

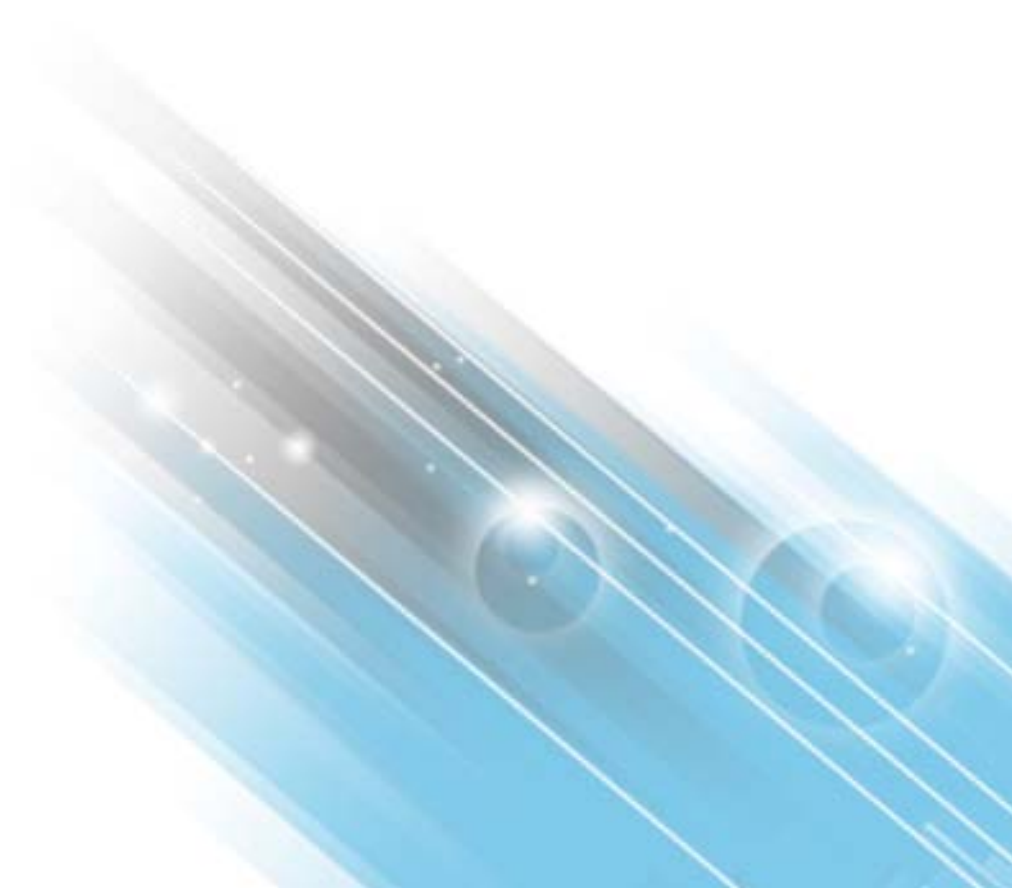


HP ArcSight Web

HP ArcSight ESM 5.6

User's Guide

August 20, 2015



Copyright © 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

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

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Contact Information

Phone	A list of phone numbers for HP ArcSight Technical Support is available on the HP Enterprise Security contacts page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	http://softwaresupport.hp.com
Protect 724 Community	https://protect724.hp.com

Revision History

Date	Product Version	Description
08/20/2015	5.6	Updated for ESM 5.6 release.

Contents

Chapter 1: Welcome to ArcSight Web	7
Chapter 2: Navigating ArcSight Web	9
Basic Navigation	9
Navigating the Home Page	11
Recent Notifications	11
My Cases	11
Dashboards	11
Active Channels	12
Monitoring with Active Channels	12
Monitoring with Dashboards	12
Reporting	13
Chapter 3: Using Active Channels	15
Opening Active Channels	15
Viewing Active Channels	17
Using Active Channel Headers	17
Using Active Channel Grids	18
Supported Expressions for Inline Filtering	19
Inspecting Events	19
Event Inspector Header Features	20
Event Inspector Field Features	20
Show Details for Event Attributes	21
Event Categories	21
Event Data Fields	28
Connector Group	28
Attacker Group	31
Category Group	35
Destination Group	36
Device Group	39
Device Custom Group	42
Event Group	44
Event Annotation Group	49
File Group	52

Final Device Group	52
Flex Group	55
Manager Group	56
Old File Group	56
Original Connector Group	57
Request Group	59
Source Group	60
Target Group	64
Threat Group	67
Resource Attributes	68
Geographical Attributes	68
Audit Events	69
Resources (Configuration Events Common to Most Resources)	69
Active Channel	71
Active List	71
Actor	71
Authentication	72
Archive	72
Authorization	73
Connectors	73
Connector Connection	73
Connector Exceptions	74
Connector Login	75
Connector Registration and Configuration	75
Dashboard	75
Data Monitors	75
Last State Data Monitors	76
Moving Average Data Monitor	76
Reconciliation Data Monitor	76
Statistical Data Monitor	76
Top Value Counts Data Monitor	77
Domains (for Domain Fields)	77
Global Variables	77
Group Management	78
License Audit	78
Manager Activation	79
Manager Database Error Conditions	79
Manager External Event Flow Interruption	79
Notifications	79
Notification	80
Notification Acknowledgement, Escalation, and Resolution	80
Notification Testing	81
Pattern Discovery	81

Partition Archiver	81
Partition Manager	81
Query Viewers	82
Reports	82
Resource Quota	83
Rules	83
Rule Actions	83
Rule Activations	84
Rules Scheduled	84
Rule Firings	84
Rule Warnings	84
Scheduler	85
Scheduler Execution	85
Scheduler Scheduling Tasks	85
Scheduler Skip	85
Session Lists	85
Stress	86
Trends	86
Trends	86
Trend Partitions	87
User Login	88
User Management	88
Chapter 4: Using Cases	89
Managing Cases	89
Default Case Management Columns	90
Security Classification Default Letter Codes	90
Creating Cases	91
Initial Tab	92
Follow Up Tab	94
Final Tab	94
Events Tab	96
Attachments Tab	96
Notes Tab	97
Chapter 5: Handling Notifications	99
Chapter 6: Using Reports	101
Running and Viewing Reports	101
Running and Saving Archived Reports	102
Report Parameters	102
Viewing Archived Reports	103
Downloading an Archived Report	103
Adding New Archived Reports	104

Deleting Archived Reports	104
Advanced Configuration for Report Performance	104
Configurations for Large Reports	104
Configurations for Reports with Large Time Ranges	105
Chapter 7: Monitoring Dashboards	107
Viewing and Managing Dashboards	107
Changing Dashboard Layouts	107
Row Limits	108
Chapter 8: Using the Knowledge Base	109
Chapter 9: Using Reference Pages	111
Chapter 10: Setting Preferences	113
Options Menu	113
Hide Exception Reporting Details	113
Chapter 11: Custom Branding and Styling	115
Index	117

Welcome to ArcSight Web

ArcSight Web is the web interface to monitoring and reporting features of ArcSight ESM for operators and analysts engaged in network perimeter and security monitoring.

Because it can be installed at a location remote from the ArcSight Manager, it can operate outside a firewall that protects the Manager. Because of its design, it also offers opportunities for custom branding and styling.

Installing is described in the ESM Installation and Configuration Guide.

See [“Navigating ArcSight Web” on page 9](#) for a quick tour of all ArcSight Web's features.

For information about standard System or Administration content, refer to the Standard Content Guide — ArcSight System and ArcSight Administration. For information about an optional ArcSight Foundation, refer to the Standard Content Guide for that Foundation. ESM documentation is available on Protect 724 at (<https://protect724.arcsight.com>).

Chapter 2

Navigating ArcSight Web

Access the ArcSight Web server through whichever web browser you prefer: Internet Explorer or Firefox. The ArcSight Web home URL is `https://<IP address>:9443/arcsight/app`, where `<IP address>` is the IP address of the machine on which the web server is running. (A host name will work, but host names with underscores do not work on IE, so use the IP address.)



When an ArcSight Web session expires, the URL changes and you see a login screen that expects you to enter a user ID and a password. If you are using SSL, CAC, or RADIUS authentication which do not use a username/password combination to authenticate, change the URL back to `https://<IPaddress>:9443/arcsight/app` and relaunch ArcSight Web. For SSL, your certificate is used to login. For CAC or Radius, the authentication dialog prompts you for a pin or passcode, not a user ID and a password.

[“Basic Navigation” on page 9](#)

[“Navigating the Home Page” on page 11](#)

[“Monitoring with Active Channels” on page 12](#)

[“Monitoring with Dashboards” on page 12](#)







[“Reporting” on page 13](#)

Basic Navigation

Use the Dashboards, Reports, Channels, Cases, Notifications, and Knowledge Base links at the top of the display to go to those features. A link to Customer Support is also provided. The top bar also has the client's basic controls.

- Click **Help** to open this Help window. To visit previously viewed Help pages, you can use standard keyboard commands for **Back** and **Next**. For example, on most Web browsers running on Microsoft Windows systems, you can hit the **Backspace** key to show the previously viewed page (move backward in the History) and **Shift + Backspace** to move forward in the History of viewed pages.
- Click **Options** to change your preferences concerning date and time formats, locale settings, active channel setup, and your password. For information on password restrictions see the Administrator's Guide, chapter 2. "Configuration" > "Managing Password Configuration."
- Click **Logout** to leave the client and log in again, or browse elsewhere. If you leave the client idle for a period of time you may need to log in again because of an automatic security time-out.

