	Notification has been enabled because the queue of notifications is back under control.
<code>notification:104</code>	A particular notification destination has been disabled.
<code>notification:105</code>	A particular notification destination has been disabled because too much traffic was directed at it.
<code>notification:106</code>	A particular notification destination has been enabled.
<code>notification:107</code>	A notification expired without being acknowledged.
<code>notification:108</code>	A functioning destination could not be located for this notification.
<code>notification:109</code>	Old notification has been purges.

Notification Acknowledgement, Escalation, and Resolution

Table 31-34 Audit Events for Notification Acknowledgement, Escalation, and Resolution Categories

Audit Event Category	Device Event Class ID	Audit Event Description
Notification Escalated	<code>notification:110</code>	Notification has been escalated.
Notification Sent Requires Acknowledgement	<code>notification:111</code>	Notification sent requires acknowledgement.
Notification Sent (Informational)	<code>notification:112</code>	An informational notification was sent.
Notification Acknowledgement	<code>notification:300</code>	This notification has been acknowledged.
Notification Resolve	<code>notification:301</code>	This notification has been resolved.

Notification Testing

Table 31-35 Audit Event for Notification Testing Category

Device Event Class ID	Audit Event Description
<code>notification:20</code>	Sent a test notification to this destination group.

Pattern Discovery

Table 31-36 Audit Events for Pattern Discovery Category

Device Event Class ID	Audit Event Description
pattern:001	New pattern discovered.
pattern:002	Pattern rediscovered.
profile:001	Pattern discovery run started.
profile:002	Pattern discovery run finished.

Partition Archiver

Audit Event Category	Device Event Class ID	Audit Event Description
Partition Archiver	partitionarchiver:000	No pending operations for partition manager.
Partition Archiver	partitionarchiver:100	The partition was successfully archived.
Partition Archiver	partitionarchiver:200	There was a problem while archiving the partition.
Partition Archiver	partitionarchiver:300	Partition archiving is disabled.
Partition Archiver	partitionarchiver:400	Partition archiving did not complete in the allotted time.
Partition Archiver	partitionarchiver:500	Partition archiving failed.
Partition Archiver	partitionarchiver:600	There was an unexpected error while archiving partitions.

Partition Manager

Audit Event Category	Device Event Class ID	Audit Event Description
Partition Manager	partitionmanager:000	No pending operations for partition archiver.
Partition Manager	partitionmanager:100	Partitions have been successfully rotated.
Partition Manager	partitionmanager:200	There was a problem rotating partitions.
Partition Manager	partitionmanager:300	The partition manager has been disabled.
Partition Manager	partitionmanager:500	Partitions could not be rotated.
Partition Manager	partitionmanager:600	There was an unexpected error while rotating partitions.

Query Viewers

Table 31-37 Audit Events for Query Viewer Category

Device Event Class ID	Audit Event Description
<code>queryviewer:100</code>	Base query used by the query viewer succeeded.
<code>queryviewer:101</code>	Base query used by the query viewer failed.

Reports

Table 31-38 Audit Events for Report Category

Device Event Class ID	Audit Event Description
<code>report:100</code>	Generated a new archived-report configuration resource.
<code>report:101</code>	Failed to generate a new archived-report configuration resource.
<code>report:102</code>	Generated a new delta archived-report configuration resource.
<code>report:103</code>	Report cancelled.
<code>report:104</code>	Generate report started.
<code>report:105</code>	Report generate process halted because the report was empty.

Resource Quota

Table 31-39 Audit Events for Resource Quota Category

Device Event Class ID	Audit Event Description
<code>quota:100</code>	Resource usage has fallen below the fixed-quota level.
<code>quota:101</code>	Resource usage has exceeded the fixed-quota level.
<code>quota:102</code>	Asset autocreation has exceeded a fixed quota.
<code>quota:103</code>	Asset autocreation is proceeding too rapidly.

Rules

Audit events for rules are described in the following tables.

Rule Actions

Table 31-40 Audit Events for Rule Actions Category

Device Event Class ID	Audit Event Description
<code>rule:300</code>	For rule actions that do not have specific DEC IDs assigned.
<code>rule:302</code>	Set Event Attribute action.

Table 31-40 Audit Events for Rule Actions Category (Continued)

Device Event Class ID	Audit Event Description
rule:303	Send to Notifier action.
rule:304	Execute Command action.
rule:305	Export... action.
rule:306	Create New Case action.
rule:307	Add to Case action.
rule:308	Create New Case action failed.
rule:309	Add to Case action failed.
rule:310	Add to Active List action.
rule:312	Remove from Active List action.
rule:313	Run SmartConnector (agent) command.
rule:314	Send command or data to OpenView.
rule:315	AddAssetCategory.
rule:316	RemoveAssetCategory.

Rule Activations

Table 31-41 Audit Events for Rule Activations Category

Device Event Class ID	Audit Event Description
rule:700	Rule has been deactivated.
rule:701	Rule has been deactivated because it is unsafe. There was excessive recursion or event matching.
rule:702	Rule has been activated.
rule:703	Unsafe rule activation.

Rules Scheduled

Table 31-42 Audit Events for Scheduled Rules Category

Device Event Class ID	Audit Event Description
rule:801	Scheduled rule started.
rule:802	Scheduled rule finished.

Rule Firings

Table 31-43 Audit Events for Rule Firings

Device Event Class ID	Audit Event Description
rule:100	Any rule fired.

Table 31-43 Audit Events for Rule Firings (Continued)

Device Event Class ID	Audit Event Description
<code>rule:101</code>	Rule fired OnEveryEvent.
<code>rule:102</code>	Rule fired OnFirstEvent.
<code>rule:103</code>	Rule fired OnSubsequentEvents.
<code>rule:104</code>	Rule fired OnEveryThreshold.
<code>rule:105</code>	Rule fired OnFirstThreshold.
<code>rule:106</code>	Rule fired OnSubsequentThresholds.
<code>rule:107</code>	Rule fired OnTimeUnitExpiration.
<code>rule:108</code>	Rule fired on time unit.

Rule Warnings

Table 31-44 Audit Event for Rule Warnings Category

Device Event Class ID	Audit Event Description
<code>rule:501</code>	Rule is firing on events generated by itself (infinite loop).

Scheduler

Audit events related to the job scheduler are described in the following tables.

Scheduler Execution

Table 31-45 Audit Events for Scheduler Execution Category

Device Event Class ID	Audit Event Description
<code>scheduler:200</code>	A task has been executed.
<code>scheduler:201</code>	A task failed to execute.

Scheduler Scheduling Tasks

Table 31-46 Audit Events for Scheduler Scheduling Tasks Category

Device Event Class ID	Audit Event Description
<code>scheduler:300</code>	A new task has been scheduled.
<code>scheduler:301</code>	A new task could not be scheduled.
<code>scheduler:302</code>	Enabled a task.
<code>scheduler:303</code>	Could not enable a task.
<code>scheduler:304</code>	Deleted a task.
<code>scheduler:305</code>	Failed to delete a task.
<code>scheduler:306</code>	Disable a task .

Table 31-46 Audit Events for Scheduler Scheduling Tasks Category (Continued)

Device Event Class ID	Audit Event Description
<code>scheduler:307</code>	Could not disable a task.

Scheduler Skip

Table 31-47 Audit Events for Scheduler Skip Category

Device Event Class ID	Audit Event Description
<code>scheduler:100</code>	The task scheduler skipped a scheduled task execution because the scheduler was not allowed to run.
<code>scheduler:101</code>	The task scheduler skipped a scheduled task invocation because the last invocation of the task is still executing.

Session Lists

Table 31-48 Audit Events for Session List Category

Device Event Class ID	Audit Event Description
<code>sessionlist:101</code>	An entry was added to a session list.
<code>sessionlist:102</code>	An entry was removed from a session list.
<code>sessionlist:103</code>	A session list entry was updated.
<code>sessionlist:104</code>	An entry in a session list was auto-terminated as the session expired.
<code>sessionlist:201</code>	A session list partition was dropped.
<code>sessionlist:202</code>	A session list partition drop failed.
<code>sessionlist:203</code>	A session list partition was added.
<code>sessionlist:204</code>	A session list partition add failed.
<code>sessionlist:301</code>	<p>During lookup on a session list value, the value was not available in Manager memory, and the lookup was not performed on the database.</p> <p>This can occur if too many session list lookups are performed against the database. Typically, the Manager generates one audit event for any number of dropped lookups in a time period, instead of one per dropped lookup.</p>

Stress

Table 31-49 Audit Event for Stress Category

Device Event Class ID	Audit Event Description
<code>test:100</code>	<p>A stress test event.</p> <p>This event is generated only by ArcSight Quality Assurance.</p>

Trends

Audit events for trends are described in the following tables.

Trends

Table 31-50 Audit Events for Trend Category

Device Event Class ID	Audit Event Description
trend:100	Trend run started.
trend:101	Trend run success.
trend:102	Trend run failure.
trend:201	Trend scavenge success.
trend:202	Trend scavenge failure.
trend:401	Trend enabled.
trend:402	Trend disabled.
trend:501	Trend task started.
trend:502	Trend task ended.
trend:601	Trend was automatically deactivated because of too many failures.
trend:701	<p>Trend successfully updated an active list.</p> <p>You can add an action to a trend to send columns (fields) in trend results to a <i>fields-based</i> active list.</p> <p>See also, "Trend Actions (Add to Active List)" on page 377.</p>

Trend Partitions

Table 31-51 Audit Events for Trend Partitions Category

Device Event Class ID	Audit Event Description
trend:301	Trend partition added.
trend:302	Trend partition dropped.
trend:303	Trend partition add failed.
trend:304	Trend partition drop failed.

User Login

Table 31-52 Audit Events for User Login Category

Device Event Class ID	Audit Event Description
authentication:100	Successful client login.
authentication:101	Failed client login.
authentication:102	Client logout.

Table 31-52 Audit Events for User Login Category (Continued)

Device Event Class ID	Audit Event Description
<code>authentication:103</code>	Client timed out due to inactivity.
<code>authentication:104</code>	Too many client login failures occurred within a time period.

See also [“Group Management” on page 820](#), which reflects adds, deletes, and updates of groups, including user groups.

User Management

Table 31-53 Audit Events for User Management

Audit Event Category	Device Event Class ID	Audit Event Description
User Delete	<code>user:100</code>	A user account was deleted.
User Update	<code>user:101</code>	A user account was updated. This audit event is generated when an existing user account is modified or a new user is inserted.
User Inserted	<code>user:102</code>	A user account was added. When a new user account is inserted, two audit events are generated: this User Inserted event, and a User Update event (<code>user:101</code>).

See also, [“Group Management” on page 820](#), which reflects adds, deletes, and updates of groups, including user groups.

Batching

Batching is a mode in which ArcSight SmartConnectors receive or send collections of events at one time rather than immediately after each occurrence.

Case Editor Tab Fields


This topic is a directory to reference information about the fields on the Case Editor tabs.

The Case Editor displays case information organized in five major tabs:

Table 31-54 Fields on Case Editor Tabs

Case Editor Tab	Description
Initial	Basic case information: case ticket attributes, description and security classification.
Follow-Up	Description of actions taken, planned, or recommended.
Final	Ticket resolution and reporting including attack mechanism, attack agent, incident information, and vulnerability information.
Events	List of events included in case.

Table 31-54 Fields on Case Editor Tabs (Continued)

Case Editor Tab	Description
Attachments	List of attachments in the case. Provides option to attach or detach items to the case.
Notes	Miscellaneous case information.
 <p>To edit a saved case, you first need to select the Lock Case checkbox, so other users can't modify it while you're editing.</p>	

This organization lets you separate information based on the workflow and handling or resolution of individual cases.

Initial Tab

[Case Editor Initial - Attributes Tab](#)

[Case Editor Initial - Description Tab](#)

[Case Editor Initial - Security Classification Tab](#)

Follow-up

[Case Editor Follow-Up Tab](#)

Final

[Case Editor Final - Attack Mechanism Tab](#)

[Case Editor Final - Attack Agent Tab](#)

[Case Editor Final - Incident Information Tab](#)

[Case Editor Final - Vulnerability Tab](#)

[Case Editor Final - Other Tab](#)

Events

[Case Editor Events Tab](#)

Attachments

[Case Editor Attachments Tab](#)

Notes

[Case Editor Notes Tab](#)

Case Editor Events Tab

The fields on this tab provide a list of the events included in a case.

Table 31-55 Case Editor Events Tab

Field	Description
Description	Events auto-populated from events included in a case.

Table 31-55 Case Editor Events Tab (Continued)

Field	Description
Event Info and Payload fields	For selected events, displays event field values and payload fields, if available.

Case Editor Attachments Tab

This tab lists attachments (if any) for the case, and provides options to attach new items via a file browser or detach items.

Case Editor Final - Attack Agent Tab

Fields on this tab provide ticket resolution and reporting information related to the attack agent associated with a case.

Table 31-56 Case Editor Attack Agent Tab

Field	Description
Attack Agent	Auto-populated from Security Classification tab. Possible values are I (Insider), C (Collaborative), O (Outsider), and U (Unknown).
Attack Location Id	Text field allowing entry of up to 255 characters.
Attack Node	Text field allowing entry of up to 255 characters.
Attack Address	Text field allowing entry of up to 255 characters.

Case Editor Final - Attack Mechanism Tab

The fields on this tab provide final ticket resolution and reporting information for the attack mechanism associated with a case.

Table 31-57 Case Editor Attack Mechanism Tab

Field	Description
Attack Mechanism	Auto-populated from Security Classification tab. Possible values are P (Physical), O (Operational), I (Informational), and U (Unknown).
Attack Protocol	Text field allowing entry of up to 64 characters.
Attack OS	Text field allowing entry of up to 64 characters.
Attack Program	Text field allowing entry of up to 255 characters.
Attack Time	Date field.
Actions Target	Text field allowing entry of up to 4000 characters.
Attack Service	Text field allowing entry of up to 4000 characters.
Attack Impact	Text field allowing entry of up to 4000 characters.
Final Report Action	Text field allowing entry of up to 4000 characters.

Case Editor Final - Incident Information Tab

The fields on this tab provide final incident information associated with a case.

Table 31-58 Case Editor Incident Information Tab

Field	Description
Incident Source 1	Auto-populated from Security Classification tab.
Incident Source 2	Auto-populated from Security Classification tab.
Incident Source Address	Text field allowing entry of up to 200 characters.

Case Editor Final - Other Tab

The fields on this tab provide miscellaneous ticket resolution and final reporting information.

Table 31-59 Case Editor Other Tab

Field	Description
History	Selections include: Known Occurrence and Unknown
No Occurrences	Numeric value
Last Occurrence Time	Enterable time or selector.
Resistance	Selections include: High, Low, Unknown
Consequence Severity	Auto-populated from Initial Attributes tab
Sensitivity	Auto-populated from Initial Attributes tab
Recorded Data	Text field allowing entry of up to 4000 characters.
Inspection Results	Text field allowing entry of up to 4000 characters.
Conclusions	Text field allowing entry of up to 4000 characters.

Case Editor Final - Vulnerability Tab

The fields on this tab provide final ticket resolution and reporting information related to the vulnerabilities associated with a case.

Table 31-60 Case Editor Vulnerability Tab

Field	Description
Vulnerability	Auto-populated from Security Classification tab. Possible values are D (Design), O (Operational), E (Operational Environment), and U (Unknown).
Vulnerability Type 1	Selections include: Accidental or Intentional
Vulnerability Type 2	Selections include: EMI/RFI, Insertion of Data, Theft of Service, Unauthorized, Probes, Root Compromise, DoS Attack, User Account
Vulnerability Evidence	Text field allowing entry of up to 4000 characters.

Table 31-60 Case Editor Vulnerability Tab (Continued)

Field	Description
Vulnerability Source	Text field allowing entry of up to 4000 characters.
Vulnerability Data	Text field allowing entry of up to 4000 characters.

Case Editor Follow-Up Tab

The fields on this tab describe follow-up entries for a case.

Table 31-61 Case Editor Follow-Up Tab

Field	Description
Actions Taken	Text field allowing entry of up to 4000 characters.
Planned Actions	Text field allowing entry of up to 4000 characters.
Recommended Actions	Text field allowing entry of up to 4000 characters.
Followup Contact	Text field allowing entry of up to 4000 characters.

Case Editor Initial - Attributes Tab

The fields on this tab provide basic case information.

Table 31-62 Case Editor Attributes Tab

Field	Description
Case:	
Name	Required field specifying name of case.
Display ID	An identification provided by an external tracking system.
Ticket:	
Ticket Type	Drop-down list includes Internal, Client, and Incident types.
Stage	Indicate workflow stage of ticket; default selections include Queued, Initial, Follow-Up, Final, and Closed.
Frequency	Indicates how often reported issue occurs. Values assigned are 0 (never or once), 1 (less than 10 times), 2 (10 to 15 times), 3 (15 times), 4 (more than 15)
Operational Impact	Impact of reported issue. Values assigned are 0 (no impact), 1 (no immediate impact), 2 (low priority impact), 3 (high priority impact), 4 (immediate impact)
Security Classification	Values assigned are 1 (Unclassified), 2 (Confidential), 3 (Secret), 4 (Top Secret)
Consequence Severity	Values assigned are 0 (None), 1 (Insignificant), 2 (Marginal), 3 (Critical), 4 (Catastrophic)
Reporting level	Number calculated based on Ticket info values entered.
Incident Information:	
Detection Time	Automatically assigned from event info.

Table 31-62 Case Editor Attributes Tab (Continued)

Field	Description
Estimated Start Time	Automatically assigned from event info.
Estimated Restore Time	Automatically assigned from event info.



You can also use entries in all Case Ticket fields to generate reports so you can categorize cases based on specific case information.

Case Editor Initial - Description Tab

The fields on this tab further describe a case.

Table 31-63 Case Editor Description Tab

Field	Description
Affected Services	Text field allowing entry of up to 4000 characters.
Affected Elements	Text field allowing entry of up to 4000 characters.
Estimated Impact	Text field allowing entry of up to 4000 characters.
Affected Sites	Text field allowing entry of up to 4000 characters.

Case Editor Initial - Security Classification Tab

The fields on this tab describe the security classification for a case.

Table 31-64 Case Editor Security Classification Tab

Field	Description
Security Classification:	
Attach Mechanism	Selections include: P (Physical), O (Operational), I (Informational), and U (Unknown)
Attack Agent	Selections include: I (Insider), C (Collaborative), O (Outsider), and U (Unknown)
Incident Source 1	Editable text.
Incident Source 2	Editable text.
Vulnerability	Selections include: D (Design), O (Operational), E (Operational Environment), and U (Unknown)
Sensitivity	Selections include: U (Unclassified), C (Confidential), S (Secret), and T (Top Secret)
Associated Impact	Selections include: A (Availability), C (Confidentiality), I (Integrity), and U (Unknown)
Action	Selections include: B (Block/Shutdown), M (Monitoring), and O (Other)

Table 31-64 Case Editor Security Classification Tab (Continued)

Field	Description
Security Classification Code:	
Code	Value automatically calculated from other Security Classification field entries.

Case Editor Notes Tab

The fields on this tab provide a place to enter miscellaneous case information and notes.

Table 31-65 Case Editor Notes Tab

Field	Description
Notes	Text field allowing entry of up to 4000 characters that you can save per note.
Table and List Tabs	Table lists saved notes that you can select to display contents; List provides a combined listing of the all saved notes, in chronological order.

Cases

Cases are entries in an event-tracking system used to track, investigate, and resolve suspicious events in a workflow-type environment. When suspicious events occur, cases are created and assigned to users, who then investigate and resolve them based on enterprise policies and practices.

ArcSight has two ways to create and handle cases. First, it has its own complete case-management system. You can use this system to create new cases and assign them to specific groups and users who are notified and receive the cases and relevant data and information associated with the case. Those users can then act on the assigned cases, specifying resolution or other actions taken on the case, which gets reported back and recorded in the ongoing or final resolution of a case.

In addition to using the built-in case management system that ArcSight provides, you can also integrate it with other external case management systems such as Remedy. In that situation, adding new cases exports event information and bring up forms of the external case management system for you to create and assign new cases. The integration with external case management system can also be customized so that case resolution is reported back and recorded.

Case attachments enable you to attach files to any case you are able to edit, for example log files. You are also able to delete cases and attachments; if you delete a case, it deletes the attachment. You can add a file to a case, making it public or private. Private means that the attachment is never shared with other cases; Public means that everyone has access to the latest edited version of that file. Sharing attachments makes it possible to share files that are common among many cases, for example as with a non-disclosure agreement.

For complete information on working with cases, see [“Managing Cases” on page 585](#).

Case Groups

Cases are organized into these groups:

Table 31-66 Case Groups

Case Group	Description
<User Name>'s Cases	Those assigned to the user ID.
Shared Cases	Cases that the logged-in user has permission to access.
Public Cases	Cases to which all users have read permission.
Unassigned	Cases that are not assigned to any user.

If you have Administrator access you also have a group named All Cases that contains all user case groups and their cases.

Categories

ArcSight uses six primary categories and a flexible set of supporting attributes to more precisely distinguish the events reported by SmartConnectors or generated internally by Managers. You see these under the Category heading in tools such as the [Common Conditions Editor \(CCE\)](#), [Rules Editor](#), or [Event Inspector](#). This ability to recognize more detailed and specific event conditions greatly increases your analytic and reactive options.

These categories and attributes are designated by ArcSight, based on the information offered to SmartConnectors by sensors. Keep in mind that the applicability of a category always depends on the actual configuration of the environment.

If you create a new SmartConnector, remember that you are responsible for establishing the ArcSight categories it should report. The category groups are shown below:

Table 31-67 Categories for SmartConnector Data

Category	Description
Object Category	Events are always about a certain object. An object can, for example, be an application, the operating system, a database, a file or the memory of a server. It is important to realize that we are referring to the targeted object. It is not about who is doing something, but what is the object being accessed, altered, etc. (See "Object Category" on page 837.)
Behavior Category	Events not only refer to certain objects, but there is generally an action or a behavior associated with an event. What is being done to an object? Behaviors include access, execution, or modification, and so on. (See "Behavior Category" on page 839.)
Outcome Category	With the first two dimensions, we know what object is being referred to and what action targeted the object. However, we do not know whether the behavior was successful or not. Therefore, the outcome is a success, a failure or an attempt. An attempt really indicates that something was neither a success nor a failure and the outcome is not clear or there is no statement that could be made about the outcome. (See "Outcome Category" on page 840.)

Table 31-67 Categories for SmartConnector Data (Continued)

Category	Description
Device Group Category	Many security devices serve a multitude of purposes in one product. Intrusion Prevention Systems for example, generate events associated with their fire wall capabilities, as well as their intrusion detection capabilities. To be able to distinguish between these types of events, we introduced a dimension called deviceGroup . This dimension allows us to query, for example, for all of the firewall-type events as opposed to all of the events generated by a firewall. The distinction being that the former query also returns all the firewall messages, for example, in the operating system logs (for example, ip tables). (See “Device Group Category” on page 841.)
Technique Category	Frequently in a security context, we would like to obtain information about the type of events with respect to a security domain. Is an event talking about a denial of service, a brute force attack, IDS evasions, exploits of vulnerabilities, etc. (See “Technique Category” on page 841.)
Significance Category	We need to know the significance of an event. We need the capability, for example, to separate normal events from hostile events. We also need to know whether certain activity reported by the device impacts the availability, confidentiality, or integrity of our systems. All this information is captured in significance. (See “Significance Category” on page 843.)

Object Category

Table 31-68 Object Category Details

Host	Any end-system on the network, such as a PDA, a Windows computer, or a Linux computer.
Operating System	The system software that controls execution of computer programs and access to resources on a host.
Application	A software program that is not an integral part of the operating system.
Service	An application that normally executes at operating system startup. A service often accepts network connections.
Database	A database application.
Backdoor	An application, visible on a host, that listens for network connections and can give a non-authorized user control over that host.
DoS Client	A host that is displaying an application that can participate in a (possibly distributed) denial-of-service attack.
Peer to Peer	An application that listens for, and establishes network connections to, other installations of the same application (for example, Kazaa, Morpheus, Napster).

Table 31-68 Object Category Details (Continued)

Resource	Virus	A host that is displaying a replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A host that is displaying a self-replicating program that spreads itself automatically over the network from one computer to the next.
	File	A long-term storage mechanism (for example, files, directories, hard disks, etc.).
	Process	A single executable module that runs concurrently with other executable modules.
	Interface	An interface to the network.
	Interface Tunnel	Packaging a lower network protocol layer within a higher layer (for example, IPSec Tunnel, HTTP tunneling).
	Registry	The central configuration repository for the operating system and the applications. Application-specific information is not stored here.
	CPU	Events directed at this object relate to consumption or use of the overall processing power of the host.
	Memory	Events directed at this object relate to consumption or use of the overall memory of the host.
	Network	Events that cannot be clearly associated with a host's subitem. Events that involve transport, or many hosts on the same subnet.
Actor	Routing	Routing related events such as BGP.
	Switching	Switching related events such as VLANS.
Vector	User	A single human identity.
	Group	A named collection of users, such as an employee division or social group.
Vector	Virus	A replicating infection of a file that also executes other behaviors on the infected host.
	Worm	A self-replicating program that automatically spreads itself across the network, from one computer to the next.

Table 31-68 Object Category Details (Continued)

Backdoor	An application that listens for network connections and can give a non-authorized user control over that host.
DoS Client	An application that participates in a (possibly distributed) denial-of-service attack.

Behavior Category

Table 31-69 Behavior Category Details

Access	Refers to accessing objects, as in reading.
Start	The start of an ongoing access, such as login.
Stop	The end of an ongoing access, such as logging out.
Authentication	Actions that support authentication.
Add	Adding new authentication credentials.
Delete	Deleting authentication credentials.
Modify	Modifying authentication credentials.
Verify	Credential verification, such as when logins occur.
Authorization	Authorization-related actions.
Add	Adding a privilege for the associated object (for example, a user).
Delete	Removing a privilege for the associated object (for example, a user).
Modify	Modifying the existing privileges for the associated user or entity.
Verify	An authorization check, such as a privilege check.
Communicate	Transactions that occur over the wire.
Query	Communicating a request to a service.
Response	Communicating a response to a request, from a service.
Create	Seeks to create resources, install applications or services, or otherwise cause a new instance of an object.
Delete	The reverse of creation events. Includes uninstalling applications, services, or similar activity.
Execute	Involves loading or executing code, booting or shutting systems down, and similar activity.
Start	The beginning of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.

Table 31-69 Behavior Category Details (Continued)

	Stop	The termination of execution of an application or service. This event is clearly distinguished from a lone "Execute" attribute.
	Query	A query sent to a specific entity - but not over the network (for example, as when generating a report).
	Response	The answer returned by an Execute/Query. For example, a report delivered back from an application, or status messages from applications.
Modify		Involves changing some aspect of an object.
	Content	Changing the object's content, such as writing to or deleting from a file or database.
	Attribute	Changing some attribute of an object, such as a file name, modification date, or create date.
	Configuration	Changing an object's configuration. For example, application, operating system, or registry changes.
Substitute		Replacing files, upgrading software, or service or host failovers.
Found		Noticing an object or its state.
	Vulnerable	An exploitable state that is characteristic of a particular hardware or software release.
	Misconfigured	An exploitable state caused by a weak configuration or similar mishandling.
	Insecure	An exploitable state that arises from poor management or implementation. For example, weak authentication, weak passwords, passwords passed in the clear, default passwords, or simplistically named accounts.
	Exhausted	The targeted object was found to be exhausted (for example, not enough file descriptors available).

Outcome Category

These attributes indicate the probable success or failure of the specified event, within an overall context. For example, the outcome of an event such as an `operation failed` error message can be reported as a `/Success` given that the operation can be presumed to have actually caused a failure. Another example would be an event that identifies a Code Red infection: on a host running Linux the outcome would be `/Failure` (Code Red is Windows-only) while the same event directed at a host with an unknown OS would be reported as an `/Attempt`.

Table 31-70 Outcome Category Details

Attempt	The event occurred but its success or failure cannot be determined.
Failure	The event can be reasonable presumed to have failed.
Success	The event can be reasonable presumed to have succeeded.

Device Group Category

Table 31-71 Device Group Category Details

Application		An application program
Assessment Tool		A network- or host-based scanner that monitors issues such as vulnerability, configurations, and ports
Security Information Manager		A security-event processing correlation engine (the Manager). This "device" deals only in correlated events.
Firewall		A firewall
IDS		An intrusion-detection system
	Network	A network-based intrusion-detection system
	Host	A host-based intrusion-detection system.
	Antivirus	An anti-virus scanner
	File Integrity	A file-integrity scanner
Identity Management		Identity management
Operating System		An operating system
Network Equipment		Network equipment
	Router	A network device with routing (layer 3) capabilities
	Switches	A network device with switching (layer 2) capabilities
VPN		A virtual private network

Technique Category

Table 31-72 Technique Category Details

Traffic		An anomaly in the network traffic, such as non-RFC compliance.
	Network Layer	Anomalies related to IP, ICMP, and other network-layer protocols.
	IP Fragments	Fragmented IP packets.
	Man in the Middle	A man-in-the-middle attack.
	Spoof	Spoofing a source or destination IP address.
	Flow	A problem in network-layer communication logic, such as an out-of-order IP fragment.
	Transport Layer	Anomalies related to TCP, UDP, SSL, and other transport-layer protocols.

Table 31-72 Technique Category Details (Continued)

		Hijack	Hijacking a connection.
		Spoof	Spoofing a transport layer property (for example, a TCP port number, or an SSL entity).
		Flow	A problem in TCP connections or flows, such as a SYNACK without SYN, a sequence number mismatch, or time exceeded.
		Application Layer	Application-layer anomalies.
		Flow	A peer does not follow the order of commands.
		Syntax Error	A syntax error in an application-layer command.
		Unsupported Command	A command which does not exist or is not supported.
		Man in the Middle	A man-in-the-middle attack on the application layer.
	Exploit	Vulnerability	Exploiting a vulnerability (for example, a buffer overflow, code injection, or format string).
		Weak Configuration	Exploitation of a weak configuration. This is something that could be remedied easily by changing the configuration of the service (for example, weak passwords, default passwords, insecure software versions, or open SMTP relays).
		Privilege Escalation	A user identity has received an increase in its user privileges.
		Directory Transversal	A user identity is attempting to browse or methodically review directories for which it may not have appropriate privileges.
	Brute Force		Brute-force attacks.
		Login	Continued trials for logins.
		URL Guessing	Continued trials for URLs to access information or scripts.
	Redirection		Redirecting an entity.
		ICMP	ICMP redirects.
		DNS	Unauthorized DNS changes.
		Routing Protocols	Attacks aimed at routing protocols (for example, BGP, RIP, OSPF).
		IP	Redirection using the IP protocol (for example, source routing).
		Application	Redirection attacks on the application layer (for example, cross-site scripting, mail routing, or JavaScript spoofing).

Table 31-72 Technique Category Details (Continued)

Code Execution		Either the execution or transmission of executable code, or the transmission of a distinctive response from executed code.
	Trojan	The code in question is concealed within other code that serves as a Trojan Horse. In other words, it appears to be one thing (that is safe) but is really another (which is unsafe).
	Application Command	The code in question is intended to invoke an application command.
	Shell Command	The code in question is intended to be executed in a shell.
	Worm	Code associated with a worm.
	Virus	Code associated with a virus.
Scan		Any type of scanning. A network, host, application, or operating system scan can be identified through the specified object.
	Port	Multiple ports are scanned.
	Service	A service is scanned (for example, DDoS client discovery, backdoors, RPC services, or scans for a specific application such as NMB).
	Host	Scanning for hosts on a network.
	IP Protocol	A search for responding protocols. Note that TCP and UDP are not the only transport protocols available.
	Vulnerability	A scan for vulnerabilities.
DoS		A DoS attack is in progress.
Information Leak		Information leaking out of its intended environment (for example, mail messages leaking out, system file access, FTP data access, or web document access).
	Covert Channel	Leakage was detected from a covert channel, such as Loki.
Policy		Policy-related violations such as pornographic web site access.
	Breach	A policy-related security breach occurred.
	Compliant	A policy-compliant event occurred.

Significance Category

Table 31-73 Significance Category Details

Compromise	A potentially compromising event occurred.
Hostile	A malicious event has happened or is happening.

Table 31-73 Significance Category Details (Continued)

Informational	Events considered worthy of inspection; for example, those produced by polling.
Error	An execution problem.
Warning	A possible problem.
Alert	A situational problem that requires immediate attention.
Normal	Ordinary or expected activity that is significant only for forensic purposes.
Recon	Relates to scans and other reconnaissance activity.
Suspicious	A potentially malicious event occurred.

Custom Event Categorization


Events received from ArcSight supported devices are automatically **categorized** (appended with classification information) by ArcSight SmartConnectors per the ArcSight event categorization taxonomy. Event [Categories](#) are used to classify events based on criteria such as object type, behavior, outcome, technique, device group, and significance. This additional information about an event (together with normalization and other filtering) helps to identify the significance events from different devices and vendors based on a consistent model.

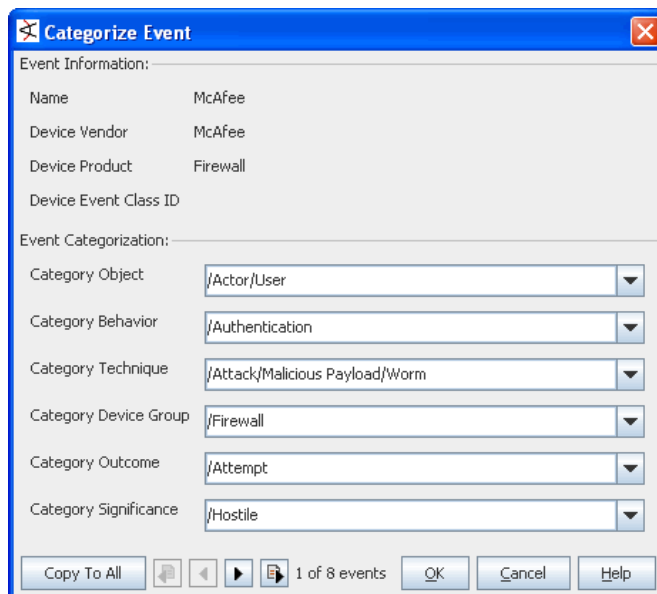
However, events from unsupported or custom devices can generate events that the provided connectors do not know how to categorize. For example, if your organization has developed and deployed ArcSight FlexConnectors to collect and process events specific to customized network nodes, these custom events are not categorized per the usual method.

From the ESM Console, you can manually apply categorization to one or more custom events from a FlexConnector (or other custom or unsupported device). Once you apply categorization to events from a particular device (and its associated connector), the categorization is automatically applied to other events of the same type.

To apply event categorization to one or more events:

- 1 Select one or more of the same type of events that you want to categorize.

- 2 Choose Select one or more events and choose the **Categorize Event** command from the System menu (or click the  toolbar button).



The **Categorize Event** dialog box is used to categorize a selected event. It contains two main sections: **Event Information** and **Event Categorization**.

Event Information:

- Name: McAfee
- Device Vendor: McAfee
- Device Product: Firewall
- Device Event Class ID: (empty)

Event Categorization:

- Category Object: /Actor/User
- Category Behavior: /Authentication
- Category Technique: /Attack/Malicious Payload/Worm
- Category Device Group: /Firewall
- Category Outcome: /Attempt
- Category Significance: /Hostile

At the bottom, there are buttons for **Copy To All**, navigation arrows, **1 of 8 events**, **OK**, **Cancel**, and **Help**.

- 3 Select values from the given categories from the drop-down menus.
- 4 Click **OK** to apply the categorization information to events of this type.

This generates a SmartConnector update file (.aup) containing the new categorization files on the Manager. The Manager polls for new SmartConnector update files every 5 minutes, and updates the SmartConnectors when it finds new .aup files. So, within 5 to 20 minutes after you apply event categorization, new events of the same type are categorized in the same way.

Note that if a certain type of event is already categorized, this custom categorization has no effect. If not, the custom categorizations take effect on all events of the same type going forward.

Collaboration

The ESM Console collaboration capability is a collection of features that make it possible for analyst teams to select certain security events for further on-going investigation. Investigation involves a workflow-style process of information collection that leads through a series of analysis stages to a final disposition.

In the ESM Console, you locate events for analysis through the active channels in the Viewer panel. You use the Annotate Events dialog box or the Event Inspector to annotate an event, or collection of events, and set it up for follow-on analysis. Once you have placed the event or collection in the collaboration "pipeline" by assigning it a disposition stage (such as **Initial**), you or other analysts manage it through to resolution using the assigned stages as filter arguments.

ArcSight provides a set of default collaboration stages, but your enterprise may well use others created specifically for your workflow needs. Owners, disposition stages, comments, and other factors change as an event's handling progresses. The collaboration cycle usually ends when someone marks the event's **Stage** field as **Closed** (or the equivalent).

Compare collaborative annotation to cases, which are a more formal way to track sets of events that are under investigation.

Table 31-74 Default Collaboration Stages

Stage	Meaning
Queued	The event has not yet been inspected.
Initial	The event has been inspected.
Follow-up	The event is under investigation.
Final	The investigation has concluded.
Closed	The investigation is closed.
Monitoring	The event is being watched, especially in regard to a reoccurrence in support of a pattern.
Rule Created	The event has been used to create a rule that assists in monitoring for a reoccurrence, especially in regard to patterns, and potentially to respond in some way such as with a notification.
Flagged as Similar	The event is similar to one already under investigation.

See [“Collaborating on Events” on page 216](#) for descriptions of the tasks involved.

Common Conditions Editor (CCE)

The [ESM Console](#) has a Boolean logic editor, which is also referred to as the Common Conditions Editor (CCE). If the criteria are met, the evaluation returns a Boolean true or false. All conditions constructed by the CCE are expressions that consist of a value or variable on the left, an operator (not, and, or), and a value on the right, for defining the conditions you use to help analyze resources such as filters, rules, and reports. This topic is your reference for using the CCE, wherever it appears.

See also [Chapter 11, Filtering Events, on page 223](#), especially subtopics on [“Creating Filters” on page 223](#) and [“Debugging Filters to Match Events” on page 227](#).

Editor Features

The CCE has two tabs; **Edit** and **Summary**. In the **Edit** tab, logical operators are represented in a tree form.

In the **Summary** tab, conditions are presented in an easily readable, summary view. Resource references in the **Summary** tab are hyperlinked. (From the Summary tab, click a resource link to open its definition in a resource editor in the Inspect/Edit panel.)

Conditions are editable only on the **Edit** tab. Wherever the CCE appears, you use these features to build or change conditional expressions.

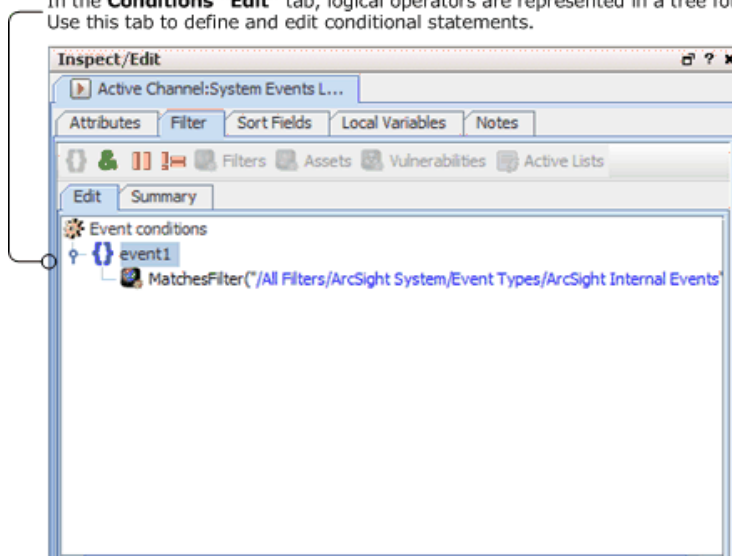
- The condition tree shows the complete set of expressions you are building or changing.
- The root of the tree indicates whether the expression concerns [Filters \(Filter By\)](#), [Correlation \(Correlate\)](#), or [Reports \(Report On\)](#), as you see in the Filters Editor, Rules Editor, or Report Editor, respectively.

- From the root, there are branches for one or more [Events](#). For each event branch, there are sub-branches for one or more condition statements.
- To add an event for a rule, select the root and click the **New Event Definition** button (see below) or right-click the root and choose the same command. Note that only rules can add events because filters and reports do not need additional events for correlation.
- To act on a specific event or [Conditional Statements](#), select it in the tree. Once selected, you can use several features to modify it, as described here and below.
- Use the new event, [Logical Operators](#), and resource selector buttons above the tree to add events, operators, or resource-based constraints to condition statements, if applicable.
- Use the right-click menus that are available for any selected branch of the condition tree to choose commands that are applicable to that statement in that context.
- When you use the right-click **Edit** command to edit a selected statement directly in the tree (rather than through the event fields table), you can use the Enter key to update the condition without having to click **Apply** or **OK**.
- Do use single- or multiple-selection copying and pasting of statements for efficiency. You can use the right-click menu commands or **Ctrl+C** for copy, **Ctrl+X** for cut, and **Ctrl+V** for paste.
- Use the [Field Sets](#) selector to choose an appropriate group of event fields when an event-related statement is selected in the condition tree.
- To **undo/redo** an action, right-click in the Edit panel and choose either **Undo** or **Redo**, depending upon the action you want to use. For example, if you decide to delete a node, a message asks you to confirm. If you want to undo this delete, right-click in the Edit panel and choose **Undo Delete**. (You can also use the standard keyboard commands **Ctrl+Z** for undo and **Ctrl+Y** for redo.)
- To **Search** for a resource, simply click in the field column (on the left side of the list) and start typing. A Search popup is displayed when you start typing, and shows the term as you type it. The search is "predictive" in that it navigates to and select matching fields as you type. Click **Enter** to select this resource. For details see ["Searching for Fields in Event Inspector, Resource Editors or CCE"](#) on page 103.

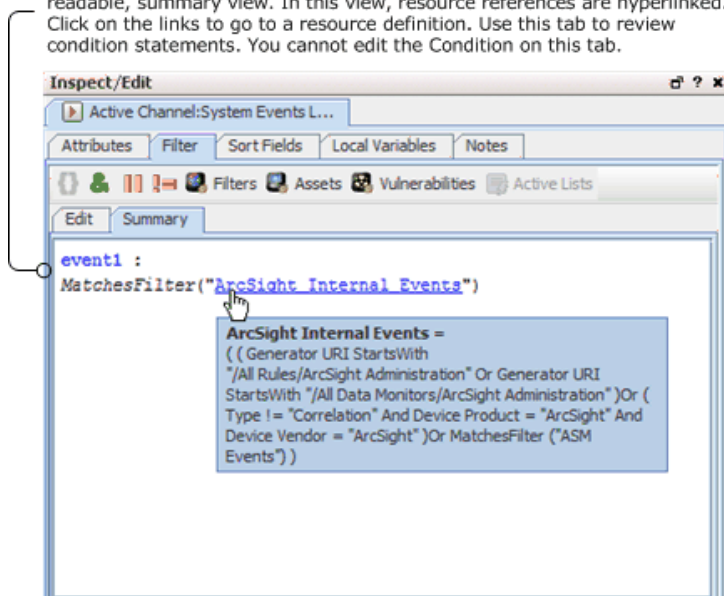


Both tabs provide syntax and error highlighting. As an example of error highlighting, if a condition uses resources that are later removed, references to the missing resources are highlighted as errors in the condition statements in the CCE.

In the **Conditions "Edit"** tab, logical operators are represented in a tree form. Use this tab to define and edit conditional statements.



In the **Conditions "Summary"** tab, conditions are shown in an easily readable, summary view. In this view, resource references are hyperlinked. Click on the links to go to a resource definition. Use this tab to review condition statements. You cannot edit the Condition on this tab.



Condition Tree Command Buttons

All of the following options are available from buttons at the top of the Conditions Editor and also from right-click menu options. The exception is the "In Case" Condition which is only available from a right-click menu option.

Table 31-75 Condition Tree Command Buttons











Button	Name	Use
	New Event Definition	Insert a new condition tree in the editor.

Table 31-75 Condition Tree Command Buttons (Continued)

Button	Name	Use
	AND	Insert an AND condition.
	OR	Insert an OR condition.
	NOT	Insert a NOT condition.
	"Matches Filter" Condition	This resource-based command browses the Filters tree of the Navigator panel. Note that this operator applies only to rules.
	"Assets" Condition	This resource-based command browses the Assets tree of the Navigator panel. Note that this operator applies only to rules.
	"Categories" Condition	This resource-based command browses the Categories tab of the Navigator panel's Assets tree.
	"Has Vulnerability" Condition	This resource-based command browses the Vulnerabilities tree in the Navigator panel.
	"InActiveList" Condition	<p>This command browses the Navigator panel's Active Lists tree, and operates on items in the event and actor schemas. It is used to map a field or a global variable in the event schema to a corresponding field in an active list. It does not evaluate items in other non-event schemas (such as cases or assets).</p> <p>Note: The InActiveList operator option evaluates single-value attributes and multi-value attributes. The field you map could return multiple values. In the case of multi-value attributes, if any one value matches, the condition evaluates to true.</p> <p>Consider this scenario for multi-value attributes: An active list keeps track of actor roles where role values can be one of Normal, Restricted, or Privileged. You can test if an actor has one of these roles. If your list has a field called RoleName, you map the actor's RoleName attribute to this field. Keep in mind that an actor's RoleName attribute is multi-valued because an actor can have multiple roles. Through the InActiveList condition, you can have a query that will check if one of the actor's roles is Privileged.</p> <p>A condition that tests for whether all or any values in a list match is only available to specify on queries and on in-memory operations such as rules, filters, data monitors.</p>
	"InCase" Condition	<p>This resource-based command browses the Navigator panel's Cases tree.</p> <p>Note: This option is only available from a right-click menu option. There is no button for it.</p>
	"Join" Condition	<p>Inserts a JOIN condition.</p> <p>Note: This option applies only to Rules.</p>

Condition Tree Context Menu Commands

Table 31-76 Condition Tree Context Menu Commands

Command	Description	Applies To
New Condition	Add a new condition statement below the selected element. Type the statement directly in the tree or choose a field from the pop-up menu.	operator, event field
New Logical Operator	Add a new logical operator to the selected element. (See "Logical Operators" on page 947.)	Event alias, operator, event field
New Constant Condition	Add a Boolean (True/False) AND operator to the selected branch.	operator
New "Matches Filter" Condition	Use the Filter selector to identify a particular filter as a matching argument for a condition. See also Creating Matching or Join Conditions in "Specifying Rule Conditions" on page 442.	operator, event field
New "Assets" Condition	Use the Assets selector to identify an asset or group as the argument for a condition. See also Adding Asset Conditions in "Specifying Rule Conditions" on page 442.	operator, event field
New "Has Vulnerability" Condition	Use the Vulnerability selector to identify a vulnerability as the argument for a condition. See also Adding Vulnerability Conditions in "Specifying Rule Conditions" on page 442.	operator, event field

Table 31-76 Condition Tree Context Menu Commands (Continued)

Command	Description	Applies To
New "InActiveList" Condition	<p>Use the Active List selector to identify a particular active list that contains the argument for a condition. It is used to map a field or a global variable in the event schema to a corresponding field in an active list. It does not evaluate items in other non-event schemas (such as cases or assets).</p> <p>When the InActiveList condition is used to compare values in two lists, an additional option is shown where you can specify whether All values in list field must match. If this option is checked, the Active List condition evaluates to true only if all values in both lists match. If it is not selected, the condition evaluates to true if any field is in both lists.</p> <p>Note: The InActiveList operator option evaluates single-value attributes and multi-value attributes. The field you map could return multiple values. In the case of multi-value attributes, if any one value matches, the condition evaluates to true.</p> <p>Consider this scenario for multi-value attributes: An active list keeps track of actor roles where role values can be one of Normal, Restricted, or Privileged. You can test if an actor has one of these roles. If your list has a field called RoleName, you map the actor's RoleName attribute to this field. Keep in mind that an actor's RoleName attribute is multi-valued because an actor can have multiple roles. Through the InActiveList condition, you can have a query that will check if one of the actor's roles is Privileged.</p> <p>A condition that tests for whether all or any values in a list match is only available to specify on queries and on in-memory operations such as rules, filters, data monitors.</p> <p>See also Adding Active List (InActiveList) Conditions in "Specifying Rule Conditions" on page 442.</p>	operator, event field
New "InCase" Condition	Use the Cases resource tree to identify a particular case as the argument for a condition.	operator, event field
New Event Definition	<p>Create and name a new event alias to add to the root.</p> <p>Note: This option applies only to Rules.</p>	root
Set Global Expiration time	<p>For rules, set the amount of time that qualifying events for all aliases are retained in memory for evaluation, based on Manager receipt-time. Setting an alias expiration overrides a global expiration, if present. See "Specifying Rule Thresholds and Aggregation" on page 449 for more information.</p> <p>Note: This option applies only to Rules.</p>	root
Edit	Open a text box in which to change the selected element.	operator, event field

Table 31-76 Condition Tree Context Menu Commands (Continued)

Command	Description	Applies To
Undo	Undo an action.	all actions
Redo	Redo an action.	all actions
Cut	Cut the selected elements of the condition tree to the Clipboard.	root, event alias, operator, asset, event field
Copy	Copy the selected elements of the condition tree to the Clipboard.	root, event alias, operator, asset, event field
Paste	Paste the conditional element currently on the Clipboard to the end of the selected element in the tree.	root, event alias, operator, asset, event field
Delete	Delete the selected elements of the condition tree.	event alias, operator, asset, event field
Set Alias Expiration Time	For rules, set the amount of time that a qualifying event for this alias (only) is retained in memory for evaluation, based on Manager receipt-time. See "Specifying Rule Thresholds and Aggregation" on page 449 for more information. Note: This option applies only to Rules.	event alias
Set Matching Time	Sets the maximum time difference between the partially-matched aliases. Note: This option applies only to Rules.	matching event operator
Print Conditions and Tree Summary	Prints the condition definition as shown on the Edit tab and the Summary statement. Selecting this menu option brings up a Print Preview dialog where you can view what will print, and set printer options.	event alias, operator, asset
Help	Open the online Help system for information about the type of resource being edited.	root, event alias, operator, asset, event field

Adding Conditions

When adding conditions, you have to decide how the new condition ties to existing conditions. If And is used, the new condition has to occur in addition to existing conditions. If Or is used, the new condition or any existing conditions have to occur. If Not is used, all but the new condition has to occur.