Click the ArcSight logo in the upper-left corner of the Home display to see version and licensing information. The six pages available are indicated by icon tabs across the top of the display:

Button	Description
	Home
	Dashboards
	Reports
	Active Channels
	Cases
	Recent Notifications

Home

The Home link returns you to the home page from any other view.

Dashboards

The Dashboards section lists a set of data monitor dashboards that expose selected analytical security information about your enterprise. Click a dashboard's name to open it.

Reports

The Reports section lists available reports. Reports are captured views or summaries of data extrapolated from the ArcSight System by means of queries and trends. Reports communicate the state of your enterprise security. Click a report, set the parameters or accept the defaults (HTML or PDF), and click **Run Report**. You have the option of saving the Report results in a variety of file formats to your local system, or just viewing the results in the ArcSight Web window.

Active Channels

Active Channels display the filtered events as they stream through the system. Click a channel to open it as a grid view in which you can inspect individual events. You can pause channels, and sort event columns in the grid.

Cases

The Cases section summarizes currently tracked, event-related security situations by the area they fall into (rows) and the workflow-style stage they have reached (columns). Click a type and stage cell to see more detail.

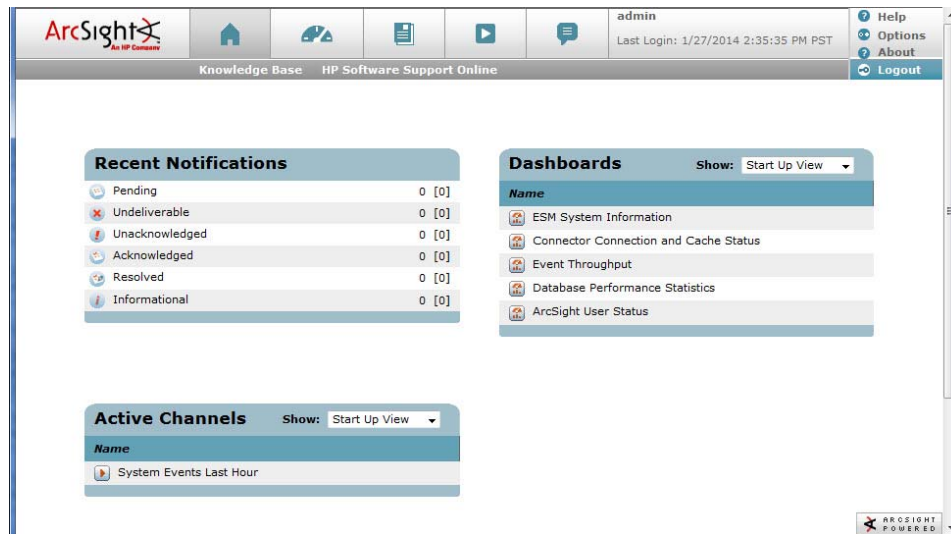
Recent Notifications

The Recent Notifications section summarizes ArcSight notifications by workflow-style categories. Click a category to see more detail.

Navigating the Home Page

The ArcSight Web client opens to the Home display. From here you can easily reach everything the client offers.

The ArcSight Web home page displays a series of basic views designed to give you an overview of activity that concerns you. These views are described below.



The Home display's summaries are quick references and links to the most-appropriate or most-interesting security resources in your enterprise. The initial or default information in each group is configured by your ArcSight administrator. In the sections that offer a **Show** menu, you can choose **Start Up View** to see this default or **Personal Folder** to switch to resources selected by or assigned to you.

The information summarized in the Home display is identical to, although possibly a subset of, the same information managed through the ArcSight Console. It is simply presented in a browser-compatible format.

Recent Notifications

Recent notifications show the status of notifications generated by correlated events that concern you. To view the details of a notification, click any line item to go to the Notifications page. For more about notifications, see ["Handling Notifications" on page 99](#).

My Cases

My cases show a snapshot of cases assigned to the user who is currently logged in. For details, click the cases icon to go to the Cases page. For more about cases, see ["Using Cases" on page 89](#).

Dashboards

Dashboards show a selection of key dashboards. You can select among these views:

- **Start Up View:** The start-up view provides quick access to the Security Activity Statistics and Current Event Sources dashboards. These dashboards give you a comprehensive general view of the security state of your environment and the sources where the events are generated.
- **Personal Folder:** This view contains dashboards that you have modified and saved.
- **Recent Dashboards:** This view shows the last five dashboards you viewed to enable you to easily toggle among several dashboards without having to navigate to them in the Dashboard tab.

Click any of these links to display the dashboard itself.

Active Channels

- **Start Up View:** The start-up view provides a link to the Correlated Alerts channel, which shows all events generated by rules. These events are considered to be events of interest that warrant attention.
- **Personal Folder:** This view contains active channels that you have modified and saved.
- **Recent Channels:** This view shows the last five active channels you viewed to enable you to easily toggle among several active channels without having to navigate to them in the active channels tab.

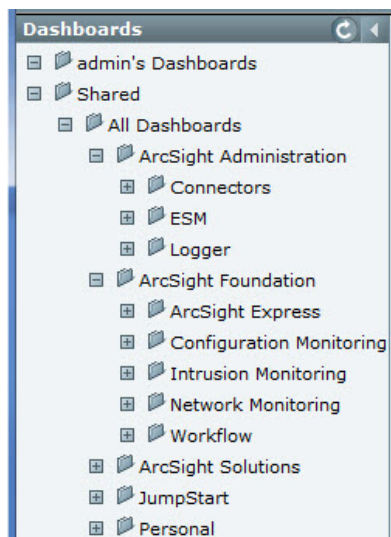
Monitoring with Active Channels

The active channels contain folders for groups of channels. They vary according to the packages you might have installed. The standard active channels you see in this view depend on the packages installed on the Manager, and the permissions granted the user.

For instructions about how to use active channels, see [“Using Active Channels” on page 15](#).

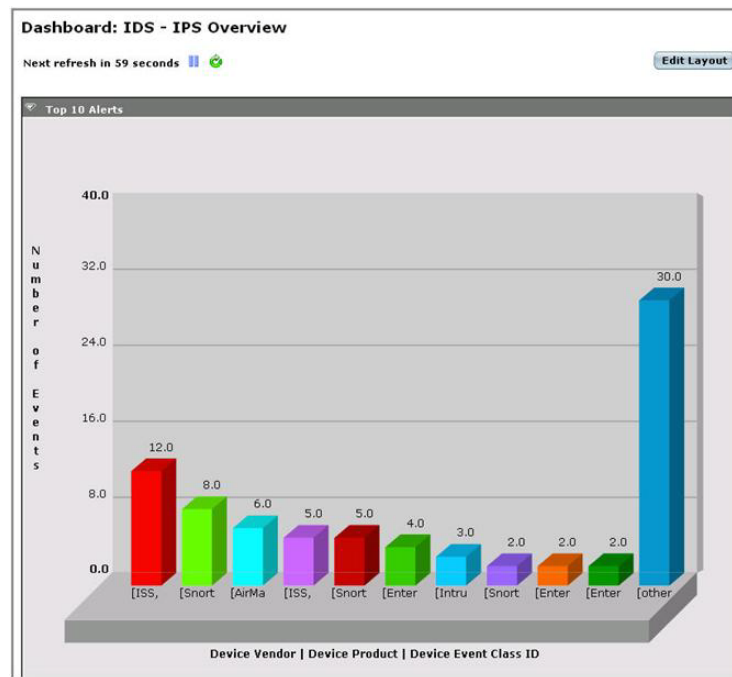
Monitoring with Dashboards

The dashboards contain folders for dashboard groups. They vary according to the packages you might have installed. Explore the dashboards to find views you are interested in. Here is an example:



The ArcSight Administration dashboards display information about the health of the specified component.

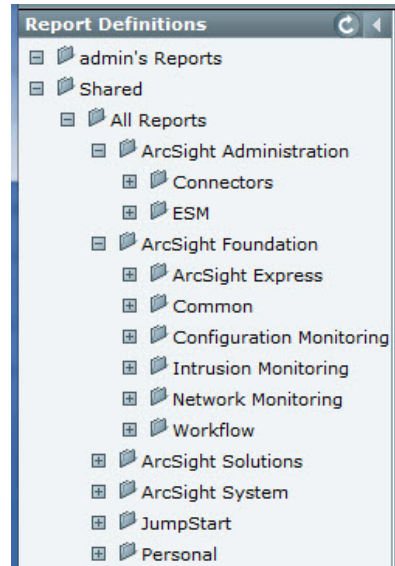
The example below shows the IDS-IPS dashboard, which summarizes the number of events from IDS and IPS systems. Click on any bar to view the details of the events represented in this bar in a channel.