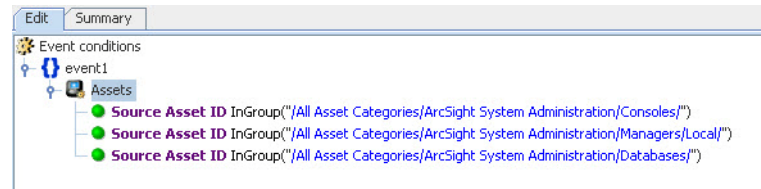
You use the AND, OR, and NOT operators to define relationships between condition statements. When you use AND, the new condition must occur in addition to the selected

condition. Using OR means either the selected or new condition must occur. Using NOT means all but the new condition must occur.

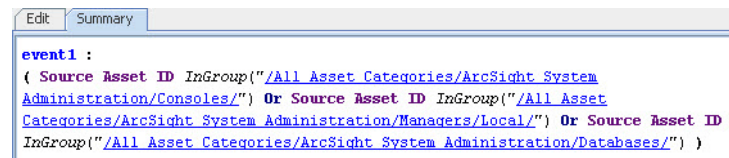


Multiple assets and asset categories added to a single asset condition are always OR'ed together (not AND'ed).

For example, create a new rule, click the **Conditions** tab in the Rule Editor, select **Assets**, and add some asset categories to the condition. (To do this, select them on the Asset Categories tab at the bottom of the Editor and click **Apply**.)



Now click the **Summary** tab to view the detail of the Boolean logic. This shows that the assets are OR'ed together.



If you want to AND an asset condition to other conditions, go back to the **Edit** tab, select the event definition again, and add other conditions based on the fields shown in the lower half of the editor.

To add more condition statements, right-click an existing statement and choose **New Logical Operator**, then **And**, **Or**, or **Not**, or click a logical operator or resource-selection button. Then, create the new condition statement.

Event-definition and Join conditions are allowed (only) with rules to include separate "events" or aliases, or correlation of these separate "events" respectively.

In the data field table, scroll to a data field in the Name column to create a condition statement.

Data fields provide event details from all devices deployed throughout your enterprise. Event details from these devices are normalized into common data fields and stored in the ArcSight Database to allow investigative and analytical comparison of all incoming events. See ["Data Fields" on page 867](#) and ["Timestamp Variables" on page 1003](#) for more information.

The data field table displays a **Name**, **Operator**, and **Condition** column. These three columns are combined to create `<data field> <logic operator> <data field value>` condition statements. For example, if monitoring a Cisco Router, you could define a condition statement to specify `Device Product = Cisco Router`: `Device Product` as the data field, equals (=) as the logic operator, and `Cisco Router` as the data field value.

Search Box to Find Fields in the List



Search Shortcuts

- Type part of the field name you want to find (for example, Name) in the Search box.
- Use the up/down arrow keys to jump to each instance of "Name" in the available fields.
- When you find the field name you want, hit Return to add it to the condition statement
- Ctrl+F gets the Search box back in display if it's hidden

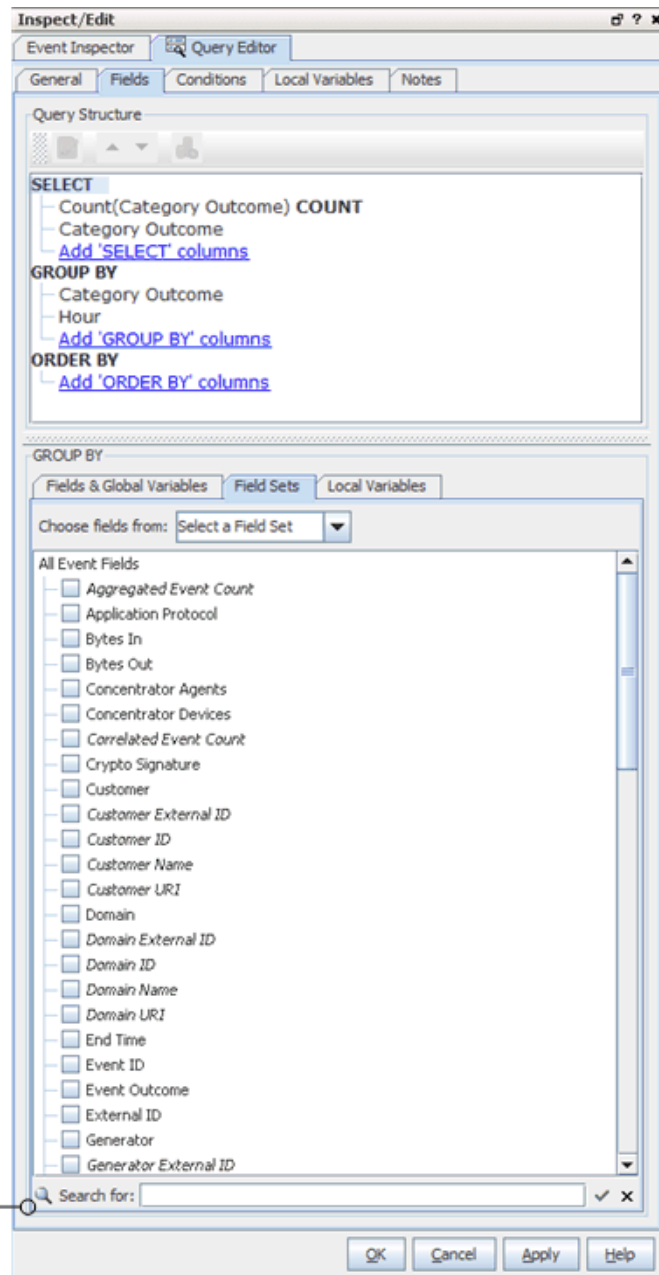
Search Shortcuts:

Type part of the field name you want to find (e.g., Name) in the Search box.

Use the up/down arrow keys to jump to each instance of "Name" in the available fields.

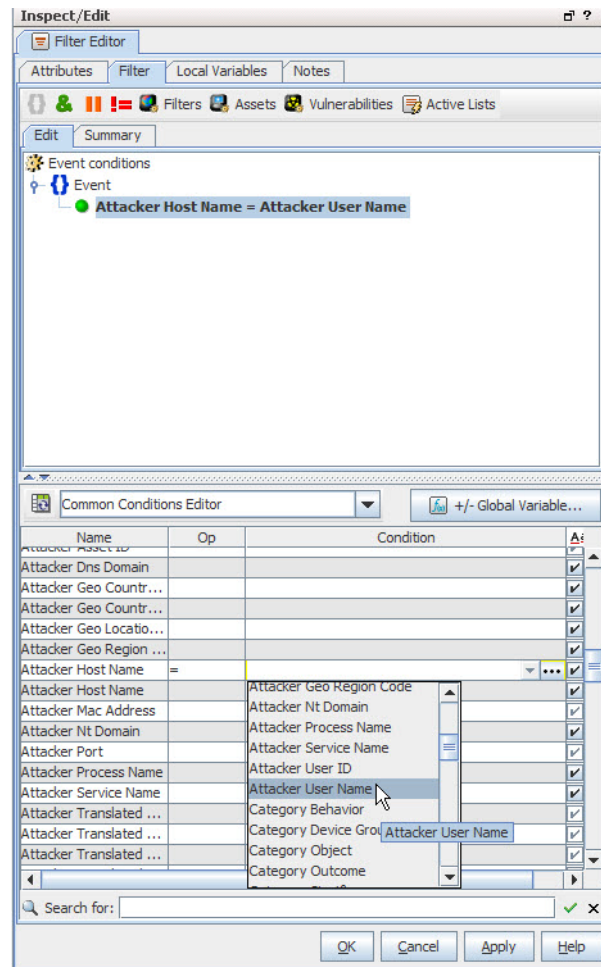
When you find the field name you want, hit Return to add it to the selected query structure sections (SELECT, GROUP BY, or ORDER BY)

Ctrl+F gets the Search box back in display if it's hidden



Field Comparisons with Variable or Static Values

For any field comparison, a drop-down menu of variables is provided for the *right* side of the statement. Or you can type a value here.




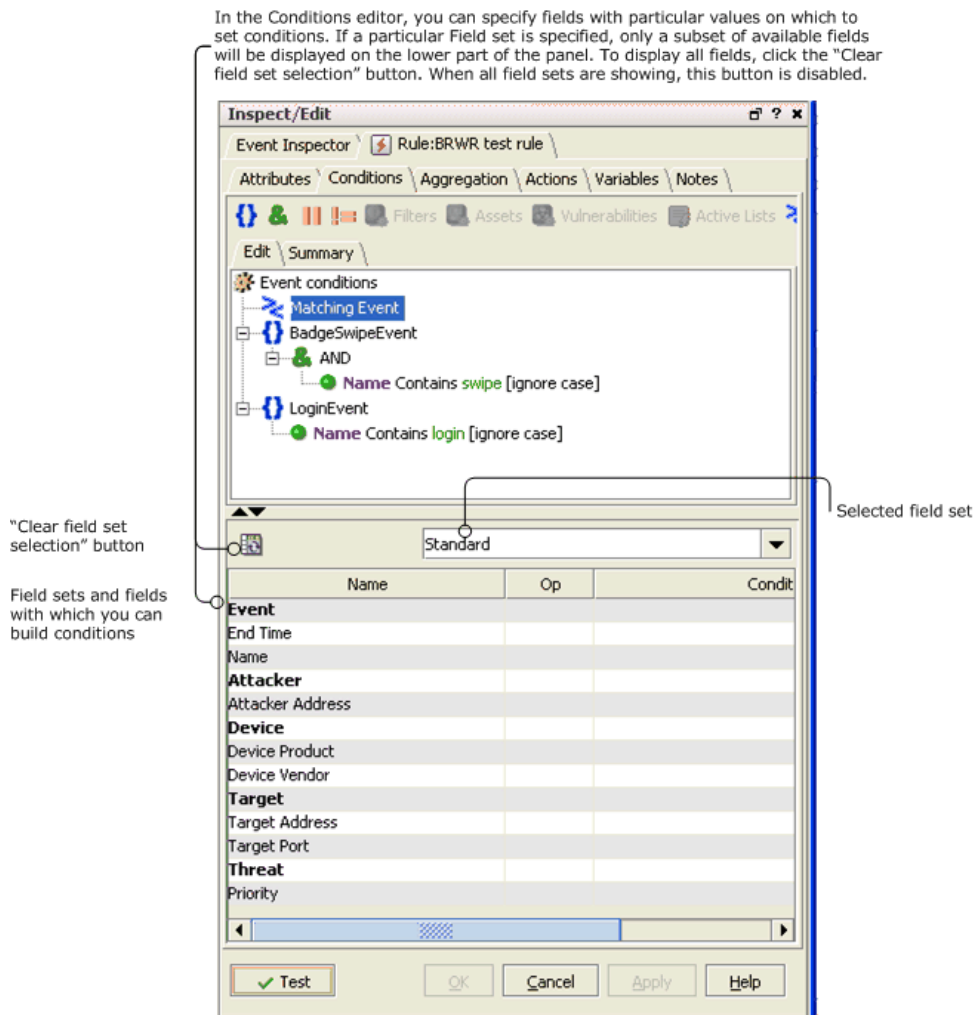
The CCE provides a field comparison ability that allows you to compare one field to another field (for example, `AttackerHostName = AttackerUserName`). This functionality is available on the ESM Console wherever the CCE is available (in [Rules](#), [Reports](#), [Filters](#), and so on). If the fields you are comparing are numeric, the fields can be of different numeric types, for example, a long type compared to a floating point type.

Left-side event attributes can be compared to right-side conditions (represented as variables or static values) using operators like equals (`=`), is not equal to (`!=`), is less than or equal to (`<=`), is greater than or equal to (`>=`), is less than (`<`), is greater than (`>`), and so forth.

Using Field Sets

The Common Conditions Editor provides access to all available [Field Sets](#), including domain field sets you created. You can specify fields with particular values as part of conditions statements. See also [“Creating and Using Field Sets” on page 204](#) and [Chapter 18, Domain Field Sets, on page 491](#).

You can select a particular field set, which limits the fields shown to a subset of all available field sets. If you cannot find a field, click the "Clear field set" button  to clear the field set selection and show the complete list of field sets. This clears the field set selection and shows the complete list of field sets. A common problem is having the common conditions editor (CCE) field display limited to a field set that does not include some fields you want to use in the condition.



For example, suppose you define a condition to look for two matching events; one in which Event Name contains "swipe" and another in which Event Name contains "login". You can set this condition with the "Standard" field set shown above because it includes the Event Name field in the list of available fields from which to choose. But if you wanted to add conditions based on an Event field for "Correlated Event Count" or Threat field for "Model Confidence", you would need to clear the Field Set and view all fields to get access to these fields.



Tip

Fields shown in italics are *derived* from data in other fields. Derived fields show up in various places on the ESM Console UI including on the Field Set editor, and the Common Conditions Editor (CCE) aggregation tabs (for example, Rules, Filters, and so forth).

Adding or Removing Global Variables Using the CCE

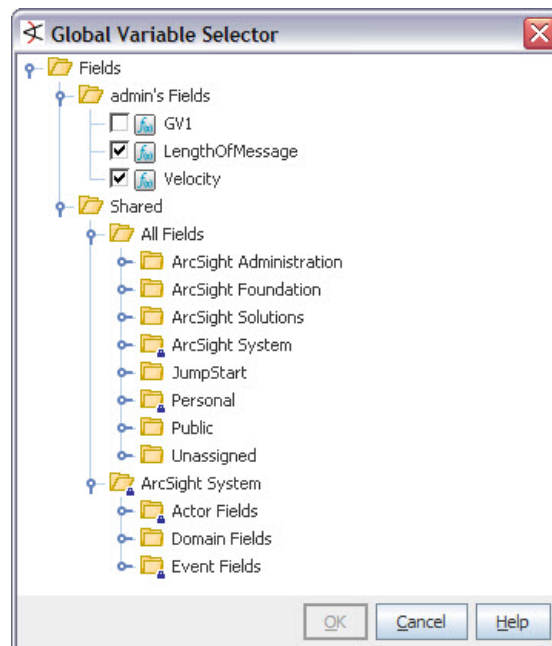
The Common Conditions Editor enables you to define a local variable to apply to the condition statement for that resource, and it also enables you to place [Global Variables](#) in the condition by using the **+/- Global Variables** button (next to the Field Set selector) on the CCE.

To add global variables and make them available for conditional statements in a resource:

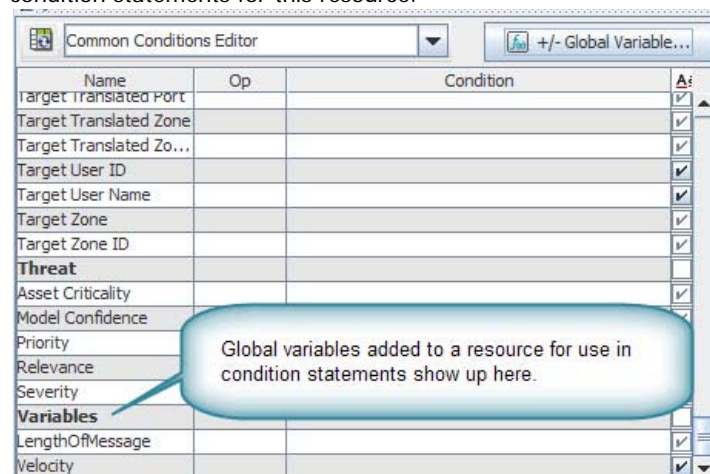
- 1 In the CCE for a given resource, click the +/-Global Variable button



- 2 On the Global Variable Selector dialog, select one or more variables you want to add and click **OK**.



- 3 The added variables show up as available fields under the group selected for it in the Global Variables editor (such as the Variables group). You can use these variables in condition statements for this resource.



To remove one or more global variables from the available fields list in the CCE for a resource:

- 1 In the CCE for a given resource, click the +/-Global Variable button



- 2 On the Global Variable Selector dialog, click to de-select one or more variables you want to remove and click **OK**.
- 3 The variables are removed from the list of available fields in the CCE.

For more information about global variables, see [Chapter 17, Global Variables, on page 477](#).

For information about variables in general, see ["Variables" on page 1006](#).

For information about using variables with velocity expressions, see ["Velocity Templates" on page 1019](#).

Testing for Zone Relevance

Events include several [Data Fields](#) that are related to zones (see ["Assets" on page 799](#)). In the Common Conditions Editor you can compare these fields with asset groups or categories, to test whether the field's event does or does not correlate with those asset properties. This comparison is performed by the **InGroup** operator.

For example, if an event's Attacker Zone field value and a Source Asset ID's System Asset Categories' Criticality value correlate, then the InGroup operator would test True. You can apply this outcome in your reports, rules, or filters.



Note

The InGroup operator is inserted automatically when you create zone-asset correlation statements in the Common Condition Editor. There is no button or command to manually insert it.

The InGroup operator tests True for specified asset resources and their parents but not for their own peers or their parent's peers.

- 1 In the Conditions tab of any appropriate editor, set a logical operator for a zone-related field (for example, Destination Zone).
- 2 In the same field, click the ellipses button (...). In the Select a Zone dialog, enter a prompt for the condition, select the **Parameter** checkbox, then choose a zone from the resource tree.
- 3 Right-click the new statement in the editor and choose **AND**, then right-click the AND statement and choose **New Assets Condition**.
- 4 In the Asset resources panel below, choose the Source, Target, or other type of relevant asset ID.
- 5 For that asset ID type, click the **Assets** or **Asset Categories** tab and select an asset group or category to test with the InGroup operator.
- 6 Click **Apply** in the Assets resources panel to add the asset group or category to the condition statement, with the embedded Ingroup operator.

How to Create a Matching or Join Rule

A matching or join condition is a condition statement that joins two data fields together with the Matching or Join condition logic operator on the Conditions Tab. Creating matching or join conditions using data fields provides the flexibility of creating conditions without knowing the specific data field's values. The following join data field conditions can be created:

- Same data field for two events: `EventOne <data field A> <logic operator> EventTwo <data field A>`. For example, `EventOne Source Address = EventTwo Source Address`. In this example, both event data field must have the same value. This rule is useful when monitoring activity from an unknown Source Address that is generating numerous events.
- Different data fields for two events: `EventOne <data field A> <logic operator> EventTwo <data field B>`. For example, `EventOne Source Address = EventTwo Target Address`. In this example, the Source Address of the first event must equal the Target Address of the second event.
- Different data fields for the same event: `EventOne <data field A> <logic operator> EventOne <data field B>`. For example, `EventOne Source Address = EventOne Target Address`. In this example, the Source Address must equal the Target Address of the same event.



There is a relatively high memory cost for join rules with low-selectivity join conditions (such as same source IP or same target IP). Just like queries in SQL, the more selective the conditions (the conditions on the individual events as well as the join conditions), the less memory it takes to execute, because fewer conditions match.

When authoring a rule you should order conditions on the events to be correlated (or joined) by placing the most restrictive conditions first, for example, adding join conditions like `"event1's Source Address = event2's Source Address"` or `"event2's Detect Time > event1's Detect Time"`. This dramatically reduces the memory consumption by the Cross-Correlation Engine, as much as 50% in some cases.

Conditional Statements

This table offers sample conditional expressions you can create using various operators, event fields, and data types.

Table 31-77 Conditional Statements

ArcSight Data Types	Description
Number or Integer	Using numeric (integer) fields, you can specify operators including <code>=</code> , <code>!=</code> , <code><</code> , <code><=</code> , <code>>=</code> , <code>></code> , and <code>In</code> to specify a numeric comparison expression, for example: <code>CustomNumber1 = 50</code> . To use <code>In</code> , you can specify any number of comma-separated values to match (or equal).
String	Using string fields, you can specify operators including <code>=</code> , <code>!=</code> , and <code>In</code> , <code>Contains</code> , <code>Matches</code> , <code>Starts With</code> , <code>Ends With</code> , and <code>Like</code> to define a string comparison expression. For example: <code>ArcSightCategory StartsWith /Attack</code> or <code>ArcSightCategory = /AttackSuccess</code>

Table 31-77 Conditional Statements (Continued)

ArcSight Data Types	Description
DateTime	<p>Using DateTime fields, you can specify operators including <code>=</code>, <code>!=</code>, <code>Between</code>, <code>In</code>, and <code>On</code> to specify a datetime comparison expression. For example: <code>DetectTime Between 4/1/03 11:30:01AM, 4/1/03 4:30:01PM</code>.</p> <p>You can enter DateTime values directly or click the ellipsis (...) button to select a date from a pop-up calendar or a special date keyword list. Special date keywords you can use are: <code>Now</code>, <code>1 or 2 hours ago</code>, <code>1 or 2 days ago</code>, <code>1 or 2 weeks ago</code>, or a replay start and end time. You can also use special system variables such as:</p> <ul style="list-style-type: none"> • <code>\$CurrentDateTime</code>: for the date and time the report is run; the system variable is replaced by the current date and time value." • <code>\$CurrentDate</code>: for the date the report is run; the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run. <p>You can specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: <code>\$CurrentDate - 7d</code> for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or <code>\$CurrentDateTime - 12h</code>, which evaluates to the current date time minus 12 hours.</p>
IP Address	<p>Using IP address fields, you can specify operators including <code>=</code>, <code>!=</code>, <code>In</code>, <code>InSubnet</code>, and <code>Between</code> to specify an IP comparison expression. For example: <code>TargetAddress = 178.168.11.211</code>. With the <code>In</code> operator, you can also specify a comma-separated list of IP addresses to match and, with <code>InSubnet</code>, can also specify IP address ranges in CIDR format, or use <code>InSubnet</code> to specify an range of addresses in a specific subnet.</p>

These same rules apply to the conditions editor used in defining rules, creating conditional reports, and filters.

ArcSight Variables

You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as `$Now` and `$CurrentDateTime`. The same is true for time elements, including `s` (second), `m` (minute), `d` (date), `M` (month), `w` (week), and `y` (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign; for example, "Source Address" would be `$sourceAddress`. See the complete discussion in the topic "[Variables](#)" on page 1006.

Conditions

Conditions are logical expressions (see [Logical Operators](#)) used to qualify [Events](#) or other grouping of elements. Conditions can be specified in a number of places using a common condition editor; for example, to define rules or filters.

Parameterized Conditions

Some conditions can be parameterized, for example in reports, where the exact value specified for a condition match is provided at the time of running the report, through a

parameter pop-up box. This lets report authors give default parameter values, which can be overridden by the user running the report.

Name	Value
Report Parameters	
* Start	8/17/05 4:32:37 PM
* End	8/17/05 5:32:37 PM
Common	
Report File Format	PDF
Report Page Size	Letter [8.5x11 in]
Run Report as	Select a User
Filter results by	Select a Filter
Email To	
Email Format	Send URL

☐ Save Report Output

This is a convenience for people running the report as it does not require write permissions while running the report, but effectively provides the same flexibility as being able to modify the report. Note that when defining parameters for detect time, you should always include a BETWEEN condition so that the report is limited to a certain time range, and does not scan the entire event table. Otherwise, it can severely impact the Manager information-retrieval performance.

- 1 You can select the ellipsis (...) button and then select the **Parameter** checkbox to create a parameter prompt for selected data fields of a report. When users run the report, they are first prompted to enter values for these parameters. When specifying a report parameter, you can define the prompt that is displayed to users, as well as specify a default value that is displayed in the prompt field.
- 2 In the case-sensitive column (**Aa**), select the checkbox if the data field needs to be case-sensitive.
- 3 In the negate condition column (the "No" symbol), select the checkbox to change conditions to **all but this** statements.

For example, if the condition statement is Device Product = Cisco Router and the negate condition checkbox is selected, all events but those from the Cisco Router generate a correlation event.



Note

Some conditions can be parameterized such that the exact value is provided at the time of running the report through a parameter pop-up box. This lets report authors give default parameter values, which can be overridden by the user running the report. This is a very useful convenience for people running the report as it does not require write permissions while running the report but effectively provides the same flexibility as being able to modify the report. Note that when defining parameters for detect time, you should always include a BETWEEN condition so that the report is limited to a certain time range, and does not scan the entire event table. Otherwise it can severely impact the performance of Manager, retrieving information from the database.

- 4 Click outside the data field row.

The condition statement (<data field> <logic operator> <data field value>) appears as a branch under the logical operator.

- 5 On the Conditions tab, click **OK**.

These same rules apply to the conditions editor used in creating other resources such as rules and reports.

ESM Console

The ESM Console is a centralized view into an enterprise. A graphical user interface that provides centralized intelligent real-time monitoring to secure your enterprise.

ESM Console settings consist of your color selections, preferences, temporary filters, window sizes, etc., and are saved in a `.ast` file. The current setting file you are using is displayed in the ESM Console title bar (by default, `machine:username.ast`). You can perform operations to save or load `.ast` files stored locally, on the same machine where the ESM Console is installed, on save or load `.ast` files stored and maintained by the Manager. After settings are saved in a file, the `.ast` file is listed in the File menu. The File menu lists the last four `.ast` files that have been accessed.

Concerning ESM Console-Manager connections, you may want to note that while each Manager connects to many ESM Consoles, each ESM Console connects to only one Manager. Also, when an ESM Console is connected to a Manager, it affects only that Manager, regardless of how that Manager may be linked within a larger Manager hierarchy.

For information on viewing various articles, information, reports, or command results in a Web browser, see [“Web Browsers \(Internal and External\)” on page 1030](#).

See related topics [Chapter 6, Working in the ESM Console, on page 93](#) and [Chapter 30, Personalizing the ESM Console, on page 771](#).

Content

ArcSight provides preconfigured [Resources](#), also known as *content*, in the form of [Packages](#). Content packages are automatically installed to provide out-of-box resource suites that you can start using immediately to monitor and protect your network. Also, you can develop your own custom content with the editors and tools provided.

Content Packages

ArcSight ships with system content already developed that addresses common security and regulatory use cases. These use cases combine many resources to address multi-faceted issues. You can use system content as is, or modify it with data specific to your network environment.

System content is delivered as packages. (See [“Packages” on page 951](#).) System content packages are automatically installed as a part of ArcSight to provide out-of-box resource suites that you can start using immediately to monitor and protect your network. (See also [“Resources” on page 967](#).)

The content packages provided with a standard installation are:

- ArcSight Administration
- Configuration Monitoring
- Intrusion Monitoring
- Network Monitoring
- Workflow

Custom Content

The term "custom content" refers to resources and solutions created by customers using ArcSight software. Examples of custom content are user-configured [Rules](#), [Filters](#), [Active Channels](#), [Queries](#), [Trends](#), and [Reports](#) designed to address customer-specific scenarios.

SmartConnector Content

ArcSight continuously develops new SmartConnector event categorization mappings, which are often called "content." All existing content is included with major product releases, but it is also possible to get regular content updates to stay completely current.

ArcSight makes available to subscribing customers downloadable packages of new SmartConnector content. These releases occur frequently, generally on a bi-weekly basis. The download files are offered through a special subdirectory on the ArcSight software server. This directory is visible only to subscribers, who receive a notification e-mail from ArcSight Customer Support when the files are posted.

The content is packaged in [.aup](#) (update) files which may be wrapped in [.ZIP](#) files for transmission convenience. You place these [.aup](#) files in the Manager's [/updates](#) directory, where the Manager automatically finds the content and pushes it to the SmartConnectors. The affected SmartConnectors each register an internal event when the update occurs and can notify you by e-mail through the Manager.

You arrange for a content subscription through ArcSight Customer Support. Subscribers also have access to related articles in the ArcSight Customer Support Center's Knowledge Base.

Correlation

Logically linking events based on multiple conditions.

See [Chapter 20, Identity Correlation, on page 543](#) for more information on using session correlation, and see [Chapter 16, Rules Authoring, on page 439](#).

Correlation Rule

A programmed procedure that expresses conditions and actions, and evaluates normal or correlation events. A rule has two parts: a condition and an action.

A condition determines whether a state exists and satisfies related expressions. If so, an action expression defines the response to the condition.

A rule can have one or more conditions. If there is one condition, the rule acts as a filtering tool. If there is more than one condition, the rule acts as a correlation tool. A rule can be created for any incoming event from one or more event generators, with various conditions, logic statements, and thresholds.

See [Chapter 20, Identity Correlation, on page 543](#) for details on using session correlation.

Customers

To support managed security service providers (MSSPs), and larger enterprises that need to track activity related to cost centers or divisions, ArcSight can identify particular customers as the source of specific events.

"Customers" can be any client, tenant, or internal identity scheme you designate.

To use the Customers resource, you first model your existing customer or client base into the Customers resource tree in the Navigator panel, as described in ["Managing Customers" on page 766](#). Then, using the Customer URI values established in the resource tree, you configure the appropriate SmartConnectors to report these values through their Customer URI attributes.

Once you have implemented your Customer resource tree in the ESM Console, and configured the relevant SmartConnectors to report these Customer URIs, you can apply the Customer resources as filter condition arguments.

For example, your Customers resource tree might include a branch that translates into a Customer URI of: `/All Customers/Brokerages/Central States/Kansas City/Jones&Co.`

In the SmartConnectors resource tree, for those connectors that apply to this customer, you would apply this same string as the value for those connectors' Customer URI attribute, found under the Network section of the **Connector: Default: Content** tab. Thereafter, events reported by those connectors can be filtered in or out by referencing that branch of the Customers resource tree.

Dashboards

Dashboards are a graphical display of data gathered from one or more [Data Monitors](#). Dashboards can display data in a number of graphical formats, including pie and bar charts, tables, and custom layouts.

Data monitors are views within the dashboard that can be configured to report on events, filters, rules, and other data or information that is of particular interest to you. Data monitors can be arranged within dashboards in numerous viewing layouts.

When you right-click in a dashboard, you can choose from these options.

Dashboard Context Menu Commands

Table 32-1 Dashboard Context Menu Commands

Option	Description
Save Dashboard	Save any changes you have made to the dashboard and its data monitors.
Save As	Save the configured data monitors and dashboard under a different name.
Close Dashboard	Close the dashboard and remove it from the Viewer panel.
Dashboard>Zoom In / Zoom Out / Fit in	Visually enlarge or reduce the data monitors presented in the Viewer panel. Size the data monitors to allow them to all appear simultaneously in the current Viewer panel.

Table 32-1 Dashboard Context Menu Commands (Continued)

Option	Description
Data Monitor>Edit	Edit the current data monitor in the Inspect/Edit panel.
Data Monitor>Disable	Turn off the current data monitor.
Data Monitor>Float / Minimize / Close	Float, minimize, or close the current data monitor.
Show>DataMonitorName	Restore minimized data monitors.
Show Details / Show Detailed Channels	Show the event details for the currently selected element in a data monitor graphic, such as a pie chart, or display each of the monitor's elements in detail in separate active channel grids. This is also called "drilling down."
Investigate	Create an active channel or filter condition based on the highlighted event. The Investigate command uses the event's attribute type (its column heading), and the particular event's field value (for example, an exact IP address), to formulate filtered channels based on these two factors. The operators can include Create Channel [X = Y] and Add Condition [X = Y] to Editor .
Tools	Choose one of the network tools to explore the origin of the selected event item.
Show Scroll Bar	Toggles a scroll bar on and off in the selected data monitor. Use the scroll bar to show additional rows of tabular data if present.
Export > Data Monitor/Dashboard as ...	Save the selected data monitor or the dashboard in the JPEG (graphic), CSV (comma-separated value or text-based), or HTML file format.

Database

The ArcSight Database is a central repository for all events. Once an event occurs, its [Data Fields](#) such as severity, create time, rules triggered, and so forth are stored in the ArcSight Database. The ArcSight Database stores all enterprise events in a normalized schema. You can then investigate and analyze the event information. The Manager is the only component that communicates with the database.

Schema Design

The ArcSight Database is optimized to normalize data and support resources in terms of schema, event field usage, and event categorization.

Event Fields

- Most information reported by sensor devices are in the main event fields.
The information is accessible from Rules, Filters, and Reports. The events from a supported sensor might include three different fields - encryption failure, encryption success, and error - that all contain messages. These three are all mapped to the 'message' field.
- Usage clarification for many fields.
As an example, the 'protocol' field in v2.5 was split into 'transport protocol' and 'application protocol'. And the field 'domain' was split into 'NT domain', 'DNS domain',

and 'Device domain'. Because the previous fields could contain many different types of information, it could be difficult to write rules or data monitors that used the variety of possible values. The new fields, with their stricter definitions, are much more useful.

More Efficient Field Usage

Ordinarily, using more fields would cause ESM to occupy more disk space even more rapidly. However, a number of other changes mitigated this issue. The result is that ArcSight ESM events now consume significantly less disk space than events in pre-v.3.0 versions of ArcSight ESM, and provide much faster event storage and retrieval. The design changes that made this possible are:

- The database schema has been normalized so that highly repetitive sets of values are now stored in side tables.

Examples include the Connector and Device description fields. Normally, the values on these fields remain constant for days or weeks at a time. ArcSight ESM v3.x stores the set of values once and then includes a reference to the correct value set in the main event table.

- No single event uses all of the new fields.

Essentially, the v3.x schema defines a super-set of the most commonly used and useful fields presented by sensor events. It requires minimal space to store the empty fields.

- The original (or raw) log entry can also be preserved for each event.

This is controlled on a per-connector basis. This can be particularly useful in conjunction with Turbo Level 1 since a minimal event is generated but the details can still be inspected in the raw event, and with Turbo Level 2 where the data that would have appeared in the additional data table can now be found in the raw event.

- As a result of these changes, event storage and retrieval speeds have increased significantly.

These changes manifest in increased throughput capacity (a higher events-per-second ceiling), enhanced grid performance, and faster report runs.

Precise Event Categorization

Events are categorized more precisely in newer versions of ESM (see [“Categories” on page 836](#)). Before to ArcSight ESM v3.0, an event category was a single URI (such as [/Attack/BruteForce/Success](#)). On this basis it was difficult to include sufficient information to allow proper event correlation.

ESM now categorizes events across six dimensions: the object acted on by the event, the action represented by the event, the technique used to achieve the action, whether or not the action succeeded, the security significance of the event, and the class of device that reported the event. This scheme is designed to support focused rule authoring and data monitor construction.

For example, a Snort SID 103 ([BACKDOOR subseven 22](#)) event in the old model would have been categorized as [/Compromise/Backdoor](#). Such a categorization lacks detail. Was this an attempt to install a back door? Or does it indicate communication between a back door and an external connector? Or is an external connector scanning for pre-installed back doors?

The newer categorization model brings clarity to such a situation. Events describe either an action or a state. Actions are attempted against a particular object and may succeed or fail. There may be many ways to attempt a particular action against an object (such as different ways to exploit an exposed vulnerability). States describe the status of a particular object,

and these states may be known to be true -- or they may be hearsay. Events all have some significance to the security profile of the protected network. Finally, it is interesting to know what sort of device is reporting the event.

If we look at Snort SID 103, we discover that it is a report of a scan searching for pre-installed subseven 22 back doors. Now, we would categorize these events

Security Significance	/Recon
Behavior	/Communicate/Query
Technique	/Scan/Service
Device Type	/IDS/Network
Outcome	/Attempt
Object	/Host/Application/Backdoor

In this case, a network intrusion detection system (IDS) would observe an attempt to communicate with a backdoor and infer that this was part of a service scan attempting to discover pre-installed instances of that backdoor. Naturally, this implies an external connector is performing reconnaissance on the protected network.

Data Fields

Processed events are composed of several attributes, each of which is a data field with its own characteristics. These event schema data fields fall into the groups shown in the following sections.

Each attribute has both a **Label** that you see in the ESM Console and a unique **Script Alias** you use to refer to the attribute in filters, rules, or Velocity templates. The **Data Type** lets you know how to handle the attribute, and the **Default Turbo Level** indicates whether an attribute is, by default, classified as **1** (essential, or "fastest") or **2** (optional, or "faster"). Turbo Level 3 ("complete") isn't designated because it applies to additional data not represented here.

The easiest way to view all event fields is on the Event Inspector (Event tab) or [Common Conditions Editor \(CCE\)](#) on the ESM Console. (To bring up the Event Inspector select an event in a grid view like an active channel. Right-click and choose **Show event details**. The event's details appear in the Event Inspector.) To view *all* event fields, make sure that no field set is selected to limit the set of fields shown. (Select **Clear** from the drop-down menu above the list of event fields. With no field set selected, the drop-down shows "Select a Field Set".)



For a list of ArcSight's Common Event Format (CEF) abbreviations, ask your ArcSight Support representative for the tech note entitled *Implementing ArcSight CEF*.

Connector Group

This group category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting Final Device before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy, the chain

includes handling by **Connector** stages that are the ArcSight Forwarding Connectors that facilitate Manager-to-Manager connections.

Table 32-2 Connector Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Connector Group Field Description
Address	connectorAddress	IP address	1	The IP address of the device hosting the SmartConnector.
Asset ID	connectorAssetId	Resource	1	The asset that represents the device hosting the SmartConnector.
Asset Name	connectorAssetName	String	1	The connector's asset name.
Asset Resource	connectorAssetResource	Resource	1	The connector resource.
Descriptor ID	connectorDescriptorId	ID	1	The connector descriptor.
DNS Domain	connectorDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the SmartConnector.
Host Name	connectorHostName	String	1	The name of the device hosting the SmartConnector.
ID	connectorId	String	1	The identifier associated with the SmartConnector configuration resource. The format is connectorID(1) connectorID(2) ...
MAC Address	connectorMacAddress	MacAddress	1	The MAC address associated with the SmartConnector (which may or may not be the MAC address of the host device.)
Name	connectorName	String	1	The user-supplied name of the associated SmartConnector configuration resource.
NT Domain	connectorNtDomain	String	1	The Windows NT domain associated with the device hosting the SmartConnector.
Receipt Time	connectorReceiptTime	DateTime	2	The time the event arrived at the SmartConnector.
Severity	connectorSeverity	Connector Severity Enumeration	1	The normalized ArcSight form of the event severity value provided by the SmartConnector.
Time Zone	connectorTimeZone	String	1	The time zone reported by the device hosting the SmartConnector (as TLA).

Table 32-2 Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Connector Group Field Description
Time Zone Offset	connectorTimeZoneOffset	Integer	1	The time zone reported by the device hosting the SmartConnector (shown as a UTC offset). Note that device times may be less accurate than other sources.
Translated Address	connectorTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the SmartConnector.
Translated Zone	connectorTranslatedZone	Zone	1	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the SmartConnector.
Translated Zone External ID	connectorTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Translated Zone ID	connectorTranslatedZoneID	String	1	See the common set of resource attributes.
Translated Zone Name	connectorTranslatedZoneName	String	1	See the common set of resource attributes. Returns the name from the URI. It assumes that the name is always the last field of the URI.
Translated Zone Reference ID	connectorTranslatedZoneReferenceID	ID	1	See the common set of resource attributes. Returns the unique descriptor ID for this reference.
			This is populated only if this reference is stored and uniquely identified in the database.	
Translated Zone Resource	connectorTranslatedZoneResource	Resource	1	See the common set of resource attributes. Locates the resource described by this reference.
Translated Zone URI	connectorTranslatedZoneURI	String	1	See the common set of resource attributes.

Table 32-2 Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Connector Group Field Description
Type	connectorType	String	1	A description of the type of SmartConnector that reported the event.
Version	connectorVersion	String	1	The software revision number of the SmartConnector that reported the event
Zone	connectorZone	Zone	1	The network zone in which the device hosting this SmartConnector resides.
Zone External ID	connectorZoneExternalID	String	1	See the common set of resource attributes.
Zone ID	connectorZoneID	String	1	See the common set of resource attributes.
Zone Name	connectorZoneName	String	1	See the common set of resource attributes.
Zone Reference ID	connectorZoneReferenceID	ID	1	See the common set of resource attributes.
Zone Resource	connectorZoneResource	Resource	1	See the common set of resource attributes.
Zone URI	connectorZoneURI	String	1	Returns the URI for this reference.

Attacker Group

Table 32-3 Attacker Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
Address	attackerAddress	IP address	1	The IP address of the device hosting the attacker.
Asset ID	attackerAssetId	Resource	2	The asset that represents the device hosting the attacker.
Asset Name	attackerAssetName	String	2	The name of the asset that represents the device hosting the attacker.
Asset Resource	attackerAssetResource	Resource	2	See the common set of resource attributes
DNS Domain	attackerDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the attacker.

Table 32-3 Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
FQDN	attackerFqdn	String	2	The fully qualified domain name associated with the device hosting the attacker.
Geo	attackerGeo	GeoDescriptor	1	See the common set of geographical attributes.
Geo Country Code	attackerGeoCountryCode	String	1	See the common set of geographical attributes.
Geo Country Flag URL	attackerGeoCountryFlagUrl	String	1	See the common set of geographical attributes.
Geo Country Name	attackerGeoCountryName	String	1	See the common set of geographical attributes.
Geo Descriptor ID	attackerGeoDescriptorId	ID	1	See the common set of geographical attributes.
Geo Latitude	attackerGeoLatitude	Double	1	See the common set of geographical attributes.
Geo Location Info	attackerGeoLocationInfo	String	Location	See the common set of geographical attributes.
Geo Longitude	attackerGeoLongitude	Double	1	See the common set of geographical attributes.
Geo Postal Code	attackerGeoPostalCode	String	1	See the common set of geographical attributes.
Geo Region Code	attackerGeoRegionCode	String	1	See the common set of geographical attributes.
Host Name	attackerHostName	String	2	The name of the device hosting the attacker.
MAC Address	attackerMacAddress	MAC address	2	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).
NT Domain	attackerNtDomain	String	2	The Windows NT domain associated with the device hosting the attacker.
Port	attackerPort	Integer	1	The network port associated with the source of the attack.
Process ID	attackerProcessId	Integer		The ID of the process associated with the source of the attack.

Table 32-3 Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
Process Name	attackerProcessName	String	2	The name of process associated with the source of the attack.
Service Name	attackerServiceName	String	2	The name of service associated with the source of the attack.
Translated Address	attackerTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the attacker.
Translated Port	attackerTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack. This can happen in a NAT environment.
Translated Zone	attackerTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the attacker.
Translated Zone External ID	attackerTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Translated Zone ID	attackerTranslatedZoneID	String	1	See the common set of resource attributes.
Translated Zone Name	attackerTranslatedZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Translated Zone Reference ID	attackerTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Translated Zone Resource	attackerTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Translated Zone URI	attackerTranslatedZoneURI	String	1	See the common set of resource attributes.
User ID	attackerUserId	String	2	The identifier associated with the OS or application of the attacker, at the source of the attack.

Table 32-3 Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
User Name	attackerUserName	String	2	The name associated with the attacker, at the source of the attack.
User Privileges	attackerUserPrivileges	String	2	The user-privilege associated with the attacker, at the source of the attack.
Zone	attackerZone	Zone	1	The network zone in which the attacker's device resides.
Zone External ID	attackerZoneExternalID	String	1	See the common set of resource attributes.
Zone ID	attackerZoneID	String	1	See the common set of resource attributes.
Zone Name	attackerZoneName	String	1	See the common set of resource attributes. It is assumed that the name is always the last field of the URI.
Zone Reference ID	attackerZoneReferenceID	ID	1	See the common set of resource attributes.
Zone Resource	attackerZoneResource	Resource	1	See the common set of resource attributes.
Zone URI	attackerZoneURI	String	1	See the common set of resource attributes.

Category Group

Table 32-4 Category Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Category Group Field Description
Behavior	categoryBehavior	String	1	Describes the action taken with or by the object.
Custom Format Field	categoryCustomFormatField	String	1	Describes the content of a custom formatted field, if present.
Descriptor ID	categoryDescriptorId	ID	1	The unique ID for the sensor that reported the event
Device Group	categoryDeviceGroup	String	1	Describes the type of event this event represents.
Device Type	categoryDeviceType	String		New for v5.0

Table 32-4 Category Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Category Group Field Description
Object	categoryObject	String	1	Describes the physical or virtual object that was the focus of the event
Outcome	categoryOutcome	String	1	Indicates whether the action was successfully applied to the object.
Significance	categorySignificance	String	1	Characterizes the event from a network-intrusion-detection perspective.
Technique	categoryTechnique	String	1	Describes the method used to apply the action to the object.
Tuple Description	categoryTupleDescription	String	1	The prose description of the event category, assembled from the category components.

Destination Group

Table 32-5 Destination Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Address	destinationAddress	IP address	1	The IP address of the destination device.
Asset ID	destinationAssetId	Resource	2	The asset that represents the device that was the network traffic's destination.
Asset Name	destinationAssetName	String	2	See the common set of resource attributes.
Asset Resource	destinationAssetResource	Resource	2	See the common set of resource attributes.
DNS Domain	destinationDnsDomain	String	2	The Domain Name Service domain name associated with the user at the destination device.
FQDN	destinationFqdn	String	2	The fully qualified domain name associated with the destination device.
Geo	destinationGeo	GeoDescriptor	GeoDescriptor	See the common set of geographical attributes.
Geo Country Code	destinationGeoCountryCode	String	1	The country code.

Table 32-5 Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Geo Country Flag URL	destinationGeoCountryFlagUrl	String	1	The country flag.
Geo Country Name	destinationGeoCountryName	String	1	The country name.
Geo Descriptor ID	destinationGeoDescriptorId	ID	1	See the common set of geographical attributes.
Geo Latitude	destinationGeoLatitude	Double	1	The destination latitude.
Geo Location Info	destinationGeoLocationInfo	String	1	The destination location.
Geo Longitude	destinationGeoLongitude	Double	1	The destination longitude.
Geo Postal Code	destinationGeoPostalCode	String	1	The destination postal code.
Geo Region Code	destinationGeoRegionCode	String	1	See the common set of geographical attributes.
Host Name	destinationHostName	String	2	The name of the destination device.
MAC Address	destinationMacAddress	MAC address	2	The MAC address associated with the network traffic's destination (which may or may not be the MAC address of the host device).
NT Domain	destinationNtDomain	String	2	The Windows NT domain associated with the destination device.
Port	destinationPort	Integer	1	The network port associated with the network traffic's destination.
Process ID	destinationProcessId	Integer		The ID of the process associated with the network traffic's destination.
Process Name	destinationProcessName	String	2	The name of the process associated with the network traffic's destination.
Service Name	destinationServiceName	String	2	The name of service associated with the network traffic's destination.

Table 32-5 Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Translated Address	destinationTranslatedAddresses	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's destination.
Translated Port	destinationTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.
Translated Zone	destinationTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device at the network's traffic's destination.
Translated Zone External ID	destinationTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Translated Zone ID	destinationTranslatedZoneID	String	1	See the common set of resource attributes.
Translated Zone Name	destinationTranslatedZoneName	String	1	See the common set of resource attributes.
Translated Zone Reference	destinationTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Translated Zone Resource	destinationTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Translated Zone URI	destinationTranslatedZoneURI	String	1	See the common set of resource attributes.
User ID	destinationUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's destination.
User Name	destinationUserName	String	2	The name associated with the user at the network traffic's destination.
User Privileges	destinationUserPrivileges	String	2	The privileges accorded the user at the network traffic destination.
Zone	destinationZone	Zone	1	The network zone in which the destination device resides.

Table 32-5 Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Zone External ID	destinationZoneExternalID	String	1	See the common set of resource attributes.
Zone ID	destinationZoneID	String	1	See the common set of resource attributes.
Zone Name	destinationZoneName	String	1	See the common set of resource attributes.
Zone Reference ID	destinationZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Zone Resource	destinationZoneResource	Resource	1	See the common set of resource attributes.
Zone URI	destinationZoneURI	String	1	See the common set of resource attributes.

Device Group

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain includes handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Table 32-6 Device Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
Action	deviceAction	String	2	The device-specific description of some activity associated with the event
Address	deviceAddress	IP address	1	The IP address of the device hosting the sensor.
Asset ID	deviceAssetId	Resource	1	The asset that represents the device hosting the sensor.
Asset Name	deviceAssetName	String	1	The name of the device.
Asset Resource	deviceAssetResource	Resource	1	The resource the asset represents.
Descriptor ID	deviceDescriptorId	ID	1	The asset's descriptor ID.

Table 32-6 Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
Direction	deviceDirection	Device Direction Enumeration	2	Whether the traffic was inbound or outbound.
DNS Domain	deviceDnsDomain	String	1	The Domain Name Service domain name associated with the device hosting the sensor.
Domain	deviceDomain	String	2	The specific domain containing the sensor device associated with the event
Event Category	deviceEventCategory	String	2	The category description included with the event as reported by the device.
Event Class ID	deviceEventClassId	String	2	The device-specific identifier associated with this type of event
External ID	deviceExternalId	String	1	The external identifier associated with this sensor device, if provided by the vendor.
Facility	deviceFacility	String	1	The sensor submodule that reported the event
Host Name	deviceHostName	String	1	The name of the device hosting the sensor.
Inbound Interface	deviceInboundInterface	String	1	The NIC card on the sensor device that received the network traffic associated with the event.
MAC Address	deviceMacAddress	MAC address	1	The MAC address associated with the source of the attack (which may or may not be the MAC address of the host device).
NT Domain	deviceNtDomain	String	1	The Windows NT domain associated with the device hosting the sensor.
Outbound Interface	deviceOutboundInterface	String	1	The NIC card on the sensor device that transmitted the network traffic associated with the event.
Payload ID	devicePayloadId	String	2	The internal identifier associated with a payload object associated with this event.
Process ID	deviceProcessId	Integer		The ID of the sensor device process that reported the event.

Table 32-6 Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
Process Name	deviceProcessName	String	1	The name of the sensor device process that reported the event.
Product	deviceProduct	String	1	The product name of the sensor device.
Receipt Time	deviceReceiptTime	DateTime	2	The time when the sensor device observed the event.
Severity	deviceSeverity	String	2	The device-specific assessment of event severity. This assessment varies with the device involved.
Time Zone	deviceTimeZone	String	1	The time zone reported by the device hosting the sensor device (shown as TLA).
Time Zone Offset	deviceTimeZoneOffset	Integer	1	The time zone reported by the device hosting this sensor device (shown as an offset from UTC).
Translated Address	deviceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device hosting the sensor.
Translated Zone	deviceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device hosting the sensor.
Translated Zone External ID	deviceTranslatedZoneExternalID	String	1	See the common set of resource attributes.
Translated Zone ID	deviceTranslatedZoneID	String	1	See the common set of resource attributes.
Translated Zone Name	deviceTranslatedZoneName	String	1	See the common set of resource attributes.
Translated Zone Resource	deviceTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.