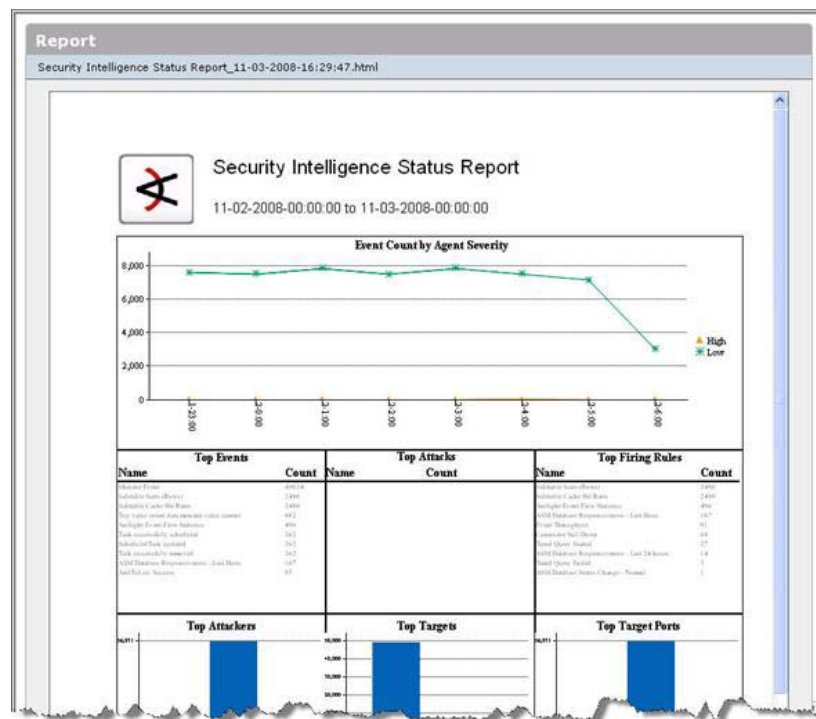
For more about working with dashboards, see ["Monitoring Dashboards" on page 107](#).

Reporting

The report definitions contains groups that might vary according to the packages you have installed. Here is an example:



For example, the Security Intelligence Status Report provides a summary of event counts and top events, attacks, targets, ports, and so on.



For more about running reports, see [“Using Reports”](#) on page 101.

Chapter 3

Using Active Channels

The event information presented in the ArcSight Web active channel views is the same data presented in the Console. The web client makes channels accessible from anywhere on your enterprise network, or even outside a firewall.

Using active channels includes opening them, controlling their views, and drilling down into the individual events that channels collect.

["Opening Active Channels" on page 15](#)

["Viewing Active Channels" on page 17](#)

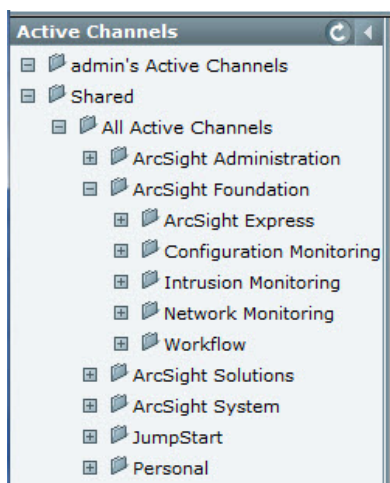
["Inspecting Events" on page 19](#)

["Event Data Fields" on page 28](#)

["Audit Events" on page 69](#)

Opening Active Channels

To open an active channel, click its name in the Active Channels section of the Home display, or click the Channels icon in the toolbar and choose a channel in the Active Channels resource tree. Channels you click in the Home display open directly, but channels you choose in the resource tree offer a setup page before opening.



Use the Open Active Channel setup display to adjust the timing, filter, and column-set parameters of the channel, if necessary. This display appears unless you have turned channel setup off (bypass channel setup) in the Channels panel of the Options display.

There is also an option to hide (collapse) the channel tree on the left panel when a channel is already running. By default, this tree remains in view. Click the Show (▶) or Hide (◀) buttons at the top of the left panel to show or hide the folder tree.

Active Channel Parameters

Option	Description
Channel	Read-only field that shows the channel name.
Start Time	The relative or absolute time reference that begins the period in which to actively track the events in the channel. Edit the time expression or clear the Date expression check box to use an absolute date and time.
End Time	The relative or absolute time reference that ends the period in which to actively track the events in the channel. Edit the time expression or clear the Date expression check box to use an absolute date and time.
Evaluate parameters continuously	Choose whether the channel shows events that are qualified by Start and End times that are re-evaluated constantly while it is running (selected), or show only the events that qualify when the channel is first run (cleared).
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.
Field Set	<p>The Field Set you choose here determines which columns show up in the active channel display. By default, a standard list of columns is shown in the channel.</p> <p>Choose an existing field set to control the selection and order of the columns in the grid or choose More Choices or click the plus sign (+) to open the Field Sets resource tree. The None option clears a field set and restores the channel to its original definition.</p> <p>Global variables make it possible to define a variable that derives particular values from existing data, then re-use it in multiple places wherever conditions can be expressed, and wherever fields can be selected. For more information about global variables, see "Global Variables" on page 445, in the ArcSight Console User's Guide.</p> <p>If your system is configured with <i>domain field sets</i> (a separately-licensed feature), these are available to select here as field set choices. For more information about domain field sets, see the "Domain Field Sets" topic in the ArcSight Console User's Guide.</p>

Option	Description
Filter Override	<p>You can use the Filter Override to narrow the event flow in the channel to only those events that satisfy conditions you specify here. You have these options for Filter Override:</p> <ul style="list-style-type: none"> Simply choose an existing filter. You can choose a recently used filter from the drop-down menu, or navigate to other filters by clicking More Choices or clicking the plus sign (+) to override the default channel filter. (The None option clears a filter choices and restores the channel to its original definition.) <p>Or</p> <ul style="list-style-type: none"> Explicitly specify new filter conditions for the channel by using event attributes (field groups and fields) or an existing filter (MatchesFilter) as part of a condition. <p>You can use <i>domain fields</i> to create conditions on channels the same way that you use other fields. If available, domain field sets show up under Event Attributes with the other field groups. For more information about domains, see the “Domain Field Sets” topic in the ArcSight Console User’s Guide.</p> <p>You can review the conditions of the filter in the active channel header (see “Using Active Channel Headers” on page 17).</p>

Viewing Active Channels

This topic explains how to understand, change, and drill into the grid views of active channels.

Using Active Channel Headers

Using active channels begins with reading and understanding their headers. You can use the **Modify** button to edit information and settings in the Header. Headers display the following information in the space above the event list:

Feature	Usage
Name and Total	The top line of the header shows the channel's name and the percentage of qualifying events that are currently loaded in the view.
Time Span	The Start Time and End Time show the chronological range of the channel.
Evaluation	This flag indicates whether the channel is set to evaluate events continuously as they are received, or only once when the channel opens.
Filter	This text describes the filter that limits what the channel shows.
Priority Totals	On the right side of the header is a column of event-priority category totals. The figures are the number of events in those categories.
Channel State	The channel state box contains a play and pause button and a refresh progress bar. This display indicates whether the channel is running or paused, and if it is running, the progress of the next refresh cycle.

Feature	Usage
Radar Display	<p>The Radar display in active channel headers indicates the activity taking place in the entire channel (not just the current page). Its graphics 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.</p> <p>To focus the grid on the event of one period, click that bar in the display. To restore the display, click Clear at the right end of the bar. Your sorting choices in the grid affect the arrangement of the activity units in the Radar.</p>
Time Range	<p>The Displaying bar below the Radar display and above the grid header shows the time range of the events selected in the Radar display and reflected in the grid. If nothing is selected, the time range shows All.</p>

Using Active Channel Grids

Event grids display the individual events that active channels capture.

To page through a grid

Click the navigation buttons on the right side of the grid column header. The numbers represent specific pages, and the advance arrows go one step or all the way forward or back.

To use field sets

Choose a named set of fields from the **Field Set** drop-down menu. The sets available are usually tailored to your enterprise. Note that the field-set variables found in the ArcSight Console are not available through ArcSight Web.

Choose the Field Set **Customize** option (if available) to temporarily add, remove, or rearrange the columns in the current grid. You can create one custom field set per channel.

If your ESM system is configured with *domain field sets*, these are also available here to select as a pre-defined **Field Set** choice and for use with the **Customize** option. For more information about domain field sets, see the Domain Field Sets topic in the ArcSight Console User's Guide.

To sort a grid

Click any grid column heading to sort the whole view by that column. Each click toggles between ascending and descending. The default order of grids is usually determined by the End Time of events, as selected in the current active channel display.

To filter a grid

To apply an inline filter, click **Inline Filter** in the grid header and choose an available value from the drop-down menus for one or more columns. This enables you to filter by values already available in the channel. Click **Apply** to put the filter into effect.

You can also filter by entering custom expressions into the text field for each column. To customize an inline filter, type a value in the text field above the column on which you want to filter, and click **Apply**. Supported expressions for custom filtering are shown in the table below.

Supported Expressions for Inline Filtering

Type	Supported Expressions and Examples
String-based Columns	<p>The Contains and StartsWith operators are supported. The values for the operator must be in quotes.</p> <p>Examples:</p> <p>Contains "Event"</p> <p>Contains "Event" OR Contains "Top"</p> <p>Contains "Web" AND Contains "denied"</p> <p>StartsWith "Web"</p> <p>StartsWith "Web" OR Contains "denied"</p> <p>StartsWith "Web" AND Contains "denied"</p> <p>You can use OR and AND Boolean operators in between the expressions. The Column field name is implicitly used as the left-hand parameter.</p>
Integer and IP Address Columns	<p>The Between operator is supported. The values in the Between expression must be in quotes.</p> <p>Examples:</p> <p>For the port column: Between("20", "80")</p> <p>For the IP address column: Between("10.0.0.1", "10.0.0.255")</p> <p>For priority column: Between("1", "2") OR Between("7", "8")</p> <p>You can use OR and AND Boolean operators in between the expressions. The Column field name is implicitly used as the left-hand parameter.</p>

To change a grid's options

Click **Options** in the grid header to change the display's update frequency and its number of rows per page.