Table 32-6 Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
Translated Zone Resource	deviceTranslatedZoneResource	Resource	1	See the common set of resource attributes.
Translated Zone URI	deviceTranslatedZoneURI	String	1	See the common set of resource attributes.
Vendor	deviceVendor	String	1	The vendor who manufactured or sold the sensor device.
Version	deviceVersion	String	1	The software revision number of the sensor device.
Zone	deviceZone	Zone	1	The network zone in which the sensor's device resides.
Zone External ID	deviceZoneExternalID	String	1	See the common set of resource attributes.
Zone ID	deviceZoneID	String	1	See the common set of resource attributes.
Zone Name	deviceZoneName	String	1	See the common set of resource attributes.
Zone Reference ID	deviceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been persisted and given a unique database identifier.
Zone Resource	deviceZoneResource	Resource	1	See the common set of resource attributes.
Zone URI	deviceZoneURI	String	1	See the common set of resource attributes.

Device Custom Group

Table 32-7 Device Custom Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Device Custom Group Field Description
Date1	deviceCustomDate1	DateTime	2	First customDate
Date1 Label	deviceCustomDate1Label	String	2	First customDate label
Date2	deviceCustomDate2	DateTime	2	Second customDate
Date2 Label	deviceCustomDate2Label	String	2	Second customDate label

Table 32-7 Device Custom Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Custom Group Field Description
Number1	deviceCustomNumber1	Long	2	First customNumber
Number1 Label	deviceCustomNumber1Label	String	2	First customNumber label
Number2	deviceCustomNumber2	Long	2	Second customNumber
Number2 Label	deviceCustomNumber2Label	String	2	Second customNumber label
Number3	deviceCustomNumber3	Long	2	Third customNumber
Number3 Label	deviceCustomNumber3Label	String	2	Third customNumber label
String1	deviceCustomString1	String	2	First customString
String1 Label	deviceCustomString1Label	String	2	First customString label
String2	deviceCustomString2	String	2	Second customString
String2 Label	deviceCustomString2Label	String	2	Second customString label
String3	deviceCustomString3	String	2	Third customString
String3 Label	deviceCustomString3Label	String	2	Third customString label
String4	deviceCustomString4	String	2	Fourth customString
String4 Label	deviceCustomString4Label	String	2	Fourth customString label
String5	deviceCustomString5	String	2	Fifth customString
String5 Label	deviceCustomString5Label	String	2	Fifth customString label
String6	deviceCustomString6	String	2	Sixth customString
String6 Label	deviceCustomString6Label	String	2	Sixth customString label
Floating Point1 Label	deviceCustomFloatingPoint1	String		First custom floating point
Floating Point1	deviceCustomFloatingPoint1Label	Double		First custom floating point label
Floating Point2 Label	deviceCustomFloatingPoint2	String		Second custom floating point
Floating Point2	deviceCustomFloatingPoint2Label	Double		Second custom floating point label
Floating Point3 Label	deviceCustomFloatingPoint3	String		Third custom floating point

Table 32-7 Device Custom Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Custom Group Field Description
Floating Point3	deviceCustomFloatingPoint3Label	Double		Third custom floating point label
Floating Point4 Label	deviceCustomFloatingPoint4	String		Fourth custom floating point
Floating Point4	deviceCustomFloatingPoint4Label	Double		Fourth custom floating point label
IPv6 Address1 Label	deviceCustomIPv6Address1	String		First custom IPV6 address
IPv6 Address1	deviceCustomIPv6Address1Label	IPv6 address		First custom IPV6 address label
IPv6 Address2 Label	deviceCustomIPv6Address2	String		Second custom IPV6 address
IPv6 Address2	deviceCustomIPv6Address2Label	IPv6 address		Second custom IPV6 address label
IPv6 Address3 Label	deviceCustomIPv6Address3	String		Third custom IPV6 address
IPv6 Address3	deviceCustomIPv6Address3Label	IPv6 address		Third custom IPV6 address label
IPv6 Address4 Label	deviceCustomIPv6Address4	String		Fourth custom IPV6 address
IPv6 Address4	deviceCustomIPv6Address4Label	IPv6 address		Fourth custom IPV6 address label

Event Group

Table 32-8 Event Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Additional Data	additionalData	AdditionalData	3	Reference to additional data.
Aggregated Event Count	(not applicable)	(not applicable)	N/A	A derived field that reports the number of actual events collectively represented by the event in question. (See “Aggregation” on page 798.)
Application Protocol	applicationProtocol	String	2	A description of the application layer protocol. May be set, but defaults to Target Port lookup (FTP).

Table 32-8 Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Base Event IDs	baseEventIds	ID	2	The array of event IDs that contributed to generating this correlation event. This is populated only in correlated events.
Bytes In	bytesIn	Integer	2	Number of bytes transferred into the device during this transaction (this would typically be associated with entries in HTTP logs).
Bytes Out	bytesOut	Integer	2	Number of bytes transferred out of the device during this transaction (this would typically be associated with entries in HTTP logs).
Concentrator Connectors	concentratorConnectors	ConnectorDescriptor	2	The chain of concentrators that forwarded the event. This is not yet exposed in the user interface.
Concentrator Devices	concentratorDevices	DeviceDescriptor	2	The list of devices that concentrate events, if applicable. This is not exposed in the user interface.
Correlated Event Count	(not applicable)	(not applicable)	N/A	A derived field that reports the number of actual events that had to occur to cause a correlation event to occur.
Crypto Signature	cryptoSignature	String	2	The signature of the event object (meaning in this alert, as opposed to the occurrence represented by the event). Not yet supported.
Customer	customer	Customer	1	The "customer" resource reference. This is used in MSSP environments to describe the client or divisional entity to whom the event applies.
Customer External ID	customerExternalID	String	1	Returns the external ID for this reference.
Customer ID	customerID	String	1	Returns the ID for the resource in this resource reference.
Customer Name	customerName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.

Table 32-8 Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Customer Reference ID	customerReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Customer Resource	customerResource	Resource	1	Locates the resource described by this reference.
Customer URI	customerURI	String	1	Returns the URI for this reference.
Domain	domain	Resource		New for v5.0
End Time	endTime	DateTime	1	Event ends (defaults to deviceReceiptTime).
Event ID	eventId	ID	1	Long value identifying an event.
Event Outcome	eventOutcome	String		New for v5.0
External ID	externalId	String	2	A reference to the ID used by an external device. This is useful for tracking devices that create events that contain references to these IDs (for example, ManHunt).
Generator	generator	null	1	The "generator" resource reference (the resource that generated the event. This is the subcomponent in the connector that generates the event.
Generator External ID	generatorExternalID	String	1	Returns the external ID for this reference.
Generator ID	generatorID	String	1	Returns the ID for the resource in this resource reference.
Generator Name	generatorName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Generator Reference ID	generatorReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Generator Resource	generatorResource	Resource	1	Locates the resource described by this reference.

Table 32-8 Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Generator URI	generatorURI	String	1	Returns the URI for this reference.
Locality	locality	LocalityEnumeration	2	The locality associated with the event.
Message	message	String	2	A brief comment associated with this event.
Name	name	String	1	An arbitrary string that describes this type of event. Event details included in other parts of an event shouldn't be used in the event name.
Originator	originator	OriginatorEnumeration	1	Holds the value of Source Destination. This determines whether source and destination should be translated to attacker and target or they should be reversed.
Persistence	persistence	PersistenceEnumeration	2	There are two states: Persisted or Transient. Events default to being Transient and are marked as Persisted as soon as they reach the Batch Alert Persister or when they are loaded by the Alert Broker.
Raw Event	rawEvent	String	1	The original log entry reported by the sensor (synthesized when the sensor does not log to a file or text stream).
Reason	reason	String		New for v5.0.
Rule Thread ID	ruleThreadId	String	2	A single rule can issue many events, based on several triggers, starting with On First Event and ending with On Threshold Timeout. All such events for a single Rule and a single Group By tuple is marked with the same identifier using this attribute.
Session ID	sessionId	Long	2	Tags for events created by a correlation simulation, as part of a particular simulation.
Start Time	startTime	DateTime	1	Event begins (defaults to deviceReceiptTime).

Table 32-8 Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Transport Protocol	transportProtocol	String	1	The format of the transmitted data associated with the event from a network transport perspective (for example, TCP, UDP).
Type	type	TypeEnumeration	1	One of the event types: Base, Correlation, Aggregation, or Action.
Vulnerability	vulnerability	Vulnerability	2	The vulnerability resource that represents the vulnerability or exposure that may be exploited by this event and is present on the targeted device according to our network model.
Vulnerability External ID	vulnerabilityExternalID	String	2	Returns the external ID for this reference.
Vulnerability ID	vulnerabilityID	String	2	Returns the ID for the resource in this resource reference.
Vulnerability Name	vulnerabilityName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Vulnerability Reference ID	vulnerabilityReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Vulnerability Resource	vulnerabilityResource	Resource	2	Locates the resource described by this reference.
Vulnerability URI	vulnerabilityURI	String	2	Returns the URI for this reference.

Event Annotation Group

Table 32-9 Event Annotation Group

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
Audit Trail	eventAnnotationAuditTrail	String	2	The text log of annotation changes. Changes are recorded as sets of comma-separated-value entries.

Table 32-9 Event Annotation Group (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
Comment	eventAnnotationComment	String	2	A text description of the event or associated information.
End Time	eventAnnotationEndTime	DateTime	2	The timestamp for an event annotation.
Event ID	eventAnnotationEventId	ID	2	The event ID for the annotation event.
Flags	eventAnnotationFlags	FlagsValueSet	2	The state of the collaboration flags.
Manager Receipt Time	eventAnnotationManagerReceiptTime	DateTime	2	The time the Manager received the event annotation.
Modification Time	eventAnnotationModificationTime	DateTime	2	The time the annotation was modified.
Modified By	eventAnnotationModifiedBy	User	2	The user ID of the person who last edited this annotation.
Modified By External ID	eventAnnotationModifiedByExternalID	String	2	Returns the external ID for this reference.
Modified By ID	eventAnnotationModifiedById	String	2	Returns the ID for the resource in this resource reference.
Modified By Name	eventAnnotationModifiedByName	String	2	Returns the name from the URI (the last field of the URI).
Modified By Reference ID	eventAnnotationModifiedByReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Modified By Resource	eventAnnotationModifiedByResource	Resource	2	Locates the resource described by this reference.
Modified By URI	eventAnnotationModifiedByURI	String	2	Returns the URI for this reference.
Stage	eventAnnotationStage	Stage	2	The current disposition of the event. This enables annotation workflow.
Stage Event ID	eventAnnotationStageEventId	ID	2	The reference to an internal identifier for another event. It is used by 'Mark Similar'.

Table 32-9 Event Annotation Group (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
Stage External ID	eventAnnotationStageExternalID	String	2	Returns the external ID for this reference.
Stage ID	eventAnnotationStageID	String	2	Returns the ID for the resource in this resource reference.
Stage Name	eventAnnotationStageName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Stage Reference ID	eventAnnotationStageReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.
Stage Resource	eventAnnotationStageResource	Resource	2	Locates the resource described by this reference.
Stage Update Time	eventAnnotationStageUpdateTime	ID	2	The time of the last stage change (in UTC).
Stage URI	eventAnnotationStageURI	String	2	Returns the URI for this reference.
Stage User	eventAnnotationStageUser	User	2	The user associated with the current stage. This implements assignment within workflow.
Stage User External ID	eventAnnotationStageUserExternalID	String	2	Returns the external ID for this reference.
Stage User ID	eventAnnotationStageUserID	String	2	Returns the ID for the resource in this resource reference.
Stage User Name	eventAnnotationStageUserName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Stage User Reference ID	eventAnnotationStageUserReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference is stored and uniquely identified in the database.
Stage User Resource	eventAnnotationStageUserResource	Resource	2	Locates the resource described by this reference.

Table 32-9 Event Annotation Group (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
Stage User URI	eventAnnotationStageUserURI	String	2	Returns the URI for this reference.
Version	eventAnnotationVersion	Integer	2	The editing version number which increments with each change. This enables optimistic locking.

File Group

Table 32-10 File Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	File Group Field Description
Create Time	fileCreateTime	DateTime	2	The time the file was created (in UTC).
Hash	fileHash	String	2	The hash code associated with the file's contents (for example, MD5).
ID	fileId	String	2	The external identifier associated with the file.
Modification Time	fileModificationTime	DateTime	2	The time the file was last changed (in UTC).
Name	fileName	String	2	The name of the file.
Path	filePath	String	2	The directory path to the file in the file system.
Permission	filePermission	String	2	The user permissions associated with the file (sensor specific).
Size	fileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
Type	fileType	String	2	The type of file contents (sensor specific).

Final Device Group

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. In cases where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy the chain includes handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Table 32-11 Final Device Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
Address	finalDeviceAddress	IP address	2	The IP address of the trusted reporting device.
Asset ID	finalDeviceAssetId	Resource	2	The asset that represents the trusted reporting device.
Asset Name	finalDeviceAssetName	String	2	The name of the trusted reporting device.
Asset Resource	finalDeviceAssetResource	Resource	2	The resource represented by the trusted reporting device.
Descriptor ID	finalDeviceDescriptorId	ID	2	The descriptor ID of the trusted reporting device.
DNS Domain	finalDeviceDnsDomain	String	2	The Domain Name Service domain name associated with the trusted reporting device.
External ID	finalDeviceExternalId	String	2	The external ID for the trusted reporting device, if provided by the vendor.
Facility	finalDeviceFacility	String	2	A facility or capability of a device. This accommodates concentrators (for example, like syslog, which has a concept of device logging for "parts" of a device).
Host Name	finalDeviceHostName	String	2	The host name of the trusted reporting device.
Inbound Interface	finalDeviceInboundInterface	String	2	The NIC card on the sensor device that received the network traffic associated with the event.
MAC address	finalDeviceMacAddress	MAC address	2	The MAC address associated with the trusted reporting device.
NT Domain	finalDeviceNtDomain	String	2	The Windows NT domain associated with the trusted reporting device.

Table 32-11 Final Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
Outbound Interface	finalDeviceOutboundInterface	String	2	The NIC card on the trusted reporting device.
Process Name	finalDeviceProcessName	String	2	The process name of the trusted reporting device.
Product	finalDeviceProduct	String	2	The product name of the trusted reporting device.
Time Zone	finalDeviceTimeZone	String	2	The time zone reported by the trusted reporting device.
Time Zone Offset	finalDeviceTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the trusted reporting device. Note that connector and device times are not always reliably accurate.
Translated Address	finalDeviceTranslatedAddress	IP address	2	If network address translation is an issue, this is the translated IP address of the trusted reporting device.
Translated Zone	finalDeviceTranslatedZone	Zone	2	If network address translation is an issue, this is the network zone associated with the translated IP address of the trusted reporting device.
Translated Zone External ID	finalDeviceTranslatedZoneExternalID	String	2	Returns the external ID for this reference.
Translated Zone ID	finalDeviceTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Translated Zone Name	finalDeviceTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference ID	finalDeviceTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Translated Zone Resource	finalDeviceTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Translated Zone URI	finalDeviceTranslatedZoneURI	String	2	Returns the URI for this reference.

Table 32-11 Final Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
Vendor	finalDeviceVendor	String	2	Device vendor.
Version	finalDeviceVersion	String	2	The software revision number of the trusted reporting device.
Zone	finalDeviceZone	Zone	2	The network zone in which the trusted reporting device resides.
Zone External ID	finalDeviceZoneExternalID	String	2	Returns the external ID for this reference.
Zone ID	finalDeviceZoneID	String	2	Returns the ID for the resource in this resource reference.
Zone Name	finalDeviceZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Zone Reference ID	finalDeviceZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Zone Resource	finalDeviceZoneResource	Resource	2	Locates the resource described by this reference.
Zone URI	finalDeviceZoneURI	String	2	Returns the URI for this reference.

Flex Group

Table 32-12 Flex Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Flex Group Field Description
Date1	flexDate1	DateTime	2	First flex Date.
Date1 Label	flexDate1Label	String	2	Label of first flex Date.
Number1	flexNumber1	Long	2	First flex Number.
Number1 Label	flexNumber1Label	String	2	Label of the first Flex Number.
Number2	flexNumber2	Long	2	Second flex Number.
Number2 Label	flexNumber2Label	String	2	Label of the second Flex Number.

Table 32-12 Flex Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Flex Group Field Description
String1	flexString1	String	2	First flex String
String1 Label	flexString1Label	String	2	Label of the first Flex String.
String2	flexString2	String	2	Second flex String.
String2 Label	flexString2Label	String	2	Label of the second Flex String.

Manager Group

Table 32-13 Manager Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Manager Group Field Description
Receipt Time	managerReceiptTime	DateTime	1	The time at which the current Manager first received the event.

Old File Group

Table 32-14 Old File Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Old File Group Field Description
Create Time	oldFileCreateTime	DateTime	2	The time the file was created (in UTC).
Hash	oldFileHash	String	2	The hashcode associated with the file's contents (for example, MD5).
ID	oldFileId	String	2	The external identifier associated with the file.
Modification Time	oldFileModificationTime	DateTime	2	The time the file was last changed (in UTC).
Name	oldFileName	String	2	The file's name.
Path	oldFilePath	String	2	The directory path to the file in the file system.
Permission	oldFilePermission	String	2	The user permissions associated with the file (sensor specific).
Size	oldFileSize	Long	2	The size of the file's contents (typically in bytes; sensor specific).
Type	oldFileType	String	2	The type of the file's contents (sensor specific).

Original Connector Group

This category falls into the device-to-Manager information chain. The chain begins at **Device**, which is the actual network hardware that senses an event. Where data is concentrated or otherwise pre-processed, it may be passed to a trusted reporting **Final Device** before reaching an **Original Connector**. Although the **Original Connector** is usually the only connector, if the data passes up through a Manager hierarchy, the chain includes handling by **Connector** stages that are the Manager SmartConnectors that facilitate Manager-to-Manager connections.

Table 32-15 Original Connector Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Original Connector Group Field Description
Address	originalConnectorAddress	IP address	2	The IP address of the device hosting the first reporting SmartConnector.
Asset ID	originalConnectorAssetID	Resource	2	The asset that represents the device hosting the first reporting SmartConnector.
Asset Name	originalConnectorAsset Name	String	2	The first reporting connector's asset name.
Asset Resource	originalConnectorAsset Resource	Resource	2	The first reporting connector's resource.
Descriptor ID	originalConnectorDescriptor Id	ID	2	The first reporting connector's descriptor.
DNS Domain	originalConnectorDns Domain	String	2	The Domain Name Service domain name associated with the device hosting the first reporting SmartConnector.
Host Name	originalConnectorHostName	String	2	The name of the device hosting the first reporting SmartConnector.
ID	originalConnectorId	String	2	The ID of the connector. The format is connectorId(1) connectorId(2) ...
MAC address	originalconnectorMac Address	MAC address	2	The MAC address associated with the first reporting Smartconnector (which may or may not be the MAC address of the host device.)
Name	originalconnectorName	String	2	User-supplied name of the first reporting connector.
NT Domain	originalconnectorNtDomain	String	2	The Windows NT domain associated with the device hosting the first reporting Smartconnector.

Table 32-15 Original Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Original Connector Group Field Description
Time Zone	originalconnectorTimeZone	String	2	The time zone reported by the device hosting the first reporting Smartconnector.
Time Zone Offset	originalconnectorTimeZoneOffset	Integer	2	Returns the raw time-zone offset for the first reporting connector's time zone. Note that device and connector times may not be reliably accurate.
Translated Address	originalconnectorTranslatedAddress	IP address	2	If network address translation is an issue, this is the translated IP address of the device hosting the first reporting Smartconnector.
Translated Zone	originalconnectorTranslatedZone	Zone	2	If network address translation is an issue, this is the Network Zone associated with the translated IP address of the device hosting the first reporting Smartconnector.
Translated Zone External ID	originalconnectorTranslatedZoneExternalID	String	2	Returns the external ID for this reference.
Translated Zone ID	originalconnectorTranslatedZoneID	String	2	Returns the ID for the resource in this resource reference.
Translated Zone Name	originalconnectorTranslatedZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference ID	originalconnectorTranslatedZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Translated Zone Resource	originalconnectorTranslatedZoneResource	Resource	2	Locates the resource described by this reference.
Translated Zone URI	originalconnectorTranslatedZoneURI	String	2	Returns the URI for this reference.
Type	originalconnectorType	String	2	A string that describes the type of the first reporting connector. This is not the same as the device type.

Table 32-15 Original Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Original Connector Group Field Description
Version	originalconnectorVersion	String	2	The software revision number of the Smartconnector that first reported the event.
Zone	originalconnectorZone	Zone	2	The network zone in which the device hosting the first reporting Smartconnector resides.
Zone External ID	originalconnectorZoneExternalID	String	2	Returns the external ID for this reference.
Zone ID	originalconnectorZoneID	String	2	Returns the ID for the resource in this resource reference.
Zone Name	originalconnectorZoneName	String	2	Returns the name from the URI, which is always assumed to be the last field of the URI.
Zone Reference ID	originalconnectorZoneReferenceID	ID	2	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and is uniquely identified in the database.
Zone Resource	originalconnectorZoneResource	Resource	2	Locates the resource described by this reference.
Zone URI	originalconnectorZoneURI	String	2	Returns the URI for this reference.

Request Group

Table 32-16 Request Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Request Group Field Description
Client Application	requestClientApplication	String	2	The client application (such as a web browser) used to issue the request.
Client Application	requestClientApplication	String	2	A description of the client application used to initiate this request, for example, the HTTP User connector.
Context	requestContext	String	2	A description of the content from which the request originated, for example, the HTTP Referrer.

Table 32-16 Request Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Request Group Field Description
Cookies	requestCookies	String	2	Cookie data offered by the client application as part of the request.
Method	requestMethod	String	2	The style of the request, i.e., for an HTTP request this could be PUT or GET.
Protocol	requestProtocol	String	2	The communication protocol used when issuing the request.
URL	requestUrl	String	2	A universal resource locator associated with the event.
URL Authority	requestUrlAuthority	String	2	The URL component used for authentication and authorization.
URL File Name	requestUrlFileName	String	2	The URL component that refers to the file containing the resource.
URL Host	requestUrlHost	String	2	The URL component that specifies the host device where the resource resides.
URL Port	requestUrlPort	Integer	2	The URL component that specifies the port to contact on the host device where the resource resides.
URL Query	requestUrlQuery	String	2	The URL component that specifies the query to use to request the resource.

Source Group

Table 32-17 Source Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
Address	sourceAddress	IP address	1	The IP address of the source device.
Asset ID	sourceAssetId	Resource	2	The asset that represents the device that was the network traffic's source.
Asset Name	sourceAssetName	String	2	See the common set of resource attributes.
Asset Resource	sourceAssetResource	Resource	2	See the common set of resource attributes.

Table 32-17 Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
DNS Domain	sourceDnsDomain	String	2	The Domain Name Service domain name associated with the user at the source device.
FQDN	sourceFqdn	String	2	The fully qualified domain name associated with the source device. This has no value if either the host name or DNS domain are without a value.
Geo	sourceGeo	GeoDescriptor	1	The geographical information.
Geo Country Code	sourceGeoCountryCode	String	1	Country Code.
Geo Country Flag URL	sourceGeoCountryFlagUrl	String	1	County Flag.
Geo Country Name	sourceGeoCountryName	String	1	Country Code.
Geo Descriptor ID	sourceGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Geo Latitude	sourceGeoLatitude	Double	1	See the common set of geographical attributes.
Geo Location Info	sourceGeoLocationInfo	String	1	See the common set of geographical attributes.
Geo Longitude	sourceGeoLongitude	Double	1	See the common set of geographical attributes.
Geo Postal Code	sourceGeoPostalCode	String	1	See the common set of geographical attributes.
Geo Region Code	sourceGeoRegionCode	String	1	See the common set of geographical attributes.
Host Name	sourceHostName	String	2	The name of the source device.
MAC Address	sourceMacAddress	MAC address	2	The MAC address associated with the network traffic's source (which may or may not be the MAC address of the host device).
NT Domain	sourceNtDomain	String	2	The Windows NT domain associated with the source device.

Table 32-17 Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
Port	sourcePort	Integer	1	The network port associated with the network traffic's source.
Process ID	sourceProcessId	Integer		The ID of the process associated with the source of the network traffic.
Process Name	sourceProcessName	String	2	The name of the process associated with the source of the network traffic.
Service Name	sourceServiceName	String	2	The name of the service associated with the network traffic's source.
Translated Address	sourceTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the device that was the network traffic's source.
Translated Port	sourceTranslatedPort	Integer	1	If network address translation is an issue, this is the translated source port associated with the attack.
Translated Zone	sourceTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the device that was the network traffic's source.
Translated Zone External ID	sourceTranslatedZone ExternalID	String	1	Returns the external ID for this reference.
Translated Zone ID	sourceTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Translated Zone Name	sourceTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference ID	sourceTranslatedZone ReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Translated Zone Resource	sourceTranslatedZone Resource	Resource	1	Locates the resource described by this reference.

Table 32-17 Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
Translated Zone URI	sourceTranslatedZoneURI	String	1	Returns the URI for this reference.
User ID	sourceUserId	String	2	The OS- or application-based identifier associated with the user at the network traffic's source.
User Name	sourceUserName	String	2	The OS- or application-based name associated with the user at the network traffic's source.
User Privileges	sourceUserPrivileges	String	2	The privileges afforded the user at the network traffic's source.
Zone	sourceZone	Zone	1	The network zone where the source device resides.
Zone External ID	sourceZoneExternalID	String	1	Returns the external ID for this reference.
Zone ID	sourceZoneID	String	1	Returns the ID for the resource in this resource reference.
Zone Name	sourceZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Zone Reference ID	sourceZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Zone Resource	sourceZoneResource	Resource	1	Locates the resource described by this reference.
Zone URI	sourceZoneURI	String	1	Returns the URI for this reference.

Target Group

Table 32-18 Target Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
Address	targetAddress	IP address	1	The IP address of the device hosting the attacker.
Asset ID	targetAssetId	Resource	2	The asset that represents the attacked device's host.

Table 32-18 Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
Asset Name	targetAssetName	String	2	See the common set of resource attributes.
Asset Resource	targetAssetResource	Resource	2	See the common set of resource attributes.
DNS Domain	targetDnsDomain	String	2	The Domain Name Service domain name associated with the attacked device.
FQDN	targetFqdn	String	2	The fully qualified domain name associated with the attacked device.
Geo	targetGeo	GeoDescriptor	1	The geographical information.
Geo Country Code	targetGeoCountryCode	String	1	Country code.
Geo Country Flag URL	targetGeoCountryFlagUrl	String	1	Country flag.
Geo Country Name	targetGeoCountryName	String	1	Country name.
Geo Descriptor ID	targetGeoDescriptorId	ID	1	Unique descriptor for the geo field.
Geo Latitude	targetGeoLatitude	Double	1	Latitude.
Geo Location Info	targetGeoLocationInfo	String	1	Location information.
Geo Longitude	targetGeoLongitude	Double	1	Longitude.
Geo Postal Code	targetGeoPostalCode	String	1	Postal code.
Geo Region Code	targetGeoRegionCode	String	1	Region code.
Host Name	targetHostName	String	2	The name of the attacked device.
MAC Address	targetMacAddress	MAC address	2	The MAC address associated with the target of the attack (which may or may not be the MAC address of the host device).

Table 32-18 Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
NT Domain	targetNtDomain	String	2	The Windows NT domain associated with the attacked device.
Port	targetPort	Integer	1	The network port associated with the target of the attack.
Process ID	targetProcessId	Integer		The ID of the process associated with the attack's target.
Process Name	targetProcessName	String	2	The name of the process associated with the attack's target.
Service Name	targetServiceName	String	2	The name of service associated with the attack's target.
Translated Address	targetTranslatedAddress	IP address	1	If network address translation is an issue, this is the translated IP address of the attacked device.
Translated Port	targetTranslatedPort	Integer	1	If network address translation is an issue, this is the translated port associated with the attack.
Translated Zone	targetTranslatedZone	Zone	1	If network address translation is an issue, this is the network zone associated with the translated IP address of the targeted device.
Translated Zone External ID	targetTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Translated Zone ID	targetTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Translated Zone Name	targetTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference ID	targetTranslatedZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Translated Zone Resource	targetTranslatedZoneResource	Resource	1	Locates the resource described by this reference.

Table 32-18 Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
Translated Zone URI	targetTranslatedZoneURI	String	1	Returns the URI for this reference.
User ID	targetUserId	String	2	The OS- or application-based identifier associated with the attacker, at the target of the attack.
User Name	targetUserName	String	2	The OS- or application-based name associated with the attacker, at the target of the attack.
User Privileges	targetUserPrivileges	String	2	The privileges afforded the attacker, at the target of the attack.
Zone	targetZone	Zone	1	The network zone in which the attacked device resides.
Zone External ID	targetZoneExternalID	String	1	Returns the external ID for this reference.
Zone ID	targetZoneID	String	1	Returns the ID for the resource in this resource reference.
Zone Name	targetZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Zone Reference ID	targetZoneReferenceID	ID	1	Returns the unique descriptor ID for this reference. This is populated only if this reference has been stored and uniquely identified in the database.
Zone Resource	targetZoneResource	Resource	1	Locates the resource described by this reference.
Zone URI	targetZoneURI	String	1	Returns the URI for this reference.

Threat Group

Table 32-19 Threat Group Data Fields

Label	Script Alias	Data Type	Default Turbo Level	Threat Group Field Description
Asset Criticality	assetCriticality	Integer	2	The relative measure of the importance of the targeted device, on a scale of 0 to 10.

Table 32-19 Threat Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Threat Group Field Description
Model Confidence	modelConfidence	Integer	2	The relative measure of ArcSight's confidence in its model of the attacked device, on a scale of 0 to 10.
Priority	priority	Integer	1	The relative measure of importance of investigating this event on a scale of 0 to 10. This field incorporates Model Confidence.
Relevance	relevance	Integer	2	The relative measure of likelihood that this event succeeded, on a scale of 0 to 10.
Severity	severity	Integer	2	The relative measure of possible damage to network security represented by the event on a scale of 0 to 10. It may be noted that event severity is supplied by the device; connector severity is supplied by the Smartconnector; and attack severity is supplied by the threat evaluation process.

Resource Attributes

Table 32-20 Resource Attributes Data Fields

Attribute Suffix	Description
External ID	The user-defined identifier associated with a configuration resource.
ID	The internal identifier associated with a resource (a UUID).
Reference ID	The internal identifier associated with the resource reference (an integer).
Type Name	The type of configuration resource.
URI	The URI associated with the resource (for example, /All Users/Administrators/Mlow).

Geographical Attributes

Table 32-21 Geographical Attributes Data Fields

Attribute Suffix	Description
Descriptor ID	The internal ID of the geographical reference.
Country Code	The identifier for the national-political state in which a device resides.
Country Flag URL	The URL of an image of the flag of the national-political state in which the device resides.
Country Name	The name of the national-political state where a device resides.
Latitude	The latitude of a device (Float).
Location Info	Other, free-form text information about the device's location.
Longitude	The longitude of a device (Float).
Postal Code	The postal code of the device's location, as assigned by the national-political state where it resides.
Region Code	The identifier of the sub-region of the national-political state where a device resides. The style of the identifier varies with the host country.

Data Monitors

Data monitors are views within [Dashboards](#) that can be configured to report on [Events](#), filters (see [Filters](#)), [Rules](#), and other areas that are of particular interest to you. Data monitors can be arranged on dashboards in numerous viewing layouts. Data monitors collect summary information on top events, most recent event activity, partial rule occurrences, hourly event counts, or event averages.

Data Monitors on Dashboards

Once data monitors are created, they can be used to display information on dashboards. You can add one or more data monitors to the same dashboard to create a collection of different "instrument panel" monitors appearing in the Dashboard display in the Viewer panel. Both the data monitors themselves and dashboards on which they are published can be shared among multiple Console users.

Permissions on Data Monitors

Data monitors display only those events for which you have permission. In addition, if you do not have access to a data monitor, the data monitor does not function. Administrators can limit visibility of or control access to dashboards and data monitors by changing access control lists (ACLs) as needed. For more about this, see ["Managing Permissions and Resources" on page 646](#) and ["Controlling Who Has Permissions to Deploy Data Monitors" on page 656](#).

Data Monitor Types

The ESM Console offers several predefined types to choose from when creating a new data monitor. The following topics describe the parameter entries and other options you can specify for each supported data monitor type.

You specify the Data Monitor type when you create a data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#). (Also, the data monitors provided with ArcSight are examples of these various types of data monitors.)

Asset Category Count Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

This data monitor enumerates the number of real-time hits (events) that occur per asset category, by priority, within a time interval.

Table 32-22 Asset Category Count Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	Turn on the monitor and collect data from the Manager. If cleared, the monitor does not display data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161 .
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the asset categories.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here determines the columns (fields) shown in the drill-down channel. (See “Inspecting Events in Dashboards” on page 154 for information on data monitor drill-downs.)
Root Asset Category Group	Choose an asset-category resource group to monitor.
Levels	Set the number of resource hierarchy levels below the chosen Root Asset Group to monitor. A value of 1 monitors only the next level down. A value of -1 monitors all levels.
Aggregation	Turn on (True) or off (False) the ability to aggregate all hits to the asset group URI, including those above the leaf level, to reveal disparities or unanticipated counts that may merit drilling down.
Show Root URI	Choose whether to display (True) or not display (False) the complete URI for affected asset categories.

Table 32-22 Asset Category Count Data Monitor (Continued)

Parameter	Description
Show Root Series	Specify whether to include (True) or not include (False) the root series. This is used to select how many levels down in the hierarchy to include in the data monitor display. Using a combination of this, Show Root URI, Aggregation, and Levels, you can slice out single levels in the display.

Event Correlation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

This data monitor provides flow-volume level correlation between two different event streams. The data monitor specifies two filters to identify two sub-streams of events within the overall stream of events coming into Manager. It then reports how closely the volume of events in the two streams correlate, that is, when the volume of events in Stream 1 decreases, does the volume in Stream 2 increase, decrease, or just change with no relation to the changes in Stream 1? For example, if a network intrusion detection system (NIDS) were deployed in front of several web servers in a cluster, one might expect that the flow of reported events from each NIDS would be roughly equivalent. If the event flow from one of the NIDS suddenly rose or fell out of sync with the other NIDS, then it might indicate a possible problem.

Table 32-23 Event Correlation Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	Enable the data monitor and collect data from the Manager. If cleared, the associated viewer configuration does not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161 .
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the asset categories.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here determines the columns (fields) shown in the drill-down channel. (See “Inspecting Events in Dashboards” on page 154 for information on data monitor drill-downs.)
Filter 1	Select a filter for the first event flow.
Filter 2	Select a filter for the second event flow.

Table 32-23 Event Correlation Data Monitor (Continued)

Parameter	Description
Restrict by Filter	Choose to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves.
Sampling Interval	Enter the interval (in seconds) for performing correlation calculations.
Number of Samples	Number of samples to keep in memory to perform calculations.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Alarm Condition	Condition on which to fire an alarm, for example: $c > 90 \ \&\& \ x > 0 \ \&\& \ y > 0$. In this example, c represents the correlation count from -100 to +100, x and y represent the actual count of events. See "Data Monitor Expressions" on page 938 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.

The formula for calculating the correlation values displayed in data monitors is:

$$cor = \frac{1}{N} \sum ((x_j - \bar{x}) \cdot (y_j - \bar{y})) / (\sigma_x \cdot \sigma_y)$$

where \bar{x} is the mean of x_j and σ_x is the variance of x .

The data monitor sampler takes all samples in memory and continually calculates correlation values using this formula. As an example, you could define an event correlation data monitor that displays a correlation between the number of times a network is being reconnoitered, and if that is related to the number of attacks that the network is receiving.

Event Graph Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

This data monitor draws real-time diagrams of selected event activity. In effect, it does automatically and in real-time what you can do manually, as described in ["Graphing Attacks" on page 176](#).

Table 32-24 Event Graph Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.

Table 32-24 Event Graph Data Monitor (Continued)

Parameter	Description
Enable Data Monitor	<p>Select this check box to "switch on" the monitor and collect data from the Manager. If cleared, the monitor is "off" and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161.</p>
Restrict by Filter	Choose a filter resource with which to restrict the events that the graphic includes.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here determines the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)</p>
Show Event Nodes	Choose a basis for visually expanding or aggregating event nodes, relative to their source and target node instances. See "Changing User Preferences" on page 772 for the option details.
Max Event Count	Set the greatest number of most-recent events the graphic can show.
Show Source/Target Nodes as	When one source-event target chains to another, you can choose to graph a source/target IP address as a single (simple) node, or to graph both the source and target instances of such an IP address (distinct).
Source Node Identifier	Choose an event attribute to use as the identifier for source nodes. The default attribute is Source Address. Note that while all attributes are available, not all are appropriate choices for this purpose.
Event Node Identifier	The fields that are available to use to uniquely identify the event type in a transaction.
Target Node Identifier	Choose an event attribute to use as the identifier for target nodes. The default attribute is Target Address. Note that while all attributes are available, not all are appropriate choices for this purpose.

Event Reconciliation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

The Event Reconciliation data monitor correlates events arriving from one sensor with events arriving from another sensor. When qualifying events occur on either or both sensors, the Event Reconciliation data monitor issues a new event to signal it.

You typically use this data monitor to determine the effectiveness of a firewall or IDS deployed in your environment.

One application is to place identically configured NIDS on either side of a firewall to determine which attacks are blocked by the firewall and which are not. Identical NIDS may also be wired in series to guarantee that none of the NIDS have been tampered with. Different NIDS may be wired in series to compare what each detects, either for evaluation purposes or to predict what attacks they may be missing as a group.

For example, you could define an event reconciliation data monitor that displays information about the number of events originating within the outside IDS (IDS1), and the inside IDS (IDS2), and the events that are filtered through the firewall. This presumes that events have the same custom string 1 source address, and that the target address field values are similar.

The Event Reconciliation and [Session Reconciliation Data Monitors](#) are similar in many respects. Their main difference is in the way each handles the scope of reconciliation sessions. Event Reconciliation focuses on accomplishing a certain number of event matches; Session Reconciliation permits an indeterminate number of matches while appropriate events continue to occur.

Table 32-25 Event Reconciliation Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration does not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161 .
Restrict by Filter	Specifies whether to restrict the data monitor to a particular filter. Filtering reduces the number of events the data monitor has to process. From the drop-down menu, double-click a filter or accept the default to receive all events.
Availability Interval	Sets the number of seconds to use as the interval between data monitor updates.
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here determines the columns (fields) shown in the drill-down channel. (See “Inspecting Events in Dashboards” on page 154 for information on data monitor drill-downs.)
Matching Fields	The set of fields to consider when establishing whether two events match.
Filter 1 Fields	Fields passed by Filter 1 that can be included in resulting correlation events. These correlation events contain a union of the Filter 1 and Filter 2 Fields.
Filter 1 Population Fields	Select a filter for the first device's event flow.

Table 32-25 Event Reconciliation Data Monitor (Continued)

Parameter	Description
Filter 2 Fields	Fields passed by Filter 2 that can be included in resulting correlation events. These correlation events contain a union of the Filter 2 and Filter 1 Fields.
Filter 2 Population Fields	Select a filter for the second device's event flow.
Matching Time Window	The period of time (in seconds) within which two appropriate events need to be received to qualify as a match.
Event Expiration Time	This is the amount of time (in seconds) that an event is kept in memory while seeking a matching event from the other device's event flow.
Correlate On	Choose an event-receipt circumstance for generating a reconciliation event. The options are as follows. <ul style="list-style-type: none"> Matching Events Filter 1 Events Only Filter 2 Events Only
Correlation Thresholds	This specifies the threshold(s) at which correlation events are created for the events specified in the Correlate On parameter. This field takes one number or a comma-separated list of three numbers. If you specify one number, it is used as the threshold for all the conditions. If you specify three numbers, they are applied respectively to the Correlate On values.
Correlation Interval	The interval (in seconds) to require between correlation events.

The data monitor displays a table view of qualifying events. You can sort on individual fields to display the most interesting cases on top. The following fields generate correlation events.

Correlation-Event-Generating Fields

The Event Reconciliation Data Monitor displays a table view of qualifying events. You can sort on individual fields to display the most interesting cases on top. The following fields generate correlation events.

Table 32-26 Fields Generating Correlation Events

Correlation Event	Description
Moving Average Event Fields (and the group-by fields are set)	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Custom Number 1	$\text{abs}(\text{count} - \text{moving_avg}) / \text{moving_avg} * 100$
Custom Number 2	$\text{count} - \text{moving_avg}$
Custom Number 3	statistics
Base Event Count	count

Table 32-26 Fields Generating Correlation Events (Continued)

Correlation Event	Description
eventCategory, CustomString 1	if (count - statistics = 0): eventCategory = /datamonitor/movingaverage/threshold Custom String 1 = datamonitor:002 if(< 0) eventCategory = /datamonitor/movingaverage/threshold/fallingCustom String 1 = datamonitor:003otherwise:eventCategory = /datamonitor/movingaverage/threshold/risingCustom String 1 = datamonitor:004
Statistics Events (and the group-by fields are set)	
Event Name	Name of the data monitor
ArcSight Category	metaevent
Event Category	/datamonitor/statistics/<Statistics Name>
Custom String 1	datamonitor:006
Custom Number 1	count
Custom Number 2	statistics
Correlation Data Monitor	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Event Category	/datamonitor/correlation
Custom String 1	datamonitor:007
Custom Number 1	Filter 1 count
Custom Number 2	Filter 2 Count
Custom Number 3	Correlation Value
Event Reconciliation (the rule chain and matching fields are set)	
Event Name	Name of the data monitor
ArcSight Category	/metaevent
Event Category	Event Reconciliation
Custom String 1	Filter 1 Events/Filter 2 Events/Matching Events
Event Type	Correlated

Geographic Event Graph Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

This data monitor draws a real-time geographic map of selected events. In effect, it does automatically and in real-time what you can do manually, as described in [“Graphing Attacks” on page 176](#).

Table 32-27 Geographic Event Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	<p>Select this check box to “switch on” the monitor and collect data from the Manager. If cleared, the monitor is “off” and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161.</p>
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the graphic. Filtering reduces the number of events the data monitor has to process. From the drop-down menu, double-click a filter or accept the default to receive all events.
Availability Interval	Sets the number of seconds to use as the interval between data monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here determines the columns (fields) shown in the drill-down channel. (See “Inspecting Events in Dashboards” on page 154 for information on data monitor drill-downs.)</p>
Max Event Count	Set the greatest number of most-recent events the map can show.

Hierarchy Map Data Monitor

The data monitor type is chosen when you create a new data monitor. (For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).) This data monitor draws an image made up of proportionally sized panels where each panel represents a group of events selected by group fields selected in the source node identifier. A source-node criteria could be a combination of fields.

Feature Enhancements

The Hierarchy Map data monitor includes the following enhancements.

- The data monitor now shows the complete hierarchy, with the hierarchy path built not just by using the delimiter within a field value but also across different field values. (Previous versions of the data monitor did not show the complete hierarchy.)
- *Group By* fields now provide options to specify a list of delimiters for use by each selected Group by field. By default, no delimiters are used, if no delimiters are specified then the whole field is taken as a single level for hierarchy. (Previous versions built the hierarchy path within a field value based on only one type of separator, a forward slash, which did not support fields that use other separators like a backward slash, “\”, or a dot, “.”)

Group By fields also provide an option to set the maximum depth level of hierarchy within a field. The default depth level is equal to the number of delimiters in the field. Entering 0 for this option signifies no depth level for the selected field, effectively defining the field as a single-level hierarchy.

- A list of *Group Attributes* can be specified as a drill-down display to show when a user drills down into a group. For each attribute, the user can select a field and a function (max, min, count, average, count unique) on that field value.
- Enhanced visualization tools for *label*, *size by*, and *color by* provide fine-grained control of hierarchy map display with regard to Group By and Group Attributes fields and values.

Use Cases

Following is a list of example use cases for which the Hierarchy Map data monitor is a useful monitoring tool.

- Display the number of matches for all the rules within a given time frame, with the hierarchy groups based on the File path field of the rule audit events. The value is the count of the events for each group. The goal would be to show which rules fired the most in a given time frame.
- Show table space usage of ArcSight ESM correlation resources, particularly session lists and active lists.
- Show memory usage for ArcSight ESM correlation resources, particularly session lists and active lists.
- Show assets hierarchy by networks, zones and subnets. Within subnets, the assets can be sub-divided into asset ranges.
- Show assets hierarchy divided by the location of assets, where the value on the map is the count of the events targeting those assets.
- Show assets hierarchy divided by the location of assets, where the value on the map is the count of the assets within those locations.
- Monitor ArcSight ESM resource distribution; that is, how many rules, reports, data monitors and so on are being used in the system, where the count is system storage space.
- Display events by device to show how many events are generated from each device in a given time frame (for example, the past two days).
- Show assets by the number of attacks each receives, to determine which assets are the most vulnerable.

The following topics show how to create a hierarchy map data monitor. Woven into these topics is a simple example that shows how to map high priority, significant events and targeted systems.

Defining a Hierarchy Map Data Monitor

First, create a new data monitor and select **Hierarchy Map** as the Data Monitor Type in the Data Monitor editor. (For information on how to create a data monitor and define the type, see [“Creating a Data Monitor” on page 160](#).)

To define the details of the Hierarchy Map Data Monitor, specify these attributes in the editor.

Table 32-28 Hierarchy Map Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.
Enable Data Monitor	<p>Select this check box to "switch on" the monitor and collect data from the Manager. If cleared, the monitor is "off" and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161.</p>
Restrict by Filter	Choose a filter resource with which to restrict the events that can affect the graphic.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here determines the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)</p>
Source Node Identifier	<p>This is a <i>group by</i> identifier. Blocks in the hierarchy map will represent events or objects that have matching values for all fields chosen here. Also, identifiers specified here will be available as Label By, Size By, and Color By choices on the displayed data monitor.</p> <p>Choose one or more event attributes by which to group events. The default attribute is Category Behavior, but you can include multiple attributes.</p> <p>For example, if you select only Category Behavior for this field, events will be grouped by category behavior (for example, all events with a category behavior value of /Access will be shown in one block, all events with a category behavior of /Authentication/Verify in another block, and so on).</p> <p>If you select more than one source node identifier, each block in the hierarchy map will represent events or objects that have the same values for all identifiers.</p> <p>For example, if you select Category Behavior and Event Name as source node identifiers, then each block in the map will represent events of the same behavior and event name.</p> <p>See "Specifying the Source Node Identifiers" on page 916 for more information.</p>

Table 32-28 Hierarchy Map Data Monitor (Continued)

Parameter	Description
Group Attributes	<p>You can specify one or more <i>group attributes</i> for fields with numerical values (for example, calculate the maximum priority of all events in a field group). The attributes you specify here are shown as drill-down tooltips when you mouse over a field on a hierarchy map display. You can add these attributes by specifying a label, a field, and a function to apply to the field. The functions can be applied on numeric fields only. See “Specifying Group Attributes” on page 917 for more details.</p> <p>Also, group attributes specified here will be available as Label By, Size By, and Color By choices on the displayed data monitor.</p>



If data monitor attributes are changed (edited) while a user is viewing the data monitor in a dashboard, the current data is flushed and the map defaults to red until new data arrives and the map display is redrawn.



Adding Variables

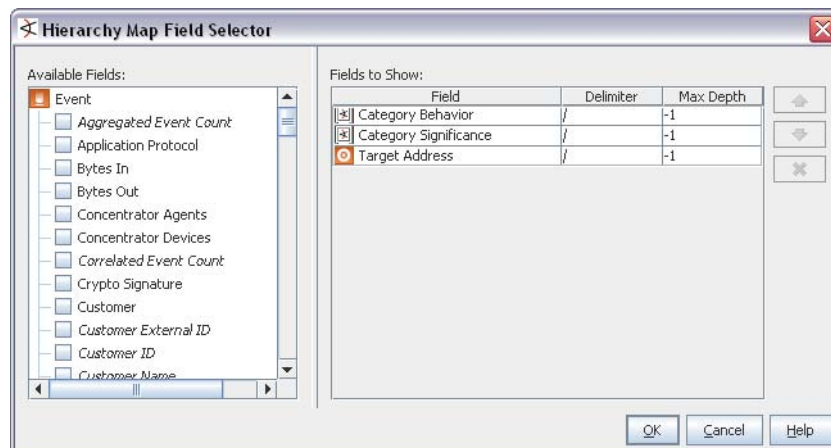
To add a variable, click the Variables tab. For more on using variables in resources, see [“Variables” on page 1006](#).

Specifying the Source Node Identifiers

Source node identifiers are “group by” attributes. For example, if you select only Category Behavior for this field, events will be grouped by category behavior. Each block in the hierarchy map will represent a different type of category behavior (for example, /Authentication, /Authentication/Verify, /Execute Response/Informational, etc). If you select both Category Behavior and Target Address here, each block in the hierarchy map will represent events with the same category behavior on the same target system (IP address or host name).

To specify one or more Source Node Identifier (Group By) fields, click in the **Source Node**

Identifier field, then click the button  to open the Field Selector dialog. Specify the fields by which you want to group events or objects by clicking Available Fields checkboxes, which adds them to “Fields to Show”. (To remove a field, select it under Fields to Show and click the delete button . Click up/down arrows to re-order fields.)



For example, we can group by Category Behavior, Category Significance, and Target Address. This will provide meaningful groups (events with the same category behavior, significance, and target address), and give us some interesting label, size, and color display options for mapping significant events and targeted systems on the data monitor.

Hierarchy Levels and Group Delimiters


You can specify how many levels of hierarchy you want to display for a field group by specifying one or more (a group of) delimiters and the maximum depth of hierarchy to display. For example, if you have a field value, <http://www.foo.com>, for which you have specified the depth level (Max Depth) as 2 with delimiters set to a group (consisting of `://.`), you will see:

- First level: <http://>
- Second level: <http://www.foo.com>

For the same example, if you set the Max Depth to 3, you get:

- First level: <http://>
- Second level: <http://www>
- Third level: <http://www.foo.com>

To select a field to display and set its hierarchy depth level:

- 1 Open the Hierarchy Map Field Selector dialog by clicking the browse button  that is displayed when you click in the Source Node Identifier field.
- 2 To add a field, check (click) the check box next to the field in the **Available Fields** scroll box. As you select a field, it will be displayed in the Fields column in the “Fields to Show” table on the right side of the dialog.
- 3 Double-click the **Delimiter** column for the field you just selected and enter one or more delimiters based on which you want to show the hierarchy depth.

By default, a forward slash (/) is set as the delimiter. To set a single level of hierarchy, delete the “/” and do not specify any delimiters. Also, set the **Max Depth** (as explained in the next step) to zero for that field. If you set a comma (,) as a delimiter, the hierarchy in the panel will display a backslash (\).

- 4 To specify the depth of the field hierarchy within a field, double-click the **Max Depth** cell for the field.



Note

Negative integers are not allowed. If you enter a negative integer, it will default to -1 which represents a depth level equal to the number of delimiters in the field.

If you leave this field blank, it will default to a depth level equal to the number of delimiters in the field and -1 will be displayed in the Max Depth column.

To display the whole field as a single level of hierarchy, set the **Max Depth** value to 0.



Specifying Group Attributes

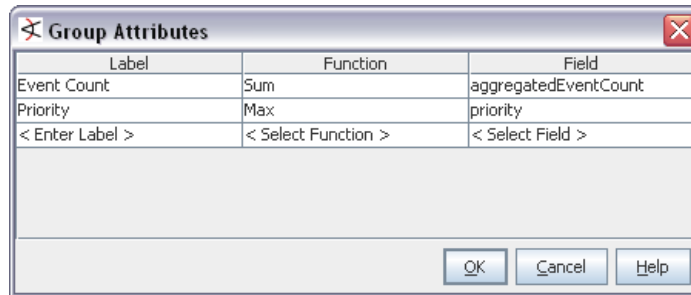
Optionally, you can specify group attributes, which are functions on numerical fields. These attributes are shown as mouse-over tooltips on groups (blocks) on a displayed hierarchy map. They will also be available as label, size, and color options.

For each attribute you want to add, provide a label, a function, and a field to which to apply the function. This can be done on numeric fields only. For example, if you add an Event

Count label, select the Sum function, and apply this to the aggregatedEventCount field, the function will find the sum of event count value.

To add group attributes:

- 1 Click the **Group Attributes** cell. A browse button  is displayed.
- 2 Click the browse button . The Group Attributes dialog opens.



- 3 Click the **Label** column and enter a name for the attribute you want to create. You can add multiple labels.
- 4 Click the **Function** column for a label and select a function to be applied to a field that you select in the next step. You can set a function for a numeric field only.
- 5 Click the **Field** column against a label and select a field to which to apply the function.

For example, we'll create two labels, Event Count and Priority, and map them as follows.

Label	Function	Field
Event Count	Sum	aggregatedEventCount
Priority	Max	priority

On the displayed map, the mouse-over tooltip on each block (group) will show both the event count and the highest priority event(s) included in that block. Also, specified group attributes (Event Count and Priority, in this case) will be available as Label By, Size By, and Color By options on the data monitor.

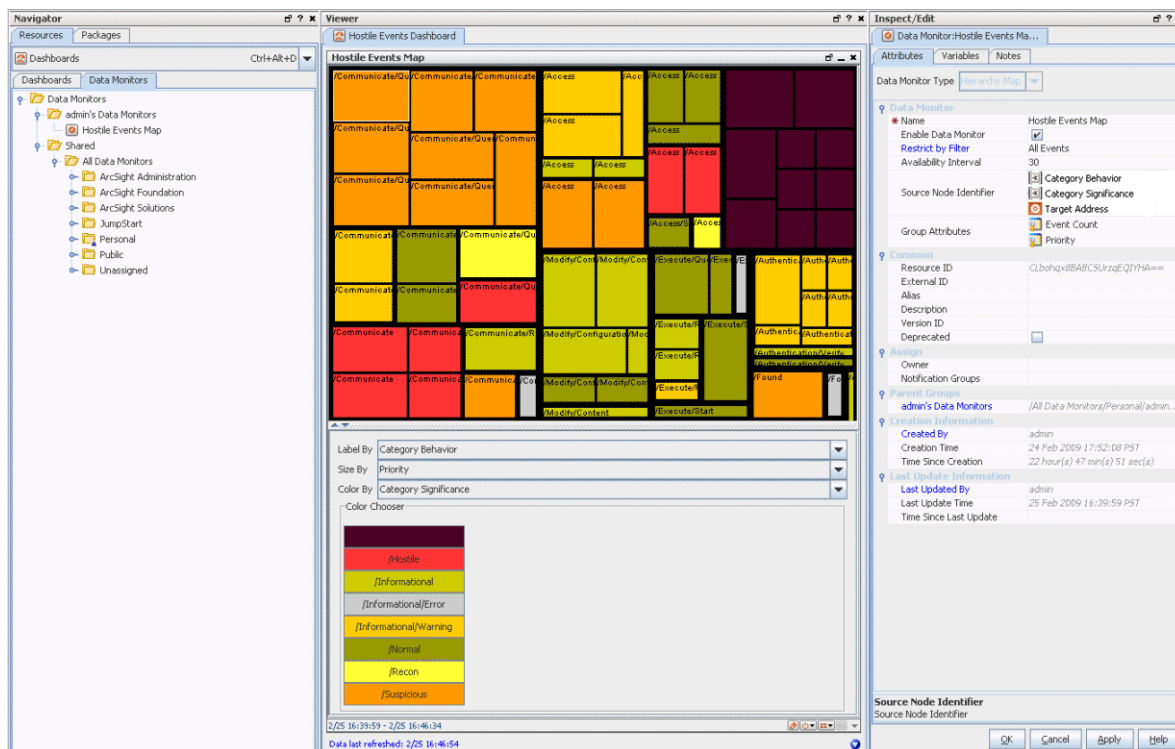
Hierarchy Map Display and Visualization Controls

Once you create a Hierarchy Map Data Monitor, you need to add it to a dashboard to display it and make further adjustments to the display.

Map Display and An Example

If no dashboards are displayed in the Viewer, simply right-click the Data Monitor you created, and select **Add to Dashboard As->Area Map**. This will create a new, untitled dashboard and add the data monitor to it. (You can also add it to an existing dashboard.)

The hierarchy map shown below is an example of the data monitor displayed on a dashboard.



You can choose “Hierarchy Map” as the Data Monitor type when you create a new Data Monitor. To display the data monitor, add it to a Dashboard.



- Before you can edit the visualization controls on the Hierarchy Map data monitor, you need to first add the data monitor to a dashboard and display the dashboard, as described just before figure above.
- If data monitor attributes are changed (edited) while a user is viewing the data monitor in a dashboard, the current data is flushed and the map defaults to red until new data arrives and the map display is redrawn.

The **example** data monitor above shows events grouped by category behavior, significance and target address. The labels show category behavior, and the blocks are sized by priority and colored by significance. Mouse-over tooltips show event count and priority for each group. Note that we can change the display on-the-fly by choosing a different label, size, and color options. For example, instead of coloring the blocks by Category Significance, we could color by Target Address. Or, instead of labeling by Category Behavior, we could label by Target Address. In this way, we can get quick, real-time, graphical overviews of network activity and adjust options to emphasize different details.

Labels, Size, and Color Controls

The visualization controls for Hierarchy Map Data Monitors are **Label By**, **Size By**, and **Color By** controls. (You might need to float the Viewer panel and expand the floating Viewer to see these controls. See [“Floating a Console Panel” on page 772.](#))

- **Label By** - Select a label. The value of the label you select will be displayed on each block.



- The **default** for "Label By" is all the fields specified for the source node identifier and the event count for that grouping. This shows as "Default" in the field. (The values available for use in the Label By field come from the attributes defined for Source Node Identifier and Group Attributes fields on the data monitor Editor. See ["Source Node Identifier" on page 915](#) and ["Group Attributes" on page 916](#) for more information.)
- If "Label by" is set to something other than the default, the last (bottom-most) field value in the hierarchy will not show on the map because the custom Label by setting will overwrite it. However, data for all fields, including the last field, is always taken into account on the map.

Use the default "Label By" option to show/visualize the complete hierarchy, including the last field value.

- **Size By** - Select an identifier or attribute by which you want to size the blocks. Once you select the Size By attribute, the blocks will be resized proportionate to the value selected. Only attributes that have numeric values are available, because you cannot size a block based on a non-numeric value.



The values available for use in the Size By field come from the attributes defined for the Group Attributes field on the data monitor Editor. See ["Group Attributes" on page 916](#) for more information.

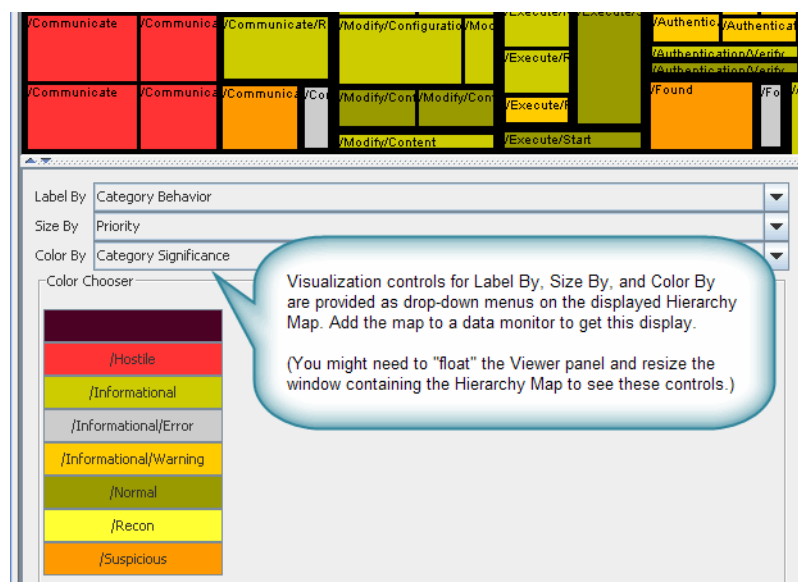
- **Color By** - Select identifier or attribute by which you want to color the blocks.



The values available for use in the Color By field come from the attributes defined for Source Node Identifier and Group Attributes fields on the data monitor Editor. See ["Source Node Identifier" on page 915](#) and ["Group Attributes" on page 916](#) for more information.

If you select a non-numeric field, you can change the color for any discrete value. If you select a numeric field, you get the option to select either a color for a discrete value or a color for a range of values. (For more on this option, see ["Selecting Colors for the Blocks" on page 921](#).)

After you select label, size, and color values, be sure to save the dashboard. The next time you open the dashboard, the attributes you saved will be applied to the next set of data.



Format controls for the Hierarchy Map are available as drop-down menus on the map display in a data monitor.



After an edit of tree map attributes, there might be a time lag before there is a visual indication of the updates. You can force a redraw of the tree map by dragging the slider to resize the panel that contains the map.

Selecting Colors for the Blocks

You can color the blocks by selecting any of the Source Node Identifiers or Group Attributes that are displayed in the **Color By** drop down menu. For example, if you select Priority in the **Color By** menu, then all blocks that have the same priority will be displayed in the same color, such as all blocks with priority 1 may be displayed in red and all blocks with priority 2 may be displayed in blue, and so on.

If the Color By attribute you select is discrete but non-numeric, you can define the colors for each value of the attribute. For attributes that have numeric values, you can individually assign a color per attribute value or specify a range and assign a color for that range. However, if the Color By attribute is Priority, you cannot specify a range. This is because there are already predefined colors for each level of priority. You will be allowed to change a predefined color to a color of your choice for each priority level.

Below the Label By, Size By and Color By fields, is the Color Chooser box. This box displays all the values for the **Color By** group/field that you select. To individually assign a color for an attribute:

- 1 Click the **Discrete** radio button (This button is visible only if you selected a numeric Color By attribute).
- 2 Double-click a value button to open the **Color Chooser** dialog.
- 3 Select a color that you want to display for all the boxes for which that value is applicable.
- 4 Click **OK**.

All the boxes that have that value will be displayed in the new color.

You can set a threshold for the maximum number of discrete values for which you can set a color. Set the `console.ui.hmDataMonitor.discrete.threshold` property in the `console.defaults.properties` file. If the number of discrete values exceeds this threshold, for all values that cross the threshold, the color will be set to white.

To assign a color for a range of values (for numeric fields only):

- 1 Click the **Range** radio button.
- 2 Click **Add** button to set a range and a color for that range. The Add a color mapping dialog opens.
- 3 Select a value from the **Min Attribute Value** and **Max Attribute Value** menus to set the range.

For example, if you want to set a range for Priority that falls in 3-to-6 range, select 3 from the Min Attribute Value menu and 6 from the Max Attribute Value menu.
- 4 Click the Color Chooser button to open the color chooser.
- 5 Select a color by clicking it and click **OK**. The color you choose will be used to display all values falling in that range. In our range example in step 3, all blocks that display priority of 3, 4, and 5 will have the color you just chose for the 3-6 range.



If new data comes in after you change the color mapping but before you save the new mapping, you will get a dialog asking you whether you want to save the changed mapping. If you select **Yes**, the Data Monitor will not be refreshed with new data until you save the new mapping. When you save it, the new mapping will be applied to the existing blocks and all future data displayed on the dashboard.

If you select **No**, the new color mapping will be applied to the existing data on the dashboard, but will not be saved in the database. So, as soon as new data arrives, the new color mapping will be overwritten by the original color mapping that exists in the database.

Hourly Counts Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

The Hourly Counts Data Monitor displays the total count of events on an hourly basis along with their Priority. The hourly count for the first hour segment starts when you open the dashboard. For example, if you open the dashboard at 2:25 PM, though the first time segment displays **14:00 - 15:00**, the count will begin at **2:25 PM**.

Table 32-29 Hourly Counts Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161 .

Table 32-29 Hourly Counts Data Monitor (Continued)

Parameter	Description
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.
Restrict by Filter	Choose a filter resource to restrict the data monitor's contents.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)

As an example, you could design an Hourly Counts data monitor that displays hourly counts of data being collected, for example, the number of events that Manager receives.

Last N Events Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

The Last NEvents data monitor orders events based on its configuration. In the Table Viewer, the monitor displays the most recent events by Priority, Event Name, Protocol, and Category. With the BarChartTable configuration, the order is by Priority and Event Name. The PieChart configuration is ordered by Priority.

Table 32-30 Last N Events Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161 .
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Restrict by Filter	Choose a filter resource to use as an additional restriction on the events displayed.

Table 32-30 Last N Events Data Monitor (Continued)

Parameter	Description
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)
# of Events	Specify how many events the data monitor displays.
Field Names	Choose field names to include in the data monitor display. By default, the data monitor includes EventName, EventCategory, ArcSight Severity, and Protocol fields. You can select additional fields or remove currently selected fields by Shift or Ctrl-clicking field names in the drop-down list.

As an example, you could design a Last N Events data monitor that displays the latest N events that meet the condition specified in the dashboard definition.

Last State Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

This monitor is somewhat different than others in that it provides an extra level of abstraction that you can use to simplify the information presented to operators. Sometimes called "indicator lights" or "heads-up displays," these monitors show graphics that translate more complex values into simple, rapidly observable results such as green/amber/red "signal lights" or checkmark/asterisk/exclamation point symbols. "Last State" data monitors could also be called "most recently known state" monitors.

Last State data monitors are built on the information collected by [Active Lists](#). The qualifying events in active lists are identified on the basis of selected key fields such as Source Zone and Source Address (see [Data Fields](#)).

Having focused on the events that apply, you then select a field to use as the basis of the values the indicators will simplify. For example, the Priority field has a range of values you could divide into sub-ranges that you choose to translate into good/okay/bad groups.

With a value-range and status-scheme decided, you can map the field values to the status names, and the status names to the visual indicators operators will see.

Table 32-31 Last State Data Monitor

Parameter	Description
Data Monitor Name	A unique name for the monitor.


Table 32-31 Last State Data Monitor (Continued)

Parameter	Description
Enable Data Monitor	<p>Select this check box to "switch on" the monitor and collect data from the Manager. If cleared, the monitor is "off" and displays no data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161.</p>
Restrict by Filter	Choose a filter resource to use as an additional restriction on the events summarized through the indicators, if necessary.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)</p>
Restrict by Active List	Choose an active list from the resource tree to use as the primary guide for event selection.
Key Fields	Choose the fields to use as identifiers for the indicators, and the order in which to display them.
Value Fields	Select the field(s) that will provide the range(s) of values to be mapped into indicators, and the order in which they will be evaluated.
Max Number of Indicators	Set the greatest number of qualifying indicators the data monitor will show. If more indicators are generated, the displayed set will be the those with the most recent event traffic.
Mapping	<p>Use the Define Status Map dialog box in two steps: first, on the Statuses tab, to associate status Titles with Image graphics, then, on the Mapping tab, to associate Value items contained by the Value Fields with the Statuses titles just defined. Be sure to define and select one "catch all" status to react to values that may fall outside the range you set.</p> <p>In the Value field, associate only one value at a time with the Status values you've defined. For example, if the values 0, 1, and 2 should all be associated with a Status of "Okay," enter each digit separately and click Add.</p>
Use as Timestamp	Choose whether to use the device's reported end-time or the Manager's receipt time as the definitive timestamp.
History Function	Use this option to add a Min or Max column to grid views that shows the minimum or maximum value for the indicator, over the most-recent time period specified by History Time Range.

Table 32-31 Last State Data Monitor (Continued)

Parameter	Description
History Time Range	Used with the History Function. The (most recent) period of time, in minutes, for which to retain minimum or maximum value information for an indicator. For example, a value of 60 could cause an indicator's Max column in a table to show its highest registered value over the previous hour.
Timeout	Used with the History Function. Sets the time limit, in seconds, after which the Min and Max column values are purged if not already updated.

Options for Table and Tile Views

In dashboards, you can see Last State data monitors as **Table** or **Tile** views. Click the **View as icon** () button at the lower-right corner to choose Table or Tile view.


The Table view will show more items than a *modified* Tile view. If the Tile view is customized to show results with particular values for key fields, it will show only a subset of the data monitor results.

A color chooser is available to apply to the **Table** view.

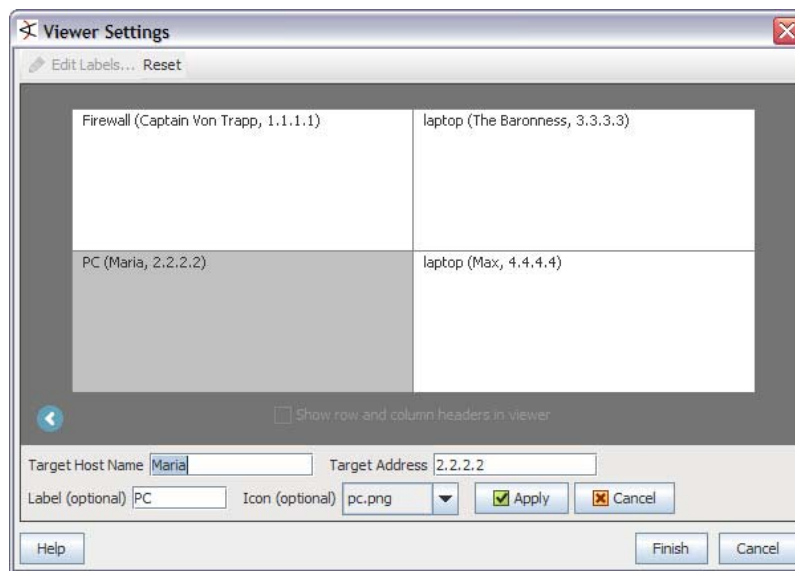
Table View (Color Chooser and Remove Entry)

Also in Table view, you can right-click an entry in a Last State data monitor and choose **Remove Entry**. However, keep in mind the data monitor's [Availability Interval](#) setting. Removal does not visibly take place until the next refresh, during which time a new instance of the entry could occur. Depending on the entry and the interval, a removed entry may appear to have remained.

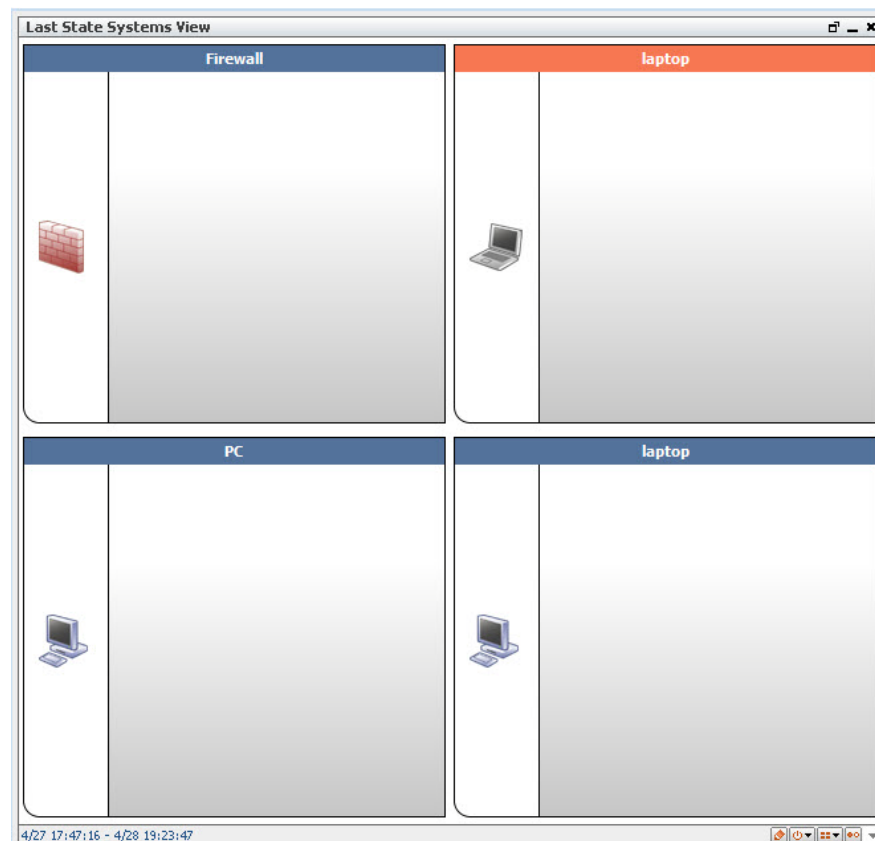
Tile View (Customize View)

When in **Tile** view, you can use the **Customize** button () to change the way data is ordered in the tabular (tiled) presentation, and limit the view to a subset of data monitor results. The customization choices are **by row-and-column** and **by cell**. Row-and-column is quicker to set up than cell because there are fewer adjustments, but cell does give you the option to set the contents of each tile in the data monitor. The custom settings here, in effect, filter your view based on values you specify for key fields. For example, if you are interested in monitoring state changes on only four systems identified by target

host name and target address; you can customize the view on a dashboard to show only those four systems.



These tiled views are "fixed" meaning that the tiles in the array will hold their positions, relative to each other and to the dashboard.



The customize view option on the Last State Data Monitor tile view gives Console users a way to design their own views and then get quick visuals on a few key assets or attackers:

- Set up a custom, focused view of a few items that you are interested in (assets like servers that might be targets of attacks, suspicious nodes that might be attackers, etc.). You do this by submitting values for the items you want to monitor (for example, host names and addresses, if those are your key fields).
- In a single glance, get information on state changes in different priority events (low, medium, high) in these few items. Since the positions of the items in your custom tile view does not change, and because you have limited the view to a few key items, you can get last state status with a quick glance.
- ESM Console users can customize dashboard views that use the same underlying Last State Data Monitor, but focus in on different items or assets (depending on how the data monitor custom view is set up on each dashboard). Fred could have a dashboard set up to monitor a few key servers based on host name and address, while Ethel could have a dashboard set up to monitor some firewalls, and both could be using the same underlying data monitor.



Notes on Customize view option for Last State Data Monitor

- This is a dashboard-level customization that essentially filters the view based on values you provide for key fields. The key fields that show up in the Viewer Settings come from the key fields set in the data monitor.
- A priority mapping needs to be configured in the data monitor in order for the quick-glance tile view to provide useful last state information
- Customizations made to the Last State Data Monitor are saved to the dashboard that holds the data monitor, not to the data monitor itself. This allows the same data monitor to be used as a basis for different, customized views (dashboards) for quick-glance, priority state changes related to incoming events.
- The Customize view option applies only to the **Tile** view (not Table view).

When you switch to the **Table** (, you can see results for other items in addition to the ones you “filtered” for on the customized Tile view.

Moving Average Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

The Moving Average data monitor displays the moving average of events by a selected data field. The display provides a running count of events within a specified time frame and generates an event when the moving average changes significantly.

If a Moving Average data monitor is configured to display multiple graphs simultaneously, you can open it using the Statistics Chart or Tile format options described in [“Managing Dashboards” on page 156](#).

This data monitor calculates its statistics based on the number of requested samples. Until a full set of samples accumulate, the statistics approach their nominal value. This is indicated by appending /Partial to the event category if the values represent an incomplete sample. The purpose is to prevent false positives. This is most applicable to [/DataMonitor/MovingAverage/Threshold/](#) events.

When either the Moving Average or Statistics data monitors gain or lose a value grouping during processing (for example, Priority), they issue an internal event. The data monitor's event categorization shows a Value/Add or Value/Remove suffix. This makes it possible to detect anomalous drops to zero, which can otherwise be missed if the monitor is removed because the discard threshold and a [Threshold/Falling](#) event could not be sent (due to exceeding the Maximum Alarm Frequency setting).

Both the Moving Average and Statistics data monitors have a **Stats Value Field**. When used, this attribute focuses the monitor's statistical analysis on the numeric value of a specified field rather than on the quantitative flow of events. Analyzing numeric fields within events enables a broad number of possibilities for status monitoring, especially with custom strings and ArcSight [Audit Events](#).

The **Value Calculation** field offers additional time-sensitive options for monitoring in second or minute increments. Monitoring per-second can catch abrupt spikes or drops; monitoring per-minute allows the same capability but may be more appropriate for larger integer values.

Table 32-32 Moving Average Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161.</p>
Restrict by Filter	Specifies whether to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves. From the drop-down menu, double-click a filter or accept the default to receive all events.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)</p>
Stats Value Field	<p>Specify a particular numeric field within events to use for statistical evaluation, rather than the overall flow of events. For example, specifying the Priority field would focus the data monitor on changes to the value of the Priority field in events, instead of on changes to the number of events encountered.</p> <p>The default is Aggregated Event Count, which is the sum of all aggregated events.</p> <p>Tip: Events can be <i>aggregated</i> at the Connector on specified fields. This pares down the number of events of the same type that the Manager must process.</p>

Table 32-32 Moving Average Data Monitor (Continued)

Parameter	Description
Value Calculation	<p>Controls the way the time-based accumulation of values is evaluated against the number of events involved.</p> <p>The default is Sum of values, which is the sum of all Stats Value Field event values.</p> <p>Average value per event divides the value by the number of events in the unit.</p> <p>Average value per second divides the value by the number of seconds in the unit.</p> <p>Average value per minute divides the value by the number of minutes in the unit.</p> <p>For finer time-sensitive value calculations, also consider using the Number of Samples and Sampling Interval so results are neither too shallow or too acute to be meaningful.</p>
Group By	Group by the specified field (for example, Priority)
Sorted By	Sort by the values found in fields or by the percentage of change in those values.
Alarm Change Threshold (%)	Specifies the moving average threshold, the percent change from the moving average, that will send a threshold exceeded event to the ESM Console. The threshold exceeded event is sent to the ESM Console and can be used to create a rule. For more information on rules, see "Creating Rule Actions" on page 451 . Type in a percentage. The default is 50.
Number of Samples	Type the number of Sampling Intervals to use to calculate the moving average, in seconds. The most recently stored Sampling Intervals are used to calculate the moving average. For example, if five Number of Samples are used, the last five Sampling Intervals are used to calculate the moving average.
Number of Visible Groups	Set the number of rows of results to display in the data monitor for each combination of ordering fields specified in the Group By parameter.
Sampling Interval	Type the time interval used to calculate the moving average, in seconds. For example, if the Sampling Interval is 5 minutes, the moving average is calculated every 5 minutes. The default is 300.
Group Discard Threshold	Specifies the minimum event counts needed to generate a threshold exceeded event. For example, event count could change from 1 to 2, a 100% change that results in a threshold exceeded event. To prevent these types of changes from generating a threshold exceeded event, specify the minimum event counts needed. If you want all events generated regardless of the event count, type 0.
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.

For example, you could design a Moving Average data monitor that displays the moving average of events on a per-source-address basis.

In the report "ArcSight Reports/Custom Reports/Moving Average Report", you can specify the name of the dashboard as a parameter (same as the moving average event name), and specify the detect time range to report on.



You can also have a rule trigger based on the moving average of events coming in, independent of defining reports based on moving average events.

Rules Partial Match Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

Displays rules that have partial matches and the total number of partial match events within a specified time frame. For more information on partial matches, see ["Creating Rule Actions" on page 451](#).

Table 32-33 Rules Partial Match Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161 .
Window Size	Specifies the time interval used to report partial match counts, in seconds. For example, if using 1 hour as the Window Size, each window displays partial match counts in hour intervals. The default is 3600.
Number of Windows To Display	Type the number of Window Sizes to display. The default is 5.
Fixed or Sliding	Specifies when to begin the Window Size time interval. Choose Fixed to begin at time units, such as every hour, 1:00, 2:00, and so forth, or Sliding to begin at the current time and move backwards in Window Size time intervals. For example, if the window size is 10 minutes, and the current time is 1:15 PM and Fixed was selected, the window time frames would be 1:00 to 1:09 and 1:10 to 1:15. If Sliding was selected, window time frames would be 1:00 to 1:04 and 1:05 to 1:15.

For example, you could design a Rules Partial Match data monitor that displays all events that have partially matched and enabled real-time rule conditions, and are currently stored in memory.

Session Reconciliation Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see ["Creating a Data Monitor" on page 160](#).

The Session Reconciliation data monitor correlates events on the basis of their occurrence within a relevant time period, as established by a "session" event. When an event is qualified as session-initiating by the Session Filter, a session begins. The session persists until it times out or a new primary event occurs. Point events (occurring within the session time period) cause a correlation event that contains selected information from both events.

You typically use this data monitor to watch network devices that involve longer-term concerns, such as DHCP leases.

The [Event Reconciliation Data Monitor](#) and Session Reconciliation Data Monitor are similar in some respects. Their main difference is in the way each handles the scope of reconciliation sessions. Event Reconciliation focuses on accomplishing a certain number of event matches; Session Reconciliation permits an indeterminate number of matches while appropriate events continue to occur.

The Session Reconciliation data monitor automatically compensates for session-initiating events that arrive out of order.

Table 32-34 Session Reconciliation Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data. Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161 .
Restrict by Filter	Specifies whether to restrict the data monitor to a particular filter. This filter precedes the Session Filter and Point Filter . From the drop-down menu, double-click a filter resource.
Availability Interval	Sets the number of seconds to use as the interval between monitor updates.
Select Field Set	Specify a field set for use in data monitor drill-downs. When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event. The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)
Session Filter	The filter for those events that will initiate data-monitoring sessions. Compare to Point Event Filter.
Matching Fields	The set of fields to consider when establishing whether two events match.
Session Inclusion Fields	The fields to add to the generated event, from the session-initiating event, when correlation occurs.
Point Event Filter	The filter for the events that may match the events that initiate data-monitoring sessions. Compare to Session Filter.

Table 32-34 Session Reconciliation Data Monitor (Continued)

Parameter	Description
Point Inclusion Fields	The fields to add to the generated event, from the point event, when correlation occurs.
Expired Session Timeout	The amount of time (in minutes) to retain a record of expired or replaced active sessions so that late or out-of-order point events can be properly processed.
Active Session Timeout	The time (in minutes) to allow before timing out a session if no new session events or point events occur.
Point Event Holding Period	The amount of time (in seconds) to retain point events to allow late or out-of-order session events to arrive and initiate sessions.
Events to Generate	Choose which types of correlation events are eligible to generate when session and point events match. <ul style="list-style-type: none"> Point Event Matched Sessions - A session/point event-match occurred. A correlation event was generated containing the events' selected information. No Session Matched Point Event - A point event occurred without a live matching session. No information is included in the correlation event. Session Expired Event - Session expiration or replacement generates an event. Note that expiration or replacement is not complete deletion. Session Pruned Event - Complete deletion of the session generates an event.
Aggregation Threshold	The number of matches to use as the threshold for generating a correlation event.
Reporting Interval	The interval (in seconds) to require between correlation events.

Statistics Data Monitor



The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

Provides a broader generalization of Moving Average data monitor functionality, except that it allows selection of other statistical methods in addition to Moving Average. Statistical methods include Average, Moving Average, Standard Deviation, Skew and Kurtosis, as well as Moving Average. These added capabilities could be used to detect anomalous behavior that could not be detected using moving average alone.

For example, monitoring the standard deviation of event data allows alarms to be triggered when there are sudden shifts in the rate of change of an event flow. This would allow alarms to be triggered when the protected network has been infected with a worm, but not when the network traffic rises due to normal use.

Both the Statistics and Moving Average data monitors have a **Stats Value Field**. When used, this attribute focuses the monitor's statistical analysis on the numeric value of a specified field rather than on the quantitative flow of events. Analyzing numeric fields within events enables a broad number of possibilities for status monitoring, especially with custom strings and ArcSight [Audit Events](#).

In dashboards, you can see Statistics data monitors as **Statistics Chart** or **Tile** views.

Click the **View as icon** button () at the lower-right corner to choose. When in Tile view, you can use the **Customize** button () to change the way data is ordered in the tabular (tiled) presentation. The customization choices are **by row-and-column** and **by cell**. Row-and-column is quicker to set up than cell because there are fewer adjustments, but cell does give you the option to set the contents of each tile in the data monitor.

When either the Moving Average or Statistics data monitors gain or lose a value grouping during processing (for example, Priority), they issue an internal event. The data monitor's event categorization shows a [Value/Add](#) or [Value/Remove](#) suffix. This makes it possible to detect anomalous drops to zero, which can otherwise be missed if the monitor is removed because the discard threshold and a [Threshold/Falling](#) event could not be sent (due to exceeding the Maximum Alarm Frequency setting).

These tiled views are "fixed," meaning that the tiles in the array will keep their positions, relative to each other and to the dashboard.

Table 32-35 Statistics Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see "Enabling or Disabling a Data Monitor" on page 161.</p>
Restrict by Filter	Choose to restrict the data monitor to a particular filter. When restricting by filter, you focus on a filter that is of particular interest to you and also reduce the number of events the data monitor retrieves.
Availability Interval	Set the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here will determine the columns (fields) shown in the drill-down channel. (See "Inspecting Events in Dashboards" on page 154 for information on data monitor drill-downs.)</p>
Statistics Type	Choose the type of statistical calculation the data monitor will perform. The available types are Average, Identity, Kurtosis, Skew, Standard Deviation, and Variance.
Stats Value Field	Specify a particular numeric field within events to use for statistical evaluation, rather than the overall flow of events. For example, specifying the Priority field would focus the data monitor on changes to the value of the Priority field in events, instead of on changes to the number of events encountered.

Table 32-35 Statistics Data Monitor (Continued)

Parameter	Description
Group By	Group by the specified field (for example, Name)
Sorted By	Choose to sort results by value, sample count, statistics, or triggering criteria.
Alarm Trigger Condition	<p>Enter a conditional expression on which to trigger alarms.</p> <p>You can use any mathematical expression that employs these two variables: <i>c</i> (the count in the current Sampling Interval), and <i>s</i> (the calculated statistics value for that interval).</p> <p>For example, this expression would trigger when the current count goes beyond 500: <code>c >= 500</code>. An expression that triggers when the statistics reach 500 would be: <code>s >= 500</code>.</p> <p>As a matter of interest, the Moving Average data monitor is in effect a special case of the Statistics data monitor, based on this expression: <code>s != 0 && (abs((c - s)/s) * 100) > 0.5</code></p> <p>where 50 is the percent of change you specify in the Moving Average data monitor.</p> <p>Concerning custom numbers for devices, <code>Custom Number 1 == variable c</code>; and <code>Custom Number 2 == variable s</code>.</p> <p>See "Data Monitor Expressions" on page 938 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.</p>
Number of Samples	Specify the number of most-recent Sampling Intervals to retain in memory and use to calculate event statistics. For example, if you set it to retain 5 sampling intervals, the last five periods (as specified in the Sampling Intervals attribute) are used to calculate the moving average.
# of Groups to Display	Set the number of rows of results to display in the data monitor for each combination of ordering fields specified in the Group By parameter.
Sampling Interval	Enter the time interval for recalculating event statistics, in seconds. For example, if the Sampling Interval is 5 minutes, the moving average is calculated every 5 minutes.
Group Discard Condition	<p>Enter a condition (a filtering expression) by which to remove certain result rows from consideration in statistical calculations, based on the result ordering set in the Group By attribute.</p> <p>See "Data Monitor Expressions" on page 938 for more information about the operators and functions supported in this and similar data monitor parameters that accept conditional expressions.</p>
Maximum Alarm Frequency	Minimum time (in seconds) to wait before sending alarms for the same group.

The Statistics Data Monitor is similar to the moving average data monitor; in fact, the Statistics data monitor specifying a statistics type of "Average" displays the same results as the Moving Average data monitor. The difference between the two is that the statistics monitor parses mathematical conditions rather than the fixed threshold values as they are used in the moving average event.

System Monitor Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

The System Data Monitor provides measurements based on Manager internal monitoring system Java classes and attributes. A number of system monitors that may be particularly useful to administrators are provided as predefined System Data Monitors that you can include in your dashboard displays to monitor system performance.

Table 32-36 System Monitor Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161.</p>
Monitor Types	From the drop-down menu, select the name of ArcSight Java class for which you want to display attribute measurements, for example, Throughput meter or Status

System Monitor Attribute Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

The System Monitor Attributes Data Monitor is similar to System Monitor, except that, rather than providing measurements for all attributes of a specified Java class, focuses on a single specific attribute of a given ArcSight Java class. (Used primarily for measurements on attributes that provide complex data structures.) A number of predefined system monitors are provided that you may want to include in your dashboard displays to monitor system performance.

Table 32-37 System Monitor Attribute Data Monitor

Parameter	Description
Data Monitor Name	Type a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161.</p>

Table 32-37 System Monitor Attribute Data Monitor (Continued)

Parameter	Description
Monitor Types	From the drop-down menu, select the name of ArcSight Java class for which you want to display attribute measurements, for example, Throughput meter or Status.
Attribute Name	Specify the individual attribute of the specified ArcSight Java class for which you want to display information. You can obtain the names of specific attributes in a class by viewing the results of a System Monitor defined for that class.

Top Value Counts Data Monitor

The data monitor type is chosen when you create a new data monitor. For information on how to create a data monitor, see [“Creating a Data Monitor” on page 160](#).

Displays top events by selected data field, the total number of events, and the event Severity within the total number of events with the Table and BarChartTable viewer configurations.

Top Value Counts uses an aggregation mechanism that precisely and predictably controls the time dimension of the data being evaluated. "Bucketized" means that the monitor evaluates a specific number of time-based event data units of a certain size (buckets). As time increments forward, the evaluation refreshes, using the most recent set of qualifying buckets.

Table 32-38 Top Value Counts Data Monitor

Parameter	Description
Data Monitor Name	Enter a data monitor name.
Enable Data Monitor	<p>Select the check box to enable the data monitor and collect data from the Manager. If not selected, the associated viewer configuration will not display any data.</p> <p>Depending on the permissions associated with the user group to which you belong, you may or may not have an option to Enable (<i>deploy</i>) or disable (<i>un-deploy</i>) the data monitor. For more information, see “Enabling or Disabling a Data Monitor” on page 161.</p>
Restrict by Filter	Specify a filter to focus on events that are of particular interest and to reduce the number of events the data monitor processes. Use a filter when the number of possible Aggregate Field values can exceed the maximum for # of Distinct Events .
Availability Interval	Sets the number of seconds to use as the interval between monitor updates.
Select Field Set	<p>Specify a field set for use in data monitor drill-downs.</p> <p>When this data monitor is displayed, the user can double-click on a chart area or table row that represents an event to bring up a drill-down channel for that event.</p> <p>The field set specified here will determine the columns (fields) shown in the drill-down channel. (See “Inspecting Events in Dashboards” on page 154 for information on data monitor drill-downs.)</p>

Table 32-38 Top Value Counts Data Monitor (Continued)

Parameter	Description
Bucket Size in Seconds	The time dimension for individual event data units. A number of these units make up the value used in Number of Buckets . For example, you might use a value of 300 to create five-minute buckets. Bucket size and frequency (increasing freshness and resolution) does have a performance cost so it is wise to set buckets to run only as small and fast as actually necessary.
Number of Buckets	The overall time dimension to evaluate, expressed as the appropriate number of Bucket Size units. For example, to evaluate the most recent hour using five-minute buckets, you would enter 12 . Bucket size and frequency (increasing freshness and resolution) does have a performance cost so it is wise to set buckets to run only as small and fast as actually necessary.
Time Field	Choose the specific event timestamp to use to apply events to time buckets.
# Top Entries	The number of entries to show as "top" values.
# of Distinct Events	<p>This value must equal or exceed the maximum number of values that the Aggregate Field can possibly have. The default is 1,000. The maximum is 10,000. This value controls the upper limit on the number of aggregate field values. If it is smaller than necessary, then when it encounters one more Aggregate Field value than allowed, the Data Monitor resets all the counters, clears the data, and starts over at zero.</p> <p>If you specify more than one Aggregate Field, the maximum number of possibilities is the product of the possible values of all fields. For example, if you are aggregating by users and zones in an environment with 200 users and 15 zones, the number of possibilities is $200 \times 15 = 3,000$. If the number of possibilities is larger than the maximum of 10,000, use a filter to reduce them.</p>
Aggregate Field	Specify one or more data fields to monitor. For more information, see "Data Fields" on page 867 . To monitor the top 10 source IP addresses, for example, select the Source Address data field from the drop-down menu. If you specify more than one field, the total number of possible combinations is the product of the number of possible values for each field you specify. Make sure that the # of Distinct Events field is large enough to accommodate this number.
Value Field	<p>Specify what the data monitor will use when determining the top value counts: the number of matching events, or the sum of a particular data field value in all matching events.</p> <ul style="list-style-type: none"> To count events, leave this field empty. (This is equivalent to selecting the Aggregated Event Count field. When the Value Field is not specified, the data monitor uses the data field specified in the Aggregate Field to count events.) To sum the values from a particular data field, use the data field selector for the "Value Field" attribute to select the desired field. <p>In either case, counts from aggregated events will be properly adjusted.</p>

Data Monitor Expressions

Certain data monitor parameters can specify their own conditional expressions with which to flexibly define triggers or results. For example, you use these expressions in the

Statistics data monitor's Alarm Trigger Condition and Group Discard Condition parameters to evaluate when to send an alarm or to remove result rows from statistical calculations.

The type of expression supported is a conventional infix mathematical expression with each basic expression separated by parentheses.

All common arithmetic operators are supported. Boolean operators are also fully supported and Boolean expressions evaluate as either 1 or 0 (true or false).

Supported Data Monitor Expression Operators

All common arithmetic operators are supported. Boolean operators are also fully supported and Boolean expressions evaluate as either **1** or **0** (true or false).

Table 32-39 Data Monitor Expression Operators

Operator	Symbol	Operator	Symbol
Power	^	Less Than or Equal	<=
Boolean Not	!	More Than or Equal	>=
Unary Plus	+x	Less Than	<
Unary Minus	-x	Greater Than	>
Modulus	%	Not Equal	!=
Division	/	Equal	==
Multiplication	*	Boolean And	&&
Addition	+	Boolean Or	
Subtraction	-		

Supported Data Monitor Expression Functions

Table 32-40 Data Monitor Expression Functions

Name	Function	Name	Function
Sine	sin()	Inverse Hyperbolic Cosine	acosh()
Cosine	cos()	Inverse Hyperbolic Tangent	atanh()
Tangent	tan()	Natural Logarithm	ln()
Arc Sine	asin()	Logarithm Base 10	log()
Arc Cosine	acos()	Angle	angle()
Arc Tangent	atan()	Absolute Value / Magnitude	abs()
Hyperbolic Sine	sinh()	Random Number (between 0 and 1)	rand()
Hyperbolic Cosine	cosh()	Modulus	mod()

Table 32-40 Data Monitor Expression Functions (Continued)

Name	Function	Name	Function
Hyperbolic Tangent	tanh()	Square Root	sqrt()
Inverse Hyperbolic Sine	asinh()	Sum	sum()

Device

See [“Assets” on page 799](#) for a discussion of network devices.

Event Inspector

The Event Inspector is a tool for examining [Events](#) details. It is located in the [ESM Console](#)'s Inspect/Edit panel. To open the Event Inspector, double-click an event line in a grid view (see [“Views” on page 1028](#)).

There are two panels in the Event Inspector. The top panel displays selected events with associated rules. The events listed here have a set of right-click menu commands similar to those described in [“Using Grids” on page 145](#). The bottom panel displays event details for one or more events that have been selected from the top panel. If you select more than one event from the top panel, only their common values are displayed in the bottom panel.


The Event Inspector can display the chain of events that trigger a rule (see [“Rules” on page 974](#)) and generate a correlation event. From the Event Inspector you can view each event and rule in the chain for details.

Depending on the information available for an event, you may also be able to review its business significance in the Impact Analysis tab or its actual content in the Payload tab.



Viewing global variables in the Event Inspector

When you view events in an active channel and open an event that contains a global variable field in the Event Inspector, you may need to refresh the Event Inspector view to see the global variable fields, because the Manager processes global variable data differently from regular event data.

- If your Hide Empty Rows icon  is toggled on (so that empty rows are not displayed), you may not see the global variable field(s) in the event inspector.
- To refresh the view, de-select, then re-select the Hide Empty Rows icon.

See also: [“Inspecting and Editing” on page 102](#).

Field Sets

The overall set of event-attribute fields is defined in [Data Fields](#), but you can make or use custom subsets with the Field Set Editor (see [“Field Sets” on page 942](#)). Choose a set name to see only that predefined set of fields.

Events

Events begin at network [Devices](#) that can sense and record instances of security-sensitive activity. Examples include a database record change, a syslog entry, a firewall transit, a router access, or scanning a door access card.

Such initial events are typically recorded in logs, and are sometimes called **base** or **raw** events.

When numerous source devices are reporting large volumes of relatively similar events, it is desirable to funnel these events through central event **concentrators** that forward a much-reduced set of representative or summary events.

When these events reach ArcSight [SmartConnectors](#), several things can happen.

- All received events are **normalized** (restructured) to make their information consistent and ready for analysis.
- All received events are **categorized** (appended with classification information) using ArcSight's event categorization taxonomy.
- If appropriate and the SmartConnector is configured to do so, events are **aggregated** to issue fewer and more meaningful events and to reduce network traffic.
- If appropriate and the SmartConnector is configured to do so, selected events are **filtered** out, to eliminate them as a further traffic or processing burden.
- For certain devices, the option may be available for the SmartConnector to apply analysis rules to incoming events and to issue **correlation** events concerning them.

At SmartConnectors, filtering **removes** events from the system. Aggregation **replaces** events with fewer new ones bearing summary information.

When the events from SmartConnectors pass to [Managers](#) they can again be considered **base** events in the sense that they are in a state prior to processing. More specifically, any event that is subject to further processing, even if the result of previous processing, can be considered a base event.

All base events entering the Manager are subject to:

- **Correlation** to derive more intelligence from the events. Correlation **adds** new events containing the results of correlation activity. You apply correlation through the rules and data monitors in their respective resource trees of the Navigator panel. Correlation events have flash icons in grid views.
- **Filtering** to selectively see and report on events. Filtering within the Manager does not actually discard events. You apply filtering with the resources in the Filters tree in the Navigator panel.

Note that all aggregation actually occurs at SmartConnectors, not within the Manager. You apply aggregation through the resources in the [Rules](#) tree of the Navigator panel.

There are only **base**, **aggregation**, and **correlation** [Events](#). It is important to note that any such event in the system can (if the right rules and data monitors are present) become the input to produce new correlation events. You should also note that the Manager's rules engine is designed to prevent infinite loops.

Apart from the events that originate on the network, and the correlation events the Manager issues in response to them, the Manager generates many other events of its own for a variety of purposes.

These *internal events* can be divided into [Audit Events](#) and [Status Monitor Events](#). You can use audit events to track, or react to, system **activity** at all levels of operation from data monitors to the database. [Status Monitor Events](#) events are valuable for getting system **state** information. Review these topics ([“Audit Events” on page 811](#) and [“Status Monitor Events” on page 988](#)) to become familiar with the characteristics of all the available events.

You can apply all analytic tools to any events present, whether base or correlation, originating externally or internally.

Field Sets

Field sets are named subsets chosen from the available [Data Fields](#). Field sets can help you quickly focus a grid view, Event Inspector, or other field array on a particular context such as customer accounts or vulnerability.

Field sets are a shareable resource that you can manage and apply through the Field Sets resource tree in the Active Channels section of the Navigator panel. (In the Navigator, choose **Active Channels**, and click the **Field Sets** tab.) These field sets also support the [Variables](#) data fields. Field sets supercede and include the previous concept of column sets.

There is a default list of field sets for out-of-the-box use, and to serve as examples.

See [“Creating and Using Field Sets” on page 204](#) (in [Chapter 7, Monitoring Events, on page 129](#)) for information on how to create custom field sets, modify existing ones, and share them with other Manager administrators or operators.

See [“Sortable Field Sets” on page 987](#) for information on creating and using sortable field sets.

See [“Using Field Sets” on page 855](#) (in the [Common Conditions Editor \(CCE\)](#) reference topic) for information on how to access field sets to build conditions.

Filters

Use filters to specify criteria that narrows the scope of monitored data and reduces the number, or constrains the nature, of the [Events](#) displayed through the [ESM Console](#). Filtering criteria are based on the ESM Console's event [Data Fields](#), used in various combinations and with various conditions placed on their content. As you apply more restrictive filter parameters, the number of events reaching the ESM Console may decrease, but the likelihood increases that the events are significant.


For example, you can create a filter that contains every firewall for the western region of the United States, and create another filter that contains every Intrusion Detection System (IDS) for the same region. You can also be more specific, by creating a filter wherein you only want to view firewalls and IDSs with certain IP addresses because they are labeled as **suspicious** IP's or IP's that may pose a possible threat to an enterprise. On the other hand, you can create filters that only contain networks that are labeled as **friendly** and seem to pose no threat at all, but you still want to monitor them. For display purposes, you can select a unique color for any filter. If an event matching the filter's conditions is generated, the event appears in the grid view in the specified color.

Applying filters to get optimum results is a core skill for network security analysis. While it isn't possible to anticipate specific solutions here, you should know the most efficient way to use the ESM Console's filtering tools.

Filtering Options

In the ESM Console, filtering is available in multiple ways, and how you choose to use these options can have a significant effect on your ability to precisely, flexibly, and rapidly author new analyses over the long term.