To save a modified channel

Click Save Channel As in the channel header to add a modified channel to your personal folder in the Active Channels resource tree. In the Save Channel As dialog box, name the channel and click **Save**.

To inspect an event

Click any individual event in the grid to show that event in the Event Inspector as described in Inspecting Events.

Inspecting Events

Use the Event Inspector display to examine the details of events that appear in active channels. To open the Event Inspector, click an event in an active channel's grid view. The Event Inspector shows the data fields and categories associated with the event you selected. Apart from these fields, the display has the features described below.

Event Inspector Header Features

Feature	Usage
Associated Articles	If a knowledge base article exists for this event, the View Articles link displays the article from the Knowledge Base.
Associated References	If a reference page exists for this event, the View References link displays the reference page. Reference pages provide additional background on an event or a resource. These may be pre-populated by ArcSight, provided by vendors, or added by technologists in your organization.
Additional Details	Click this link to view Additional Details on the event, such as vendor and product information, event category information, reference pages, and vulnerability pages.
View Event Context Report	Click this link to run an Event Context Report that shows the events that occurred within a specified number of minutes (a window) before and after this event.
View Rule Context Report	Click this link to run a Rule Context Report that shows the events that occurred within a specified number of minutes (a window) before and after the current rule was invoked.
Payload Viewer	Click this link to view the payload for the event. The Payload Viewer option is available only if the event has a payload associated with it. A "payload" is information carried in the body of an event's network packet, as distinct from the packet's header data. Events include payloads only if the associated SmartConnectors are configured to send events with payloads.
View iDefense Incident Report	Click View iDefense Incident Report to view information about vulnerability IDs related to the event. This option is available only if you have VeriSign iDefense software installed and configured to interact with the Arcsight system, and if the selected event has a vulnerability ID associated with it. In that case, the iDefense report provides more details on the vulnerability.
Field Sets	Choose Field Sets to see a predefined set of event data fields rather than all fields. Use the None option to restore the default view.
Hide Empty Rows	By default, the Hide Empty Rows check box is checked, so the display isn't filled with unused fields. Clear the check box to see all fields, even if empty.

Event Inspector Field Features



The values for fields in events are also links. Click these values to open new channels or to filter current channels using them.

Option	Use
Create Channel [Field Name = Value]	Open a channel containing only those events that have matching values for the selected field.

Option	Use
Create Channel [Field Name != Value]	Open a channel that shows only those events that do not have a matching value for the selected event.
Add to Channel [Attribute = Value]	Add the attribute-value pair to the channel's filter (require that they match).
Add to Channel [Attribute != Value]	Exclude the attribute-value pair from the channel's filter (require that they do not match).

Show Details for Event Attributes

View details for each attribute associated with an event.

- To view event attribute details inline, click the **Details** button () next to the attribute.
- To view event attribute details on a new Web page, click the **Show detail in a new page** button () next to the attribute.

Event Categories

ESM uses six primary categories and a flexible set of supporting attributes to more precisely distinguish the events reported by SmartConnectors or generated internally by ArcSight Managers. These categories appear as a field in the Event Inspector.

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.

The category groups are:

- **Object:** The physical or virtual object that was the focus of the event. (See [“Object Category” on page 22.](#))
- **Behavior:** The action taken on the object. (See [“Behavior Category” on page 23.](#))
- **Outcome:** An indication of whether the action succeeded on the object. (See [“Outcome Category” on page 25.](#))
- **Device Group:** The type of device from which the sensor reported the event. (See [“Device Group Category” on page 25.](#))
- **Technique:** The method used to apply the action to the object (i.e., the type of attack). (See [“Technique Category” on page 26.](#))
- **Significance:** A description of the security significance of the event from the reporting sensor's perspective. (See [“Significance Category” on page 28.](#))

Object Category

Object Category	Description
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 such as Kazaa, Morpheus, or Napster.
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.
Resource	An operating system resource that is characteristically limited in its supply.
File	A long-term storage mechanism (e.g., 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 such as IPSec Tunnel and 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.

Object Category		Description
Actor	Routing	Routing related events such as BGP.
	Switching	Switching related events such as VLANs.
	User	A single human identity.
	Group	A named collection of users, such as an employee division or social group.
Vector		The replication path for a section of malicious code.
	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.
	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

Behavior Category		Description
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.

Behavior Category	Description
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.
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 such 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 are 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`.

Outcome Category	Description
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

Device Group Category	Description
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 (such as 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

Technique Category	Description
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 Fragment	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.
Hijack	Hijacking a connection.
Spoof	Spoofing a transport layer property such as 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 such as 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. Examples of a weak configuration are 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.

Technique Category	Description
ICMP	ICMP redirects.
DNS	Unauthorized DNS changes.
Routing Protocols	Attacks aimed at routing protocols such as BGP, RIP, and OSPF.
IP	Redirection using the IP protocol (source routing).
Application	Redirection attacks on the application layer such as cross-site scripting, mail routing, or JavaScript spoofing.
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, DoS 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 denial of service (DoS) attack is in progress.
Information Leak	Information leaking out of its intended environment such as mail messages leaking out, system file access, FTP data access, or web document access.
Convert 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

Significance Category	Description
Compromise	A potentially compromising event occurred.
Hostile	A malicious event has happened or is happening.
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 historical analysis purposes.
Recon	Relates to scans and other reconnaissance activity.
Suspicious	A potentially malicious event occurred.

Event 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 ArcSight 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 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".)



Note

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.



Since connectors are not registered to the local Manager, the Original Agent is not known and all the Original Agent fields are therefore blank and do not need to be displayed.

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.

Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Connector Group Field Description
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).
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	Returns the external ID for this reference.
Translated Zone ID	connectorTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Translated Zone Name	connectorTranslatedZoneName	String	1	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	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	Locates the resource described by this reference.

Connector Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Connector Group Field Description
Translated Zone URI	connectorTranslatedZoneURI	String	1	Returns the URI for this reference.
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	Returns the external ID for this reference.
Zone ID	connectorZoneID	String	1	Returns the ID for the resource in this resource reference.
Zone Name	connectorZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Zone Reference ID	connectorZoneReferenceID	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	connectorZoneResource	Resource	1	Locates the resource described by this reference.
Zone URI	connectorZoneURI	String	1	Returns the URI for this reference.

Attacker Group

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.

Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
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	The Resource of the asset that represents the device hosting the attacker.
DNS Domain	attackerDnsDomain	String	2	The Domain Name Service domain name associated with the device hosting the attacker.
FQDN	attackerFqdn	String	2	The fully qualified domain name associated with the device hosting the attacker.
Geo	attackerGeo	GeoDescriptor	1	The geographical information.
Geo Country Code	attackerGeoCountryCode	String	1	The identifier for the national-political state in which a device resides.
Geo Country Flag URL	attackerGeoCountryFlagUrl	String	1	The URL of an image of the flag of the national-political state in which the device resides.
Geo Country Name	attackerGeoCountryName	String	1	The name of the national-political state where a device resides.
Geo Descriptor ID	attackerGeoDescriptorId	ID	1	The internal ID of the geographical reference.
Geo Latitude	attackerGeoLatitude	Double	1	The latitude of a device.
Geo Location Info	attackerGeoLocationInfo	String	2	Other, free-form text information about the device's location.
Geo Longitude	attackerGeoLongitude	Double	1	The Longitude of a device.
Geo Postal Code	attackerGeoPostalCode	String	1	The postal code of the device's location, as assigned by the national-political state where it resides.

Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
Geo Region Code	attackerGeoRegionCode	String	1	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.
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	2	The ID of the process associated with the source of the attack.
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.

Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
Translated Zone External ID	attackerTranslatedZoneExternalID	String	1	Returns the external ID for this reference.
Translated Zone ID	attackerTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
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	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	attackerTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Translated Zone URI	attackerTranslatedZoneURI	String	1	Returns the URI for this reference.
User ID	attackerUserId	String	2	The identifier associated with the OS or application of the attacker, at the source of the attack.
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	Returns the external ID for this reference.
Zone ID	attackerZoneID	String	1	Returns the ID for the resource in this resource reference.
Zone Name	attackerZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.

Attacker Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Attacker Group Field Description
Zone Reference ID	attackerZoneReferenceID	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	attackerZoneResource	Resource	1	Locates the resource described by this reference.
Zone URI	attackerZoneURI	String	1	See the common set of resource attributes.

Category Group

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	The type of event. For example, logging into a firewall is an Operating System type of event.
Device Type	categoryDeviceType	String	2	The type of device. For example, logging into a firewall, would show the Device Type as Firewall.
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.

Category Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Category Group Field Description
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

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	The name of the device.
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	1	See the common set of geographical attributes.
Geo Country Code	destinationGeoCountryCode	String	1	The identifier for the national-political state in which a device resides.
Geo Country Flag URL	destinationGeoCountryFlagUrl	String	1	The URL of an image of the flag of the national-political state in which the device resides.
Geo Country Name	destinationGeoCountryName	String	1	The name of the national-political state where a device resides.

Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Geo Descriptor ID	destinationGeoDescriptorId	ID	1	The internal ID of the geographical reference.
Geo Latitude	destinationGeoLatitude	Double	1	The destination latitude of the device.
Geo Location Info	destinationGeoLocationInfo	String	1	Other, free-form text information about the device's location.
Geo Longitude	destinationGeoLongitude	Double	1	The destination longitude.
Geo Postal Code	destinationGeoPostalCode	String	1	The postal code of the device's location, as assigned by the national-political state where it resides.
Geo Region Code	destinationGeoRegionCode	String	1	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.
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	2	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.
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.

Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
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	Returns the external ID for this reference.
Translated Zone ID	destinationTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Translated Zone Name	destinationTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference	destinationTranslatedZoneReferenceID	ID	1	See the common set of resource attributes.
Translated Zone Resource	destinationTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
Translated Zone URI	destinationTranslatedZoneURI	String	1	Returns the URI for this reference.
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.
Zone External ID	destinationZoneExternalID	String	1	Returns the external ID for this reference.
Zone ID	destinationZoneID	String	1	Returns the ID for the resource in this resource reference.

Destination Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Destination Group Field Description
Zone Name	destinationZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
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	Locates the resource described by this reference.
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.

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.
Direction	deviceDirection	Device Direction Enumeration	2	Whether the traffic was inbound or outbound.

Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
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	2	The ID of the sensor device process that reported the event.
Process Name	deviceProcessName	String	1	The name of the sensor device process that reported the event.

Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
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	Returns the external ID for this reference.
Translated Zone ID	deviceTranslatedZoneID	String	1	Returns the ID for the resource in this resource reference.
Translated Zone Name	deviceTranslatedZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
Translated Zone Reference ID	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.
Translated Zone Resource	deviceTranslatedZoneResource	Resource	1	Locates the resource described by this reference.

Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Group Field Description
Translated Zone URI	deviceTranslatedZoneURI	String	1	Returns the URI for this reference.
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	Returns the external ID for this reference.
Zone ID	deviceZoneID	String	1	Returns the ID for the resource in this resource reference.
Zone Name	deviceZoneName	String	1	Returns the name from the URI, which is always assumed to be the last field of the URI.
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	Locates the resource described by this reference.
Zone URI	deviceZoneURI	String	1	See the common set of resource attributes.

Device Custom Group

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

Device Custom Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Custom Group Field Description
Date2 Label	deviceCustomDate2Label	String	2	Second customDate label
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	2	First custom floating point
Floating Point1	deviceCustomFloatingPoint1Label	Double	2	First custom floating point label
Floating Point2 Label	deviceCustomFloatingPoint2	String	2	Second custom floating point
Floating Point2	deviceCustomFloatingPoint2Label	Double	2	Second custom floating point label

Device Custom Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Device Custom Group Field Description
Floating Point3 Label	deviceCustomFloatingPoint3	String	2	Third custom floating point
Floating Point3	deviceCustomFloatingPoint3Label	Double	2	Third custom floating point label
Floating Point4 Label	deviceCustomFloatingPoint4	String	2	Fourth custom floating point
Floating Point4	deviceCustomFloatingPoint4Label	Double	2	Fourth custom floating point label
IPv6 Address1 Label	deviceCustomIPv6Address1	String	2	First custom IPv6 address
IPv6 Address1	deviceCustomIPv6Address1Label	IPv6 address	2	First custom IPv6 address label
IPv6 Address2 Label	deviceCustomIPv6Address2	String	2	Second custom IPv6 address
IPv6 Address2	deviceCustomIPv6Address2Label	IPv6 address	2	Second custom IPv6 address label
IPv6 Address3 Label	deviceCustomIPv6Address3	String	2	Third custom IPv6 address
IPv6 Address3	deviceCustomIPv6Address3Label	IPv6 address	2	Third custom IPv6 address label
IPv6 Address4 Label	deviceCustomIPv6Address4	String	2	Fourth custom IPv6 address
IPv6 Address4	deviceCustomIPv6Address4Label	IPv6 address	2	Fourth custom IPv6 address label

Event Group

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.

Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
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.
Application Protocol	applicationProtocol	String	2	A description of the application layer protocol. May be set, but defaults to Target Port lookup (FTP).
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.

Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
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.
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	2	The domain the event belongs to. You can have multiple event domains (with licensing), and this identifies the domain.
End Time	endTime	DateTime	1	Event ends (defaults to deviceReceiptTime).
Event ID	eventId	ID	1	Long value identifying an event.
Event Outcome	eventOutcome	String	2	The outcome of the event as reported by the device (when applicable). For example, Windows reports an event as audit_success or audit_failure.
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.

Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
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.
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).

Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
Reason	reason	String	2	The cause of the event when applicable. For example, Invalid Password
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).
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, Aggregated, 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.

Event Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Group Field Description
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

Event Annotation Group Data Fields

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.
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. Note: The following event fields: isReviewed, Closed, Hidden, Correlated, inCase, hasAction, and Forwarded, are derived from eventAnnotationFlags. You cannot add those individual event fields into a field set, but you can add eventAnnotation fields instead.
Manager Receipt Time	eventAnnotationManagerReceiptTime	DateTime	2	The time the Manager received the event annotation.

Event Annotation Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
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'.
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.

Event Annotation Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Event Annotation Group Field Description
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.
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

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.

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.

Final Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
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.
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.

Final Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
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.
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.

Final Device Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Final Device Group Field Description
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

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.
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.

Flex Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Flex Group Field Description
String2 Label	flexString2Label	String	2	Label of the second Flex String.

Manager Group

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**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.

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	originalConnectorAssetName	String	2	The first reporting connector's asset name.
Asset Resource	originalConnectorAssetResource	Resource	2	The first reporting connector's resource.
Descriptor ID	originalConnectorDescriptorId	ID	2	The first reporting connector's descriptor.
DNS Domain	originalConnectorDnsDomain	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	originalconnectorMacAddress	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.

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.

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

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.

Request Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Request Group Field Description
Context	requestContext	String	2	A description of the content from which the request originated, for example, the HTTP Referrer.
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

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.

Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
Asset Name	sourceAssetName	String	2	The name of the device.
Asset Resource	sourceAssetResource	Resource	2	See the common set of resource attributes.
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	The identifier for the national-political state in which a device resides.
Geo Country Flag URL	sourceGeoCountryFlagUrl	String	1	The URL of an image of the flag of the national-political state in which the device resides.
Geo Country Name	sourceGeoCountryName	String	1	The name of the national-political state where a device resides.
Geo Descriptor ID	sourceGeoDescriptorId	ID	1	The internal ID of the geographical reference.
Geo Latitude	sourceGeoLatitude	Double	1	The latitude of a device.
Geo Location Info	sourceGeoLocationInfo	String	1	Other, free-form text information about the device's location.
Geo Longitude	sourceGeoLongitude	Double	1	The Longitude of a device.
Geo Postal Code	sourceGeoPostalCode	String	1	The postal code of the device's location, as assigned by the national-political state where it resides.
Geo Region Code	sourceGeoRegionCode	String	1	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.

Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
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.
Port	sourcePort	Integer	1	The network port associated with the network traffic's source.
Process ID	sourceProcessId	Integer	2	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	sourceTranslatedZoneExternalID	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.

Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
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	sourceTranslatedZoneReferenceID	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	sourceTranslatedZoneResource	Resource	1	Locates the resource described by this reference.
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.

Source Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Source Group Field Description
Zone URI	sourceZoneURI	String	1	Returns the URI for this reference.

Target Group

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.
Asset Name	targetAssetName	String	2	The name of the device.
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	The identifier for the national-political state in which a device resides.
Geo Country Flag URL	targetGeoCountryFlagUrl	String	1	The URL of an image of the flag of the national-political state in which the device resides.
Geo Country Name	targetGeoCountryName	String	1	The name of the national-political state where a device resides.
Geo Descriptor ID	targetGeoDescriptorId	ID	1	The internal ID of the geographical reference.
Geo Latitude	targetGeoLatitude	Double	1	The latitude of a device.

Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
Geo Location Info	targetGeoLocationInfo	String	1	Other, free-form text information about the device's location.
Geo Longitude	targetGeoLongitude	Double	1	The Longitude of a device.
Geo Postal Code	targetGeoPostalCode	String	1	The postal code of the device's location, as assigned by the national-political state where it resides.
Geo Region Code	targetGeoRegionCode	String	1	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.
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).
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	2	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.

Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
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.
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.

Target Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Target Group Field Description
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

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.
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.

Threat Group Data Fields (Continued)

Label	Script Alias	Data Type	Default Turbo Level	Threat Group Field Description
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

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

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.

Geographical Attributes Data Fields (Continued)

Attribute Suffix	Description
Location Info	Other, free-form text information about the device's location.
Longitude	The longitude of a device.
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.

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, 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)," in 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.

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)

Audit Events on Resources

Audit Event Category	Device Event Class ID	Audit Event Description
Resource (Delete)	resource:100	Resource deleted. The Event Name describes the action and resource type (<ResourceName> deleted); for example, deleting a filter results in an event named Filter deleted.
Resource (Update)	resource:101	Resource updated. This audit event is generated when an existing resource is modified or added. See Resource (Add). The Event Name describes the action (update) and resource type (<ResourceName> updated); for example, modifying a report, results in an event name of Report updated.
Resource (Add)	resource:102	Resource added (inserted). The Event Name describes the action (insert) and resource type (<ResourceName> inserted); for example, adding a case, results in an event name of Case inserted. Adding a Case group results in an event name of Group [Case] inserted.
Resource (Lock)	resource:103	Resource locked <ResourceName> locked.
Resource (Unlock)	resource:104	Resource unlocked <ResourceName> unlocked.
Resource	resourcereference:100	Could not locate a resource through the supplied universal resource identifier (URI).

Active Channel

Audit Events on Active Channel Category

Device Event Class ID	Audit Event Message
channel:001	An active channel [Channel Name] was opened/started.
channel:002	The channel [Channel Name] is empty; that is, there are no matching events for the built-in channel filter.
channel:003	The channel [Channel Name] query completed.
channel:004	The channel [Channel Name] query is slow.

Active List

Audit Events on Active List Category

Device Event Class ID	Audit Event Message
activelist:101	An entry was added to an active list.
activelist:102	An entry was removed from an active list.
activelist:103	An entry was changed in an active list.
activelist:104	An entry has expired in an active list.
activelist:105	An entry has been evicted from an active list. The active list is full and an entry is dropped.

Actor

Audit Events on Actor Category

Device Event Class ID	Audit Event Message
actor:100	An actor was deleted.
actor:102	An actor was created.
actor:110	One or more Actor Attributes were updated.
actor:111	A Multi-Valued Actor Attribute was added to an actor.
actor:112	A Multi-Valued Actor Attribute was removed from an actor.

Authentication

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 ArcSight Console authenticating itself to the Manager triggers this audit event.)</p> <p>For information on how to configure a non-FIPS client (such as ArcSight Console) to log in to a FIPS-enabled Manager, see the Administrator's Guide.</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 document, Installing FIPS-Compliant SmartConnectors.</p>

Archive

Audit Events on Manage Archives Category

Device Event Class ID	Audit Event Description
archive:100	Archive created
archive:101	Archive deleted
archive:102	Event archive settings updated
archive:103	Event archive disk space used
archive:110	Archive activated
archive:111	Archive activation cancelled

Audit Events on Manage Archives Category (Continued)

Device Event Class ID	Audit Event Description
archive:112	Archive activation failed
archive:120	Archive operation succeeded
archive:121	Archive operation cancelled
archive:122	Archive operation failed
archive:130	Archive deactivated
archive:131	Archive deactivation cancelled
archive:132	Archive deactivation failed
archive:140	Archive scheduled
archive:141	Archive schedule cancelled
archive:142	Archive schedule failed

Authorization

Device Event Class ID	Audit Event Description
authorization:100	Manager refused to authorize client.

Connectors

Audit events related to SmartConnectors are described in the following tables.

Connector Connection

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:041	Event flow on connector has been started, stopped, or paused.
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.

Audit Events on Connector Connections Category (Continued)

Device Event Class ID	Audit Event Description
agent:105	A connector presented an incorrect shared secret when authenticating.

Connector Exceptions**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.
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.
agent:035	Connector sent an event with a bad timestamp; it is beyond the retention period.
agent:107	Connector is generating too many events that causes what should be the same device to be referenced in too many different ways.

Connector Login

Device Event Class ID	Audit Event Description
authentication:200	Successful connector authentication.
authentication:201	Connector authentication failed.

Connector Registration and Configuration

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

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.
dashboard:100	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

Audit Events for Last State Data Monitors

Audit Event Category: Statistical Data Monitor

Device Event Class ID	Audit Event Description
datamonitor:400	A Last State data monitor entry has exceeded its time-out period and was automatically removed.
datamonitor:401	A Last State data monitor entry value was manually changed by the user.
datamonitor:402	A Last State data monitor entry was manually removed by the user.

Moving Average Data Monitor

Audit Events for Moving Average Data Monitor Category

Device Event Class ID	Audit Event Description
datamonitor:101	Moving average threshold.
datamonitor:102	Moving Average data monitor detected a rapidly falling moving average
datamonitor:103	Moving Average data monitor detected a rapidly rising moving average.
datamonitor:104	Moving Average data monitor reporting the current moving average.
datamonitor:105	A value was added to a Moving Average data monitor, which is now monitoring a new Group-By set of values.
datamonitor:106	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

Device Event Class ID	Audit Event Description
datamonitor:300	Correlation data monitor reporting a correlated or non-correlated event.

Statistical Data Monitor

Audit Events for Statistical Data Monitor Category

Device Event Class ID	Audit Event Description
datamonitor:200	Statistical Data Monitor reported a change in status.

Audit Events for Statistical Data Monitor Category (Continued)

Device Event Class ID	Audit Event Description
datamonitor:201	A value was added to a Statistical Data Monitor, which is now monitoring a new Group-By set of values.
datamonitor:202	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**Audit Events for Top Value Counts****Audit Event Category: Moving Average Data Monitor**

Device Event Class ID	Audit Event Description
datamonitor:500	For a Top Value Counts Data Monitor, the top N counts (N events).
datamonitor:501	Counts that were most recently added to the data monitor (from 0 ... N events).
datamonitor:502	Counts that were most recently removed from the data monitor (from 0 ... N events).

Domains (for Domain Fields)

Audit Event Category	Device Event Class ID	Audit Event Description
Domain	domain:100	All out of underlying database columns of type <x>, delete a Domain Field of the same type to free up a column.

Global Variables

The following events also apply to resources in general. See “Resources (Configuration Events Common to Most Resources).”

Audit Events for Global Variables Category

Device Event Class ID	Audit Event Description
resource:100	Global variable deleted.
resource:101	Global variable updated.
resource:102	Global variable inserted.
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 the User Management category.)

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.

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 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.
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

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

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

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

Audit Events for Notification Category

Device Event Class ID	Audit Event Description
notification:100	Notification has been disabled.
notification:101	Notification has been disabled because the queue of notifications to be sent is too large.
notification:102	Notification has been enabled.
notification:103	Notification has been enabled because the queue of notifications is back under control.
notification:104	A particular notification destination has been disabled.
notification:105	A particular notification destination has been disabled because too much traffic was directed at it.
notification:106	A particular notification destination has been enabled.
notification:107	A notification expired without being acknowledged.
notification:108	A functioning destination could not be located for this notification.
notification:109	Old notification has been purges.

Notification Acknowledgement, Escalation, and Resolution

Audit Events for Notification Acknowledgement, Escalation, and Resolution Categories

Audit Event Category	Device Event Class ID	Audit Event Description
Notification Escalated	notification:110	Notification has been escalated.
Notification Sent Requires Acknowledgement	notification:111	Notification sent requires acknowledgement.
Notification Sent (Informational)	notification:112	An informational notification was sent.
Notification Acknowledgement	notification:300	This notification has been acknowledged.
Notification Resolve	notification:301	This notification has been resolved.

Notification Testing

Device Event Class ID	Audit Event Description
notification:200	Sent a test notification to this destination group.

Pattern Discovery

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 Events for 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 Events for 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.

Audit Events for Partition Manager (Continued)

Audit Event Category	Device Event Class ID	Audit Event Description
Partition Manager	partitionmanager:500	Partitions could not be rotated.
Partition Manager	partitionmanager:600	There was an unexpected error while rotating partitions.

Query Viewers

Audit Events for Query Viewer Category

Device Event Class ID	Audit Event Description
queryviewer:100	Base query used by the query viewer succeeded.
queryviewer:101	Base query used by the query viewer failed.
queryviewer:102	Base query used by the query viewer has started.

Reports

Audit Events for Report Category

Device Event Class ID	Audit Event Description
report:100	Generated a new archived-report configuration resource.
report:101	Failed to generate a new archived-report configuration resource.
report:102	Generated a new delta archived-report configuration resource.
report:103	Report cancelled.
report:104	Generate report started.
report:105	Report generate process halted because the report was empty.

Resource Quota

Audit Events for Resource Quota Category

Device Event Class ID	Audit Event Description
quota:100	Resource usage has fallen below the fixed-quota level.
quota:101	Resource usage has exceeded the fixed-quota level.
quota:102	Asset autocreation has exceeded a fixed quota.
quota:103	Asset autocreation is proceeding too rapidly.

Rules

Audit events for rules are described in the following tables.

Rule Actions

Audit Events for Rule Actions Category

Device Event Class ID	Audit Event Description
rule:300	For rule actions that do not have specific DEC IDs assigned.
rule:302	Set Event Attribute action.
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

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

Device Event Class ID	Audit Event Description
rule:801	Scheduled rule started.
rule:802	Scheduled rule finished.

Rule Firings

Audit Events for Rule Firings Category

Device Event Class ID	Audit Event Description
rule:100	Any rule fired.
rule:101	Rule fired OnEveryEvent.
rule:102	Rule fired OnFirstEvent.
rule:103	Rule fired OnSubsequentEvents.
rule:104	Rule fired OnEveryThreshold.
rule:105	Rule fired OnFirstThreshold.
rule:106	Rule fired OnSubsequentThresholds.
rule:107	Rule fired OnTimeUnitExpiration.
rule:108	Rule fired on time unit.

Rule Warnings

Device Event Class ID	Audit Event Description
rule:501	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

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

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 .
<code>scheduler:307</code>	Could not disable a task.

Scheduler Skip

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

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.

Audit Events for Session List Category (Continued)

Device Event Class ID	Audit Event Description
sessionlist:102	An entry was removed from a session list.
sessionlist:103	A session list entry was updated.
sessionlist:104	An entry in a session list was auto-terminated as the session expired.
sessionlist:201	A session list partition was added.
sessionlist:202	A session list partition was dropped.
sessionlist:203	A session list Partition add failed.
sessionlist:204	A session list Partition drop failed.
sessionlist:301	<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

Device Event Class ID	Audit Event Description
test:100	<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

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.

Audit Events for Trend Category (Continued)

Device Event Class ID	Audit Event Description
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	Trend successfully updated an active list. You can add an action to a trend to send columns (fields) in trend results to a <i>fields-based</i> active list.

Trend Partitions**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

Audit Events for User Logins

Device Event Class ID	Audit Event Description
authentication:100	Successful client login.
authentication:101	Failed client login.
authentication:102	Client logout.
authentication:103	Client timed out due to inactivity.
authentication:104	Too many client login failures occurred within a time period. Note: After the third login failure, future logins are prevented. The next time this user logs in, the generated event is authentication:101, Failed client login with the reason, User disabled.