The primary event-filtering options are:

- **Filters resources:** The Navigator panel's Filters resource tree is (or should be) your master repository for filtering solutions. Using the Filters tree is the best way to work out an organized filter library. You can and should use the filters you develop here, through the Filters Editor, in other resources such as active channel views, reports, or rules. You can even use filter resources in other filter resources. By basing your solutions on hierarchical, resource-based filters, you gain the type of leverage granted by style sheets.
- **Active Channels resources:** The active channel resources in the Navigator panel can each store an individual filtering solution that is unique to a given channel or based on a Filters resource. When you use an existing active channel to create another, you carry forward and perhaps modify its filter.
- **Active Channel Editor:** You use the Active Channel Editor to create or modify the filters in individual active channels. Changes you make to active channels through this editor are limited to those channels and channels created from them. Such changes shouldn't be considered long-term or enterprise-wide.
- **Inline view filters:** In any active channel grid view you can use the fields of the grid's top line to select filtering event-attribute values for certain columns, which will be used with implied AND operators to impose ad hoc filters. These filters are not retained with the prior active channel, but you can give the revised channel a name and save it through the Active Channel Editor.
- **Event-based filters:** Another quickly applied and contextual category of event filtering is offered by the event-attribute **Investigate** command. When you right-click an event attribute in a grid view you can choose Investigate and one of several filtering options that vary based on the data involved. Like inline filters, **Investigate** filters apply only to the current view and are temporary unless saved in a different named view.
- **Inline Filters:** You can add an inline filter to a channel view by clicking the Edit Inline Filter () button at the top right of the grid view to display the inline filtering fields. (For more information see, ["Filtering Grid Views with Inline Filters" on page 150.](#))

You should always remember that your most primary filter is the one imposed by your system administrator. Each user operates under the constraints of the access control lists (ACLs) configured for their user identity. These ACLs automatically filter out some portion of the total available event flow before it reaches you. Any filter you use or create adds to this fundamental constraint.

For more about putting filters to work, see [Chapter 11, Filtering Events, on page 223.](#)

Global Variables

You can create variables that derive unique values from existing data fields, which you can apply locally in the resource you're working on to make monitoring and correlation more specific to particular scenarios.

In addition to these local variables, there is a global variable resource, which makes it possible to define a variable once, then re-use it in multiple places wherever conditions can be expressed (active channels, rules, filters, data monitors, and queries), and wherever fields can be selected (CCE, field sets).

Global variables are centralized and reusable, which make them an essential building block for user correlation in the Actors feature, and other advanced correlation scenarios.

Once created, global variables appear in the [Common Conditions Editor \(CCE\)](#) as additional fields on the Filters or Conditions tabs, as [Group By](#) arguments for data monitors and queries, and in rule conditions and actions. You can add variables to field sets in the Field Set Editor to extend the event and resource schema with values derived from other data fields.

The global variables feature also makes it possible to easily promote local variables defined for a particular resource into a global variable, where it can be re-used in other condition statements.

For details about the Global Variables feature, see [“Global Variables” on page 477](#).

Grid View

A grid view is a type of view in the ESM Console, or in an ArcSight Web client, that shows [Events](#) summary information organized in rows and columns, or other types of information such as for certain [Resources](#). As new events occur, they are inserted at the top of the grid as new rows. Rows contain events while columns contain data fields. You can learn about working with grids in [“Using Grids” on page 145](#).

iDefense

If your ArcSight system is integrated with a VeriSign iDefense database, you can view iDefense incident reports for events that have vulnerabilities associated with them.

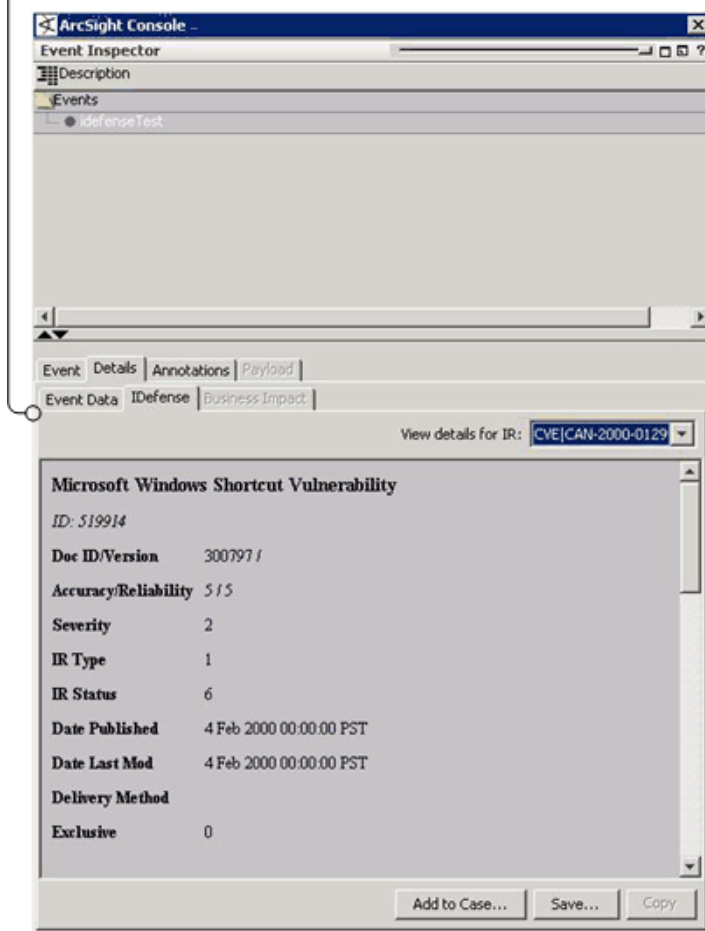
To view iDefense information for an event:

Select an event in a channel, right-click, and choose Show Event Details.

If there is iDefense information available for the selected event, the iDefense tab will be enabled. Click the **iDefense** tab, then choose an incident report from the **View details for IR** menu at the top right of the iDefense sub-tab. The reports are displayed on the iDefense tab.

This option is available only if you have the third party iDefense software installed and configured to interact with the Arcsight ESM, and if the selected event has a vulnerability ID associated with it. In that case, an iDefense tab is available as a sub-tab under the Details tab for the selected event. The iDefense reports provide more details on the vulnerability.

Typically, multiple incident reports are available for a selected event. To view a report, choose a report name from the **View details for IR** drop-down menu.



Inspect/Edit Panel

Located on the right side of the [ESM Console](#), the Inspect/Edit panel contains all the various [Resources](#) editors you use to create and modify analytic tools, as well as the Event Inspector you use to examine the contents of [Events](#). Using the Event Inspector and the resource editors is explained in the topics that relate to events and those resources.

Job Scheduler

See [“Scheduling Jobs” on page 977](#).

Knowledge Base

The Knowledge Base is a problem-solving database that can contain information on event data, associated if-then-else rules, cases, and so forth. All information is derived from community expertise within your enterprise or based on your internal practices and policies.

Compare Knowledge Base articles to [Reference Pages](#), which provide built-in reference information about certain resources.

When you create a Knowledge Base article, you provide a URL or directory path to a specific vulnerability or exposure. You can add notes to Knowledge Base articles to relay information about the article. Using a note, you can write reminders, messages to the next shift, or any related information. Articles display in the ESM Console or in an ArcSight Web client, with associated links and article information. Knowledge Base articles are stored in these default groups:

- **Shared:** lists Knowledge Base groups and articles to which the logged-in user has access:
 - ◆ **All Knowledge Base:** lists all user Knowledge Base groups and articles.
 - ◆ **Personal Knowledge Base:** lists each user's own Knowledge Base groups and articles.
 - ◆ **Public Knowledge Base:** lists Knowledge Base groups and articles accessible to all users.
 - ◆ **Unassigned:** lists Knowledge Base articles that do not belong to a group.

Logical Operators

This table describes the logical operators you can use in condition statements. Certain operators don't appear in circumstances where they are not applicable.

Table 33-1 Logical Operators for Conditional Statements

Logical Operator	Description
=	Equals Use this operator when the entire string is known, such as for an event Name or User name.
!=	Not equals Use this operator to exclude one or more known values, such as events involving a specific network domain or user.
<	Less than
<=	Less than or equal to
>=	Greater than or equal to
>	Greater than
Between	Event occurs within the specified date-time bracket
In	Standard SQL operator for membership test
Contains	Contains the specified substring Use this operator to exclude a large set of events, such as all events whose name contains "virus." Use this operator with caution as it is relatively slow and prone to matching more events than you intended.
StartsWith	Starts with specified substring Use this operator for testing URIs such as event categories or resource locations (for example, Customer or Connector locations in their respective Navigator trees), or to test the root of a hostname (for example, if your web servers are named WebServer1, WebServer2, etc., you could use "hostname startsWith WebServer").
EndsWith	Ends with specified substring Use this operator for domain names. For example, you might want to match events involving the .mil domain.
Like	Standard SQL operator for simple pattern matching for string type: "_" wildcard for single character; "%" wildcard for multiple characters
Matches	For extended regular expression pattern-matching for string types using Perl 5 syntax Supports regular expressions (regex). Note that Matches is used in rules only.
InSubnet	For IP addresses in the specified subnet

Table 33-1 Logical Operators for Conditional Statements (Continued)

Logical Operator	Description
InActiveList	<p>Event appears in the specified active list. InActiveList operates on items in the event and actor schemas. It does not evaluate items in other non-event schemas (such as cases or assets).</p> <p>For example, (a, b, c) InActiveList (a, b, c, d).</p> <p>Note: The InActiveList operator only evaluates single-value attributes, and treats multi-value attributes, such as Actor Account ID and Role, as single-value attributes.</p>
On	Event occurs on this date
Is	<p>Tests "true" for the selected state, null or not-null</p> <p>Use this operator to test whether or not a value has been supplied. You would use this in rules to tell the difference between a string that does not match versus a string that was not supplied. For example, you could use this to find all events that were missing their event names.</p>
BitAnd	Equals, for bitmap fields
EqualsList	<p>Compares one list to another (for example, active list, session list). If the two lists have the same entries, the statement evaluates to "true".</p> <p>For example, (a, b, c) EqualsList (a, b, c).</p>
InList	Determines whether a given item is in a list and, if so, evaluates to "true".
ContainsList	<p>Compares one list to another to see if the second list is a subset of the first.</p> <p>For example, (a, b, c) ContainsList (a, b).</p>
IntersectsList	<p>Compares one list to another. If the two lists have one or more entry in common, the statement evaluates to "true".</p> <p>For example, (a, b, c) IntersectsList (b).</p>

Managed Security Service Providers (MSSPs)

Managed Security Service Providers (MSSP) can use slicing and dicing query-trend approaches to create focused reports for multiple customers built from what are initially broad range queries.

Manager

The Manager is the component that manages, cross-correlates, filters, and processes all security-event occurrences in your enterprise. The Manager includes a Cross-Correlation Engine, Connector Data Manager, tracking and resolution functions, and analytics and reporting capabilities. The Manager also accesses the ArcSight Database.

Navigator Panel

Located on the left side of the [ESM Console](#), the Navigator panel contains all the trees you use to organize analytic and operational [Resources](#), tools, and targets. These resources

come in many types, such as active lists, connectors, rules, and users, all of which are summarized in the topic [“Navigating” on page 94](#).

Notifications

“Notifications” usually refers to the event-related messages sent to e-mail addresses, pagers, or cell phones.


Sending notifications is one among several rule actions that can be performed when a rule is triggered (See [“Rules” on page 974](#)). When you create a rule and add a Send To Notifier action, you will be able to select the notification group that will receive the message. For more information on rule actions, see [“Creating Rule Actions” on page 451](#).

The key entities in the notification structure are Notification Groups, Escalation Levels, and Destinations.

Notification Operation

When a rule that has a notification action triggers, the notification engine notifies all **active** destinations in the first escalation level within that group. The notification engine then waits for a certain time period to receive an acknowledgment to that notification.

You can acknowledge notifications by any one of these methods:

- Reply to the e-mail or page (requires a two-way pager), depending on the type of destination.
- Click the **Notifications** button () in the ESM Console's toolbar to use the Notifications Manager in the Viewer panel. (See [“Managing Received Notifications” on page 658](#).)
- Use ArcSight Web's Notifications feature to read and respond.

The length of time that the notification engine waits for acknowledgement depends on the event severity, and can be configured through the context (right-click) menu's Wait Time setting.

If no acknowledgment is received within the specified time interval, the same notification is escalated to the next level within the group.

This process repeats until there are no more escalation levels or the notification is acknowledged by any of the recipients. The one exception to this procedure is the escalation procedure carried out for **informative** notifications (the Informative option was set while defining the notification action in the rules editor). In this case, notifications are only sent to the first escalation level in the group and do not require acknowledgment.

SMTP is used to send e-mail. An SMTP server must be configured either at install time or through Context (right-click) menu e-mail settings. For notifications, the relevant fields are "from address", which designates the e-mail address of notification e-mail sent from the system, and the "outgoing e-mail server," which is the SMTP server used to send e-mail. It is important to ensure that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses.

POP3 and IMAP can be used to check for e-mail acknowledgments. You can specify these options at install time, or through Context (right-click) menu e-mail option settings. For acknowledgments, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox

from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager providers with host and port information using the Context (right-click) menu Pager Settings option.

Notification Groups are the point of interface between the rules engine that specifies the notification action and the notification engine that sends out the notification. Within each notification group, there can be any number of escalation levels. Each escalation level can contain multiple destinations.

The following groups can help you manage and organize groups and destinations.

Table 33-2 Notification Groups and Destinations

Destination Group	Purpose
Shared	Notification groups and destinations to which logged-in users have permission.
All Destinations	All groups and notification destinations (only Administrators have permissions to this group). Administrators who have inspect and edit permission on the All Destinations group also have permission to change notification settings.

Testing Notification Escalations

Escalation procedures are tested by generating an internal Low Severity event. This event triggers the escalation within the group tested as though a real Low Severity event occurred. Notifications are immediately sent to all destinations within the 1st level (1). If 1st level destinations do not respond to the notifications within the set wait time for Low Severity events (default is 2 hours), the test notification escalates to the 2nd level (2), and so on.

Notification Destinations

Notifications are sent to destinations. Notification destinations may optionally be associated with a user, and when that is done, destination information, such as e-mail address, phone, and pager number, is automatically populated from the user's profile. You can also change the user's destination information without changing the user's profile.

Each destination can be an e-mail, pager, or cell phone contact and have an associated start and end time, which is the time period during the day when the destination is expected to be active. Each destination can also be optionally associated with a user. Associating a destination with a user has these effects:

- When the destination receives a notification and the user is logged into an ESM Console, the user is notified through the notification status button on their display.
- Notifications sent to this destination can also be seen and acknowledged by the user in an ArcSight Web client.

Notification destinations can be managed with drag and drop functionality. You can move or copy notification destinations into escalation levels within the same or other notification

groups from the Administration window. If a group is deleted, the destinations within that group are also deleted.



To copy multiple resources at once, use Copy and Paste. You can drag and drop only one resource at a time.

Notification Acknowledgements

Once you receive a notification, it is important that you acknowledge it within the allotted time window, to prevent automatic escalation to the next-level notification destination.

Immediately acknowledging and resolving significant events is crucial to securing any enterprise. Use the ESM Console's Notifications Manager, or an ArcSight Web client, to check status and help resolve issues. (See also [“Managing Received Notifications” on page 658.](#))

Packages

A **Package** is an resource that contains a set of related resources. A package of resources can be installed or unloaded as a unit. ArcSight Solutions are delivered as packages, but you can create your own packages, as well.

A **Bundle** is a file (with extension `.arb`) that contains one or more packages. You can import and export bundles and install and uninstall the packages that the bundles contain. When you import a bundle, the source file is saved as a file resource (see [“Managing File Resources” on page 665](#)). You can view the original package contents (the package archive) or the current package contents at any time.

An **uninstalled package** is a package that has been imported or created, but not yet installed in the system resource tree (see [“Resources” on page 967](#)). Packages that have been installed can also be manually uninstalled. The default behavior is to install the package when it is imported.

When a package is deleted, the resources it contains can be left in the system resource tree or they can be deleted along with their package.

Packages can have dependencies on other packages or on features such as Pattern Discovery. Two ArcSight Solution packages may share a third package in common, for example.

See also: [“Managing Packages” on page 686.](#)

Partitions

Because the amount of security-event information can be voluminous, it is important to be able to “package” chronological sections of past data for archiving and reasonable retrieval and reuse.

The Database Partition Manager and its initial configuration are established during installation, as described in the ESM Installation and Configuration Guide. Administrators can use the ESM [ESM Console](#) to supervise partitioning activity through a Partitions resource tree in the [Navigator Panel](#).

A database partition is a time-delimited record of database activity. The default period is a day. You use partitions as a means of controlling, storing, and restoring volumes of past security-event information to facilitate later forensic analysis and auditing.

The overall database partition lifecycle includes active (in the database), inactive (archived outside the database), and reactivated (restored to the database) phases. Partitions are generated automatically per schedule, and remain in the Active Partitions branch of the Partitions resource tree according to the time limits set initially during installation. Once a partition's upper bound passes beyond the lower bound of the retention period, it is archived and compressed and refiled in the **Archived Partitions>Inactive Partitions** branch. Once archived, it remains there unless you reactivate it, which moves it to the **Archived Partitions>Reactivated Partitions** branch.



Notes:

- Only partitions beyond the current retention period are eligible for archiving.
- Only ESM users with Administrator privileges can interact with the Partitions resource tree.
- With Oracle databases, past partitions can be compressed online, stored offline, and be restored to the database at any time.

For information on working with partitions from the ESM Console, see [Chapter 29, Managing Partitions, on page 767](#).

Pattern Discovery

ArcSight's Pattern Discovery can detect subtle, specialized, or long-term patterns that might otherwise go undiscovered in the flow of events. This topic discusses pattern concepts. To use pattern discovery, see ["Pattern Discovery" on page 179](#).

A pattern is a distinct, repeating network transaction (event) that is uniquely identified by its source and target IP addresses. Patterns are further qualified by the involvement of selected attributes such as event names or categories. There are, of course, many such patterns and most are normal or benign. The point is to establish and mask out normal traffic in order to let new or atypical traffic stand out. Separating "signal from noise" in this way makes possible very early (day zero) detection and very subtle (low and slow) detection. Once detected, such traffic can be analyzed or responded to.

Pattern discovery uses a **profile** to specify potentially qualifying events on the basis of attributes and time spans. When you apply a profile, manually or on a schedule, it captures a **snapshot** of the events that did qualify, on the basis of raw associations. The contents of snapshots are then reviewed by an analyst to identify event **patterns** to explore in pattern views or the Pattern Inspector.

You define profiles in the Profile Editor in the Inspect/Edit panel. You manage your profiles, snapshots, and discovered patterns through the Profiles, Snapshots, and Patterns tabs of the Navigator panel's Patterns resource tree.

You use the Viewer panel to observe the graphical results of executed snapshots and the patterns those snapshots discover.

Pattern Concepts

A pattern can be any recurring relationship between one or more pairs of source and target IP addresses, that you deem to be significant in relation to certain event attributes. You can regard the patterns you discover as benign or hostile, depending on your policies and postures.

Event-pattern profiles are also constrained by Start and End time limits, filters, and by minimum numbers of associated events (pattern length) and times discovered (occurrences, or pattern support).

Once captured in snapshots, you can examine the event data as raw association information in graphical snapshots, or as graphical patterns in the Patterns tab of the Patterns resource tree.

Each box in a pattern view represents one pattern. The line items in the box are the individual events that were discovered to have associations. Each event component of a pattern (box) relates to the chain of links from which the pattern was derived, in the visual snapshot.

A snapshot view is a graphic hierarchy of related event nodes. The "support" value for each node is the number of times that event occurred in conjunction with its related events. This overall hierarchy is a raw presentation of the events, useful for analysts but not meaningful to operators.

The discovered events all share the attributes specified in the profile. The pattern-discovery process first tests for equality in the values found for the specified attributes. Secondly, it tests for a selected transaction scheme. When the specified minimum number of event relationships reoccur, a pattern exists.

Discovering Patterns

Patterns are identified by first dividing the event stream into multiple transactions. For example, all of the events with a given source and target IP address may constitute a transaction - they represent all the traffic flowing from that source to that target. It may also be helpful to cluster transactions into super-transactions to identify patterns that involve cascading exploits toward multiple devices (that is, device A attacks device B which, in turn, attacks device C).

The events occurring in each transaction are then characterized using a subset of the event fields (for example, the event name or the event category).

Finally, events that frequently occur together in multiple transactions are identified and grouped together. These events are further sub-grouped by support level. For instance, events A and B may occur together 2,000 times while events C and D occur in the same transactions but only 10 times. Pattern Discovery would create two patterns in this case: one for A and B and a second one for C and D. To give another example, events F, G, and H may occur together in the same transactions 100 times while F and G occur without H in 5 additional transactions. All of these occurrences would be rolled together into the same pattern. F and G would have a support of 105 while H would have a support of 100.

Pattern Analysis

Pattern analysis, overall, falls into two basic phases: initial collection, identification, and sorting, and on-going routine processing.

Initial Phase

To accomplish phase one, you generally use broader profiles and more frequent snapshots in an attempt to capture examples of **all** the patterns that appear in your networks.

Once collected, there is a period of initial analysis in which you identify the patterns that are normal or benign. Making these evaluations requires in-depth knowledge and familiarity with the traffic in your enterprise, as well as using the analysis tools. There is no set procedure for this basic collecting and sorting process.

However, the best method for moving officially "uninteresting" patterns **out** of the analysis workflow is to use annotation. While it is possible to use filters for this purpose, it is more reliable to move patterns by annotation to a stage such as **Closed** because this assures that the pattern has actually been inspected and classified.

Routine Pattern Processing

In an environment where the routine event patterns are mostly known and appropriately classified, you focus on the new and as-yet unclassified.

The basic approach to routine pattern analysis consists of two phases: managerial (or triage or workflow initiation), and analysis.

Workflow Management

As ArcSight Pattern Discovery turns up new or unclassified patterns, a designated user needs to review them and start them through the workflow.

Newly discovered patterns are handled by using the Annotations feature to assign them to a stage such as **Follow-up**, or simply **Closed**, and optionally to a particular user.

Specific procedures and decisions, of course, depend on the internal processes of your enterprise and the patterns encountered.

Pattern Analysis

As an analyst dealing with day-to-day pattern discoveries, your basic process can be as follows.

Using the appropriate filters, view the patterns that are new and assigned to you in the Pattern Inspector.

Review these patterns in the Pattern Inspector and compare their transactions historically to those found in other snapshots, using the Snapshot menu.

Use the Show Related Events feature to gain more intelligence about the sources and targets that appear in the patterns.

Remember that events in a grid view are subject to all the ordering, graphing, filtering, reporting, and inspection tools available in the Viewer panel.

Visualize the source and target relationships using Show Event Graph.

Pattern Disposition

Acting on reviewed patterns can include:

- Assigning a new stage or user

The pattern may need further analysis or some other handling, by another user, or can simply be closed. Use the **Annotate Pattern** command to make this disposition.

■ Creating a rule

If a pattern represents activity that needs to be reported, monitored, evaluated, or otherwise acted upon automatically, use the Create Rule command to build a rule based on the pattern's items.



Remember to express an appropriate Time Frame value in the Aggregation tab of the Rules Editor. The scope of a rule's time frame is critical to its effectiveness.

■ Deploying a rule

Once created, if a rule is of value to the enterprise, you should copy or move it to the Rules/Shared/All Rules/Real-time Rules group in the Navigator panel's Rules resource tree.

Pattern Expertise

On a work-a-day basis, the following points will help you make the best use of ArcSight Pattern Discovery.

Workflow

Pattern discovery analysis may also be scheduled. For example, once per hour the prior hour may be analyzed using three different profiles. The patterns discovered by each profile will be stored in a designated group in the Patterns resource tree.

Each pattern also has certain annotation features associated with it that will be familiar to users of trouble-ticket systems. Each pattern can be flagged as being at a given stage (for example, Queued, Acknowledged, Under Investigation, Under Observation, Normal Activity, etc.). Patterns may also be assigned to an user for further investigation.

Initially, many new patterns will be observed and will need to be characterized. Does the pattern represent a threat or is it a result of normal activity on the network? Should a rule be generated? Or is more observation of the pattern required in order to understand it?

Over time, only a few new patterns will be observed each day. These will be delivered in the Queued stage. In the simplest workflow, the ArcSight operator must resolve these patterns or assign these patterns to others for resolution each day.

When patterns are observed again, ArcSight can be instructed to either quietly mark the pattern as observed again or to bring the pattern to the attention of the operator.

Visualization

Event graphs have a clustering ability that makes them very useful when illustrating the interactions represented by a pattern resource.

Suppose events F, G, and H occur together in the same transactions 100 times while F and G occur in 5 additional transactions. All these occurrences would be rolled together into the same pattern. The event graph would cluster the 100 sources where F, G, and H occur together. It would also cluster the sources where only F and G occurred.

To use a somewhat more concrete example, one cluster might represent a Nimda Worm's attempts to infect IIS installations. The second cluster might represent successful infections.

Applications

Pattern Discovery can be used to characterize the traffic on newly protected networks (for example, new customers for MSSPs, new divisions for large corporations, etc.). It can also characterize traffic from new sensors.

Pattern Discovery is also a key element in the ongoing operation of an installation. Using periodic, scheduled analysis, operators can always be kept up to date as new event patterns appear. Frequently, these patterns will indicate new worm or exploit behavior.

Payload

"Payload" refers to the **information carried in the body of an event** network packet, as distinct from the packet's "header" data. (See ["Events" on page 941](#).) While security event detection and analysis usually centers on header data, packet payload (🟩) may also be forensically significant.

Typically, devices discard payloads after a certain period of time. As described in ["Showing Event Payloads" on page 219](#), you can retrieve, preserve, view, or discard payloads using the [ESM Console](#). Since event payloads are relatively large, they are not stored by default. Instead, you can request payloads from devices, for selected events, through the ESM Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the ESM Console. (See ["SmartConnectors" on page 984](#).)

Payloads are downloaded and stored only on demand. Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event source) is stored. Payload retention periods are controlled by the configuration of each source device.

A payload that has already been downloaded and stored in the ArcSight Database can either be manually selected and deleted, or removed based upon the event-retention policy.

If the payload's format is not recognized by the ArcSight Database, its data will not be lost; instead it appears "unparsed" in the event. The event name attribute generally contains the complete data in this case.

Prioritization Fields

[Events](#) include fields whose values help you evaluate each event's overall priority and importance, and determine which events you should investigate first. The prioritization field values take into account a number of factors including:

- Vulnerability of the Target Asset
- Active List Contents
- Open Ports on the Target Asset
- Asset Criticality

The following table lists the event prioritization fields and describes how values for each field are calculated.

Table 33-3 Event Prioritization Fields

Data Field	Description
Model Confidence	Is the target asset modeled and if so, to what degree? This factor depicts the confidence we have in our model. This value depends heavily on whether target assets of interest are modeled in the system. If the only data point for an asset is its ID, then it is likely that this is either an asset range, or an asset that was modeled manually. The fact that the target asset is in the system at all provides some degree of model confidence. Model confidence is higher, though, if the target asset has been scanned for open ports and vulnerabilities.
Asset Criticality	How important is the Asset? This factor encompasses the criticality of the attacked asset.
Relevance	Does it appear probable that the attack succeeded? This factor performs an open port correlation (check to see if the target port is open) and vulnerability correlation (check to see if one of the exploited vulnerabilities is exposed).
Severity	How serious is this attack? This factor encompasses the severity of the event (ArcSight Severity), the severity of the exploited vulnerability (how much it is exposed), any user-supplied filter weighting, and the presence of the Source IP Address in various compromised and hostile active lists.
Priority	Should this event be investigated right away or not? This factor encompasses the criticality of the targeted Asset, user-specified weighting using Filter/weighting pairs, attack severity, and attack success from the other prioritization field values. This value is used to prioritize the investigation of events.

Also see [“Priority Calculations and Ratings” on page 957](#).

Priority Calculations and Ratings

Priority is defined as a value used to prioritize the investigation of [Events](#). This topic describes the calculations used to determine an event's *priority rating* ([“Priority Rating” on page 960](#)).

The calculation of event priority field values is controlled by formulas and weighting specified in the file `$ARCSIGHT_HOME/config/server/ThreatLevelFormula.xml`, which is located with the [Manager](#).

The priority value assigned to an event is essentially the severity the event was assigned by the original reporting SmartConnector, as modified by the weighting schemes set in `ThreatLevelFormula.xml` for model confidence, relevance, severity, and asset criticality.

Each of the factors in `ThreatLevelFormula.xml` evaluates to a value in the range of 0 to 10, and that value has a specific degree of positive or negative influence (weight) on the

original SmartConnector severity value. See [“Prioritization Fields” on page 956](#) for definitions of these factors.

The priority formula consists of 4 factors that combine to generate an overall priority rating. Each of the criteria described in the table below contributes a numeric value to the priority formula, which calculates the overall importance, or urgency, of an individual event.

All values fall in the range between 0 and 10, where 0 is low and 10 is high. A high priority factor generally indicates an event with a higher risk factor. Not every high priority event is necessarily a threat, however. For example, if a critical e-mail server fails, the priority of the events reporting it may be very high, although it does not necessarily represent a threat to your network.

Table 33-4 Priority Factors and Weights

Priority Factor	Factor Weighing
SmartConnector Severity	Connectors report severity values based on the device, the situation, and their configuration. The values range from 0 to 10, and display as Unknown, Low, Medium, High, and Very High. For example, a value of 6 often translates to Medium.
Model Confidence and Relevance	<p>Model Confidence and Relevance (MCR) each have a range of 0 to 10 and are combined to give a net value in the 0 to 10 range. For example, a Model of 10 and a Relevance of 5 would return a value of 0.5.</p> <p>This combined factor establishes the degree of support for the original SmartConnector severity value. A combined MCR of 10 would be full support for an Connector severity value, whereas a 6 would remain a 6. An MCR value of 0 will always force a priority value of 0.</p> <p>The actual formula for MCR is relevance divided by relevance plus model, minus relevance times model, divided by 10, or:</p> $MCR = R / (R + M - R \times M / 10)$ <p>The asset aging function keeps track of the last time an asset was scanned, and incrementally diminishes an asset's model confidence over time to 0 if it hasn't been scanned in over 120 days (the time range can be configured). For more about the asset aging feature, see “Asset Aging and Model Confidence” on page 735.</p>
Severity	An event's potential attack Severity has a range of 0 to 10, with the highest value (10) adding a weight factor of 30%. In other words, if a SmartConnector originally reported a value of 6, and Model Confidence and Relevance supported it, then a Severity value of 10 would add 30% to the 6, boosting it to 7.8. A Severity value of 0 would add nothing.

Table 33-4 Priority Factors and Weights

Priority Factor	Factor Weighing
Criticality	<p>Asset criticality measures how important the target asset is in the context of your enterprise as set by you in the network modeling process by using the standard asset categories /System Asset Categories/Criticality/Very High, High, Medium, Low, and Very Low.</p> <p>Asset Criticality ranges from 0 to 10. The criticality multiplication factor is:</p> $1 + ((c - \text{criticalityZeroPoint})/10) * \text{criticalityBoost} / 100$ <p>Assuming criticality boost = 20 and criticality zero point = 8, the criticality factor weighting will be:</p> <p>C (criticality) value of 10 = $1 + ((10-8)/10) * 0.2 = 1.04$</p> <p>C value of 8 = $1 + ((8-8)/10) * 0.2 = 1$</p> <p>C value of 6 = $1 + ((6-8)/10) * 0.2 = 0.96$</p> <p>C value of 4 = $1 + ((4-8)/10) * 0.2 = 0.92$</p> <p>C value of 2 = $1 + ((2-8)/10) * 0.2 = 0.88$</p> <p>C value of 0 = $1 + ((0-8)/10) * 0.2 = 0.84$</p>

You can modify the formula XML file to customize weighting to reflect your own security priorities and environment.



Changes made to the ThreatLevelFormula.xml file must conform to the format described in [\\$ARCSIGHT_HOME/schema/xml/arcsight-threatLevelFormula.dtd](#).

The priority calculation formulas are made up of basic elements organized by operators called "Sum" and "Difference." These elements are based on simple condition expressions.

- ["Priority Elements" on page 959](#)
- ["Priority Operators" on page 960](#)

Priority Elements

The basic formula elements each return a positive numeric value or zero. Individual element values can be configured by changing the Value attribute associated with the XML element for each condition.

Some of the elements are predicates that test a specific condition. If the condition for a specific element is satisfied, these elements return a positive value; otherwise, the element returns zero.

Predicate elements can also be negated using the Negated attribute. In that case, they return a specified value if the condition is not satisfied, and zero if the condition is satisfied.

Table 33-5 Priority Elements

Prioritization Element	Description
HasOpenPort	Takes a non-zero value if the target asset has a particular port open.

Table 33-5 Priority Elements (Continued)

Prioritization Element	Description
HasVulnerability	Takes a non-zero value if the target asset is vulnerable to the attack captured by the alert under consideration.
HasVulnerabilityMapping	Takes a non-zero value if the signature of the context event has not been mapped to a vulnerability.
HasValue	Takes a non-zero value if the specified event attribute has a value.
InActiveList	Takes a non-zero value if the target address belongs to one of the active lists whose URI is provided in the formula.
Constant	Evaluates to a constant non-zero value. It does not rely on event-specific conditions or any other variable; it remains constant, as the name implies.

Priority Operators

There are two aggregation operators used in the priority calculation formula, **Sum** and **Difference**. The **Sum** operator adds the values of all of the elements that it contains. The **Difference** operator subtracts the sum of all of the values of the subsequent elements from the value of the first element it contains.

Both operators have two attributes, **maxValue** and **weight**.

MaxValue Attribute

MaxValue is used to clip the result after the operator aggregation is carried out. After aggregating, the result is also normalized, which is achieved by dividing the result with **MaxValue**. For example, if we have an element like

```
<SUM maxValue = 100>
```

and it has two child elements, each of which evaluate to 80, the pre-normalization value will still be 100 and not 160. After normalization, the final result for this example will be 1. Similarly, there is an implied lower limit or minimum value of zero on these elements.

Weight Attribute

The Weight attribute is used to scale the result after operator aggregation and normalization are carried out. So, as in the example previously described, if the aggregating element was:

```
<SUM maxValue = 100 weight = 7>
```

the result after normalization is 1, and after scaling, it becomes 7.

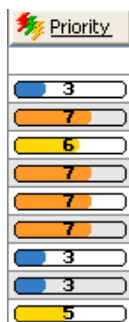
Each of the formulas have an implied maxValue of 10 since each of the four fields in the alert take values in the range 0-10 (inclusive).

Priority Rating

The priority of an event is a calculated overall rating based on **agentSeverity** adjusted by Model Confidence, Relevance, Severity, and Criticality using a detailed formula. (See

“Priority Calculations and Ratings” on page 957.) All five factors are fields in the event schema, and can thus be used in correlation.

The priority rating is color coded and displayed in [Active Channels](#). You can sort events in the grid view according to priority. Priority is a good basis for deciding what to look at first in your event monitoring workflow, and priority is one of many useful criteria on which to build filters, rules, reports, and data monitors.



Priority Ratings in Active Channels: The Priority column in the default live channel view shows the overall priority rating for each event based on calculations from the other five priority criteria.

The score and color scale used in the priority display are as follows:

Table 33-6 Priority Ratings

Priority	Color	Description
0-2	Green	Very low. This event is likely a routine function, such as routine file access or a successful authentication by an authorized user. An event that may have started out with a higher priority can become very low priority when it is proved to have failed.
3-4	Blue	Low. This event is likely a common function, such as a setting change or a scheduled system scan.
5-6	Yellow	Medium. This event is a potential concern, such as pre-attack scan activity, policy violations, and identified vulnerabilities. Medium priority events are often hostile attempts whose success or failure is not confirmed.
7-8	Orange	High. This event is a concern, such as attack formations, potential breaches, or misuse, including traffic to a dark address space, incorrect registry values, or a SYNflood.
9-10	Red	Very high. This event is a grave concern, such as verified breaches or a DHCP packet that does not contain enough data. Items with a very high priority should be investigated immediately.

Queries

A query is an ArcSight resource that defines the parameters of the data you want to report on derived from an ArcSight data source. Queries are used in [Reports](#) either directly or as the basis for [Trends](#) reporting.

Queries can use as a data source the ArcSight Database of events, cases, notifications, modeled network objects (assets), trend data, active list, or session list. Reports then bind data results from queries and/or trends into a display format based on a report template.

See [“Building Reports” on page 331](#) for an overview of all reporting tasks and tools, including how to build queries or trends and how to use a provided or custom [Templates](#).

Queries and Trends

You can use the result of a query as the basis for one or more reports or trends. For a detailed description of how queries and trends can be used together, see [“Query-Trend Relationships in Reporting” on page 370](#).

Building and Running Queries

You can access queries and associated editors in the Reports resource in the ESM Console.

See [“Building a Query” on page 356](#) for information on how to navigate to and use the Query Editor to define query settings (as described in [“Defining Query Settings” on page 357](#)).

Query Viewers

Query Viewers are a type of resource for defining and running SQL queries on other resources, including trends, assets, cases, connectors, events, and so forth. Each query viewer contains an SQL query along with other logic for establishing and comparing baseline results, analyzing historical data to find patterns in network activity, and performing drill-down investigation on a particular aspect of the results.

Previous to v4.5, the only way to run SQL queries against events and resources was to run reports, which use SQL queries and trend-queries. You can use query viewers to run the same queries used for reports, and get results quickly. Then, if desired, you can generate a simple report directly from the query viewer results. Full-featured reporting (with queries, trends, and templates) is still offered for more robust reporting requirements (see [“Building Reports” on page 331](#)), but query viewers provide a shortcut to running those same SQL queries apart from reporting.

Query viewers provide high-level summaries to monitor system health, reveal trends, and allow for drill-down investigation of all types of resources. Query viewers can work with trend tables rather than event tables, and so can return results much faster than [Active Channels](#).

See [“Query Viewers” on page 287](#) for information about using and building query viewers.

Reference Pages

Certain [Resources](#) among those you find in the trees of the [Navigator Panel](#), or events you see in the Viewer Panel ([“Views” on page 1028](#)), have pointers to additional reference information. To check for this information, you right-click an individual event, resource, or resource group and choose **Reference Pages**.

If there are pointers available, you see the Reference Pages dialog box. Select one or more items and click **View** to open them in Web Viewer tabs. If no content is available, click **OK** in the "none found" dialog box.

Some reference page pointers are pre-populated. You can edit these, or add new references, through the **Group Editor** (as described in [“Editing Groups” on page 97](#)). In the Group Editor, use the Group Page text field to specify URLs to reference pages for the group as a whole. Use the **Group Children's Page** field to specify URLs to reference pages for the individual items within the group. Member URLs can be in the form of templates that use the names of ArcSight [Data Fields](#) to query for particular files.

Note also that all the content formerly available through the feature called "Vendor Pages" continues to be available from Reference Pages.

Reports

Reports are an ArcSight resource that provide captured views or analyses of information that can be viewed in the [ESM Console](#) in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). You can also view previously generated and archived reports in an [ArcSight Web](#) client.

You can create reports on all events, cases, notifications, and assets that are in storage.

Reports gather data based on [Queries](#) and [Trends](#), and use report [Templates](#) to determine display and file formats.

For an overview of reporting in Arcsight , including information on queries, trends, and templates, see [Chapter 14, Building Reports, on page 331](#).

Working with Report Templates, Queries, and Trends

Reports show results of pre-defined queries and trends using custom-designed or provided templates. Once you have source data defined in queries and/or trends, you can design reports to present the data in charts and tables.

The Reports resource includes the following tabs and editors for the following elements that make up reporting:

- Templates ([“Using Report Templates” on page 335](#))
- Queries ([“Defining Query Settings” on page 357](#))
- Reports ([“Defining Report Settings” on page 387](#))
- Archives ([“Archiving and Scheduling Reports” on page 431](#))
- Trends ([“Defining Trend Settings” on page 372](#))

A Report Wizard is provided for creating reports quickly. (See [“End-to-End Reporting Examples” on page 407](#) for an example of using the report wizard.) From within the wizard you can choose a data source (one from among available [Queries](#), [Trends](#), [Active Lists](#), or [Session Lists](#)) and one of the available [Templates](#) to use for the report.

Viewing and Managing Reports

You have the flexibility to broaden or narrow the data extracted from the ArcSight Database using report parameters and conditional logic statements. You can also create delta reports to show the difference between two sets of parameters. With this flexibility, you can create custom reports that are tailored to meet your reporting needs. Also, there are display groupings of "Report Definitions," where you define what report you want to generate, and "Report Output," where the actual reports are generated and stored.

Archived Reports

Once a report is created, it can be saved (archived). Archived reports are retrieved for immediate viewing, without requiring you to regenerate the report. In addition, you can schedule a report for automatic archiving, on a yearly, monthly, weekly, daily, or hourly basis. All reports are displayed at the ESM Console in the Report Viewer. You can also run, archive, and delete reports through ArcSight Web clients.

Report Groups

Reports can be created and edited in the <user ID>'s Reports group or the Public Reports group on the Report Definitions tab. Reports can be deleted based on your permissions. Reports created in the <user ID>'s Reports group is available only to that user and those to whom the user gives inspect or edit permission. Reports created in the Public Reports group are available for all users to create, edit, or delete. Reports can then be run from the Reports resource tree and the Viewer panel. For more information, see ["Running Reports" on page 423](#).

You can manage reports in the Reports window of the ESM Console. The Reports resource tree has two tabs: Report Definitions where reports are managed and Report Output where archived reports are stored for viewing. The Report Definitions tab lists and organizes all reports in one of the following groups.

Table 33-7 Report Groups

Report Groups	Description
<user_ID>'s Reports	Reports the user has created.
Shared Reports	Reports that other users have already shared with the logged-in user.
ArcSight Reports	Reports provided as defaults, which you can use as-is or to create custom reports.
Public Reports	Reports to which all users have read permission.

If you have Administrator access you will have another group named All Reports that contains all user report groups and their reports.

The Reports Output tab lists all archived reports. Archived reports are listed as a file on the Report Output tab for quick access and retrieval. When you archive a report from the Report Definitions tab, that report is sent to the Report Output tab. If other users archive a report and share it, the report is listed in the Shared group on the Report Output tab.

Delta Reports

A delta report is one that shows the difference between two sets of parameters used in a single report. The report also shows the data for each of the parameters.

When you run or archive a delta report, an internal event is sent to the Manager. This event contains the following data fields and values.

Table 33-8 Delta Report Event

Delta Report Field	Description
Event Name	Delta Report Generated (Report: <i><ReportName></i>), where <i><ReportName></i> is the name of the report.

Rules can be created using the delta report data fields.

Report Parameters

For date parameters, type in the text fields, click the drop-down arrows or click the time buttons to select a time range.

For date and time data fields, you can also type an actual date value, such as 10/12/2010 8:54:00 AM, or you can use special system variables such as:

- **\$CurrentDateTime**: for the date and time the report is run, the system variable is replaced by the current date and time value when the report is run.
- **\$CurrentDate**: for the date the report is run, the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run.

You can also specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: **\$CurrentDate - 7d** for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or **\$CurrentDateTime - 12h**, which evaluates to the current date time minus 12 hours.

Select a **Report File Format** from the drop-down menu.

Reports can be archived in PDF, HTML, Excel, Comma Separated Value (csv), or Rich Text Format (rtf). The default PDF format should be used when archiving reports. Compared to PDF reports, other reports may lose formatting information and will appear differently. In addition, Excel format is more memory intensive than PDF.

Running Reports

For information on how to run a new or archived report, see [“Running Reports” on page 423](#).

ArcSight-Provided Reports

There are more than 200 reports listed in the ArcSight Reports group which you can use to immediately generate reports or use as templates to create or customize your own reports.

The ArcSight Reports group contains all reports further subcategorized in one of these report subgroups.

Table 33-9 ArcSight Reports

Report Group	Description
By Attribute	Provides various reports providing details based on connector type, severity, device, event name, source, target, and target port.
By Event Direction	Provides reports based on inbound or outbound attack and alert direction.
By Event Volume	Provides reports based on most frequent and least frequently occurring events.
By Sensor	Provides report by type of sensor or connector, for example, firewall, router, intrusion detection, etc.
By System Object	Provides reports by type of object, for example, active lists, assets, cases, and notification.
Custom Reports	Provides varied example reports demonstrating moving averages and vulnerability.
Example Canned Reports	Provides reports showing various types of asset reports and different report layout designs.
Internal Reports	Provides various reports providing information on system usage, performance, rule operation, and resources.

You can run each of the reports to see the type of detail and information each provides. In addition, you can view the notes, settings, and conditions set on each tab to see how each report is constructed. To use a report as a template for creating or customizing your own reports, copy an existing report to a new report group (using drag and drop to copy an existing report to the new report group). You can then rename the new report and start making changes to the new report.

Report Templates

Report templates are a component of Reporting resource tools.

To provide more flexibility in reporting, the report template tools include a rich offering of ready-made templates and a template design wizard for more customized [Reports](#). Template definitions determine how data from [Queries](#) and [Trends](#) is displayed in a report. You can create and adjust templates to specify which data is displayed, what visual elements are used (variations on tables, charts, graphs, and so on), the layout of those elements, the report output file format, and much more. A template consists of report design elements, such as headers, footers, title bars, charts, and tables, arranged on a page according to a layout specification.

Templates can accommodate input from multiple queries and show multiple visual elements, such as three charts and a table each pulling from a different data source, in a single report.

For more information on templates, see [“Using Report Templates” on page 335](#).

See [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools.

Resources

The Manager handles the logic used to process events as objects called **resources**. Active channels, data monitors, filters, cases, assets, queries, trends reports, rules, and packages are all examples of resources.

A resource defines the properties, values, and relationships used to configure the functions the Manager performs. Resources can also be the output of such a configuration (such as archived reports, or Pattern Discovery snapshots and patterns).

The Manager has over 30 different types of resources and comes with hundreds of these resources already configured to give you functionality as soon as the product is installed. These resources are presented in the Navigator panel of the ESM Console and ArcSight Web interfaces.

This topic provides an overview on working with resources in the ESM Console. Resources in general are discussed in more detail in the topic "Resources" in *ESM 101*.

Valid and Invalid Resources

Valid resources show up in the Navigator with their associated icons as described in ["Navigating" on page 94](#). A resource can "break" or become "invalid" either because it is constructed improperly (for example, when an active list schema does not match the underlying table) or because another resource it depends on is missing from the database (for example, when a rule references an unavailable filter). The latter can happen when a resource used in other resources is deleted from the Manager, or not retained during an upgrade, import, or export.

Invalid resources show up in the Navigator as broken or torn.

For example, the Navigator displays a valid filter like this: , and an invalid filter like this:





A valid resource is fully available to other resources that reference it, and can participate in the [Events](#) flow, [Trends](#), [Reports](#), [Data Monitors](#), [Active Channels](#), [Filters](#), [Rules](#), and so forth.

An invalid resource cannot participate in the event flow or other resources in real time. For example, invalid [Assets](#) cannot participate in event asset resolution. Correlated events in which the source or target address points to the invalid asset are not generated. Similarly, an invalid rule does not trigger and generate correlation events.

Fixing and Validating Resources

When a resource becomes invalid, its Editor includes a **Validate** button that you can use to test and validate the resource after you fix it. Clicking the **Validate** button on a resource that was previously broken results in a check of the resource logic and dependencies. If the system determines the resource is now valid, the resource icon in the Navigator is updated to reflect a working resource. If the system determines the resource is still broken, it displays an error message describing the problem.

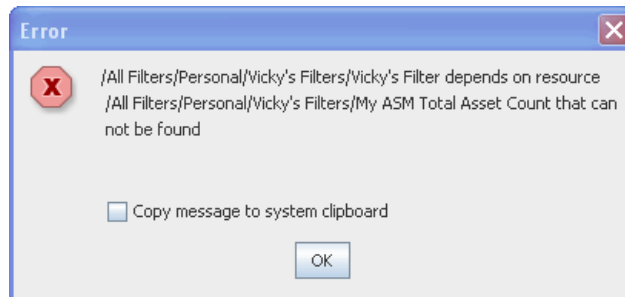
The general flow of steps to fix and validate a resource are:

- 1 Identify an invalid resource. Sometimes problems with filters (see [Filters](#)) or [Rules](#) (which are used in many other resources) are a result of broken resources. (A valid resource looks like this: , and an invalid resource looks like this: )

For example, if "My Top Threats" filter depends on "My Hotlist" filter, removing "My Hotlist" filter breaks "MY Top Threats" filter.

A scheduled job (like a scheduled rule group or archived report) can also break if one of the resources it depends on is missing. The broken icon for a scheduled job shows up on the Current Jobs list. (See ["Scheduling Jobs" on page 977.](#))

- 2 If you do not already know why a resource is broken, open its editor (double-click the resource in the Navigator panel) and click the **Validate** button in the resource editor. This will give you an error message that describes the problem. The error dialog includes a Copy button for copying longer messages to an external editor.



- 3 Fix the problems with the resource. This may involve adding back in missing resources or rebuilding the resource to fit various other requirements as described in ["Troubleshooting \(Requirements for Valid Resources\)" on page 969](#) below.

To continue with our example, adding back in the filter "My Hotlist" would fix the problem we mentioned in [Step 1.](#)

- 4 In the resource editor(s), click **Apply** to save changes to the resources you modified.



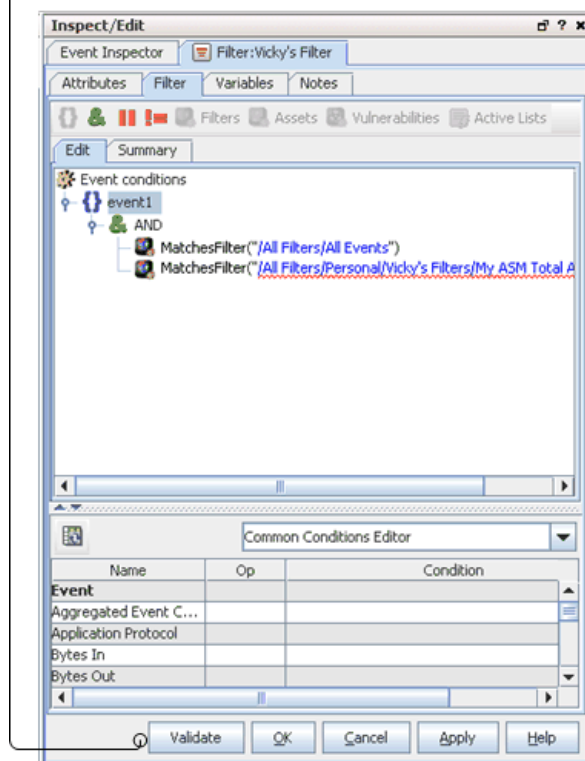
For problems that can be validated on the local client, you can click **Validate** before clicking **Apply**. If the resource is fixed, its "working" icon is immediately reflected in the Navigator. For other types of problems, however, you need to **Apply** the changes to the resource before you **Validate** the resource. This is because some types of changes must be processed on the Manager to determine dependencies and relationships to other data not available on the local client.