User Management

Audit Events for User Management Category

Audit Event Category	Device Event Class ID	Audit Event Description
User Delete	user:100	A user account was deleted.
User Update	user:101	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	user:102	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 (user:101).

Chapter 4

Using Cases

ArcSight cases provide organized, workflow-style tracking and management of interesting events or situations.

The ArcSight Web interface enables you to create, manage, or customize cases.

Cases have a large number of fields to cover a wide range of event analysis and investigation possibilities. (See [“Creating Cases” on page 91](#)).



You can add an **Export** button to the Cases display to export selected cases. Add the line `ui.export.enabled=true` to the `webserver.properties` file and restart ArcSight Web.

[“Managing Cases” on page 89](#)

[“Creating Cases” on page 91](#)

Managing Cases

The cases display shows cases that are already created in the Cases tree. From the main panel, you can select, view, and customize existing cases, and create new ones.

To view an existing case:

- 1 Navigate to and select the case in the Cases resource tree on the left.
 - ◆ Click the group folders in the tree to open or close them.
 - ◆ Click a folder to see a list of its cases in the pane to the right.
 - ◆ Click the arrow icon in the upper-right corner of the resource pane to hide it or show it.
- 2 The Cases content pane shows individual listings. Click an individual case to see its fields (see [“Creating Cases” on page 91](#)).

To edit an individual case:

- 1 Click **Lock this case**.
- 2 Make your changes and click **Submit**.
- 3 Unlock a case after you finish editing.

To remove a case

- 1 Select the check box for the case you want to remove and click **Remove**.

If you want to keep the case but not allow others to edit it, you can Lock (hold for editing) or Unlock (release for others to edit) buttons.

- 2 Click **Refresh** to update the display.

To create a new case

Click **New Case** to go to the Create a New Case display. For details about how to create a case, see [“Creating Cases” on page 91](#).

To customize a case

Click **Customize** to select, deselect, and arrange the columns of the case list.

Default Case Management Columns

Attribute	Description
Name	The name assigned to the case. Using descriptive names is important.
Locked	Whether the case is free to be edited by others. If Locked, it cannot.
Security Classification Code	The letter codes that identify the nature of the security issues the case represents. See “Security Classification Default Letter Codes” on page 90 below.
Ticket Type	The source of the case or its means of tracking.
Stage	The current collaboration or workflow stage assigned to the case.
Frequency	The numerical range of events that occur in regard to a case.
Created By	The ArcSight user ID of the person who created the case.

Security Classification Default Letter Codes

Security Classification Letter Codes	
Classification Category	Letter Codes
Attack Mechanism	I = Informational
	O = Operational
	P = Physical
	U = Unknown
Attack Agent	C = Collaborative
	I = Insider
	O = Outsider

Security Classification Letter Codes (Continued)

Classification Category	Letter Codes
Vulnerability	U = Unknown
	D = Design
	E = Operational Environment
	O = Operational
	U = Unknown
Sensitivity	C = Confidential
	S = Secret
	T = Top Secret
	U = Unclassified
Associated Impact	A = Availability
	C = Confidentiality
	I = Integrity
	U = Unknown
Action	B = Block/Shutdown
	M = Monitoring
	O = Other

Creating Cases

To create a case, choose the Initial attributes tab first. Fill in the required and other appropriate fields, tab by tab, then click **Submit** at the bottom of the display. Overall, the tabs represent:

- **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.
- **Notes** - Miscellaneous information applicable to a case.

Display ID numbers are assigned automatically when you save the case.

Initial Tab

The fields on this tab provide basic case information.

Fields on the Initial Tab		
Field	Description	
Case	Name	Required field specifying name of case.
	Display ID	An automatically assigned unique number.
Ticket	Ticket Type	Drop-down list includes Internal, Client, and Incident types.
	Stage	Indicate workflow stage of ticket; 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	This is a calculated number, based on Ticket info values entered.
Incident Information	Detection Time	This field is auto-populated.
	Estimated Start Time	This field is auto-populated.
	Estimated Restore Time	This field is auto-populated. If this field does not get set properly, set it in the ArcSight Console.
	External ID	This field is auto-populated.
	Alias	Another name by which the incident is referenced in the system.
	Description	A text description of the incident.
Assign	Owner	Users designated as owners of the case.
	Notification Groups	Pre-defined groups that should be notified when the case is created or updated.

Fields on the Initial Tab

Field	Description
Description	
Affected Services	This text field can contain up to 4,000 characters.
Affected Elements	This text field can contain up to 4,000 characters.
Estimated Impact	This text field can contain up to 4,000 characters.
Affected Sites	This text field can contain up to 4,000 characters.
Security Classification	
Attack Mechanism	I = Informational O = Operational P = Physical U = Unknown
Attack Agent	C = Collaborative I = Insider O = Outsider U = Unknown
Incident Source 1	This field is auto-populated.
Incident Source 2	This field is auto-populated.
Vulnerability	D = Design E = Operational Environment U = Unknown
Sensitivity	C = Confidential S = Secret T = Top Secret U = Unclassified
Associated Impact	A = Availability C = Confidentiality I = Integrity U = Unknown
Action	B = Block/Shutdown M = Monitoring O = Other
Security Classification Code	
Security Classification Code	This field is auto-populated.

Follow Up Tab

The fields on this tab describe follow-up entries for a case.

Fields on the Follow Up Tab

Field	Description
Actions Taken	This text field can contain up to 4,000 characters.
Planned Actions	This text field can contain up to 4,000 characters.
Recommended Actions	This text field can contain up to 4,000 characters.
Follow-up Contact	This text field can contain up to 4,000 characters.

Final Tab

Fields on this tab provide ticket resolution and reporting information related to the attack agent associated with a case.


Fields on the Final Tab

Field	Description
Attack Mechanism	
Attack Mechanism	This field is auto-populated.
Attack Protocol	The network protocol that is transporting the attack.
Attack OS	The operating system supporting the attack.
Attack Program	The program that is performing the attack.
Attack Time	The date and time of the attack.
Attack Target	The host or device at which the attack is directed.
Attack Service	The service at which the attack is directed.
Attack Impact	The effect of the attack.
Final Report Action	The action recommended for this case.
Attack Agent	
Attack Agent	This field is auto-populated.
Attack Location ID	A short description of the location under attack, of up to 255 characters.
Attack Node	A short description of the network node under attack, of up to 255 characters.

Fields on the Final Tab

Field	Description
Incident Information	Attack Address A text field in which you can record the IP address under attack, of up to 255 characters.
	Incident Source 1 This field is auto-populated.
	Incident Source 2 This field is auto-populated.
	Incident Source Address A text field in which you can record up to 200 characters.
Vulnerability	Vulnerability This field is auto-populated.
	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 This text field can contain up to 4,000 characters.
	Vulnerability Source This text field can contain up to 4,000 characters.
	Vulnerability Data This text field can contain up to 4,000 characters.
Other	History Selections include: Known Occurrence and Unknown.
	No. Occurrences A numeric value; the number of occurrences of the incident.
	Last Occurrence Time The date and time of the most recent incident.
	Resistance Selections include: High, Low, and Unknown.
	Consequence Severity This field is auto-populated.
	Sensitivity This field is auto-populated.
	Recorded Data This text field can contain up to 4,000 characters.
	Inspection Results This text field can contain up to 4,000 characters.
	Conclusions This text field can contain up to 4,000 characters.

Events Tab


You can add events to a case from the Active Channels page () as described in Using Active Channel Grids. The system then displays these events on the Cases Events tab.

Field	Description
Description	This field is auto-populated from events included in a case.
Event Info and Payload fields	For selected events, this field displays event values and payload fields, if available.

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.

Attachments Tab

The Attachments tab shows files associated with the selected case. Click the **Attach** button to attach another file to the case.


If you do not see files as expected, try clicking the Refresh button () to update the view to show recently added files.

Fields on the Attachments Tab

Field	Description
Local file	Select this option to choose a file on your local system. Specify values for the following fields, which are displayed when you choose a local file:
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.
Description	A text description of the file.
File	Click Browse and use the file browser to navigate to and select the local file you want to attach to the case. (This field requires user input.)
Text Encoding	Encoding type. The default is ISO-8859-1.
Share this file in ArcSight	Click this option if you want to make the file available as a shared resource on the ArcSight Manager.
ArcSight file	Select this option to choose a file on the ArcSight Manager.
Files to attach	Click the plus button next the drop-down menu to show the file browser on the ArcSight Manager. Navigate to and select a file on the ArcSight Manager. (This field requires user input.)

Click **Attach** to attach the file to the case. (Or click Cancel to abandon attachment edits.)

Click **Submit** to save the case with the new attachment, the same way you save new settings on the other tabs.

Once the file is attached, anyone viewing the case can view details about the file and download it. To do this, navigate to a case, and click the Attachments tab. To view more details about an attachment, click the file name. To download an attachment, click the Download button () for that file.

Notes Tab

Field	Description
Note	Use this field to record notes of up to 4,000 characters.

Handling Notifications

The Notifications feature displays notifications relevant to you that were triggered by certain event conditions.

The notifications on the display are grouped according to workflow-style stages such as pending, acknowledged, resolved, or informational. The specific groups you see have been tailored to your enterprise.

To see the details of a notification, click its listing in the relevant group.

Notification Categories	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.
Acknowledged	These are notifications to which you have responded.
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 response.

Chapter 6

Using Reports

The ArcSight Web interface enables you to run reports, and view and save the report results.