If you think you have fixed a resource but it is still not showing as fixed in the Navigator, make sure you **Apply** all the changes you made to it and then click **Validate** again.

- 5 In the resource editor for the resource that was broken, click **Validate**. If the resource passes validation, its icon in the Navigator updates to reflect a working resource.

In the resource Editor for the resource that was broken, click the **Validate** button. If the resource passes validation, its icon in the Navigator updates to reflect a working resource. Otherwise, the broken icon remains and an error message describes the problems.

Some problems require saving fixes to the Manager, so be sure to click **Apply** and save changes to resources you fix before you click **Validate**.



To validate a scheduled job, click the **Open scheduled jobs list** tool button (🕒) to display scheduled jobs in the Viewer, right-click the job you want to validate, and choose **Validate** from the context menu. If the job passes validation, its icon in the Current Jobs list updates to reflect a valid task.

Troubleshooting (Requirements for Valid Resources)

The most common cause of an invalid resource is a dependency issue; another resource that the broken resource depends on is missing from the database. Some resources have additional requirements or limits that can also affect validity. Following is a summary of requirements for creating valid resources.

If any of these requirements are not met, the resource will break. To fix the resource, edit its definition to be in line with these requirements.

- **All Resources** - If the definition for a resource references another resource, the referenced resource must be available in the Manager database. This requirement is true for all types of resources.
- **Devices and Assets** - Each asset address must be unique within a zone, an asset can belong to one zone only, and the asset IP address must fall within the address range of its network zone.

- **Device and Asset Ranges** - Start addresses must be less than end addresses, asset ranges must be within the address range of the associated network zone, and asset ranges should not overlap another asset range in the same zone.
- **Zones** - Start addresses must be less than end addresses and network zones should not overlap other zones in the same network.
- **Reports** - Report templates cannot contain more than 20 charts or more than 15 tables.
- **Active Lists** - Active List schema must match the underlying table and must not include programming errors.

For more information, see the *Administrator's Guide* topic on "Resource Validation".

Automatic and Manual Validation

You can validate individual resource manually through the ESM Console with the **Validate** button as described above.

Resource validation takes place automatically during an upgrade, [Packages](#) import or export, or when you insert or update a resource. Administrators can use a stand-alone, command-line utility on the Manager machine for validating resources and generating validation reports on an off-line Manager. This is often useful after an upgrade.

For more information, see the *Administrator's Guide* topic on *Resource Validation*.

Resource Attributes

The processed [Resources](#) are composed of several attributes, each of which is a data field with its own characteristics. The data fields common to all resources are described below.

Each attribute has both a **Label** that you see in the ESM Console and a unique **Script Alias** you use to refer to the attribute in filters, rules, or Velocity templates. The **Data Type** lets you know how to handle the attribute. (Also, see "[Resources](#)" on page 967 for information on locked and unlocked resources, and "[Common Resource Attribute Fields](#)" on page 684 for information on viewing and/or editing these fields in resource editors.)

Table 33-10 Resource Attributes

Group	Label	Script Alias	Data Type	Description
<i>Resource Type</i>	Name	name	String	The name of the resource.
Common	Resource ID			Read-only field that shows the ArcSight system resource ID.

Table 33-10 Resource Attributes (Continued)

Group	Label	Script Alias	Data Type	Description
	External ID	externalId	String	An identification string suitable for, and which can be referenced by, systems outside ArcSight. Common applications of External IDs include appropriate naming for Case and Asset resources that are tracked in common with defect reporting or vulnerability-management systems. Your administrator can advise you on the correct values for this field, if applicable. For Vulnerability resources, this field will be filled in with an ID of the format <standards body> <id>, such as CVE CVE-1999-200.
	Alias	alias	String	An identification string suitable for referencing resources. A given alias will appear in place of the resource's name everywhere it may be seen. Your administrator can advise you on the correct values for this field, if applicable.
	Description	description	String	An editable text description of the resource or other related information. This text appears as a tooltip to any user who has ESM Console access to the resource.
	Version ID			A string showing a globally unique version ID for the resource.
	Deprecated			Indicates whether a resource is current or obsolete. If this field is blank, the resource is current. If this field is check marked, the resource is "deprecated" or obsolete. Click the box to toggle the checkmark on or off.
Assign	Owner	owner	String	One or more users who are interested in this resource.
	Notification Groups	notificationGroups	String	The ArcSight user groups selected from the Users resource tree who should be notified about this resource.
Parent Group	groupName Link		Resource Group	Each resource group containing this resource. A resource exists in more than one group when you choose Link instead of Copy or Move.

Table 33-10 Resource Attributes (Continued)

Group	Label	Script Alias	Data Type	Description
Creation Information	Created By	userName	User	The identity of the ArcSight user who created this resource.
	Creation Time	creationTime	DateTime	The time that the resource was created.
	Time Since Creation	timeSinceCreation	String	The elapsed time, in days, hours, minutes, and seconds since this resource was created.
Last Update Information	Last Updated By	lastUpdatedBy	User	The identity of the ArcSight user who last updated this resource.
	Last Update Time	lastUpdateTime	DateTime	The time that the resource was last updated.
	Time Since Last Update	timeSinceLastUpdate	String	The elapsed time, in days, hours, minutes, and seconds since this resource was last updated.

Rule Actions

Rule actions are automatic procedures that occur when all rule [Conditions](#) and threshold settings have been met. (See also [“Rules” on page 974](#).) You can choose to be notified of a triggered rule at the [ESM Console](#) or through the Notifier (see [“Notifications” on page 949](#)), have information about the [Events](#) that triggered the rule sent to a case or active list (see [“Cases” on page 835](#) or [“Active Lists” on page 790](#)), or automatically execute a command line function. You can also assign more than one rule action to any rule.

The task steps for these activities are available in [“Creating Rule Actions” on page 451](#).

Active List Rule Actions

The Active List rule action automatically organizes rule-associated IP addresses in active lists. Once a rule is triggered, the Active List rule action adds IP addresses from events that have triggered the rule to an active list. The Active List rule action can also move or remove IP addresses from active lists. Rules can also be created on active lists.

When the rule is triggered, the rule action takes all associated addresses (source or target) and adds those addresses to an active list. For example, if a rule is triggered with an action that has Source Address and Suspicious List selected, all source addresses are sent to the Suspicious List in the Active Lists resource tree.

Execute Connector Command Rule Actions

Rule actions can automate the process of sending commands to SmartConnectors and through them to the devices they support. While all SmartConnectors can respond to the basic commands (for example, start, stop, pause, continue, and terminate) some that represent more complex devices can respond to more complex commands. For example, rule actions can tell the Check Point Firewall SmartConnector to tell its device to block a

particular IP address. See [“Creating Rule Actions” on page 451](#) for a description of the actual steps involved.

It may be helpful to note that this feature is in effect an automated solution for using the capabilities described in [“Sending Control Commands to SmartConnectors” on page 715](#).

The specific SmartConnectors that support this capability, and the additional commands they can process, are subject to change. Consult your administrator or representative for more information.

Rule Conditions

A rule is a programmed procedure that can analyze network [Events](#) and generate additional correlation events, as determined by security policy. (See also [“Rules” on page 974](#).) When creating rules, you define the rule events and [Conditions](#), thresholds, and [Rule Actions](#). Conditions define which events trigger the rule, thresholds set when a correlation event is generated, and actions state which responses are taken when a correlation event is generated. To define rule events and conditions, thresholds, and actions, begin by determining the following:

- Which event occurrences do I want to be aware of? This determines the rule's **events** and **conditions**.
- How many times do I want the event or events to occur and within what time frame? This determines the rule's **threshold**.
- What actions should automatically occur when an event is generated? When should those actions occur? This determines the rule's **actions**.

A rule requires at least one event and one condition. When you create or edit a rule, the ESM Console provides a Conditions tab in which you can specify events and define the conditions for a rule. (The Conditions tab is described in the topic on the [“Common Conditions Editor \(CCE\)” on page 846](#).)

Rules are first constructed by creating condition statements. Condition statements contain a data field, logic operator, and data field value; so you can create complex logical expressions by combining one or more individual conditions to match the events you want to trigger a rule.

When you first create a new rule, a default event named [event1](#) appears as a branch under the Event conditions tree for the new rule. (The event name is also commonly referred to as the event “alias”.) You can use this name or select a different event to use in the condition. Since rules can have numerous events, event names should be unique and descriptive within the same rule. For example, if monitoring Cisco Router denied events, [Cisco Router denied](#) could be the event name. The event name appears as a branch under the Event conditions tree.

When defining the condition for an event, the Conditions tab provides three columns, Name, Operator, and Condition. These three columns are combined to create [<data field> <logic operator> <data field value>](#) condition statements. For example, if monitoring a Cisco Router, the condition statement could be [Device Product = Cisco Router: Device Product](#) as the data field, [=](#) as the logic operator, and [Cisco Router](#) as the data field value.

When adding conditions, you need to decide how to tie the new condition to any existing conditions. To add more condition statements to an event, you can use logical operators AND, OR, or NOT to specify how to evaluate the condition statement that contains more than one individual condition.

Besides specifying events in a condition, you can also add filters, assets, and vulnerabilities to rules as new conditions. A filter condition monitors if an event occurs in a particular filter. If an event does occur in that filter, a correlation event is generated (see [“Specifying Rule Conditions” on page 442](#)). Asset conditions state whether your enterprise assets are targets or sources of events. An asset condition states if an event occurs and the selected asset is the source or target, generate a correlation event. Finally, you can also use an existing enterprise vulnerability to create a rule condition. A vulnerability condition states if an event occurs with the vulnerability selected, generate a correlation event. For more information on vulnerabilities, see [“About the Network Model” on page 731](#).

In some cases, however, you may want to specify more complex rule processing to restrict the events that actually cause a rule to fire. There are two additional elements you can include to specify more complex rule conditions: rule thresholds and aggregation. (See [“Specifying Rule Thresholds and Aggregation” on page 449](#).)

Rules

An ArcSight rule is a programmed procedure that attempts to correlate incoming network [Events](#) and generates new events that report on correlation when it occurs, as determined by security policy. Rules also apply [Conditions](#) and perform [Rule Actions](#).

Canned rules can be viewed, edited, and used as templates to create your own enterprise-specific or custom rules. To see what's available, browse the description provided with each rule in the [ESM Console](#).

Different users can simultaneously create rules from their ESM Consoles. Once created, all rules are sent to the [Manager](#), which updates any other individual ESM Consoles. Updates to [Resources](#), including rules, are automatically refreshed every few seconds so that clients get the latest changes from other clients.

Information on creating, deploying, and managing rules is provided in Rule Authoring.

Rules Processing and Correlation

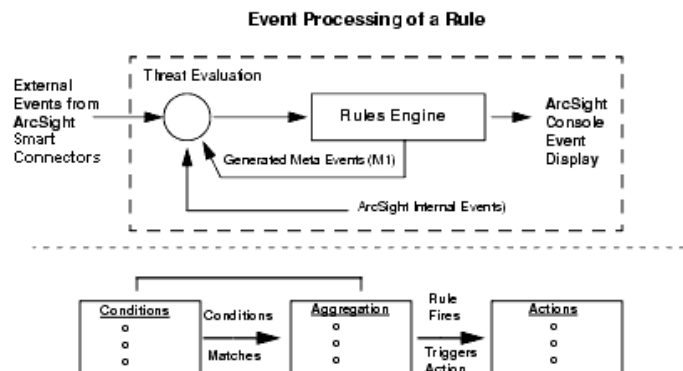
A rule has three parts: a condition, threshold and time window aggregation, and an action. The condition states `if exists` and `satisfies` expressions and the action states `do` expressions. A rule states `if [one or more conditions] exist and satisfy the rule, then do [action expressions]`. A rule can have one or more rule conditions. If there is one condition, the rule acts as a filtering tool. If there is more than one condition, the rule acts as a correlation tool. A rule can be created for any incoming event from one or more event generators, with various conditions, logic statements, and threshold and time window qualification of events.

Components of a Rule



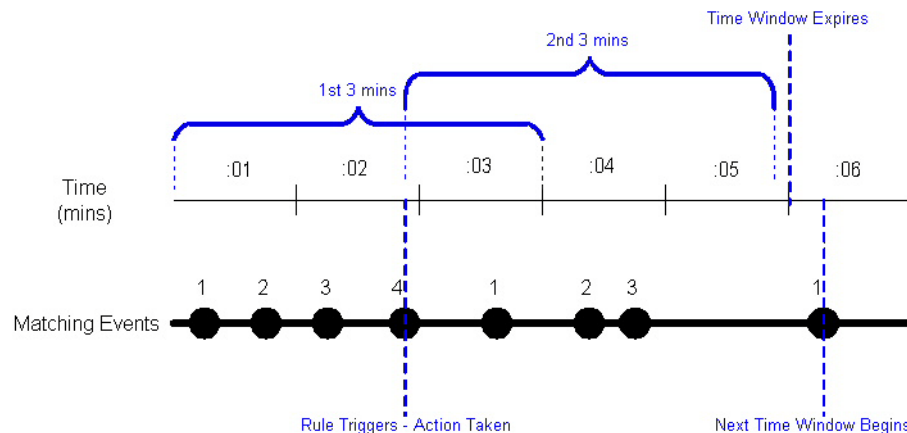
The Correlation Engine, a sub-component of the Manager that handles rules, is not the same as a database query engine. For example, the Correlation Engine can perform a complex join across several events in real-time and aggregate the response to these events. In order for the Correlation Engine to do this in an efficient manner, it keeps a list of events that match each condition. These are referred to as **partial matches** because they satisfy part, but not all, of the rule's conditions. As new partial matches occur, the Correlation Engine attempts to pair them with previous partial matches in order to construct a full match. At that point the Correlation Engine may aggregate that match with

others while it waits to pass some threshold (which can be either time or a target number of full matches). If the threshold is passed the Correlation Engine generates a derived event and performs the other actions associated with the rule.



It is important to note that all rules containing a specified threshold and a time window expiration follow a certain process in order to generate a derived event and perform an action. If a rule's threshold is passed, but the time window expiration has not been met, then the Correlation Engine compensates for this by generating a derived event, performing an action, and moving (or sliding) the time window until it expires. If this rule process was not in place, under certain conditions, rules would trigger on nearly every event in a short amount of time and which would cause a large amount of useless events to be displayed or actions taken.

For example, assume that you created a rule with an event threshold of 4 and a time expiration window of 3 minutes that sends a notification every time the threshold is met. This rule's process would look like the following:



In this example, the 4th incoming event occurred before the time window expired, so the rule triggered at the 4th event and the time window shifted adding another 3 minutes. Within the 2nd 3-minute interval, the rule restarted its incoming event count; however a 4th event did not occur so the rule did not fire. Note that the time window did not expire until the 5th minute had passed. If a 4th event had occurred before that time then the shifting process would have begun again. If you were to show the rule chain for this example, it would display the information for incoming events 1-4 that occurred within the first 3 minutes. Time windows expiration triggers fire at the minute boundary unless the next time window starts before the minute boundary.

The Rules resource tree in the Navigator panel offers a default collection of rules that you can use directly or as a template for creating your own custom rules.

For example, there are rules predefined to detect and perform actions based on ArcSight system rules processing and SmartConnector status. Other rule groups detect and respond to attacks and suspicious activity, specific types of attacks on various sensor types, network components, or assets, and report attack results or successes.

Rule Groups

Rules are organized into groups to store similar rules in one location. The Rules tree in the Navigator panel organizes rules into the following groups.

Table 33-11 Rule Groups

Rule Groups	Description
<userID>'s Rules	The user's home directory, where they have read/write permissions to author rules.
Shared Rules	Rules that establish the permissions for the current user.
Real-time Rules	Rules that are run against real-time events.
Public Rules	The rules that any user can read.
System Rules	The global rules provided by ArcSight.
Unassigned	Rules that do not belong to any directory. These can be rules that have not been inserted into any directory, or their parent directory has been deleted.

If you have Administrator access you will have another group named All Rules that contains all user rule groups and their rules.

Scheduled Rules

You can deploy scheduled rules to run at a specified time interval (such as hourly, daily, or monthly). This is a useful alternative to real-time rules in situations where you want to deploy rules that take into account historical data along with live data, or when you simply want to control when the rules are run. The scheduled rules engine can process historical data, take real actions, and generate correlated events which are the same as those generated by the real-time rules engine.

Only rule groups can be scheduled. To schedule one or more rules, you add the rule(s) to a rule group, and then edit the rule group to add a scheduled job. For more information, see [“Scheduling Rules” on page 463](#).

Rule-triggering Timing

Rule-processing sessions are associated with “Group By” tuples (for example, a particular pairing of source and target address).

A match occurs when all the conditions of the rule are met.

The first match associated with a new tuple creates a new session. It also triggers [onFirstEvent](#) and an [OnEveryEvent](#). The system then sets the start time for the first time window.

Subsequent matches will trigger [onSubsequentEvents](#) and [onEveryEvent](#).

If enough matches occur to pass the threshold count **before** the time window expires (which is defined as [start time + time window > current time](#)), then the Manager triggers [onEveryThreshold](#) and one of either [onFirstThreshold](#) or [onSubsequentThreshold](#) and it resets the start time for the next time window.

If a time window ends without meeting the threshold, then "final aggregation" occurs. The [onTimeWindowExpiration](#) option is triggered and the session is disassociated from the tuple.

The next match with the same tuple (or, in fact, any tuple, same or new) will cause the whole process to repeat.

Rule Chains

When rules are designed to trigger in a series, in order to capture or act upon correlated events within a specified interval or at a particular threshold, they are referred to as rule chains.

ArcSight Variables

You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as [\\$Now](#) and [\\$CurrentDateTime](#). The same is true for time elements, including [s](#) (second), [m](#) (minute), [d](#) (date), [M](#) (month), [w](#) (week), and [y](#) (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign; for example, "Source Address" would be [\\$sourceAddress](#).

Rules Editor

The Rules Editor is a panel in the ESM Console for creating and editing rules.

The rules you create or edit are stored in [.ARL](#) (ArcSight Rules Language) files.

For more information, see [Chapter 16, Rules Authoring, on page 439](#).

Scheduling Jobs

You can schedule some tasks to occur automatically. Specifically, this feature is available for archiving and scheduling reports, pattern discovery snapshots, and rules. See these topics for information specific to scheduling jobs for particular resources:

- ["Scheduling Report Tasks" on page 433](#) for information on how to schedule reports individually or by group
- ["Scheduling Rules" on page 463](#)
- ["Scheduling a Snapshot" on page 192](#)

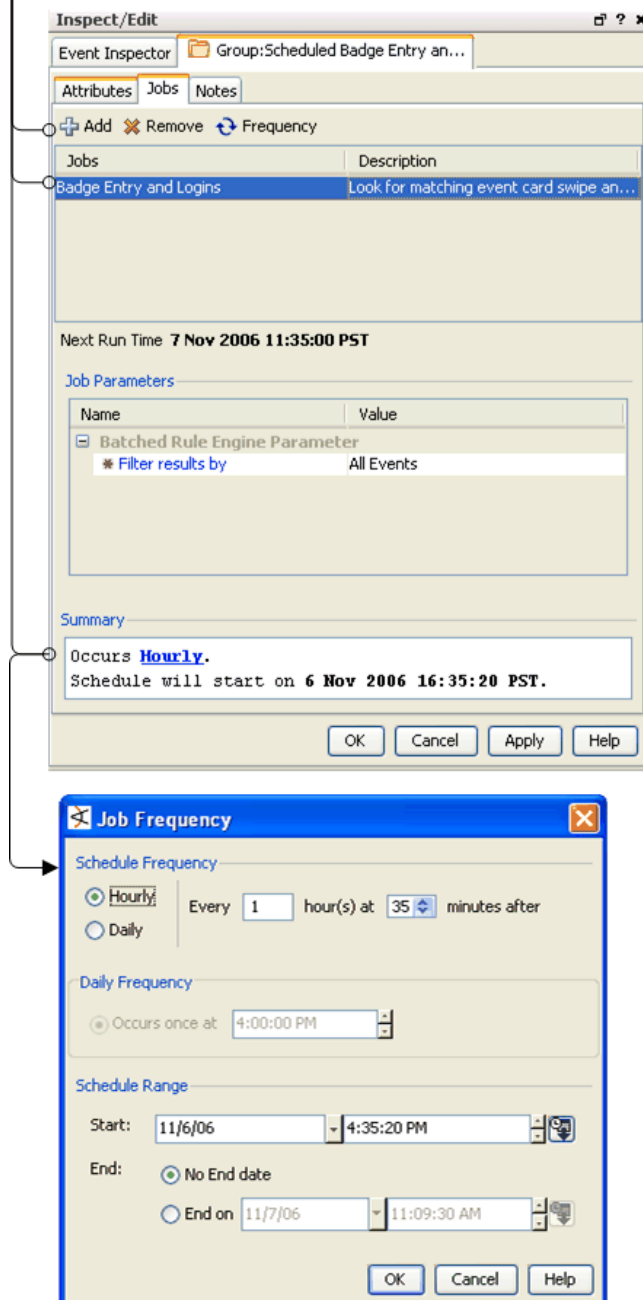
This topic provides general information on how to schedule a job for any resource and view all scheduled jobs.

To schedule a job


- 1 Click the **Jobs** tab in the Editor for a group
- 2 Click **Add** on the Jobs tab. This brings up the Job Frequency dialog.
- 3 Define the schedule frequency and range of the job (start and end dates, or indefinite).
- 4 Click **OK** to save the task and close the dialog.

Double-click to modify the default job name and description, or click **Add** to add a new scheduled job.

Click the **Hourly** link in the Summary to bring up the Job Frequency dialog where you define the schedule frequency and range of the job (start/end dates). The rule schedule can have an end date or be defined to run indefinitely.



To view all scheduled jobs

Click the **Open scheduled jobs list** tool button (). The scheduled tasks are listed in the Viewer panel under "Current Jobs".

Click a job in the list. The status of previous and pending runs for that job are shown in the "Scheduled Runs for <Task>" list on the bottom part of the Viewer panel.

Troubleshooting Tips

If the Manager system clock time is changed after jobs are scheduled, some scheduled jobs might be kept in pending status temporarily, and/or synch back up on subsequent scheduled run times. It is best not to make dramatic adjustments to the system clock on a Manager on which critical jobs are already scheduled. If this problem occurs and does not correct itself soon enough, stop the Manager and re-set the system clock to the original date/time, or re-schedule the jobs.

Schema

The schema is more than 400 data fields of the normalized data recorded by the device (sensor) that reports events to the SmartConnector. The schema is the culmination of the normalization process, and the backbone of the data structure that drives correlation.

The schema also includes fields that support resources that operate on other resources, for example, actors, assets, and cases.

The schema can now also be expanded with user-defined fields. Domain field sets leverage additional data from SmartConnectors for defining use cases beyond traditional security (see ["Domain Field Sets" on page 491](#)). Global variables enable you to define a variable that derives data from fields in the schema, which can be used in multiple places (see ["Global Variables" on page 477](#)).

Avoiding Field Naming Collisions

With the addition of user-defined fields to the schema comes the possibility of name collisions. In most cases, field names, regardless of type, must be unique to be resolved. The following attributes are checked to verify that names are unique for all types of data fields:

Table 33-12 Fields Validated for Uniqueness

Field Type	Field Validated
Event	name, alias, field name, display field name
Actor	name, alias, field name, display field name
Asset	name, alias, field name, display field name
Case	name, alias, field name, display field name
Custom columns (public)	N/A
Custom columns (private)	N/A
Global variable	name, alias, field name
Local variable	name, alias, field name

Table 33-12 Fields Validated for Uniqueness (Continued)

Field Type	Field Validated
Domain field	name, alias, field name

The Manager uses the following policy to manage potential naming collisions.

- The Manager grants names on a first-come-first-served basis. The domain field or global variable that comes later with the same name as another field will either be marked as 'disabled' if added in batch mode (such as from an archive file or package) or 'denied' when being created directly from the ESM Console.
- Name collision is allowed among resource and event-based system fields. For example, the name field of event can be the same as the name field of an actor.
- Global variable names must be unique across all types of schema fields. For example, a global variable cannot have the same name as a domain field or event.
- The name of a local variable must be unique across all types of fields: event fields, resource-based fields, global variables, and other local variables in the same containing resource.

Table 33-13 When field names can be granted a name in use by another field

When Requesting a Name for a ...	Can the name be the same when in use by		
	Global Variable	Local Variable	Event, Actor, Asset, Case
Custom Cell	Yes	Yes	Yes
Domain Field	No	Yes	No
Global Variable	No	Yes	No
Local Variable	No	No	No

The following exceptions apply to avoid naming collisions with existing customer-created fields and ArcSight-supplied global variables during upgrade to a future release:

- Existing custom columns added to active channels (see [“Customizing Grid Columns” on page 152](#)) are excluded from name collision validation. Custom columns can have the same names as event fields, resource fields, global variables, and local variables, and vice versa.
- New global variables can have the same name as an existing local variable. A new local variable cannot have the same name as an existing global variable, but if a local variable already exists with a particular name, a global variable with that same name can be added without a name collision error.

Send Logs

ArcSight components provide various types of information to log files. For example, the Manager logs are located in: `ARCSIGHT_HOME/logs/default/server.log`. Various Manager utilities write logging information into different sets of log files. (The archive utility writes to the `archive.log`, the database init utility writes to the `dbwizard.log`, and so forth). Each of those sets can consist of multiple files. The number and size of the log files are configurable on the Manager under

[ARCSIGHT_HOME/config/server.properties](#). ESM Console and ArcSight Web also generate and store log files.

ArcSight Customer Support may request log files and other diagnostic information to troubleshoot problems. The **sendlogs** utility automatically locates log files and compresses them. You can then store them or manually email them, if directed.

The Send Logs utility does not send any log files automatically.

Guidelines for Using the Send Logs Utility

- Although Send Logs is accessible to any user logged into an ArcSight component, only administrators have permission to collect logs on remote systems. Non-administrative users can only collect local logs from the component where they are logged in.
- SmartConnectors must be running version 4037 or newer to support remote collection of logs with Send Logs (using an ESM Console or the Manager)
- You can only collect local logs on SmartConnectors or ArcSight Database. That is, if you run the Send Logs utility on ArcSight Database, only the database log files are gathered.
- You can run the sendlogs utility on a component even when the component service is down. If ArcSight Database is down, you can still collect its logs using this utility. If the Manager is down, you can only collect its local logs. However, if you need to collect the database logs as well, use the arcdt command on the Manager.
- All log files for a component are gathered and compressed. That is, you cannot select a subset of log files that the utility should process.
- The sendlogs utility generates a compressed file on your local system that you can attach to an email. The compressed log file is created in [ARCSIGHT_HOME/tmp/logs<Filename>.zip](#).
- You can review the compressed file to ensure that it contains only the desired and appropriate amount of information.
- You can remove or sanitize information such as IP addresses, host names, and e-mail addresses from the log files before compressing them. The options are to (a) send logs as generated, (b) remove only IP address, or (c) remove IP address, host names, and e-mail addresses.

For full details on using the sendlogs utility both from the command line and through the ESM Console, see the *Administrator's Guide*.

Options for Running Diagnostics and Sending Logs

There are two ways to launch the **Send Logs** utility:

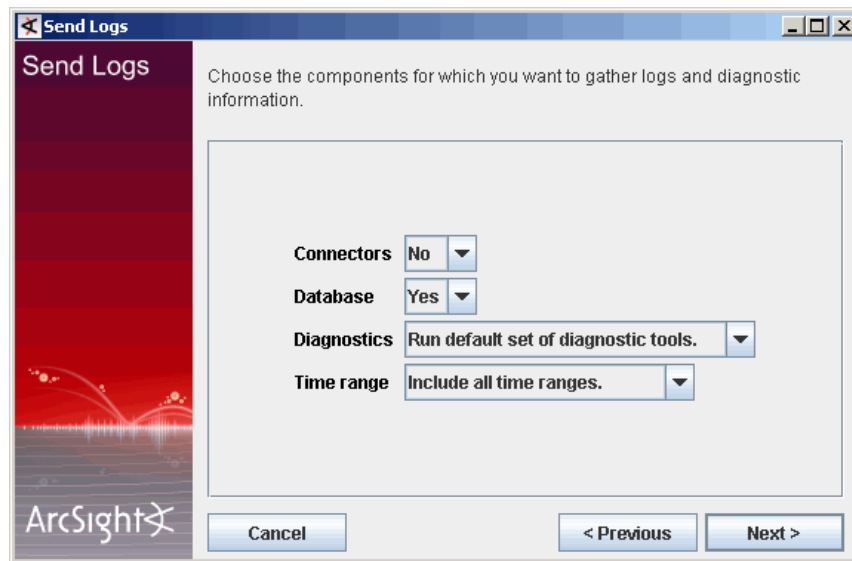
- As a wizard from the ESM Console Tools menu. (See [“Using the Network Tools” on page 107](#).)
- From the command-line interface of each component (via the command **arcsight sendlogs** from [ARCSIGHT_HOME/bin](#) on the [ESM Console](#), [Manager](#), or [ArcSight Web](#))

You can also use the **arcdt** command to run specific diagnostic utilities from the Manager command line.

Starting the Send Logs Wizard on the ESM Console

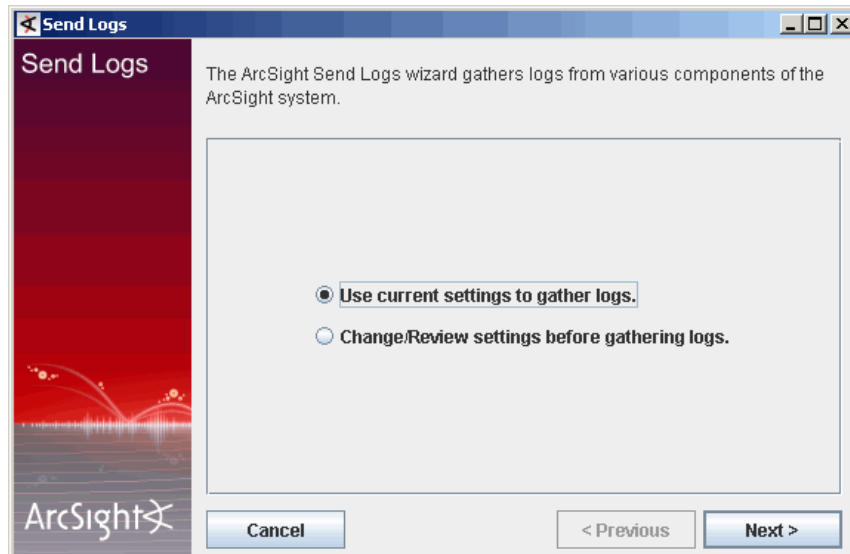
You can launch the Send Logs Wizard from the ESM Console.

Choose **Tools > SendLogs** from the ESM Console menus.



The first time you run the utility from the ESM Console, you are prompted to select the components from which to gather logs and diagnostics. Some additional first-time settings are also required (such as notification details, time ranges, and options to gather diagnostics for session wait times, thread dumps, and database alert logs). The wizard remembers most of these, so that on subsequent runs you can choose to use to retain the original configuration.

From now on when you start the Send Logs wizard, you will get this dialog. If you want to retain your original settings, select **"Use current settings to gather logs."** If you want to re-set the configuration, select the **"Change/Review settings before gathering logs."** option.



From either of these initial dialogs, the wizard guides you through the process of collecting logs and diagnostic information.

For a full description of all options and settings on the Send Logs utility, see "Configuring Manager Logging" in the *Administrator's Guide*.

Session Correlation

ArcSight considers a session to be information about the actors behind your network traffic that applies for a limited and specific period of time. Session information can be used to answer questions such as: "Who is in the New York office?" or "How many people are in meetings?" or "Are users accessing this resource according to company policy?"

Session correlation is a set of tools that capture session information to not only identify the assets involved in network traffic, but also the users, or actors, behind the traffic. (See ["Understanding Session Correlation" on page 543.](#))

Session correlation makes it possible to map users to assets at specific time periods. This is especially valuable for identifying who is doing what on your network from which assets and when, especially when the asset IDs themselves may be variable (such as DHCP or VPN logins).

Why Session Correlation Matters

Monitoring traffic on your network generally means processing data about the assets involved in the network traffic. However, there are times when asset data alone is not sufficient to detect potential threats to your network.

For example, users who log into the network on VPN or DHCP connections are assigned different IP addresses every time they log in. When sensors report events to ArcSight SmartConnectors, they are only identified by their assigned IP address, which means that you may be missing a whole spectrum of activity from mobile assets, such as laptops and PDAs and remote offices.

Whether accessing your network by using assets with fixed or variable IDs, it is often the user (the "actor") involved in the network activity whose actions you want to correlate with other event data. This enables you to track who is doing what on your network and when, and what they are doing in subsequent log-in sessions.

Capturing data about who is involved in network traffic as well as what assets are involved also adds crucial verification data to your correlation process. For example, three failed login attempts from a particular IP address can trigger a rule. But if that IP address is assigned to three different assets in the timeframe evaluated, session correlation makes it possible to clarify that the three failed login attempts were not executed by the same user.

Session Lists

Session Lists are similar to [Active Lists](#), with the following major differences:

- Session Lists always have Start Time, End Time, and Creation Time fields.
- Session Lists partition data because the lists can grow very large over a period of time.
- Session Lists do not have to fit entirely in memory.
- Session Lists are optimized for efficient time-based queries.

Session Lists can monitor activity based on any [Rules](#)-driven combination of [Events](#) attributes or set of custom fields. For example, session lists are very useful for tracking suspicious or hostile IP addresses as well as targets of attacks that may be compromised.

While you can populate session lists "manually" (adding entries from grid views or the Session List Editor), you should use session lists in conjunction with rules specifically

tailored to work with them. Rules can dynamically add and remove entries on lists, thereby making them a flexible information-gathering tool.

You can open and edit session lists in [Grid Views](#).

Session lists function differently than [Active Channels](#). Session lists are not continuously re-evaluated and are not time-window constrained. Session lists draw from the event stream on the basis of their event or field/rule definitions and any rules designed to affect them.

You can use session lists as [Filters](#) in other [Resources](#) that are not based on active channels, such as [Reports](#).

In addition to their integral definitions, you can apply temporary (not saved) filters to session list grid views. Click the status description in the **Filter** line in the view header to use the [Common Conditions Editor \(CCE\)](#).

Use the set of default items in the Session Lists resource tree for templates or for operational monitoring with minor modifications. For example, use the ArcSight User Sessions list to watch activity related to logins.

If you have Administrator access you will have another group named All Session Lists that contains all session list groups and lists.

See also: [“Session Correlation” on page 983](#).

SmartConnectors

ArcSight SmartConnectors are collectors of security event information generated by multi-vendor security [Devices](#) throughout your enterprise. SmartConnectors normalize and correlate this data into [Events](#), expressed as ArcSight Messages, which are forwarded to the Connector Data Manager (a component of the [Manager](#)) for further processing. SmartConnectors can reside on a device, on the Manager, or on a host machine. (For more information on SmartConnectors, see also [Chapter 27, Managing SmartConnectors, on page 695](#).)



Do not delete a Connector resource at the [ESM Console](#) unless the corresponding SmartConnector is first uninstalled from the device it is running on. If the SmartConnector running on the device has not been uninstalled, and its Connector resource is deleted, the SmartConnector will lose its connection to the Manager, causing the SmartConnector to start caching events and eventually dropping them.

Operational Status

ArcSight SmartConnectors display their operating status conditions next to their names in the Connectors resource tree in the Navigator panel.

Table 33-14 SmartConnector Status Conditions

Status Condition	Description
running	The SmartConnector is operating normally.
down	The SmartConnector is not connected to the ESM Console, therefore no events are being received.

Table 33-14 SmartConnector Status Conditions (Continued)

Status Condition	Description
stopped	The SmartConnector is responding to commands sent from the ESM Console, but events aren't being received.
paused	The SmartConnector is responding to commands sent from the ESM Console, but events aren't being transferred and are remaining in the SmartConnector's cache.

Configuration

You can configure ArcSight SmartConnectors to set a specific priority level for events that match specific criteria. One of the typical applications of this is to change the default priority mapping. By default, SmartConnectors will map the device priority (which may contain multiple levels) to the standard ArcSight priority levels: **Very-High**, **High**, **Medium**, and **Low**. For example, if a device has eight priority levels (0-7) where 0 is the highest priority, then most likely 0 and 1 will be mapped to Very-High, 2 and 3 to High, 4 and 5 to Medium, and 6 and 7 to Low. You can use this feature to change this behavior and make the SmartConnector set the priority based on different parameters. For example, assume two firewalls, one of which is your production firewall and the other an internal firewall used for testing. You can configure the SmartConnectors to set the ArcSight priority to Low for all the events coming from the internal firewall and leave the rest of the events with the default priority mapping.

SmartConnectors can be configured to optimize their performance and increase their functionality. SmartConnectors can be configured to enable aggregation, batching, and time zone correction functionality. You can also send control commands from the ESM Console to SmartConnectors to manage the flow of events.



Note

SmartConnector configuration also affects the ability to automatically create the assets that represent network devices. Each SmartConnector needs to report an IP address or hostname for its sensor so its events can be identified on the network. See the configuration guides for your SmartConnectors to ensure they are reporting this information.

For information on how to import and export SmartConnectors configurations, see ["Importing and Exporting SmartConnector Configurations" on page 724](#).



Tip

ArcSight SmartConnectors can send event information to the Manager in a compressed format using HTTP compression. Using compression lowers the overall network bandwidth used by ArcSight SmartConnectors dramatically, without impacting their performance. By default, all SmartConnectors have compression enabled. You can disable compression on SmartConnectors by modifying the `ARCSIGHT_HOME/user/agent/agent.properties` file as described in "Disabling Event Compression" in "Configuring ArcSight SmartConnectors" in *SmartConnector User's Guide*.

Zones

Network zones are address-based network zone information as reported by or assigned to connectors and integrated as an asset property. You can access zone through the [Zones Tab](#) of the Assets resource trees, and the Zone Editor.

The system can gather and integrate zone information by any of the methods. Only one method can apply with a given connector.

- If an AUP file (ArcSight SmartConnector [Content](#) update) is installed with a connector, the zone information, if present, provides addressed-based recognition.
- If a `defaultzones.csv` file is installed in the connector's `ARCSIGHT_HOME/system/agent/acp` directory, it overrides an AUP file if present.
- If the various zone URI values are set in the Connector Editor, in the Network section of the Networks: Content tab, they override URIs from an AUP file, a `defaultzones.csv` file, or the defaults.

Upgrading

You can centrally manage, configure, and update SmartConnectors remotely. You can use the Upgrade SmartConnector utility on the ESM Console to install newer versions of ArcSight SmartConnector software for managed devices, and to review which versions are currently installed. (See [“Upgrading SmartConnectors” on page 726](#).)

The connector upgrade utility is one of control commands available on SmartConnectors. (See [“Sending Control Commands to SmartConnectors” on page 715](#).)

Filtering

SmartConnectors can also act as a filtering tool between devices and the Manager, using filtering conditions. Filtering conditions are set with a combination of AND or OR statements and data field values. Extraneous events are filtered out to minimize the number of events sent to the Manager and analyzed in the ESM Console.



Events filtered out by ArcSight SmartConnectors are not reported to the Manager, so they won't be stored in or available later from the ArcSight Database.

For information on how to import and export filters on SmartConnectors, see [“Importing and Exporting SmartConnector Configurations” on page 724](#) (especially the topic on [“SmartConnector Filters” on page 726](#)).

SMTP

SMTP is used to send e-mail. An SMTP server must be configured either at install time or through context (right-click) menu e-mail settings. For [Notifications](#), the relevant fields are "from address", which designates the e-mail address of notification e-mail sent, and the "outgoing e-mail server," which is the SMTP server used to send e-mail. It is important to ensure that the "from address" specified is one that will not be rejected by the SMTP server, since some SMTP servers will reject unknown e-mail addresses. POP3 and IMAP can be used to check for e-mail acknowledgments.

You can specify these options at install time, or through context (right-click) menu e-mail option settings. For acknowledgements, the relevant fields are "incoming mail server," which is the POP/IMAP server to specify to check e-mail, "incoming mail protocol," which is either POP3 or IMAP, "account" and "password," which are the login name and password to access the mailbox from the incoming mail server. Note that replying to mails from the notification "from address" should reach the mailbox accessible to the "account" login.

SNPP is used to send pages. Sending notification pages requires that you configure the appropriate pager providers with host and port information using the Context (right-click) menu Pager Settings option.



For notifications sent by pager, firewalls must be configured so that the pager can connect directly to the paging service provider. ArcSight currently supports any provider that supports SNPP. For notifications sent by cell phone, any cell phone must be e-mail enabled. For notifications sent by e-mail, you need to add an address to the e-mail Address field.

Sortable Field Sets

Because the Manager processes large numbers of [Data Fields](#) from many sources, it is important to carefully manage which fields are subject to the additional indexing that supports sorting.

This sorting is represented by the ascending and descending **Sort Column** and **Remove Sort** commands you can apply in the headers of grid view columns. This is also the sorting that you apply through the **Sort Fields** tab in the Active Channel Editor when creating or editing channels.

Enabling all fields for sorting, or allowing on-the-fly sort indexing for previously unindexed fields, are both impractical for real-world performance. The practical solution is to select and index the most order-significant or frequently used fields and to make these fields readily available in clearly marked sets. Therefore, field sets are available from a Navigator panel resource in Active Channels called Sortable Field Sets. (In the Navigator, choose **Active Channels**, and click the **Field Sets** tab.)

Sortable field sets are like other [Field Sets](#), except that they are composed only of fields for which sort indexing has been enabled.

Like other resources, sortable field sets are associated with user groups to control access, through the ACL Editor, which edits Access Control Lists. (See [“Editing Access Control Lists \(ACLs\)”](#) on page 646.)

The selection of sortable fields and the named sets these fields are collected in are often customized during initial installation for an enterprise, and are usually tailored further after production use begins. Therefore, a reliable list can't be published in advance.

If you try to add an unsortable field to a sortable field set, or try to select sorting for an unsortable field in the **Sort Fields** tab in the Active Channel Editor, the ESM Console alerts you about the field's status.




Notes:

- Sortable fields belong to exclusive sets. This means that if you use a sortable field from one sortable field set to control an active channel, you cannot use sortable fields from other sets as secondary sort controls.
- The field sets in the System Field Sets folder should not be edited by users. If edits do occur by mistake, the system will auto-restore those resources to their defaults in about an hour.

To change an existing non-sortable field to sortable, contact your administrator.



[Variables](#) are not subject to indexing and therefore are not candidates for sortable field sets.

Using Sortable Columns in Grid Views

In grid views (including [Active Channels](#)), the names of sortable fields in column headers are indicated with a double arrow icon  and the **Sort Column** right-click command is enabled. Unsortable fields lack the icon and disable **Sort Column**.

To sort a list per a particular column, right-click over the column name and choose **Sort Column**.

If a field is already sorted, one of two additional icons is shown next to the column name indicating which direction the sort is applied.

- A down arrow  indicates a "top-down" sort is in effect on that field. (For example, when the event End Time field is sorted top-down, newer events are displayed at the top of the list and older events at the bottom. When the Priority field is sorted top-down, events are listed from higher to lower priority.)
- An up arrow  indicates the reverse ("low-to-high") sort in effect on that field. (For example, if the event End Time were sorted this way, older events show at the top of the list and newer events at the end. Similarly, a reverse sort on the Priority field would put low priority events at the top of the list.)

When **Sort Column** is chosen on a sortable field, a "low-to-high" sort is applied first (for example, show events from lowest to highest priority if the Priority field is sorted). If **Sort Column** is selected again, the sort order toggles to the reverse of the previous sort (high to low priority, per our example). The **Remove Sort** option disables the sort and returns the list to its unsorted state with regard to that particular column.

Multiple columns can be sorted simultaneously. The most recently applied sort will take precedence.

See also ["Applying a Field Set to an Active Channel" on page 132](#) and ["Sorting Events in an Active Channel" on page 131](#).

Status Monitor Events

The status monitor events can reveal and isolate many different quantity and time-unit issues that bear directly on performance and capacity. There are many possible applications of this system-state data, but those applications must always be interpreted within the context of your particular hardware, software, and network environment, and the deployment choices you have made.

Compare status monitoring events, which provide information about a wide variety of *system states*, to [Audit Events](#), which report on *system activity*.

Active Channel Statistics

Active channel statistics, specifically any changes that occur in the counts they report, can indicate performance issues and the use of processing cycles. These events summarize:

- The number of currently open Active Channels
- The number of events inserted into Active Channels per second

- The number of events changed across all open Active Channels per second

Table 33-15 Active Channel Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveChannels/Open	monitor:100	Open active channel count	Count, current value
/Monitor/ActiveChannels/Events/Insertions	monitor:174	Active channel event insertions per second	Count per second, since last monitor event
/Monitor/ActiveChannels/Events/Changes	monitor:175	Active channel event changes per second	Count per second, since last monitor event

Active List Statistics

Active list statistics monitor the resources being used by active lists. Active lists entries use some memory and database resources, and use CPU resources when they are referenced by other parts of the system (for example, rules, reports, and filters). While changes to these temporary lists are not persisted, they do represent some memory overhead. Note that when active lists are used by replay-with-rules, this also creates temporary lists.

Table 33-16 Active List Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveLists/ListCount	monitor:114	Open active list count	Count, current value
/Monitor/ActiveLists/EntryCount	monitor:115	Active list entry count	Count, current value
/Monitor/ActiveLists/EntryCapacity	monitor:116	Active list entry capacity	Count, current value
/Monitor/ActiveLists/EntryPercentUsed	monitor:117	Active list entry usage	Percent, current value
/Monitor/ActiveLists/TemporaryListCount	monitor:118	Temporary Active list count	Count, current value
/Monitor/ActiveLists/TemporaryEntryCount	monitor:119	Temporary Active list entry count	Count, current value
/Monitor/ActiveLists/TemporaryCapacity	monitor:120	Temporary Active list capacity	Count, current value
/Monitor/ActiveLists/TemporaryPercentageUsed	monitor:121	Temporary Active list usage	Percent, current value
/Monitor/ActiveLists/QueriesPerSecond	monitor:122	Active list queries per second	Count per second, since startup

Table 33-16 Active List Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/ActiveLists/ChangesPerSecond	monitor:123	Active list changes per second	Count per second, since startup

Asset Statistics

Asset statistics offer insight into performance areas that affect assets in the system and can help resolve source, destination, agent, and device asset issues for incoming events. These events summarize:

- **Asset resolutions per second** is the average number of end-points in events, that are resolved to assets in a second.
- **Asset resolutions average time** is the average time in milliseconds taken to resolve an end-point in an event to an asset.
- **Asset scanner events per second** is the number of scanner events processed in a second.
- **Asset scanner events average time** is the average time in milliseconds taken to process a scanner event.

Table 33-17 Asset Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Asset/TotalCount	monitor:200	Asset total count	Count, current value
/Monitor/Asset/Scanner/EventsPerSecond	monitor:201	Scanner events processed per second	Count per second, since last monitor event
/Monitor/Asset/ResolutionsPerSecond	monitor:202	Asset resolutions per second	Count per second, since last monitor event
/Monitor/Asset/Scanner/AverageTime	monitor:203	Scanner event average processing time	Count per second, since startup
/Monitor/Asset/ResolutionsAverageTime	monitor:204	Asset resolution average time	Microseconds per count, since startup
/Monitor/Asset/ResolutionsAverageTime/Source	monitor:205	Asset source resolution average time	Microseconds per count, since startup
/Monitor/Asset/ResolutionsAverageTime/Destination	monitor:206	Asset destination resolution average time	Microseconds per count, since startup
/Monitor/Asset/Size	monitor:240	Transitive closure size	Count, current value

Data Monitor Statistics

The data monitor statistics indicate how intensively the data monitors are working, which in turn can indicate situations such as filters needing adjustment or data monitors needing restructuring. These events summarize:

- **Active probes** is the number of currently enabled data monitors.
- **Evaluations per second** is the number of events times the number of enabled data monitors per second.

Table 33-18 Data Monitor Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/DataMonitors/ActiveProbes	monitor:101	Active data monitor probe count	Count, current value
/Monitor/DataMonitors/EvaluationsPerSecond	monitor:124	Data monitor evaluations per second	Count per second, since last monitor event

Event Broker Statistics

These statistics monitor reading events from, and writing events to, the database. As such, they are database health indicators. These events summarize:

- **Event count** is the number of events inserted into the database since the last monitor event.
- **Insert time** is the average time taken to insert each event into the database, in microseconds.
- **Retrieval time** is the average time taken to retrieve each event from the database in microseconds.

Table 33-19 Event Broker Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/EventBroker/InsertTime	monitor:102	Events insertion time per event	Microseconds per count, since last monitor event
/Monitor/EventBroker/InsertedEventCount	monitor:103	Events processed count	Count, since last monitor event
/Monitor/EventBroker/RetrievalTime	monitor:140	Events retrieval time per event	Microseconds per count, since last monitor event

Filter Engine Statistics

The count of in-memory filter evaluations can serve as a broad indicator of filter performance.

Table 33-20 Filter Engine Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Filters/EvaluationCount	monitor:161	Filter evaluation count	Count, since last monitor event

Main Flow Statistics

These events report statistically on the overall throughput of the Manager, for both incoming and internal events. This flow is the sequence of processing steps applied to each event and is a broad indicator or benchmark of system traffic. These events summarize:

- **Count** describes the number of events that have passed through the flow since the manager started.
- **Rate** describes the current event rate in events per second.

Table 33-21 Main Flow Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/MainFlow/EPS	monitor:230	Main flow event rate	Count per second, since last monitor event
/Monitor/MainFlow/Events	monitor:231	Main flow event count	Count, since startup

Notification Statistics

This group reports on notification activity, which can be of diagnostic value in detecting unusually high notifications activity.

- **New count** describes the number of new notifications since the last monitor event.
- **Escalated count** describes the number of notifications that were escalated since the last monitor event.

Table 33-22 Notification Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Notification/New	monitor:180	New notification count	Count, since last monitor event.
/Monitor/Notification/Escalated	monitor:181	Escalated notification count	Count, since last monitor event.

Pattern Discovery Statistics

These events provide statistics for recent or pending pattern discovery runs. Because pattern discovery is database-intensive, these statistics can indicate or help diagnose database performance issues.

Table 33-23 Pattern Discovery Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Patterns/RunCount	monitor:190	Pattern discoveries run count	Count, since last monitor event.
/Monitor/Patterns/RunsQueued	monitor:191	Pattern discoveries queued count	Count, current value.

Report Statistics

These events provide statistics about the current number of reports querying the database or being rendered. Because reports are database-intensive, these statistics can indicate or help diagnose database performance issues.

Table 33-24 Report Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Reports/Running	monitor:130	Reports running count	Count, current value.
/Monitor/Reports/RunningQueryingDB	monitor:131	Reports querying database count	Count, current value.
/Monitor/Reports/RunningRendering	monitor:132	Reports rendering count	Count, current value.

Resource Framework Statistics

Resource-framework events report on the database activity connected with updates (reads, writes, and deletions) to system resources such as rules, assets, and filters, since the last monitor event. This data can be valuable in tracking or diagnosing performance-related issues such as automatic asset maintenance, the threat-level formula, or rule-driven usage.

Table 33-25 Resource Framework Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Resource/Activity/Insert	monitor:171	Resources inserted per second	Count per second, since last monitor event.

Table 33-25 Resource FrameWork Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Resource/Activity/Update	monitor:172	Resources updated per second	Count per second, since last monitor event.
/Monitor/Resource/Activity/Delete	monitor:173	Resources deleted per second	Count per second, since last monitor event.

Rules Engine Statistics

The statistics related to the Manager's rules engine can help reveal performance issues in several areas. Remember that information about rules activity always needs to be considered in the full content of the Manager's operations. For example, a busy Moving Average data monitor, if used inefficiently, can affect several of these statistics; a poorly written rule can inadvertently drive up the rate of actions executed.

These statistics have the following performance implications

- Count of events inserted into the rule engine: CPU.
- Rate of event insertion into the rule engine: CPU.
- Count of correlated events generated by the rule engine: CPU.
- Rate of correlated event generation by the rule engine: CPU.
- Count of events that are still present in rule engine's working memory: memory.
- Count of groupBy cells that are being used by the rule engine: memory.
- Count of rules currently active in the rule engine: comparative value only.
- Rate of actions being executed by the rule engine: CPU.
- Count of events matching any rule: CPU, memory.
- Count of events matching a rule with single alias: CPU, memory.
- Count of events matching a rule with multiple aliases: CPU, memory.
- Count of events rule matches: CPU, memory.

Table 33-26 Rule Engine Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Rules/InsertedEventCount	monitor:151	Rules total event count	Count, since last monitor event.
/Monitor/Rules/InsertedEventRate	monitor:152	Rules inserted events per second	Count per second, since last monitor event.
/Monitor/Rules/GeneratedEventRate	monitor:153	Rules generated events per second	Count per second, since last monitor event.

Table 33-26 Rule Engine Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Rules/EventsInRuleEngineMemory	monitor:155	Rules in-memory event count	Count, current value.
/Monitor/Rules/GroupByCellsSize	monitor:156	Rules group by cells size	Count, current value.
/Monitor/Rules/ActiveRulesCount	monitor:157	Active rules count	Count, current value.
/Monitor/Rules/ActionsTakenRate	monitor:158	Rules actions rate	Count per second, since last monitor event.
/Monitor/Rules/GeneratedEventCount	monitor:159	Rules generated event count	Count, since last monitor event.
/Monitor/Rules/EventsMatchingAnyRule	monitor:232	Events matching any rule	Count, since last monitor event.
/Monitor/Rules/EventsMatchingFilterRule	monitor:233	Events matching filter rule	Count, since last monitor event.
/Monitor/Rules/EventsMatchingJoinRule	monitor:234	Events matching join rule	Count, since last monitor event.
/Monitor/Rules/MatchCount	monitor:235	Match Count	Count, since last monitor event.

Session List Statistics

Session list statistics monitor the resources being used by session lists. Session lists entries use some memory and database resources, and use CPU resources when they are referenced by other parts of the system (for example, rules, reports, and filters).

Table 33-27 Session List Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SessionLists/ListCount	monitor:260	Open session list count	Count, current value.
/Monitor/SessionLists/EntryCount	monitor:261	Session list entry count	Count, current value.
/Monitor/SessionLists/EntryCapacity	monitor:262	Session list entry capacity	Count, current value.
/Monitor/SessionLists/EntryPercentUsed	monitor:263	Session list entry usage	Percent, current value.

Table 33-27 Session List Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SessionLists/QueriesPerSecond	monitor:264	Session list queries per second	Count per second, since startup.
/Monitor/SessionLists/ChangesPerSecond	monitor:265	Session list changes per second	Count per second, since startup.

Session Management Statistics

This statistic tracks the current number of active user sessions.

Table 33-28 Session Management Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Sessions/Active/Total	monitor:160	Active session count	Count, current value.

Side Table Statistics

Side tables are ones held in-memory and in the database to retain common and relatively static information, similar to a cache. The purpose is to improve access times for inserts and queries. Side tables store event data that includes: geographical information, categorization information, agent information, device information and labels for custom strings and numbers.

- **Size** identifies how many entries are presently in the cache.
- **Insert** identifies the number of inserts in the past two hours.
- **Cache misses** identifies how many failed attempts to find entries occurred in the past two hours.
- **Cache hit rate** identifies how many successful attempts to find entries occurred in the past two hours.

Table 33-29 Side Table Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SideTable/GeoInfo/HitRate	monitor:210	Geo info sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/GeoInfo/Inserts	monitor:211	Geo info sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/GeoInfo/CacheMisses	monitor:212	Geo info sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/GeoInfo/Size	monitor:213	Geo info sidetable size	Count, current value.

Table 33-29 Side Table Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/SideTable/Category/HitRate	monitor:214	Category sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Category/Inserts	monitor:215	Category sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Category/CacheMisses	monitor:216	Category sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Category/Size	monitor:217	Category sidetable size	Count, current value.
/Monitor/SideTable/Agent/HitRate	monitor:218	Agent sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Agent/Inserts	monitor:219	Agent sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Agent/CacheMisses	monitor:220	Agent sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Agent/Size	monitor:221	Agent sidetable size	Count, current value.
/Monitor/SideTable/Device/HitRate	monitor:222	Device sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Device/Inserts	monitor:223	Device sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Device/CacheMisses	monitor:224	Device sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Device/Size	monitor:225	Device sidetable size	Count, current value.
/Monitor/SideTable/Labels/HitRate	monitor:226	Labels sidetable cache hit rate	Percent, over moving time frame.
/Monitor/SideTable/Labels/Inserts	monitor:227	Labels sidetable inserts	Count, over moving time frame.
/Monitor/SideTable/Labels/CacheMisses	monitor:228	Labels sidetable cache misses	Count, over moving time frame.
/Monitor/SideTable/Labels/Size	monitor:229	Labels sidetable size	Count, current value.

SmartConnector Flow Statistics

SmartAgent flow statistics record the event rates that occur at different stages of agent processing. "Sum of" statistics are sums of all values reported by all agents connected to the Manager. All values are statistics over the past 1-minute range. These events summarize:

- **Received event rate** is the rate at which agents receive events from devices.
- **Post filter event rate** is the rate of events that passed the filter (for example, were not filtered out).
- **Post aggregation event rate** is the rate of event aggregation.
- **Agent-to-manager event rate and count** describe how many events were actually sent to the Manager.
- **Cache size** describes the estimated size of the on-disk agent event cache.

Table 33-30 SmartConnector Flow Statistics

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Agents/Events/ToManager	monitor:104	Agent to-manager event count	Count, since startup.
/Monitor/Agents/EPS/ToManager	monitor:109	Agent to-manager event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/Received	monitor:110	Agent received event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/PostFilter	monitor:111	Agent post-filter event rate	Count per second, since last monitor event.
/Monitor/Agents/EPS/PostAggregation	monitor:112	Agent post-aggregation event rate	Count per second, since last monitor event.
/Monitor/Agents/CacheSize	monitor:113	Estimated agent cache size	Count, current value.
/Monitor/Agents/Total/Events/ToManager	monitor:141	Sum of agent to-manager event counts	Count, since startup.
/Monitor/Agents/Total/EPS/ToManager	monitor:146	Sum of agent to-manager event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/EPS/Received	monitor:147	Sum of agent received event rates	Count per second, since last monitor event.

Table 33-30 SmartConnector Flow Statistics (Continued)

Status Monitor Event Category	Device Event Class ID	Audit Event Description	Notes
/Monitor/Agents/Total/EPS/PostFilter	monitor:148	Sum of agent post-filter event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/EPS/PostAggregation	monitor:149	Sum of agent post-aggregation event rates	Count per second, since last monitor event.
/Monitor/Agents/Total/CacheSize	monitor:150	Sum of estimated agent cache sizes	Count, current value.

Templates

See [“Report Templates” on page 966](#).

Threat

The means by which the potential of a threat connector to adversely affect an automated system, facility, or operation, can be manifest. A potential violation of security.

Threat Evaluation

The Manager incorporates a system of security-threat evaluation that culminates in the Priority field you often see in views, reports, or event details. The Priority field uses a scale of 0-10 to rate incoming [Events](#), with 10 being the most-significant value. Naturally, you use Priority field [Threat](#)-evaluation values as a factor in many types of analyses and [Rules](#)-driven reaction or [Notifications](#) scenarios.

Evaluation Process

Threat evaluation is "always on" and applies to all the events received by the Manager. The evaluation process consists of:

- 1 Identify the targeted asset.

The identification process uses (in this order) the Target Address, Target Host Name, Target MAC Address, or relevant asset address range to classify the targeted asset.

- 2 Identify the targeted vulnerabilities.

Using the targeted asset as a key, the Manager looks up applicable vulnerabilities.

- 3 Match the targeted vulnerabilities with the vulnerabilities of the targeted asset.

When matches occur, one is chosen and placed in the Event Vulnerability field.

- 4 Compute the event's threat-priority value.

It is at this point that ESM performs the computation involving model confidence, relevance, criticality and severity (in this specific order), as described further in the next section.

Evaluation Definitions

The Priority field is a calculated value. It uses a formula that processes the contents of certain [Prioritization Fields](#) that help assess the potential security impact of an event. These fields use information about specific [Assets](#) and [Vulnerabilities](#) to establish models, and a confidence factor concerning the appropriateness of those models. Given confidence about a particular asset/vulnerability model, events directed at that asset can then be evaluated against a combination of factors that include relevance, criticality, and severity.

An event has **relevance** as a threat if it contains an [Attack](#) signature that is genuinely applicable to the targeted [Device](#), and the device is in a posture that would permit a successful attack. For example, is the event aimed at a valid port, and when the port was checked, was it open?

An asset's degree of **criticality** is based on the way it serves your enterprise, as seen from the perspective of the network's asset categories. For example, a server could be categorized among your "Very High Criticality Assets" because it handles customer financial transactions.

An event has **severity** if the targeted device is of a more sensitive type that is known to be subject to compromise, and the source of the event has been identified as a hostile or suspicious entity. Specifically, this is the value found in the Device Severity field. For example, did the event originate from an arch competitor on your Hostile List and was it aimed at a router on your Compromised List?

These three factors, when enabled by a suitable model confidence value, are averaged to produce the value that appears in the Priority field. If a suitable model confidence value isn't present, then severity and criticality are averaged to produce a value for Priority. The exploited vulnerability is also recorded in the event's vulnerability field. (See ["Investigating Views" on page 140.](#))

The exact numeric weight applied to each possible relevance, severity, or criticality state (such as unknown, low, medium, high, very high) is set through a configuration file named [ThreatLevelFormula.xml](#). This file is usually configured prior to deployment, using your enterprise policies to guide relative value choices.

Maintaining Model Confidence

The asset/vulnerability model confidence for various network devices is based on correlations between the asset and vulnerability resources you can see in the resource trees of the ESM Console's Navigator panel. Fresh vulnerability information that correlates well with a particular asset's identification results in greater model confidence.

Stated more directly, the model is the sum of the resources that describe the protected and external networks: assets, asset ranges, asset categories, network zones, and certain active lists.

While asset and vulnerability information can be updated manually, it is more practical to refresh this information by automated means such as vulnerability scanners. (See ["Managing Vulnerabilities" on page 758.](#)) ESM can automatically import vulnerability information from certain scanner products. Information drawn successively from the same scanner product is overwritten when duplicative; information from different products is additive. Information about new assets or vulnerabilities generates new resource references, and the Manager automatically matches the new references to their opposites, whether new or old.

It should also be noted that asset resources can be updated in bulk using XML files.

Using Threat Evaluation Information

While the Priority field has many obvious uses, starting with simply sorting the events in grid views, there are other ways to put this and its underlying information to work.

Rules, reports, filters, and any place you can apply logic can use the threat-evaluation operators described in [“Priority Calculations and Ratings” on page 957](#). You can also use the values described in [“Prioritization Fields” on page 956](#) to perform many threat-related functions.

Limitations and Workarounds

Because it is dependent upon a certain amount and type of event data, threat evaluation can be inhibited by these factors:

- A correlation event, produced by a rule or a data monitor, may not be populated with enough information. Only fields used to 'group by' will be populated in correlated events. Without enough information (such as targeted asset or severity) the threat evaluation will not be able to make a sound decision on the event's priority.
- Over-population of correlated events can also inhibit results. Some ArcSight rules are only used to maintain active lists. These rules do not generate useful new information, but the "group by" they need to use in order to collect the information for an active list may give them the appearance of a seriously offensive event.
- Rules offer the option to set your own priority. If a rule populates the priority attribute, then a threat model component will not change that value.

To compensate, you can use these techniques:

- Use the Priority field's value to control when you do and don't notify.
- If a rule is inferring some new piece of information (such as the classic Brute Force Login Attempt), then make sure that you "group by" sufficient information to be able to characterize the threat later. In the BFLA case, that would mean using the source and target addresses from the base events and setting the severity attribute to, for example, "Low"; the BFL Success rule, on the other hand, would set severity to "Very High".
- If the rule is a bookkeeping rule, try to copy as little information forward as you can, set the severity to low, and set the category to "/informational".

Thresholds

There are two types of thresholds: rule thresholds and event thresholds.

A rule threshold is the point at which a rule is triggered and a correlation event generated.

An event threshold is the number of times the event must occur before triggering the rule threshold.

A rule can have a threshold that states when the rule is triggered and also specify a threshold for each rule event. For example, thresholds can be created so that a rule is triggered only after all the events in the rule have occurred a set number of times.

See also, [“Rules” on page 974](#) and [“Events” on page 941](#).

Time Error Correction

In the context of the [ESM Console](#), time error correction means the synchronization of time between a network [Device](#), its ArcSight SmartConnector and the [Manager](#).

See also, "[SmartConnectors](#)" on page 984.

Timestamps

See also "[Timestamp Variables](#)" on page 1003.

Because timestamps are a key element in network security analysis, it is important to clarify the location, source, and context of the timestamps.

Security Events

Multiple timestamps are applied to events in the course of processing.

Table 33-31 TimeStamps for Events

Timestamp	Context
Device Receipt Time	The timestamp applied by the source sensor device upon receipt of the event.
Connector Receipt Time	The timestamp applied by the ArcSight SmartConnector's JVM (Java Virtual Machine) when the event is received from the originating sensor device.
Manager Receipt Time	The timestamp applied by the Manager's JVM (Java Virtual Machine) when the event is received from the ArcSight SmartConnector.
Start Time	The time at which the event actually began, as recorded by the source sensor device or, possibly, a secondary source monitored by that device.
End Time	The time at which the event actually ended, as recorded by the source sensor device or, possibly, a secondary source monitored by that device.

Resources

Timestamps are also applied to the ArcSight resources you see in the Navigator panel.

Table 33-32 TimeStamps for Resources

Timestamp	Context
Resource Created	This timestamp is applied by the Manager's JVM (Java Virtual Machine) when a resource is created.
Resource Modified	This timestamp is applied by the Manager's JVM (Java Virtual Machine) when a resource is changed.

General Information

All timestamps are stored as Coordinated Universal Time (**UTC**) times.

The ESM Console presents timestamps in the local time zone of the host computer using the Java Locale facility.

Log timestamps are produced by the local JVM for that component and are written using the Java Locale facility.

Timestamp Variables

See also [“Variables” on page 1006](#), especially the subtopic on [“Timestamps” on page 1015](#).

For date and time data fields, such as Detect Time, you can type an actual date value, such as `10/12/2002 8:54:00 AM`, or can use special system variables such as:

- `$CurrentDateTime`: for the date and time the report is run; the system variable is replaced by the current date and time value.
- `$CurrentDate`: for the date the report is run; the system variable is replaced with the date value, truncating the time of the day to 0, when the report is scheduled or run.

You can also specify certain date operations with these system variables to add or subtract a number of specified days or hours. For example, you could type: `$CurrentDate - 7d` for seven days before the date the report is run, the condition evaluates to a date which is the current date minus seven days, or `$CurrentDateTime - 12h`, which evaluates to the current date time minus 12 hours.

The time and date editing window you access through the **Detect Time** and **Detect Time Offset** fields of the ESM Console's Report Editor can accept month (uppercase "M"), minute (lowercase "m"), and current week (uppercase "W") parameters.

Use spaces to separate these special system variables or parameters from other operators when including them in a condition statement.

Inclusive Timestamps

The Detect Time timestamps reported for **correlated** events include the timestamps of the **base** events that initiated them. The timestamp is that of the most recent base event in the series of base events that caused the correlated event.

For example, an event's Detect Time field in the Event Inspector might now show `22 Sep 2003 18:18:24 PDT` instead of `22 Sep 2003 16:10:29 PDT`, with the difference being that the earlier timestamp represents the last base event rather than a later correlated event.

This refinement helps you interpret correlated events more readily, without the need to trace back through detailed rule chains.



You can also inspect the Connector Time parameter to find out just when a rule triggered (the time that was recorded as the Detect Time in prior releases.)

Time Zone Correction

The "correction" of a local time zone is the number of hours of offset to apply in order to adjust local time to another clock (often UTC or GMT) to synchronize device-time queries, correlation, and filters.

Trends

A trend is an ArcSight resource that defines how and over what time period data will be aggregated and evaluated for trends. A trend executes a specified query on a defined schedule and time duration.

Building trends is a component of Reporting resource tools. Be sure to see [Chapter 14, Building Reports, on page 331](#) for an overview of all reporting tasks and tools, and [“Understanding Reporting Workflow” on page 331](#) to see how Trends fit in to the process of creating a report.

Understanding Trends and Queries

A base trend is made up of one query. Trends can be used as the primary data source for a report. Or, a trend (based on one query) can be used as the data source to another query that further refines the initial query result. A collection of trend queries (queries that use trends as their data source) can provide focused views of a data set which can then be fed into a single report or multiple reports.

The ArcSight system evaluates source data for trends based on event conditions (such as number of worm outbreaks, incident time-to-close, or number of cases closed) or common network elements (such as operating system, business role, or regulatory compliance relevance).

This provides a means of querying not just the current model of the network but to build reports on queries of historical data, scheduled queries, and snapshot trends. Using queries in trends allows you to evaluate, for example, trending statistics on vulnerabilities and incident metrics over time to determine whether your vulnerability posture or incident closing rate is getting better or worse.

The generic trend reporting and a set of specific reports show trends on current data. For example, you can evaluate trends by operating system, by role, by compliance requirement, time to close on cases, and number closed.

You can provide a trend on a selected period of time, and pull reports that generate aggregated data. Trends can include case metrics such as time to close, open and time open, number closed, which allows for trending reports on incidents.

For more information, see [“Query-Trend Relationships in Reporting” on page 370](#) in [“Building Trends” on page 369](#).

Building Trends

You can access trends and associated editors in the Reports resource in the ESM Console.

See [“Building a Trend” on page 371](#) for information on how to navigate to and use the Trend Editor for [Defining Trend Settings](#).

Upgrade SmartConnectors

See [“Upgrading SmartConnectors” on page 726](#).

User Groups

User groups are named and organized collections of [Users](#). You can create groups based on departments, permission levels, work shifts, or whatever structure best supports your enterprise.

All users within a group inherit the group's permissions. If permissions are given to or taken from a group, all users within that group gain or lose those permissions. When users belong to more than one group, they receive permissions from all their groups. For example, if a user is in a group that has inspect permissions to all rules and is in another group with inspect permissions to all reports, the user will be able to inspect both rules and reports.

The following pre-defined groups help you manage your users:

- **Users:** Lists the current logged-in user and grants permission to inspect and edit their own information.
- **Shared:** Lists groups and users that the logged in user has permissions to.
- **All Users:** Lists all groups and users, only Administrators have permission to this group.

Groups created from the All Users group inherit permissions to only a few ArcSight resources. You can either edit the group ACL to add or remove permissions or create groups beneath one of the pre-existing groups to inherit a pre-configured set of permissions.

- **Default User Groups:** Lists groups and users with default permissions to all ArcSight resources. For more information on ArcSight resources, see ["Editing Access Control Lists \(ACLs\)" on page 646](#).
- **Administrators:** Lists groups and users with full rights and access to manage all groups and users



Note

Do not delete the Administrators group. It grants administrative access. The Administrators group contains at least one user account. This user account is created during installation.

- **Live Rules Editors:** Lists groups and users with permissions to inspect and edit rules
- **Reports Editors:** Lists groups and user with permissions to inspect and edit reports
- **Unassigned:** Lists users who do not belong to a group

Users

Users are individuals who are assigned login names, passwords, and privileges to access and perform operations using the [ESM Console](#) or [ArcSight Web](#) clients. For details on using the ESM Console for various tasks on dealing with users as an administrator, see [Chapter 26, Managing Resources, on page 665](#).

You manage users by storing user information, setting passwords, enabling or disabling login functionality, and organizing them into groups. When you create a new user account, a temporary password must be created for the user to login to the ESM Console. The user should change their password during their initial session. For more information on changing passwords, see ["Changing User Preferences" on page 772](#).

As an added security feature, user logins can be disabled. This feature may be used when the user is on an extended leave of absence, if the user ID and password have been compromised, or for any reason the user ID and password should not be used to access the ESM Console.

When users are deleted, they are removed from the Users resource tree but not the ArcSight Database. The deleted user ID is stored in the database for future offline processing and user activity auditing. If the user belongs to more than one group, the user account is deleted from all groups automatically.

User Types

User accounts serve several purposes. To enable giving all users only the minimum set of privileges that are needed for them to fulfill their duties, user accounts have a "user type." The user type specifies, at a high level, which features a user may access. This mechanism is complementary but does not replace permissions specified by access control lists (ACLs), which allow administrators to control access to resources such as assets, rules, and filters. User types are used primarily to control access to Manager services such as archiving and other management tools. See [Chapter 25, Managing Users and Permissions, on page 641](#).

Most often, user types are used to limit the risk resulting from the fact that user name and password combinations are stored on disk for components that require unattended startup but have to authenticate to the Manager. For example, the ForwardingConnector needs to authenticate to the Manager in order to obtain events, but does not need access to any of the resource management functionality provided by archive and other management tools.

The currently supported user types are:

- **Normal User:** Has full privileges to use the ESM Console or ArcSight Web client, and all tools. Only apply this user type to accounts that actually need access to the ArcSight Manager.
- **Management Tool:** Has only the privileges needed to run certain management tools used in conjunction with network management products.
- **Forwarding Connector:** Has only the privileges needed by the ForwardingConnector.
- **Archive Utility:** Has only the privileges needed to run the archive utility. Access to specific resources is controlled through ACLs.
- **Connector Installer:** A specialized identity used only to add SmartConnectors to the system.
- **Web User:** Has privileges to use the ArcSight Web client only (not the ESM Console or other tools).



Only Normal User accounts can log in to the ESM Console or an ArcSight Web client.

Unassigned users are those that do not belong to a group.

Variables

Variables are used to derive values from events, assets, and other resources (for example, a target IP address in an attack event, the MAC address or zone of a vulnerable asset, the timestamps on a user login session, entries in a hot list, and so forth).

Variable functions let you perform various operations on the derived values. To access event fields for use in **variable functions**, you either use the pick lists provided in the local or global variable dialogs or, in some cases, employ **velocity expressions** (templates) in statements. (See [“Velocity Templates” on page 1019](#) for an explanation of how to construct velocity expressions.)

You can use variables to create and tune [Active Channels](#), [Filters](#), [Reports](#), [Rules](#), [Field Sets](#), and [Data Monitors](#), or to expose more information, such as in report or grid view columns. The editors for these tools each include a **Variables** tab you click to add, edit, or remove variables.



Right-click a variable and choose **Copy**, then **Paste** it to another variable tab to avoid re-typing.

Once created, variables appear in the [Common Conditions Editor \(CCE\)](#) as additional fields on the Filters or Conditions tabs; Group By arguments for data monitors and rules; and Select, Group By, and Order By fields for queries. In the Field Set Editor, variables are an additional category that appears once variables are defined.

Variables are especially useful for situational-awareness applications such as reporting on attacks by division, or for compliance monitoring as in reporting the number of compromise events directed at Sarbanes-Oxley related devices.

Asset-category variables are based on the relevant resource ID of the modeled network asset (device). Timestamp variables are based on the start, end, or receipt times recorded by SmartConnectors, Managers, or devices.

Variables using Group, List, and Category Model functions are evaluated on the Manager, not directly on the ESM Console, and are referred to as **remote variables**.

These remote variables are evaluated only once on the ESM Console for any given event or resource. Therefore, the value of the variable on the ESM Console will not change if the underlying data is modified that would result in a different value for the variable. New events (in events channels) and resources (in resource channels) will evaluate the variable again, and you will see the updated value.

Because not all variables can be calculated on the ESM Console, there may be a delay in returning values from variables calculated “remotely” on the Manager.



Variables do increase processing overhead and can affect report-generation performance. Consider the performance sensitivity of a report before adding variables.

When you click **Add** in a Variables tab, the Add Variable dialog box can present several fields, depending on the function to be used. All field values can be edited later except the choice of function. To change a Variable from one function to another, create a new Variable and delete the old Variable.

The Add Variable dialog includes the option to **preview** (or calculate) the results for some variable functions, given test values that you specify.



- The **Preview** (calculate) feature on the **Add Variable** dialog is supported for some but not all variable functions. For example, the Type Conversion function “GetSizeOfList” does not support the “Preview” feature.
- There is no way to specify a NULL value for **Preview** input to a Variable function. The Preview assumes that a blank field for an input is an empty String. Therefore, you cannot use Preview on the Variable dialog to test inputs for a parameter with NULL values.

Local and Global Variables

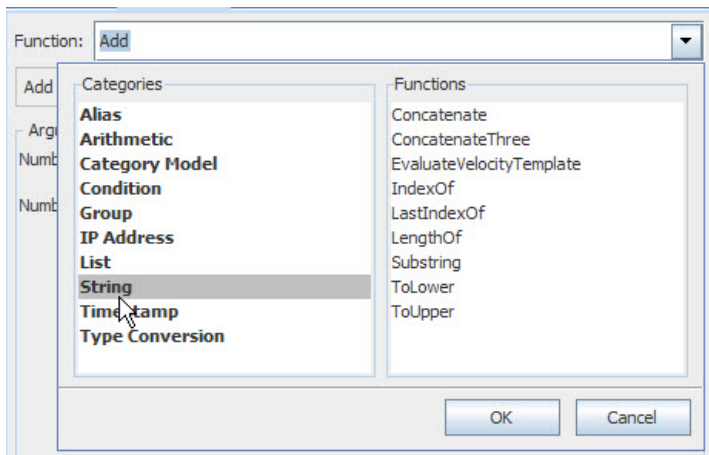
Variables you create in resources (on the Local Variables tab of a resource editor) are local to the resource for which you create them. For example, if you create a local variable in a query to get an active list value, that variable is available only to that query; not in other queries, rules, or filters. (Queries themselves are available for use in trends, reports, and query viewers, but the *local variables* used to build them are not.)

You can create *global variables* on field groups that are available across resources. The general information provided in this reference topic on variables, variable fields, and functions applies to both local and global variables. The main difference is that global variables are available across resources whereas local variables are not.

To create a **local variable**, click the Variables tab in a resource (for example, [Active Channels](#), [Filters](#), [Queries](#), [Rules](#)), name it, choose a function and provide arguments as needed.

To create a **global variable**, navigate to Field Sets, click the Fields & Global Variables tab, and use the Global Variables editor to select a function and parameters (as described in [“Global Variables” on page 477](#)).

Both local and global variables give you access to the same **functions**. All available functions are described in detail [“Variable Functions” on page 1009](#).



For more information on local variables, refer to the topics on editing any particular resource ([Filters](#), [Rules](#), [Queries](#) for Reports or [Query Viewers](#), and so forth).

For more information on global variables and field sets, see [“Global Variables” on page 477](#) and [“Field Sets” on page 203](#).

Variable Definition Fields

Table 33-33 Variable Definition Fields

Variable Field	Description
Name	<p>A name for the variable that is unique to the associated resource.</p> <p>Variable names must start with a letter, and can contain letters, numbers, underscores, and spaces. (Trailing spaces at the end of a variable name will be removed.)</p> <p>Special characters, other than those mentioned above, are not allowed.</p>
Function	<p>Each variable implements a single function. Functions are grouped into the following types; details for each type follow in the next section.</p> <ul style="list-style-type: none"> • Alias Functions • Arithmetic Functions • Category Model Functions • Condition Functions • Group Functions • IP Address Functions • List Functions • String Functions • Timestamps • Type Conversion Functions
Arguments	<p>The contents of the Arguments section vary based on the Function selected.</p> <p>Functions require one, two, or three data fields as input arguments.</p> <p>The event data field list is filtered to show only fields of the required argument type. For example, the GetMonth function requires a single argument of type <code>timestamp</code>, so the list only shows timestamp-related fields: Agent Receipt Time, Device Custom Date 1, Device Custom Date 2, Device Receipt Time, End Time, Event Annotation Modification Time, and so on.</p>

Variable Functions

Variable functions let you perform various operations on values derived from event fields. Pick lists are provided as an easy way to call the event fields you want to use as parameters or arguments to a function. For those functions without pick lists of fields ([Java Mathematical Expression](#) and [EvaluateVelocityTemplate](#)) you can use velocity expressions get values from event fields. (See “[Velocity Templates](#)” on page 1019.)

The following topics describe the functions provided for use, grouped by type.

Alias Functions

Table 33-34 Alias Functions

Function	Description
AliasField	Creates an alias (alternate name) for the specified field. Provide the alias name you want to use, and select a field from the drop-down list under Arguments.

Arithmetic Functions



The result of any arithmetic function (for example, Add) is a Long type, even if the original operands are other types (for example, Integers).

If you want to compare an Integer type field with a Long type field, you can convert the Integer to a Long by using the Add function. For example, suppose you want to compare Bytes In (which is an Integer field) to a custom variable "BytesOut" defined as: `Bytes Out + 100`. Since the variable uses the "Add" function, it will automatically convert to a Long. You cannot compare values whose data types are different. So, create *another* variable for Bytes In (for example, "BytesIn") defined as: `Bytes In + 0`, which will also convert to a Long. Now you can compare these two variables.

Table 33-35 Arithmetic Functions

Function	Description
Absolute	Returns the absolute value (its numerical value without regard to its sign) of the numeric argument. The argument may be integer, long integer, or double.
Add	Returns the result of adding the two numeric arguments together. The arguments may be integer, long integer, or double types.
Ceil	Returns the smallest integer value that is not less than the numeric argument. The argument may be integer, long integer, or double.
Divide	Returns the result of dividing the first numeric argument by the second numeric argument. The arguments may be integer, long integer, or double types, but the second argument may not evaluate to 0.
Floor	Returns the largest integer value that is not greater than the numeric argument. The argument may be integer, long integer, or double.

Table 33-35 Arithmetic Functions (Continued)

Function	Description
Java Mathematical Expression	<p>(Advanced User Feature) Returns the result of the evaluation of the specified Java expression.</p> <p>Notes: ArcSight does not provide error checking and messaging for your JEP expressions. Refer to the Java Math Expressions Parser web pages at http://www.singularsys.com/jep/ (and other links provided below) for more information on writing these expressions.</p> <p>Supported Expressions: ArcSight supports a subset of Java Mathematical Expressions (JEP), which are written like standard mathematical expressions. A JEP expression has three components: operator, function, and value.</p> <ul style="list-style-type: none"> • Operator - Examples of operators are +, -, /, *. JEP operators are documented in the table on this Web site: http://www.singularsys.com/jep/doc/html/operators.html • Function - The available functions are listed here: http://www.singularsys.com/jep/doc/html/functions.html <p>ArcSight supports the following subset of functions listed on the referenced Web site:</p> <p><i>Supported Trigonometric Functions:</i></p> <p>Sine - $\sin(x)$, Cosine - $\cos(x)$, Arc Sine² - $\text{asin}(x)$, Arc Cosine² - $\text{acos}(x)$, Arc Tangent - $\text{atan}(x)$, Arc Tan with 2 parameters - $\text{atan2}(y, x)$, Hyperbolic Sine - $\sinh(x)$, Hyperbolic Cosine - $\cosh(x)$, Hyperbolic Tangent - $\tanh(x)$, Inverse Hyperbolic Sine - $\text{asinh}(x)$, Inverse Hyperbolic Cosine¹ - $\text{acosh}(x)$, Inverse Hyperbolic Tangent¹ - $\text{atanh}(x)$</p> <p><i>Supported Log and Exponential Functions:</i></p> <p>Natural Logarithm¹ - $\ln(x)$, Logarithm base 10¹ - $\log(x)$, Exponential (e^x) - $\exp(x)$</p> <p><i>Miscellaneous Functions:</i></p> <p>Random number (between 0 and 1) - $\text{rand}()$, Modulus - $\text{mod}(x,y) = x \% y$, Square Root¹ - $\text{sqrt}(x)$, Absolute Value / Magnitude - $\text{abs}(x)$</p> <ul style="list-style-type: none"> • Value - The values are either constants of numeric type or ArcSight fields, which are referenced by the CamelCase notation just like the velocity references, but without the leading '\$'. <p>For information on how to reference ArcSight fields, refer to the "Script Alias" names in "Data Fields" on page 867. For information on velocity references, see "Velocity Templates" on page 1019</p> <p>Examples</p> <ul style="list-style-type: none"> • The expression <code>"round((bytesIn^2)/1000)"</code> squares the <code>byteIn</code> value of an event, divides the result by 1000, then rounds the result to an integer. • To determine if the ratio of "Bytes In" and "Bytes Out" for events is greater than 0.5, use this expression: <code>bytesIn / bytes_out > 0.5</code> (The expression returns "0" if True and "1" if False.)

Table 33-35 Arithmetic Functions (Continued)

Function	Description
	<p>Notes:</p> <ul style="list-style-type: none"> Unlike velocity references, JEP expressions do not use "\$" in front of (ArcField) Data Fields. Do not include mathematical operators or JME function names <i>in a variable name</i>. If you do, the JME parser interprets them as operators and yields unexpected results. Variable names that match JME function names such as <code>sqrt</code> cause similar problems. Some expressions may not be valid and do not produce results. Do not use them in queries or active channels, and filters that use them cannot be used in queries or active channels. JME variables are held only in memory and so, can be used only in Rules, Filters, and Data Monitors. They cannot be used in resources like Reports, which rely on persisted data. (There is a set of velocity references specifically for use in Reports. See “Velocity References for Reports” on page 1023 for more information.)
Multiply	Returns the product of multiplying the two numeric arguments together. The arguments may be integer, long integer, or double types.
Round	Returns the closest integer to the numeric argument. The argument must be a double.
Subtract	Returns the result of subtracting the second numeric argument from the first numeric argument. The arguments may be integer, long integer, or double types.

Category Model Functions

Table 33-36 Category Model Functions

Function	Description
HasRelationship	<p>Tests whether two actors, or an actor and a group, have the specified relationship based on a given Category Model.</p> <p>Category Model: Select an existing category model</p> <p>Parent Field or Group: Select a field or single-value variable you want to use as the parent. Use the Field/Group drop-down to indicate whether the parent is a field (single attribute) or a group.</p> <p>Child Field or Group: Select the field or single-value variable you want to use as the child.</p> <p>Inherit All Related Actors: Select true to include all the actors in the selected group and its children. Select false to include only the actors in the selected group.</p>

Condition Functions

Table 33-37 Condition Functions

Function	Description
ConditionalEvaluation	The ConditionalEvaluation function takes three arguments: a Filter which acts as a conditional expression, a value to return if the expression evaluates to True, and a value to return if the expression evaluates to False.

Group Functions

Table 33-38 Group Functions

Name	Description
FormatGroupsOfAsset	Returns a human-readable list of asset-category URIs unexclusively, meaning that all matching and related categories are included. This variable mainly formats and displays asset category-groups. It is best used with the contents of fieldsets, reports, and data monitor fields. Avoid using this variable in conditions because result order cannot be assured for multi-item groups; instead, use the "get groups" functions for superior ordering and consistency.
FormatGroupsOfNetwork Zone	Returns a human-readable list of network-zone URIs unexclusively, meaning that all matching and related zones are included. This variable mainly formats and displays asset zone-resource groups. It is best used with the contents of fieldsets, reports, and data monitor fields. Avoid using this variable in conditions because result order cannot be assured for multi-item groups; instead, use the "get groups" functions for superior ordering and consistency.
GetGroupOfAsset	Returns a single Asset Category or Asset Category Group, given a Base Field and Base Group. If there is more than one matching category or group, a single URI is chosen at random. Related categories are not included. Output is optimized for correlation operations. The "get groups" (plural) functions return lists of asset categories, therefore their results cannot be used in inGroup conditions. This "get group" (singular) function makes it possible to select one result at random, provided the variable is defined to produce a single result.
GetGroupOfNetworkZone	Return a single zone category. If multiple matches occur, a single URI is chosen at random. Related categories are not included. The "get groups" (plural) functions return lists of zones, therefore their results cannot be used in inGroup conditions. This "get group" (singular) function makes it possible to select one result at random, provided the variable is defined to produce a single result.
GetGroupsOfAsset	Returns a list of Asset Categories or Asset Category Groups, given a Base Field and Base Group. In rule and data monitor aggregations this should produce multiple sets. In reports, this produces a comma-separated list of asset-category names. No related categories are excluded. Output is optimized for correlation operations. This function complements the "format groups" functions. It simply shows XML representations of asset categories. Use this function in conditions and in "group by" elements of rules or reports because its output is both well-ordered and consistent.
GetGroupsOfNetworkZone	Returns a list of Network Zone Groups or Asset Category Groups, given a Base Field and Base Group. This function complements the "format groups" functions. It simply shows XML representations of group resources. Use this function in conditions and in "group by" elements of rules or reports because its output is both well-ordered and consistent.

IP Address Functions

Table 33-39 IP Address Function

Function	Description
ParseIPAddress	Returns an integer from 0 to 255 to represent the value of one octet of the specified IP address. For example, <code>ParseAddress(216.109.112.135, 1)</code> would return <code>216</code> . <code>ParseAddress(216.109.112.135, 4)</code> would return <code>135</code> .

List Functions



See also [ConvertListToString](#) and [GetSizeOfList](#) shown under “Type Conversion Functions” on page 1016.

Table 33-40 List Functions

Function	Description
GetActiveListValue	Returns the value associated with a specific field of the specified Active List.
GetSessionData	Returns the value associated with a specific field of the specified Session List. In previous releases, <code>GetSessionData</code> applied only to events. You can apply this function to any resource schema (actors, trends, cases, and so on). Now you can use this function for event and non-event schemas, and specify the time at which the session is evaluated using either a time field, a constant time, or a dynamic time. (In previous releases, non-event resources used end time by default.)

String Functions

Table 33-41 String Functions

Function	Description
Concatenate	Returns the string result of joining the two string arguments. For example, <code>Concatenate("Arc", "Sight")</code> returns <code>"ArcSight"</code> .
ConcatenateThree	Returns the string result of joining the three string arguments. For example, <code>Concatenate("Arc", "Sight", " Web")</code> returns <code>"ArcSight Web"</code> .
EvaluateVelocityTemplate	Advanced: Evaluates the <i>velocity template</i> argument and returns the result. This function is not available in a Query or Active Channel, and Filters which use this function cannot be used in a Query or Active Channel. For information on how to use Velocity Templates, See “Velocity Templates” on page 1019.
IndexOf	Returns the integer offset into the first string argument that is the location of the second string argument. For example, <code>IndexOf("Twas the night before Christmas", "night")</code> returns <code>9</code> . If the second string argument is not found in the first string argument, <code>IndexOf</code> returns <code>-1</code> .

Table 33-41 String Functions (Continued)

Function	Description
LastIndexOf	Returns the index (position) of the last (rightmost) occurrence of the second argument (the substring) within the first string argument (the source). If the substring is not found in the source, the function returns -1 . The first position is index 0 , as in the <code>indexOf</code> function. Examples: <code>lastIndexOf("abc/def/xyz", "/")</code> returns 7 <code>lastIndexOf("abc/def/xyz", "abc")</code> returns 0 <code>lastIndexOf("abc/def/xyz", "klm")</code> returns -1
LengthOf	Returns the number of characters in the string argument. For example, <code>LengthOf("Twas the night before Christmas")</code> returns 31 . <code>LengthOf("")</code> is 0 .
Substring	Returns a portion of the first string argument, starting with the position specified in the second, numeric, argument and including the ending position as the sum of the number of characters and the starting position, specified in the third, numeric, argument. For example, <code>Substring("Twas the night", 5, 8)</code> returns "the" .
ToLower	Returns the string argument converted to all lowercase. For example, <code>ToLower("Inline Filter")</code> returns "inline filter" . Numbers and other non-alphabetic characters are not affected.
ToUpper	Returns the string argument converted to all uppercase. For example, <code>ToUpper("Inline Filter")</code> returns "INLINE FILTER" . Numbers and other non-alphabetic characters are not affected.

Timestamps

See also the ["Arithmetic Functions" on page 1010](#).

Timestamp variables can use different Time Zones. To see the Time Zone field, click **More Options**. The choices for Time Zone are:

Table 33-42 TimeStamps with TimeZones

Time Zone	Description
Default Time Zone	The Manager time zone
Agent Time Zone	The time zone of the Connector which sent the event
Original Agent Time Zone	The time zone of the first Connector in a possible chain of connectors which sent the event
Device Time Zone	The time zone of the originally-reporting device
Final Device Time Zone	The time zone of the device which reported to the original Connector

Table 33-43 TimeStamp Functions

Function Field	Description
Get Day of Month	Returns an integer from 1 to 31 to represent the day of the month, based on the selected timestamp

Table 33-43 TimeStamp Functions (Continued)

Function Field	Description
GetDayOfWeek	<p>Returns an integer from 0 to 6 (0 is Sunday) to represent the day of the week, based on the selected timestamp. The associated day of the week (for example "Sunday") is displayed on the ESM Console.</p> <p>You can test the value returned by this function using numeric operations like <code>></code> , <code><</code> , <code>>=</code> , <code><=</code> , <code>=</code> .</p> <p>For example, for a variable called "day" that contains the value returned by the GetDayOfWeek function, you can create an AND logical operator that checks for a weekday with these conditions:</p> <ul style="list-style-type: none"> • <code>day >= Monday</code> • <code>day <= Friday</code>
GetDayOfYear	Returns an integer from 1 to 366 to represent the day of the year, based on the selected timestamp.
GetHour	Returns an integer from 0 to 23 to represent the hour of the day, based on the selected timestamp.
GetMinute	Returns an integer from 0 to 59 to represent the minute of the hour, based on the selected timestamp.
GetMonth	Returns an integer from 1 to 12 to represent the month of the year, based on the selected timestamp.
GetYear	Returns an integer for the year based on the selected timestamp and displays it as a 4-digit integer.
Time Difference	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in a human-readable format.
Time Difference in days	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in days.
Time Difference in hours	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in hours.
Time Difference in minutes	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in minutes.
Time Difference in seconds	Returns the result of subtracting the second timestamp argument from the first timestamp argument, in seconds.

Type Conversion Functions

Table 33-44 Type Conversion Functions

Function	Description
ConvertAddressToString	Converts a given IP address to a string format, similar to how these are shown in an active channel (for example, <code>192.168.1.1</code>)

Table 33-44 Type Conversion Functions (Continued)

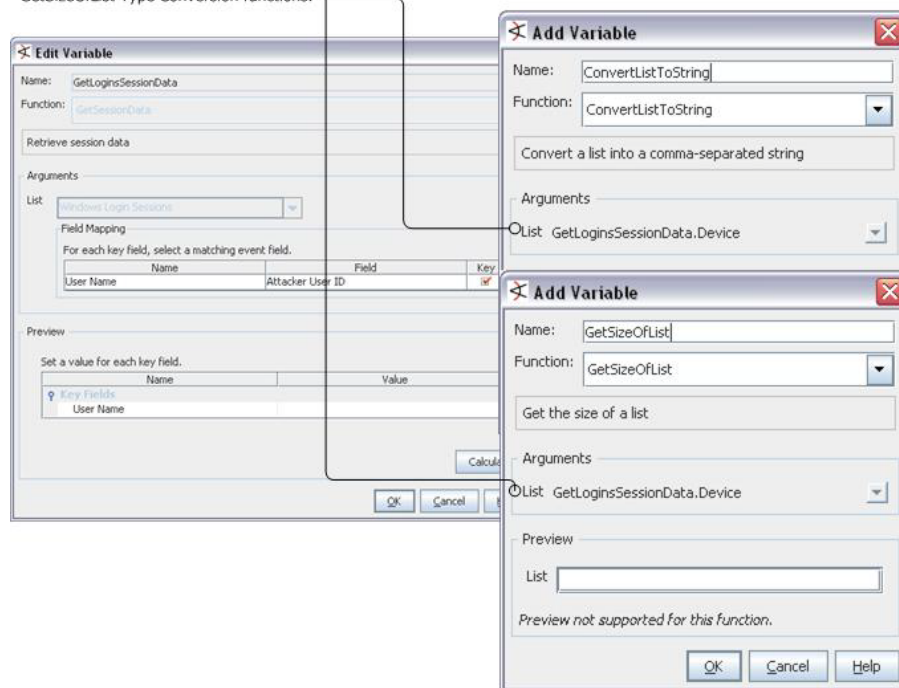
Function	Description
ConvertListToString	<p>Takes as an argument the value of a multi-valued session list entry and returns it as a comma-separated string (with each entry in the same format as displayed in a channel).</p> <p>For example, suppose you have a session list set up to show user names and IP addresses associated with login sessions. You could get user names from the session list via the <code>GetSessionData</code> variable. If there are three user names on the list (for example, darren, samantha, and endora), the <code>ConvertListToString</code> variable will return the three names (for example, <code>[darren, samantha, endora]</code>). You could do the same with IP addresses.</p> <p>To use this variable, first add a <code>GetSessionData</code> variable. The nested fields that show up in the field selector (<code><VariableNameFromSessionList>.<FieldName></code>) can then be selected as arguments to this function. See .</p> <p>For more about session lists, see "Identity Correlation" on page 543 and Chapter 21, List Authoring, on page 571.</p> <p>Notes:</p> <ul style="list-style-type: none"> • See also, ConvertStringToList. • This works for both multi-valued session lists and active lists with overlapping entries. • The <code>ConvertListToString</code> variable is held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. It cannot be used in queries for resources like Reports, which rely on persisted data. (There is a set of velocity references specifically for use in Reports. See "Velocity References for Reports" on page 1023 for more information.) • More list functions are shown in "List Functions" on page 1014.
ConvertNumberToString	Takes as an argument any number (integer, double, etc.) and returns it as a string.
ConvertStringToDouble	Returns a double (floating point number) based on the selected string. For example, if a character string event field contained <code>"3.19"</code> , <code>ConvertStringToDouble</code> would return a numeric value of <code>3.19</code> .
ConvertStringToInteger	Returns an integer based on the selected string.
ConvertStringToList	<p>Takes as an argument a comma-separated string and returns it as a multi-valued list. (See also ConvertListToString.)</p> <p>Note: <code>ConvertStringToList</code> is made available only for in-memory resources that do not involve queries. (Therefore, it does not show up as an available variable for queries.)</p>
ConvertStringToLong	Returns a long (very large integer) based on the selected string.

Table 33-44 Type Conversion Functions (Continued)

Function	Description
GetSizeOfList	<p>Takes as an argument the value of a multi-valued session list entry and returns the size of the list.</p> <p>For example, suppose you have a session list set up to show user names and IP addresses associated with login sessions. You could get user names from the session list via the <code>GetSessionData</code> variable. If there are three user names on the list (for example, darren, samantha, and endora), the <code>GetSizeOfList</code> variable will return the number of names on the list (for example, <code>[3]</code>). You could do the same with the IP addresses.</p> <p>To use this variable, first add a <code>GetSessionData</code> variable. The nested fields that show up in the field selector (<code><VariableNameFromSessionList>.<FieldName></code>) can then be selected as arguments to this function. See .</p> <p>For more about session lists, see “Identity Correlation” on page 543 and Chapter 21, List Authoring, on page 571.</p> <p>Note:</p> <ul style="list-style-type: none"> • This works for both multi-valued session lists and active lists with overlapping entries. • The <code>GetSizeOfList</code> variable is held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. It cannot be used in resources like Reports, which rely on persisted data. (There is a set of velocity references specifically for use in Reports. See “Velocity References for Reports” on page 1023 for more information.) • More list functions are shown in “List Functions” on page 1014.

To use `ConvertListToString` and `GetSizeOfList` variables, first create a `GetSessionData` variable, then you can select fields from that variable as arguments in these [Type Conversion Functions](#).

`GetSessionData` list function shows up as argument to `ConvertListToString` and `GetSizeOfList` Type Conversion functions.



Variable Availability and Contexts

Not all variables are available in all contexts.

These functions are only available for use with event schemas: [ConditionalEvaluation](#), [HasRelationship](#), and [AliasField](#).

These functions are not available for use in SQL based operations: [ConvertListToString](#), [ConvertStringToList](#), [GetSizeOfList](#), [EvaluateVelocityTemplate](#), and [Java Mathematical Expression](#).

Active Channels can evaluate [Group Functions](#), [Category Model Functions](#), and [List Functions](#) only by sending a request to the Manager. (These are not evaluated on the ESM Console side, unlike other variable functions.) If you create active channels that use these function types, keep in mind that there will be a slight delay in an ESM Console channel display of these values. This applies to all variables that use functions in any of these categories ([Group Functions](#), [Category Model Functions](#), and [List Functions](#)).

See [“Applying a Field Set to an Active Channel”](#) on page 132.

Velocity Templates

ArcSight supports the use of *velocity templates* or scripts as defined by The Apache Velocity Project (<http://velocity.apache.org/>). Velocity templates are a means of specifying dynamic or variable inputs to, or outputs from, underlying Java code.

There are a number of places where a person familiar with Velocity templates can specify inputs using Velocity, instead of a literal value, to greatly enhance the results.



Velocity Templates are an Advanced User Feature

- Because Velocity templates have such wide-ranging and intricate possibilities, mis-application or inappropriate application is entirely possible. ArcSight cannot assume responsibility for adverse results caused by user-supplied Velocity templates.
- ArcSight does not provide error checking or error messaging for user-created velocity expressions. Refer to the Apache Velocity Project web page at <http://velocity.apache.org/> for more information on using velocity templates.
- Velocity template based variables are held only in memory and, therefore, can be used only in Rules, Filters, and Data Monitors. Velocity template based variables cannot be used in resources like Reports, which rely on persisted data. (There is a set of velocity references specifically for use in Reports. See “[Velocity References for Reports](#)” on page 1023 for more information.)
- **Referencing Variables, Fields, and Domains in Velocity Expressions.** Any variable that a velocity expression references must be local to the resource. You can refer to local variables, fields, and domain fields in a velocity expression.

If you have a global variable that you want to use in a velocity expression,

use the +/-Global Variable button  on the [Common Conditions Editor \(CCE\)](#) to make it available in the resource. For more information, see “[Adding or Removing Global Variables Using the CCE](#)” on page 857.

For more information on variables in general, see “[Variables](#)” on page 1006 and “[Global Variables](#)” on page 477.

Velocity Application Points

Velocity template support appears both in the user interfaces and in certain configuration files. The designated Velocity access points are described below.

Stated briefly, Velocity templates can be applied in most places where a literal string might be enhanced by a conditional or variable string. Common examples are formatting time expressions or condensing fine units into more meaningful groupings.

Table 33-45 Velocity Template Usages

Application Point	Description
Rules Action Parameters	You can use Velocity templates in Add Action dialog boxes to create or edit fired-rule behavior. You get to these from the Actions tab or the Rules Editor. The Command and Parameters fields for Execute Command actions are Velocity candidates, as is the message-subject text in the Message field of Send Notification actions.
Custom Columns	Velocity templates are also applicable in the Cell Format and ToolTip Format panels of the Custom Columns Editor, which are described in “ Customizing Grid Columns ” on page 152.
SmartConnector Configuration	The URI strings in the Default Content tab of the Connector Editor can accept Velocity templates.

Table 33-45 Velocity Template Usages (Continued)

Application Point	Description
Case Audit Events	ArcSight audit events concerning cases can also be customized with Velocity templates, through properties files. In the case.default.properties or case.properties files (which overrides the former file), found at \$ARCSIGHT_HOME/config/audit, you can replace the expression in a key-value pair with a template variable or specify an additional field.
Notification Messages	In addition to using the Message field of Send Notification actions in the Add Action dialog box, you can also add Velocity templates to the destination-oriented notification configuration files located with the ArcSight Manager at \$ARCSIGHT_HOME/config/notification. This text controls message content (in contrast to the subject line).
Reports Text Fields	You can use a specific set of Velocity references for Report parameters when creating, editing, scheduling or running Reports and Focused Reports. Velocity references for Reports are covered in detail in “Velocity References for Reports” on page 1023 .

Using Velocity Expressions to Retrieve Values from Event Fields or Variables

Velocity expressions can be used to construct rule actions or velocity variables that need to access values in event fields or other variables. **Rule actions** can use velocity expressions in commands and notification messages. In these contexts, you need to write the velocity expression (there are no pick lists of fields provided, as there are in *rule conditions*). (See [“Creating Rule Actions” on page 451](#) and [“Rule Actions Reference” on page 455](#).)

You can construct most **global variables** and **local variables** simply by using the provided pick lists of event fields in the **functions**. However, the Arithmetic function [Java Mathematical Expression](#) and the String function [EvaluateVelocityTemplate](#) are velocity variables that require you to write a velocity expression. (See [“Local and Global Variables” on page 1008](#).)

The syntax for constructing a velocity expression is the same, whether for rule actions or velocity variables.

Retrieving Values from Event Fields

To retrieve the value of an event field, use the field name in “camel notation” without any spaces, preceded by a dollar sign (\$):

```
$<fieldNameInCamelNotation>
```

For example, to retrieve the value of the “Attacker Address” field, use:

```
$attackerAddress
```

For more about event fields, see [“Data Fields” on page 867](#).

Using Variables in a Velocity Expression

To retrieve the value of a variable, use the variable name preceded by a dollar sign (\$). If the variable name contains a dot, remove the dot and use camel case. If the variable name contains a space, use an underscore:

```
$<VariableName>
$<variable_Name>
```

For example:

Variable display name	Velocity notation
Credit Card Number	<code>\$Credit_Card_Number</code>
<code>dhcp.Hostname</code>	<code>\$dhcpHostname</code>
Login User.Account Number	<code>\$Login_UserAccount_Number</code>

For more about variables, see [“Variables” on page 1006](#).

Using Velocity Expressions in Rule Actions

You can use velocity expressions in rule actions to retrieve the value of an event field or variable. These expressions can be used in commands or notification messages in rule actions.

For details syntax and guidance on constructing velocity expressions for use in rules, see [“Using Velocity Expressions to Retrieve Values from Event Fields or Variables” on page 1021](#)

Example of Rule Action that Uses Velocity Expressions to Retrieve Values

Following is an example of using both types of velocity expressions in a rule action to retrieve values from an event field (`Attacker Address`) and a variable (`dhcp.Hostname`):

- 1 In the Navigator panel, choose **Rules** from the drop-down menu.
- 2 Create or edit a rule.
- 3 Click the **Actions** tab.
- 4 Right-click a rule action and choose the **Send Notification** rule action.

The notification subject can be constructed as follows:

```
"Brute force login attempt from IP Address: $attackerAddress
Hostname: $dhcpHostname"
```

- 5 Click **OK** or **Apply** to save the rule.

When the rule action is triggered, the notification message will replace the event field velocity expression "`$attackerAddress`" with the value of the Attacker Address field, and the variable velocity expression "`$dhcpHostname`" for the value of `dhcp.Hostname`.

Examples

You might use a Velocity template in a Zone URI field in an Connector Configuration Editor to specify a conditional target, as in:

```
#if( $deviceHostName.equals("foobar"))/All Customers/SuperCustomer#end
```

If you are setting up zones based on customers and you want to populate those values dynamically, you could use the following statement to populate fields based on host names, etc. For example, if you have one connector that collects events from devices monitoring

different customers networks, you may want to set the customer name based on the device hostname.

```
device hostname = companyx.arcsight.com
```

The following sets the customer name to "arcsight.com":

```
CustomerURI=/All
Customers/$deviceHostName.substring($deviceHostName.indexOf("."))
```

You can set the customer field from the SmartConnector as well, so events from a particular SmartConnector or device can be tagged as "customer xyz" (provided that Customer URI does exist on the Manager) and you can make ACLs limiting the customers' event privileges so they see only events tagged as "customer xyz". If you have one SmartConnector that monitors devices reporting from multiple customers, you can dynamically set the customer name to be based on the device hostname. For example, if you have a customer named "arcsight" and the device hostname is "device1.arcsight.com", the following template returns "arcsight" as the customer name:

```
CustomerURI=/All
Customers/$deviceHostName.substring($deviceHostName.indexOf("."),$
deviceHostName.lastIndexOf(".")).substring(1)
```

The result would be the URI: `/All Customers/arcsight`

For a case audit event in case.default.properties, a template could consist of:

```
deviceCustomString3=$history
```

Usage Tips

- **Strings and numeric values only.** Velocity templates apply **only** to fields that contain string or numeric values.
- **Dynamic parameters and ArcSight variables.** You can use all of the dynamic time parameters you see in the Active Channel Editor and elsewhere, such as `$Now` and `$CurrentDateTime`. The same is true for time elements, including `s` (second), `m` (minute), `d` (date), `M` (month), `w` (week), and `y` (year). To use any event data field as a variable, express its displayed name as a one-word "camel cap" string prefixed with a dollar sign. For example, "Source Address" would be `$sourceAddress`. For details about using variables in a velocity expression, see ["Using Variables in a Velocity Expression" on page 1021](#).
- **Regular expressions not supported.** Use of regular expressions is not tested or supported.
- **Test using active channel custom field.** You can conveniently test Velocity templates by trying them first in a customField of an active channel.

Velocity References for Reports

The following Velocity references are available for use in [Reports](#) anywhere where Text is used. These references pick up, contain, display, and print the given values. Generally, Velocity references in Reports are used for display and print purposes when creating, editing, scheduling or running Reports and Focused Reports. In some cases, they are used

for more than that. For example in archived reports, [\\$Archive_Report_Folder](#) and [\\$Archive_Report_Name](#) determine the location where reports will be stored.



The following table shows the complete set of applicable references for use with Reports. Other types of references (such as those discussed in the previous sections of this topic) do not apply to Reports. However, most of the [Usage Tips](#) detailed above also do apply to Velocity Templates for Reports.

Table 33-46 Velocity References for Reports

Category	Reference	Description
Report	\$ReportName	Prints the name of the report, as specified in the Name field on the Attributes tab of the Report Editor.
	\$AccessDisclaimer	Prints a disclaimer statement regarding the user permissions with which the report was run. The disclaimer statement is a read-only string which is generated when report data has been filtered due to limited access privileges of the user Reports are generated only with data for which the current user has access privileges. Depending on user permissions for the user running a given report, access to some types of events or data may be curtailed. In such cases, the report is generated with all the information for which the user has access privileges. Events and data requiring higher-level access privileges are not included in the report. The access disclaimer statement is a standard explanation of the limitations of such a report.
	\$CurrentPageNumber	Prints the current page number of the report.
	\$TotalPageNumber	Prints the total number of pages in the report.
Time	\$CurrentDateTime	Prints the current date and time. (Same as \$Now) Example output: 12-06-2010-15:32:19. Tip: Formats for dates and times depend on your Console preference settings. To change the way dates and times are displayed throughout the Console, choose Edit > Preferences , then click the Date & Time button. For more information, see "Changing User Preferences" on page 772 .
	\$CurrentDate	Prints the current date per your format preferences. Example output: 12-06-2010.
	\$CurrentMonth	Prints the current month. Example output: 12-2010.

Table 33-46 Velocity References for Reports (Continued)

Category	Reference	Description
	\$CurrentWeek	Prints the current week. Example output: 49-2010 (for December of 2010).
	\$Now	Prints the current date and time. (Same as \$CurrentDateTime) Example output: 12-06-2010-15:33:00.
	\$Today	Prints today's date. Example output: 12-06-2010-00:00:00.
	\$CurrentDateTime-<Number>d	Prints the current date and time minus the number of days you specify. For example, if you ran the report on 12-06-2010 at 15:33:00 and specified the current date and time minus 1 day (\$CurrentDateTime-1d), this reference would output 12-05-2010-15:33:00. If, on the same day, you specified the current date and time minus 3 days (\$CurrentDateTime-3d), this reference would output 12-03-2010-15:33:00
Parameters	\$Report_Format	Prints the name of the report format that is configured as the default. Output formats are: <ul style="list-style-type: none"> • pdf - Adobe PDF file. • xls - Microsoft Excel file for tables and charts. (See "Report Format" on page 402 in Creating Reports for additional notes on XLS reports.) • rtf - Rich-text format document • csv - Tabular data as a list of comma-separated values. (See "Report Format" on page 402 in Creating Reports for additional notes on XLS reports.) • html - Web page displayed by the default web browser <p>If the default output format for the report is set to html, then \$Report_Format reference simply will print the word "html".</p> <p>See "Report Parameters" on page 401 in Creating Reports for information on how to set the default output formats for reports when creating reports.</p> <p>See "Report Parameters" on page 425 in Chapter 15, Running and Managing Reports, on page 423 for information about setting parameters at report runtime.</p>
	\$Page_Size	Prints the page size of the report. Example output: Letter [8.5x11 in]

Table 33-46 Velocity References for Reports (Continued)

Category	Reference	Description
	\$Run_as_User	Prints the user name specified, if any, for the "Run as User" parameter in the report.
	\$Email_to	Prints the e-mail address specified, if any, for the "Email to" parameter in the report.
	\$Email_Format	Prints the e-mail format specified, if any, for the "Email Format " parameter in the report. For example, "Send URL" or "Attach Report".
	\$Filter_by	Prints the filter(s) used by the referenced query for this report.
	\$Archive_Report_Folder	Prints the folder location where the archived report is stored.
	\$Archive_Report_Name	Prints the name of the archived report.
	\$Archive_Report_Expiration_Time	Prints the expiration time for an archived report.
	\$<ComponentID>.Row_Limit	<p>Prints the row limit for the specified component.</p> <p>Tip: <ComponentID> refers to the data components or building blocks of a report. To view the components of a given report, right-click the report in the Navigator panel, choose Edit Report, and click the Data tab for the report.</p> <p>For example, if the report contains a component called Table, you can display related information by using the Velocity reference <code>\$Table.Row_Limit</code>, <code>\$Table.Time_Zone</code>, and so forth.</p> <p>Similarly, if the report, contains components called Chart1, Chart2, and Chart3; you can display related information on each of the charts by using references such as <code>Chart1.Time_Zone</code>, <code>Chart2.Start_Time</code>, and so forth.</p>
	\$<ComponentID>.Time_Zone	<p>Prints the time zone for the specified component.</p> <p>For example, <code>Table.Time_Zone</code> would output the time zone used for the data in a component called Table in your report.</p> <p>Example output: America/Los_Angeles</p>

Table 33-46 Velocity References for Reports (Continued)

Category	Reference	Description
	<code>\$<ComponentID>.Start_Time</code>	<p>Prints the start time for the specified component.</p> <p>For example, <code>Table.Start_Time</code> would output the start time used for the data in a component called Table in your report. (Start Time is a report parameter that can be configured on a per-component basis.)</p> <p>Example output: 12/05/2010 17:46:50.406-0800</p>
	<code>\$<ComponentID>.End_Time</code>	<p>Prints the end time for the specified component.</p> <p>For example, <code>Table.End_Time</code> would output the end time used for the data in a component called Table in your report. (End Time is a report parameter which can be configured on a per-component basis.)</p> <p>Example output: 12/05/2010 18:00:21.140-0800</p>
	<code>\$<ComponentID>.<Parameter_name></code>	Prints the value of the specified component parameter.
	<code>\$Custom.<Parameter_name></code>	Prints the value a custom component parameter.

Views

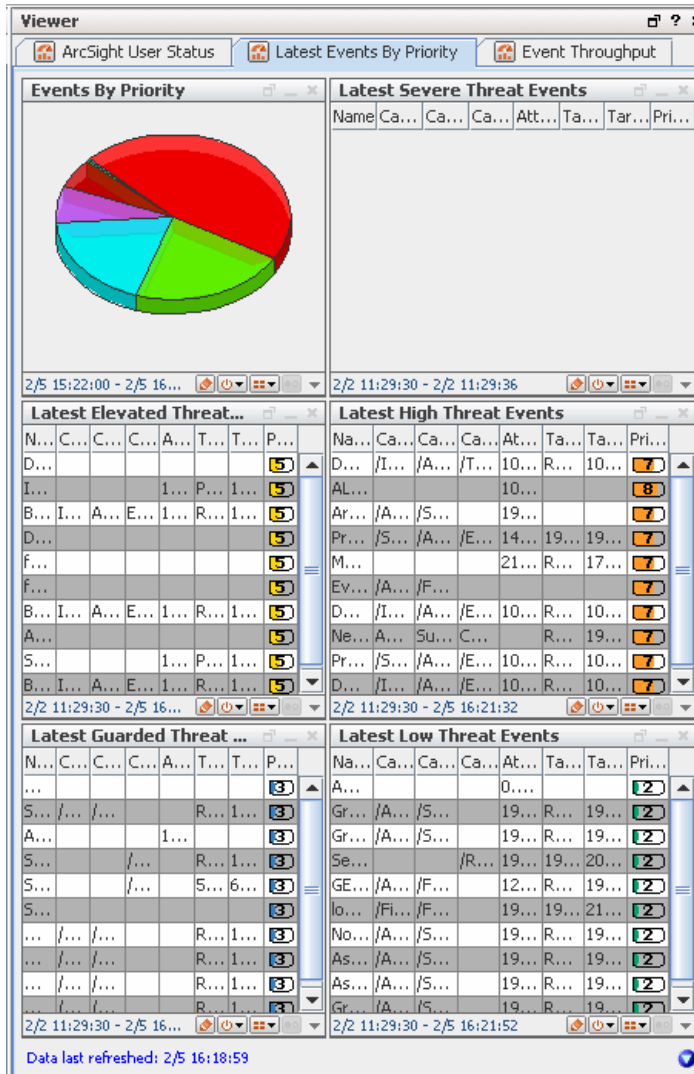
"Views" is a collective term for all the different options you have for seeing raw and processed [Events](#) information in the [ESM Console's](#) Viewer panel.

The ESM Console's Viewer panel can display event information in several formats and is readily customizable. Views may be customized to best reflect an enterprise and can be organized in a hierarchical structure with drill-down functionality. There is a list of chart-format views in addition to grids, maps, and dashboards.

See also "[Viewing](#)" on page 99 and "[Monitoring Active Channels](#)" on page 129.

View Types

Each view type represented by a tab at the **top** of the Viewer panel serves as a container for all individual instances of that type of view. For example, all data monitors opened in a dashboard remain part of it, and also inherit any visual choices you make for that view. Using the **View Layout** icon at the lower-right corner of the Viewer panel you can choose to tile or tab the individual views. When you tab the views, you select them using the tabs at the **bottom** of the panel.



With views you have the flexibility to monitor an enterprise from various perspectives. Views can be customized to best capture and reflect an enterprise's network infrastructure and can also be organized in a hierarchical structure with drill-down functionality. Views can vary in scope and scale, from broad to detailed, depending on how the enterprise is monitored and organized.

The ESM Console provides different views in which you can display event data in the Viewer panel. You can select which views to display by selecting options from the Views menu.

Other Views

The Viewer panel automatically shows HTML information such as reports, reference pages, results for the Web Search tool, and notifications in its Web Viewer tabs (as described in ["Viewing" on page 99](#).) The Viewer panel is also where you use the Find Resource query editor and result details display. (See also, ["Finding Resources" on page 671](#).)

Dashboards

Dashboards provide a more customized view of data, letting you create individual "instrument panels," each of which can display results based on different event data and filter conditions, and in different formats.

From the Viewer panel, you can change the view type or format of individual tabs from grid to line chart, bar chart, pie chart, or graphic. In addition, you can **float** the display of individual sub-view tabs, dashboards, and individual data monitors into separate windows to expand or resize individual displays.

While chart views display a summary of events, grid views display each event. Grid views display events organized in rows and columns. As new events occur, they are inserted at the top of the grid as a new row. Rows contain events while columns contain data fields.

Vulnerabilities

A vulnerability is a hardware, firmware, or software state that leaves an automated information system (AIS) open for potential exploitation. It could be due to anything, including circumstance, configuration, design, or implementation. A vulnerability can also be described as a weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

Vulnerabilities are discovered using scanners and their associated ArcSight SmartConnectors. The Manager imports the output from vulnerability scanners, recording them as items in the Vulnerabilities resource tree, in the Assets section of the Navigator panel. Vulnerabilities are mapped to their associated devices. Vulnerabilities describe asset threats and exposures and provide more information with a link to Knowledge Base articles or notes.

Vulnerability Groups

Vulnerability groups are created to store similar groups of vulnerabilities in a single location. Groups can be created within groups to meet enterprise needs. When a group is created within a group, the new group inherits the existing group's permissions. If a group is deleted, the vulnerabilities within that group are also deleted. The following groups are provided:

- **Shared:** vulnerabilities to which logged-in users have permission.
- **Unassigned:** vulnerabilities that are not assigned to a group.

If you have Administrator access you will have another group named All Vulnerabilities that contains all vulnerability groups and vulnerabilities.

Standardized Vulnerability Tracking

In the Vulnerabilities tab of the Assets resource tree, there is a branch for using the MITRE Corporation's CVE (Common Vulnerabilities and Exposures) standardized vulnerability naming and reference system.

CVE is a list (dictionary) of standardized names for vulnerabilities and other information security exposures. CVE seeks to standardize the names for all publicly known vulnerabilities and security exposures.

You can map CVE as one of its vulnerability reference authorities, within its Navigator panel resource tree. This information can serve, for example, to determine the significance of IDS events. The goal of CVE is to provide a common naming scheme, shared by vulnerability scanners and other security devices to link real-time events to asset vulnerabilities.

You can search its CVE-related Navigator panel resources by CVE name, and to include CVE names in its ESM Console or report output.

The requirements for CVE compatibility are fulfilled by the capacity to analyze event streams utilizing CVE names, generate reports for CVE-related vulnerabilities, map events to asset vulnerabilities, and the existence of documentation for CVE-related functionality.

Web Browsers (Internal and External)

You can launch HTML based information displays in an internal (ESM Console embedded) or external Web browser from the ESM Console.

Browser Preferences for HTML Displays

The ESM Console offers a general preference option for HTML display of various information in either your preferred external Web browser (external browser) or the ESM Console's built-in viewer (internal browser, displayed in a panel in the ESM Console).

The way you set these browser preferences determines display of reports, knowledge base articles, graphs and charts, and so forth. (For information on the general setting for HTML viewing preferences, see ["Preferred Web Browser" on page 773](#) in [Changing User Preferences](#).)

Browser Preference Overrides for Specific Features

Additionally, you can set your viewer preference for HTML displays specifically for certain features, and override the general preference setting for these specific displays. Some examples are:

- Integration command configurations (including integrated ArcSight Logger searches and NSP TRM commands). HTML display preferences for integrated command results are set as attributes on the command configuration. (The command *renderer* can be set to use either the internal browser or an external browser.) See ["Configurations Attributes" on page 612](#) in [Integration Commands](#) for more information.

- Online Help. You can set a preference specific to the Online Help for display in either the internal browser or an external Web browser. See [“Launch Help in external Web browser” on page 775](#) in [Changing User Preferences](#).



You can **launch an external browser** from a display shown in the ESM Console **internal browser**.

Click the URL shown at the top of any internal browser display to launch a standard Web browser and go to that URL.

Note that using an external browser is less secure. See [Advantages and Limitations](#) of [“Internal Browser Display Support” on page 1031](#).

External Browser Display Requirements

ESM Console features such as custom view dashboards, NSP TRM maps and charts, and the ESM Console Online Help require a Web browser with Adobe Flash and Javascript enabled.



External web browsers are not officially supported on Solaris (due to lack of Solaris support by Mozilla Firefox). This bars display on Solaris systems of image dashboards custom views, integration commands of URL type, and the ESM Console Help and documentation in an officially-supported Web browser.

You must have the Flash Player to view the custom view dashboards. If you have a 64-bit operating system, use a 32-bit Web browser. The Flash Player does not run on most 64-bit browsers. By default, Windows uses the 32-bit version of Internet Explorer on Windows 64-bit systems.

Internal Browser Display Support

The ESM Console internal browser is supported on Windows systems only. If you are using a system other than Microsoft Windows to run the ESM Console, use an external Web browser for HTML-based ESM Console displays. For Linux, Solaris, and Mac systems, set ESM Console preferences to:

- Use the external browser (see [“Preferred Web Browser” on page 773](#))
- Launch the Online Help in an external browser (see [“Launch Help in external Web browser” on page 775](#))

These two browser preference settings function independently, so you need to set both of them.

For integration commands of URL type that you want to run on all platforms, set the renderer to **external browser** for compatibility with Linux and Mac OS. (See [“Renderer” on page 612](#) in [“Integration Commands” on page 595](#).)

Advantages and Limitations

On Windows, the internal browser provides a focused, embedded display (in the ESM Console) and is inherently more secure than using an external browser choice, and we recommend it if security is a priority. Here is why:

The external browser process invokes the browser from a command line that enters the URL on its command line. The full URL and any authentication tokens (such as for TRM integration commands) are exposed to tools on the user's system such as a process

snapshot tool that can view a process listing. Also, the URL, along with any authentication tokens, is likely to be stored in a user's Web browser history.

Limitations of the internal browser are that it is not as versatile as an external Web browser, it has some special requirements and settings, and it is not currently supported on Mac operating systems as described below.

Flash Plug-in and Setup Requirements for Internal Browser

Allow Active X

Some ESM Console features, such as custom view dashboards (sometimes called image dashboards) and TRM integration command map results, require the Adobe Flash plug-in, which is an ActiveX control.

Set the following ESM Console properties to enable support for ActiveX controls in the internal browser. (By default, the internal browser does not allow display of ActiveX controls like Flash.) To allow ActiveX controls on the ESM Console internal browser, edit the file:

```
<ArcSight_ESM_Console_HOME>/current/config/console.properties
```

Add the following lines to the `console.properties` file:

```
jexplorer.allowRunActiveX=true  
jexplorer.allowDownloadActiveX=true
```

Install Firefox for Custom View Dashboards

By default, the ESM Console uses Windows IE technology for the internal browser. However, when you request a custom view dashboard, the ESM Console must use the Mozilla internal browser to support that type of display, so it switches. The internal switch is automatic, but you must have the Mozilla Firefox browser (and the Flash plug-in).

Install the Flash Player

For best results, install the Flash player plug-in both in Windows IE and Mozilla Firefox before you invoke the internal browser in the ESM Console. When the flash player is installed in the external browser, the internal browser uses it. If the Flash player is not installed when you invoke the internal browser, a dialog box appears with a link to a site where you can download the free Flash player plug-in.

However, the site is for the browser selected for your *external* browser. This might not be the same browser the ESM Console is trying to invoke.

For example: If your external browser is Windows IE, the link is to the Flash download for Windows IE. However if the ESM Console is trying to load a custom view dashboard, it is using the Mozilla internal browser and that link would be to the wrong site.

That is why it is best to install your Flash players in both Windows Internet Explorer and Mozilla Firefox before you start.

Index

A

- access control lists
 - for editing user group permissions 651
 - for event permissions 652
 - for operations permissions 649
 - for resource permissions 647
 - for sortable field set permissions 654
 - glossary definition 787
- acknowledge notification 186
- ACLs, *see access control lists*
- action
 - specify 185
 - summary 187
- action permissions. *See operations.*
- actions 788
- active channels 788
 - active lists and 790
 - actor channels 253
 - applying resources as filters 231
 - charts 143
 - collaborating on events 216
 - investigating actors in channels 258
 - modifying with filters 236
 - performance, best practices 137
 - query viewers comparison 138
 - replay-with-rules 470
 - report from grid view 427
 - using field sets 204
 - variables 1006
 - view panel 99
 - viewing and using 130
- active list 187
- active lists 790
 - audit events for 972
 - automating with rule actions 972
 - case-insensitive 573
 - fields-based, event-based 571
 - for identity correlation 561
 - general configuration 56, 62, 64
 - in trend actions 379
 - rules for add, remove items to 460
 - using, monitoring 174
- actors
 - about 239
 - actor channels 253
 - configuring 245
 - investigating actors in channels 258
 - model import connector 243
 - monitoring 239
- administrator 796
 - certification subjects 90
 - tasks, management 665
 - tasks, permissions and resources 646
 - tasks, send logs 980
 - users 646
- Adobe Flash
 - support in ESM Console browsers 1032
- agents
 - see SmartConnectors*
- aggregation, rule 199
- alias 185, 685
- annotate pattern 186, 196
 - editor 200
- arb file
 - see packages*
- archive
 - partitions 768
 - partitions, deactivating 769
 - partitions, reactivating 768
 - partitions, reactivating zipped or large 769
- ArcSight Console, *see Console*
- ArcSight Express
 - device list 75
- ArcSight Logger
 - integration commands 630
- ArcSight Manager, *see Manager*
- ArcSight NSP TRM
 - integration commands 623
- ArcSight Web 798
- Asian fonts in reports 406
- asset auto-creation filters
 - connector 79
 - device 81
- asset groups
 - creating 756
- asset ranges 736
 - CSV file 750
 - populating using wizard 750
- assets 733, 799
 - asset auto-creation 733, 801
 - asset ranges 736
 - asset tab 799
 - auto-zoning 755
 - categories 739
 - categories tab 800
 - category, criticality 55
 - creating 754
 - CSV file 748
 - data monitor for asset category count 906
 - deleting 755
 - editing 755
 - finding 757

- location tab 801
- modeling, protected network 54
- moving or copying 755
- networks tab 800
- populating using wizard 748
- retrieving vulnerable 760
- scalability 757
- showing in a channel 755
- vulnerabilities tab 801
- zones tab 800
- assets groups
 - deleting 757
 - editing 756
 - moving or copying 756
 - renaming 756
- attack 811
- attacker address 194
- attacks 179
- attributes, common 684
- audit events 811
- auto-zone 755
 - network model wizard 753

B

- baseline pattern 201
- baselines
 - adding to query viewers 304
- batching 829
- behavior category 836
- best practices
 - optimizing active channels 137
- browser
 - internal and external 1030

C

- case editor tab fields 829
- cases
 - attachments 589
 - creating 586
 - creating channels from 590
 - deleting 590
 - editing 587
 - exporting 591
 - finding by ID 588
 - glossary definition 835
 - properties 586
 - queries against 592
 - stages 218
- categories
 - behavior 836
 - custom 844
 - device group 837
 - grouping assets in 753
 - managing as assets 799
 - object 836
 - outcome 836
 - overview 836
 - significance 837
 - tab 800
 - technique 837
- changing a filter 224
- channel
 - create from pattern block 196

- create in grid view 194
- channels, see *active channels*
- charts
 - in channels and data monitors 143
- collaboration 845
- command string 186
- commands
 - integration 595
- common conditions editor 846
- component, pattern 180
- conditions
 - CCE 846
 - common conditions editor 846
 - editor 846
 - glossary definition 860
 - statements 859
- conditions, rule 199
- Configuration
 - integration commands 612
- configuration
 - active lists 56, 62, 64
 - asset auto-creation filters 56
 - connector asset auto-creation filter 57, 79
 - device asset auto-creation filter 59, 81
 - schedule reports 85
 - set up connectors and model the network 75
 - SNMP trap forwarding filter 60
- connector command 187
- connectors
 - see *SmartConnectors* 984
- Console
 - glossary definition 862
 - menus 114
- content 862
- context reports
 - actors 258
- correlation
 - correlation event generating fields 911
 - glossary definition 863
 - rule 863
 - session 983
- CounterACT
 - integration commands 595
- create channel 196
- create rule 194, 196
- custom view dashboards 167
- customers
 - creating 766
 - deleting 766
 - editing 766
 - managing as a resource 766
 - resource 864

D

- Daily Pattern Discovery profile 182
- dashboards
 - adding data monitors to 157
 - adding query viewers 302
 - audit events 817
 - creating 156
 - custom view dashboards 167
 - deleting 158
 - editing 158
 - glossary definition 864

- image dashboards
 - see *custom view dashboards* 167
 - data fields 867
 - derived (shown in italics) 207
 - exporting to CSV file 213
 - data monitors
 - adding to dashboards 157
 - Asset Category Count Data Monitor 906
 - charts 143
 - conditional expressions 938
 - controlling user permissions to deploy 656
 - creating 160
 - deleting 161
 - deploying, undeploying 161
 - editing 161
 - enabling, disabling 161
 - Event Correlation Data Monitor 907
 - Event Graph Data Monitor 908
 - Event Reconciliation Data Monitor 909
 - glossary definition 905
 - Hierarchy Map Data Monitor 913
 - Hourly Counts Data Monitor 922
 - Last *n* Events Data Monitor 923
 - Last State Data Monitor 924
 - Moving Average Data Monitor 928
 - overriding last state 163
 - permissions to deploy 656
 - Statistics Data Monitor 933
 - System Monitor Attribute Data Monitor 936
 - System Monitor Data Monitor 936
 - Top Value Counts Data Monitor 937
 - types 905
 - data types
 - domain fields 493
 - standard schema 493
 - database 865
 - hints for queries and reports 404
 - day-zero attack 179
 - demarcation points 191
 - dependencies
 - managing in reports 335
 - deploylicense command 181
 - deprecated 685
 - derived fields 207
 - designer, reports 338
 - device 940
 - device group category 837
 - device list
 - standard content 53
 - discovery, how it works 181
 - divisions, transaction 180
 - domain field sets 491
 - creating 500
 - domain field data types 493
- E**
- editor
 - rules 440
 - editors
 - common conditions 846
 - queries 357
 - reports 387
 - trends 372
 - empty triggers 187, 199
 - end time, snapshot 184
 - ESM schema 979
 - event
 - field-based division 180
 - fields 184
 - graph 194
 - grouping 181
 - events
 - aggregation 798
 - aliases in rule conditions 973
 - audit 811
 - categories 836
 - categorization, custom 844
 - collaborating on 216
 - context report 427
 - data fields 867
 - data monitor for event correlation 907
 - data monitor for event graph 908
 - data monitor for event reconciliation 909
 - data monitor for hierarchy map 913
 - data monitor for hourly counts 922
 - data monitor for last *n* events 923
 - data monitor for last state 924
 - data monitor for moving average 928
 - data monitor for statistics 933
 - data monitors 905
 - filtering 223
 - glossary definition 941
 - grid views 213
 - inspector 940
 - internal, audit 811
 - internal, status monitor 988
 - monitoring 129
 - payloads 219
 - prioritization fields 956
 - status monitor 988
 - system, see *internal events*
 - using attributes to show filtered views 234
 - viewing in inspect/edit panel 945
 - visualizing 176
 - export pattern 187
 - exporting
 - cases to external systems 591
 - data fields to CSV file 213
 - events to a file from grid view 147
 - see also *importing and exporting* 147
 - external ID 185
- F**
- field sets
 - creating 205
 - creating domain field sets 500
 - domain field sets 491
 - editing 211
 - glossary definition 942
 - see also *data fields* 867
 - sharing 211
 - sortable 987
 - fields
 - avoiding naming collisions 979
 - derived (shown in italics) 207
 - prioritization 956
 - see also *data fields* 867

- see also *field sets* 204
- files
 - adding to packages 669
 - as attachments to cases 588
 - creating as resources 666
 - deleting 668
 - downloading 668
 - editing resource attributes 668
 - finding 669
 - managing as resources 665
 - replacing 668
 - uploading 666
 - viewing 668
- filter groups
 - creating 232
 - deleting 233
 - editing 232
 - moving or copying 233
 - renaming 232
- filter patterns 196
- filters
 - adding an event attribute 235
 - adding to resources 231
 - creating for SmartConnectors 712
 - creating inline 225
 - creating new 223
 - debugging to match events 227
 - deleting 227
 - exporting, see *packages*
 - filtering out ArcSight events 235
 - for showing exploited vulnerabilities 236
 - for showing targeted assets 236
 - glossary definition 942
 - importing, see *packages*
 - modifying a view 237
 - modifying an active channel 236
 - moving or copying 226
 - on active channels 231
 - refining with an event attribute 234
 - removing a filter condition 231
 - removing a resource 231
 - SmartConnectors 712
- filters resource tree 184
- finding
 - resources in the Console 671
- Flash
 - Adobe Flash support in browsers 1032
- font, Unicode in reports 345
- fonts
 - Asian in reports 406
- foundations 48
- functions
 - see *variables* 1006

G

- global variables 477
- graphs
 - creating to visualize resources 674
 - using 675
- grid views
 - exporting events from 147
 - for resources 677
 - glossary definition 944
 - reports from 427

- group
 - notification 185
 - pattern 185
 - snapshot 185
- groups
 - assets 756
 - filters 232
 - notifications 659
 - reports 430
 - rules 441
 - SmartConnectors 722
 - users 1005
 - vulnerabilities 761

H

- Help
 - setting Web display preference 775
- hotkeys 779
- HP OpenView Operations 456
- HTML
 - report format 402
 - see also *Web*

I

- ID
 - external 685
 - resource 685
 - version 685
- iDefense 944
- identity correlation, see *session correlation*
- image dashboards
 - see *custom view dashboards* 167
- importing and exporting
 - active lists 577, 578
 - cases to external systems 591
 - data fields to CSV file 213
 - events to a file from grid view 147
 - filters 232
 - reports 429
 - rules 463
 - SmartConnector configurations 724
- inactivity 184
- inline filters
 - creating 225
 - modify view inline 237
 - undoing 237
- inspect/edit panel 945
- integration commands
 - ArcSight Logger 630
 - ArcSight NSP TRM 623
 - overview 595
- integration parameters 632
- internal events
 - audit 811
 - status monitor 988
- invalid resource
 - troubleshooting 680
- invalid resources
 - fixing 678
 - overview 677
- italics
 - on derived fields 207

J

Japanese characters, in reports 345
 Java heap memory, adjusting 267
 job scheduler 977

K

keys
 shortcut 779
 knowledge base 946
 article groups 639
 associating articles 640
 creating articles for 637
 getting articles 221
 getting updates 640
 managing articles 637

L

latitude
 preference setting for locations 777
 layout, snapshot 192
 learning paths 89
 length, minimum pattern 183
 license file 181
 lists
 active 790
 session 983
 locations
 describing as assets 753
 editor 765
 latitude, longitude format for 777
 managing as assets 799
 tab 801
 locks
 on resources 669
 Logger
 integration commands 630
 LoggerPort 632
 logical operators 947
 logs
 sending to ArcSight 980
 longitude
 preference setting for locations 777
 low-and-slow attack 180

M

Managed Security Service Providers, see *MSSPs*
 Manager
 glossary definition 948
 performance related to custom rules 474
 reconnecting 99
 master use cases 513
 menus 114
 Console 114
 Edit 114
 File 114
 Help 117
 System 117
 Tools 116
 Views 115
 Window 116

minimum pattern length 183
 model confidence
 in prioritization fields 956
 in priority calculations 957
 maintaining by threat evaluation 999
 model mappings
 sending to SmartConnectors 715
 MSSPs
 customer resources for 864
 glossary definition 948
 useful query-trend reporting features for 371
 myArcSight
 see ArcSight Web 798

N

naming collisions
 field names 979
 navigating resource types 94
 navigator panel 948
 network model wizard
 asset CSV file 748
 asset ranges CSV file 750
 auto-zone 753
 column types 745
 using 744
 zone CSV file 747
 network modeling
 ArcSight Express 75
 asset categories 739
 assets 733
 auto zone 753
 auto-created assets 733
 batch loading 744
 bulk loading 744
 networks 737
 what is 54
 wizard 744
 zones 736
 network tools
 as integration commands 634
 standard 107
 networks 737
 describing as assets 753
 editor 764
 managing as assets 799
 sending model mappings to SmartConnectors 715
 tab 800
 normal patterns 201
 notes
 tabs in resources 111
 notes, profile 188
 notification
 group 185
 send 186
 notifications
 acknowledging, managing received 658
 audit events 822
 categories 658
 destinations 660
 e-mail settings 662
 glossary definition 949
 groups and levels 659
 inbound 658
 messages and velocity templates 1021

- pager services 663
- popup preferences 772
- rule trigger 460
- testing groups and destinations 663
- using 110
- wait time settings 663
- Nslookup 194
- nslookup
 - integration command 635
 - standard 108
- NSP TRM
 - integration commands 623

O

- object category 836
- occurrences, pattern 183
- One-Time Password (OTP) 633
- OpenView Operations 456
- operations
 - permissions on 649
 - permissions to deploy data monitors 656
 - setting permissions on 649
- operators
 - logical 947
- OTPUser 632
- outcome category 836
- owner 185

P

- package version ID 185
- packages
 - adding files to 669
 - adding resources to 691
 - arb import bundles 689
 - creating 687
 - deleting 691
 - editor 687
 - exporting 690
 - glossary definition 951
 - importing 689
 - installing 690
 - managing 686
 - removing resources from 691
 - resolving conflicts 692
 - uninstalling 691
 - zones 763
- panel, navigator 948
- parent groups 685
- partitions
 - archiving 768
 - audit events 823
 - deactivating archives 769
 - getting information on 767
 - glossary definition 951
 - managing 767
 - properties 770
 - reactivating archives 768
 - reactivating zipped or large archives 769
 - schedules 767
 - schedules, overriding to run tasks now 769
- passwords
 - changing for user 643, 773
 - changing yours 773

- pattern
 - active list 187
 - baseline 201
 - component 180
 - definition 179
 - delete 201
 - export 187
 - group 185
 - how discovery works 181
 - in snapshot view 194
 - inspector 197
 - length 183
 - occurrences 183
 - session list 187
 - support 191
 - transaction 180
 - view filtered 196
- pattern discovery
 - audit events 823
 - glossary definition 952
- payload 956
- payloads
 - for events 219
- performance
 - active channels best practices 137
 - reports and queries 404
- permissions
 - managing users, user groups 646
- Ping 194
- ping
 - integration command 635
 - standard 108
- PortInfo 194
- portinfo
 - integration command 635
 - standard 108
- preview
 - variable inputs 1008
- prioritization fields 956
- priority
 - calculations 957
 - color code 960
 - formula, criticality asset categories 55
- profile
 - create 182
 - Daily Pattern Discovery 182
 - modify 183
 - notes 188
 - Quarter Hourly Pattern Discovery 182
- protected network
 - how ArcSight determines 77

Q

- Quarter Hourly Pattern Discovery profile 182
- queries
 - active channels comparison 138
 - and trends in reports 370
 - attributes for 357
 - creating 356
 - editing 368
 - editor 357
 - for finding resources in Console 673
 - for reports, glossary definition 961
 - overview 354

- performance for reports 404
- see also *query viewers* 287
- query viewers
 - adding to dashboards 302
 - audit events 824
 - baselines in 304
 - custom 290
 - generating reports for 303
 - overview 287
 - pre-built 289
 - see also *queries* in Reporting topics 354
 - using 291

R

- radar display
 - active channel headers 134
 - area in charts 144
 - example, operation in channel headers 790
- reference pages 962
- relevance
 - of events based on priority 956
 - of threats 999
- remote variables 1007
- replay-with-rules channels 470
- Report Designer documentation 338
- reports
 - active channels comparison 138
 - advanced example 410
 - archiving 431
 - ArcSight Express, scheduling 85
 - audit events 824
 - beginner example 407
 - copying 429
 - creating 385
 - CSV format 402
 - editor 387
 - end-to-end examples 407
 - event context 427
 - exporting 429
 - glossary definition 963
 - groups 430
 - HTML format 402
 - importing 429
 - managing dependencies 335
 - moving 429
 - on query viewers 303
 - on vulnerable assets 763
 - parameterized entries 433
 - PDF format 402
 - performance 404
 - queries 354
 - RTF format 402
 - running delta 426
 - running from grid view 427
 - running new or archived 423
 - scheduling 433
 - stopping 96
 - templates 335
 - trends 369
 - variables 1006
 - velocity references for 1023
 - wizard 407
 - workflow 331

- reports templates
 - creating new 338
 - designer 338
 - designer UI tour 339
 - designing custom 338
 - editing 338
 - glossary definition 966
 - navigating to 335
 - overview 335
 - using pre-built 336
- resources 967
 - access control lists (ACLs) 787
 - adding filters to 231
 - attributes, common 970
 - attributes, common, in editors 684
 - audit events 812
 - customers 766, 864
 - deprecated 685
 - finding 671
 - fixing 678
 - graphs 674
 - graphs, configuring 676
 - locking, unlocking 669
 - navigating 94
 - notes 111
 - printing and saving definitions 120
 - saving copies 684
 - selecting 670
 - shared resources 50
 - sharing 656
 - system core content 669
 - troubleshooting invalid 680
 - validating 677
 - viewing in grids 677
 - visualizing 674

Results 194

- rule
 - aggregation 199
 - conditions 199
 - create from pattern 196
 - create from snapshot 194
 - editor 198
- rules
 - actions 451, 972
 - aggregate thresholds 449
 - authoring 439
 - automatic disabling 475
 - chains 454, 977
 - conditions 442, 973
 - correlation 863
 - creating 441
 - custom rules and Manager performance 474
 - data monitor for partial match 931
 - deploying real-time 473
 - editor 977
 - enabling, disabling 461
 - errors 468
 - glossary definition 974
 - groups 441
 - importing and exporting 463
 - load and performance 474
 - managing 440
 - negated events 444
 - replaying events with 470
 - scheduling 463

- testing 468
- testing against events 470
- thresholds and aggregation 449
- triggering with actions 460
- variables 1006
- verify with events 470
- verifying with events 470

Rules Partial Match Data Monitor 931

S

- Save to Target 633
- Save to User 633
- saving
 - copies of resources 684
- schedule snapshot 192
- schedules
 - audit events 826
 - for partitions 767
 - jobs 977
 - overriding to run partition tasks now 769
 - reports 433
 - rules 463
- schema 979
- searching
 - for resources 671
 - query options to find resources 673
- send logs 980
 - toolbar command 108
- sequence of events 184
- session correlation 983
- session list 187
- session lists 983
 - audit events 827
- severity
 - of threats 999
 - setting levels 713
- sharing
 - resources 656
- shortcut keys 779
- significance category 837
- SmartConnector command 187
- SmartConnector groups 722
 - creating 722
 - deleting 723, 724
 - editing 723
 - moving or copying 723
 - renaming 722
- SmartConnectors
 - adding filter conditions 712
 - commands 715
 - configuration fields 696
 - configuring 695
 - default Content tab configuration fields 697
 - deleting filter conditions 713
 - editor option tabs 696
 - event severity levels 713
 - exporting configurations 725
 - filters 726
 - filters, creating 712
 - flow-control commands 715
 - for ArcSight Express content 75

- for standard content 53
- getting status 715
- glossary definition 984
- importing configurations 724
- network model mappings 715
- processing categories 711
- rollback to previous version 729
- time interval options 711
- turbo mode 706
- upgrading 726

SmartFolders 96

SMTP 986

snapshot

- controls 191
- delete 193
- end time 184
- group 185
- layout 192
- patterns 194
- re-open 193
- retention 185
- schedule 192
- start time 183
- viewer 190

sortable field sets 987

source fields 184

stages

- creating for cases 218
- editing for cases 219

standard content

- actor context reports 261
- device list 53
- foundations 48

start time, snapshot 183

status monitor events 988

sub-pattern 191

support level 181

support, pattern 191

system content 49

system events, see *audit events*, *status monitor events*, or *internal events*

T

- target fields 184
- Target, save to 633
- targets
 - integration commands 615
- technique category 837
- templates
 - reports, see report templates
 - velocity 1019
- threat
 - evaluation 999
 - glossary definition 999
- thresholds 1001
- time
 - error correction 1002
 - timestamp variables 1003
 - timestamps 1002
 - UTC times 1002
 - zone correction 1003

- time spread 197
 - time zone correction 1003
 - time-based division 180
 - timestamp expression 183
 - toolbars 105
 - tools
 - network 107
 - Traceroute 194
 - traceroute
 - integration command 635
 - standard 108
 - transaction, pattern 180
 - transactions table 197
 - trends
 - active channel comparison 138
 - and queries in reports 370
 - audit events 828
 - creating 371
 - editing or viewing definition 385
 - editor 372
 - enabling, disabling 67
 - glossary definition 1004
 - interval 370
 - overview 369
 - refreshing data 384
 - snapshot 369
 - system content, introduction to 64
 - testing 383
 - using in queries 385
 - using in reports 385
 - viewing data 383
 - trigger action 186
 - TRM
 - integration commands 595
 - turbo mode
 - on SmartConnectors 706
- ## U
- Unicode characters, in reports 345
 - uploading files 666
 - use cases 511
 - applying settings 524
 - categorizing assets/zones 526
 - installing 516
 - master 513
 - navigating to 513
 - opening 517
 - overview 511
 - scheduling daily report 532
 - scheduling monthly report 536
 - scheduling weekly report 534
 - scheduling yearly report 538
 - summary 524
 - wizard 518
 - user groups 1005
 - ACL edit permissions, deleting 651
 - ACL edit permissions, adding 651
 - creating 645
 - data monitor deploy permissions 656
 - deleting 646
 - editing 645
 - event permissions, adding 652
 - event permissions, deleting 652
 - moving or linking 646
 - operations permissions, adding 649
 - operations permissions, deleting 649
 - renaming 645
 - resource permissions, adding 647
 - resource permissions, deleting 647
 - setting startup views 646
 - sortable field set permissions, adding 654
 - sortable field set permissions, deleting 654
 - User, save to 633
 - users
 - access control lists (ACLs) 646
 - administrator 796
 - audit events 829
 - creating 641
 - deleting 644
 - editing 643
 - glossary definition 1005
 - groups, see user groups 1005
 - moving or linking 644
 - passwords 641
 - roles and learning paths 89
 - types 1006
 - user-created content 670
 - UTC times 1002
- ## V
- validating resources
 - automatic or manual 682
 - overview 677
 - requirements 680
 - variables 1006
 - arithmetic functions 1010
 - conditional functions 1012
 - field sets and 204
 - global variables 477
 - group functions 1013
 - IP address functions 1014
 - list functions 1014
 - preview 1008
 - remote variables 1007
 - string functions 1014
 - timestamp 1003
 - timestamp functions 1015
 - type conversion functions 1016
 - velocity templates
 - overview 1019
 - references for reports 1023
 - rules example 1022
 - usage tips 1023
 - VeriSign iDefense 944
 - version ID, package 185
 - viewer, snapshot 190
 - views
 - glossary definition 1028
 - graph 674
 - grid 944
 - investigating 140
 - modifying with filters 237
 - Web 99
 - vulnerabilities
 - describing as assets 753
 - vulnerabilities
 - adding an asset to 760
 - creating 759

- CVE and 1030
- deleting 760
- deleting an asset from 760
- editing 759
- editor 759
- glossary definition 1029
- managing as assets 799
- moving or copying 760
- tab 801
- vulnerability groups
 - creating 761
 - deleting 761
 - editing 761
 - moving or copying 761
 - renaming 761

W

- Web
 - browsers, internal and external 1030
 - saving, printing resource definitions as HTML 123
 - see also ArcSight Web
 - setting preference for Online Help display 775
 - setting preferred Web browser 773

- viewer panel 99
- WebSearch network tool 107
- WebSearch 194
 - integration command 635
 - standard 108
- Whois 194
- whois
 - integration command 635
 - standard 108
- wizards
 - network model 744
 - Use Case 518

Z

- zones 736
 - CSV file 747
 - describing as assets 753
 - editor 763
 - managing as assets 799
 - populating using wizard 747
 - shrinking or splitting 763
 - tab 800