The reports available to you are organized in the resource tree on the left. Click the group folders in the tree to open or close them. Click a folder to see a list of its reports in the right-hand pane. Click the arrow icon in the upper-right corner of the resource pane to hide it or show it.

["Running and Viewing Reports" on page 101](#)

["Running and Saving Archived Reports" on page 102](#)

["Report Parameters" on page 102](#)

["Viewing Archived Reports" on page 103](#)

["Advanced Configuration for Report Performance" on page 104](#)

Running and Viewing Reports

To run and view a report:

- 1 Click **Report Definitions** just below the toolbar.
- 2 Navigate to a report in the resource tree.
- 3 Click a report definition name to show it in the right pane.
- 4 Use the values already defined for the report's parameters or change them as necessary. (See ["Report Parameters" on page 102.](#))
- 5 Click **Run Report** to run the report and display the results.

If you are running the context report from the event inspector, click **View Report** to run and display the report.



- For tips about how to run large reports that make efficient use of system resources, see ["Advanced Configuration for Report Performance" on page 104.](#)
- Reports with the characters # or \ in their names may not appear correctly. Either view them in another user interface or change the name.

Running and Saving Archived Reports

To run and save a report:

- 1 Click **Report Definitions** just below the toolbar.
- 2 Navigate to a report in the resource tree.
- 3 Click a report definition name to show it in the right pane.
- 4 Use the values already defined for the report's parameters or change them as necessary. (See ["Report Parameters" on page 102.](#))
- 5 Select the **Save Output** checkbox to expose the archive report detail fields.

If you are archiving the context report from the event inspector, click **Archive Report**. The report generates and be displayed in the viewer panel. You can save the report output using the browser Save As function.

- 6 Enter the following details for saving the report output as an archived report and click **Run Report**:

Field	Enter this
Archive Report Folder	Browse to an existing folder in the ArcSight file system to save the report results. This makes the report results retrievable from the Archived Reports view later. If you do not select a folder, you can save the report once the results are displayed using the save method that applies to the report format. For example, if you chose PDF, you can use the PDF save to save the results.
Archive Report Name	Accept the default report name or enter a name for the saved report results. Spaces are OK.
Archive Report Expiration Time	Accept the default date (6 months from today), or enter a date when the archived report results are deleted. \$NOW indicates that the report results are deleted when you close the report results viewer.

Report Parameters

The following parameters are common to most reports. Depending on the query used as the source for a report, other parameters may be exposed here. For example, a report might prompt for a Start and End Date (timestamps) over which to run the report.

Report Parameter	Use
Report Format	The format in which to generate the report. Note that RTF appears by default in Word documents, XLS in Excel worksheets, CSV in Excel worksheets, and PDF and HTML in browser windows. The CSV-Plain format intentionally has fewer report header lines.
Page Size	Choose a standard paper size for the printed report (whether you send it directly to print or not).

Report Parameter	Use
Run as User	As an option, 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.
E-mail to	Select one or more e-mail addresses to send notifications to when the report runs.
E-mail Format	Choose to send the generated report or a URL to the file.
Save Output	Select this option to save the generated report to the ArcSight Manager as an Archived Report. When you select the Save Output option (toggled "on"), provide the name, location, and expiration date of the archived report.
Archive Report Folder	Indicate the name of the folder in which you want to store the report.
Archive Report Name	Enter the name of the report. You can use Velocity Template references here. By default, the report names is set to: <code>\${Today}/\${ReportName}_\${Now}</code> \$CurrentDateTime : Prints the current date and time. (Same as \$Now) \$CurrentDate : Prints the current date. \$CurrentMonth : Prints the current month. \$CurrentWeek : Prints the current week. \$Now : Prints the current date and time. (Same as \$CurrentDateTime) \$CurrentDateTime-<Number> : Prints the current date and time minus the number of days you specify.
Archive Report Expiration Time	Enter an expiration date and time for the archived report. Click the calendar button next to the date field to get a popup calendar in which to designate the date. The ArcSight system automatically removes expired reports.

Viewing Archived Reports

To view an archived report:

- 1 Click **Archived Reports** just below the toolbar.
- 2 Navigate to a report in the resource tree.
- 3 Click the name of an archived report to show it in the right pane.

Downloading an Archived Report

To download an archived report:

- 1 Click **Archived Reports** just below the toolbar.
- 2 In the Download column for the report archive you want, click the **Download** icon.

- 3 In the File Download dialog box, choose to open the file or save it to a particular location.

Adding New Archived Reports

To add a new archived report to a folder:

- 1 Click **Archived Reports** just below the toolbar.
- 2 In the resource tree, select the report folder to which you want to add the new archived report.
- 3 Above the list of available reports, click **New Report**.
- 4 In the Upload Report screen, enter a report name and specify the path to its file, or click **Browse** to locate it.
- 5 Click **Upload** to add the archived file to the others available in the folder.

Deleting Archived Reports

To delete archived reports:

- 1 Click **Archived Reports** just below the toolbar.
- 2 Navigate to a report folder in the resource tree.
- 3 In the list of archived reports on the right, check those you want to delete.
- 4 Click **Delete** to remove the checked reports, then click **OK** to confirm.

Advanced Configuration for Report Performance

Reports with large file sizes or large time ranges may require special configurations at the Manager to ensure system performance.

Set these parameters only as needed if you encounter large or complex reports that repeatedly cause performance problems or cause the Manager to restart when you try to run them. Refer to the ESM Administrator's Guide for more information on setting server properties on the Manager. The properties described here are also documented in the `server.properties` file itself.

Configurations for Large 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 that, 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.

Set up the option on the ArcSight Manager to expose the option in the ArcSight Web report parameters list. On the ArcSight Manager in the `server.properties` file, set `report.canarchiveinseparateprocess=true`. Save the `server.properties` file and restart the Manager.

Once this property is set to "true" on the Manager, the Save Output options for a selected report on ArcSight Web include a new parameter called *Generate Report In Separate*

Process. Select this option for a report you want to archive as a separate process, and run the report.

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.

Configurations for Reports with Large Time Ranges

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 ArcSight Web report parameters list.

On the ArcSight Manager in the `server.properties` file, set `report.canquerywithfullscanhint=true`. Save the `server.properties` file and restart the Manager.

Once this property is set to "true" on the Manager, the Save Output options for a selected report on ArcSight Web include a new parameter called *Query with Full Scan Hint*. Select this option for a report you want to run with the full scan hint, and run the report.

If a report is saved with the parameter set to "true", the report is archived as a separate process even if the property `report.canquerywithfullscanhint` in `server.properties` is set back to "false" later on.

Chapter 7

Monitoring Dashboards

The ArcSight Web interface enables you to view dashboards made available from the ArcSight Console.

When you click **Dashboards** in the toolbar, you see the Dashboards display, usually with the Dashboards tree open in the resource pane and the dashboards of the current branch listed in the content pane.

["Viewing and Managing Dashboards" on page 107](#)

["Changing Dashboard Layouts" on page 107](#)

Viewing and Managing Dashboards

Dashboards are organized on the ArcSight Web's resource tree on the left. Click the group folders to open or close them. Click a folder to see a list of its dashboards in the pane to the right. Click the arrow icon in the upper-right corner of the resource pane to hide or show it.

Click a dashboard's name to open it and its collection of data monitors in the right pane.

By default, the information on a dashboard refreshes automatically every 60 seconds. Click the "Pause" button (| |) to stop refreshing, or click the circular arrow to refresh immediately. Click the arrow head to resume auto-refreshing.

Run the mouse pointer over elements in graphic data monitors to see the tooltip details.

Three types of data monitors are available: Event Graph, Geographic Event Graph, and Hierarchy Map.

Changing Dashboard Layouts

You can change data monitors layouts. Click **Dashboards** and choose one to show from the resource tree. The data monitor on the right panel is the default pattern.

On a dashboard display, click **Edit Layout** to open the Dashboard Layout editor.

To rearrange data monitors, click and drag them from one of the display areas to another. Use the upper and lower "wide" areas to accommodate tables, which often run wide and cannot be resized. Use the left and right "narrow" areas to accommodate charts, which are more likely to resize successfully.

To see the results of a rearrangement, click **Save**.

Row Limits

On ArcSight Web, there is no row limit imposed on Query Viewer chart displays (unlike on the ESM Console). Query Viewer charts with more than 100 rows do not display properly and are hard to read.

On the ArcSight Console, the chart renders only the first 100 rows and displays an error message indicating that only 100 rows can be properly displayed. No such restriction is available for Query Viewer charts on ArcSight Web dashboards, so rows beyond the 100th row will not display properly on the Web.

Workaround: In the Console, set row limits on Query Viewers. This will control chart displays in the Console and ArcSight Web. Determine which Query Viewers you want to display as charts. In the ArcSight Console, edit those Query Viewers to set the Row Limit to 100 (or less).

Chapter 8

Using the Knowledge Base

ArcSight Web provides access to viewing knowledge base articles and pointers to articles as defined in the ArcSight Console. The articles available to you are organized in the resource tree on the left. Click the folders in the tree to open or close them. Click the arrow icon in the upper-right corner of the resource tree panel to hide it or show it.



ArcSight offers the Knowledge Base as a convenience for storing user-generated pointers or articles of interest. It is not pre-populated.

Using Reference Pages

An event viewed from the Event Inspector may have a reference page associated with it. The contents of a reference page is set through the ArcSight Console.

- If present in an event, click **View references** to show the reference page content in a separate browser window.
- Use the drop-down menu to navigate or other pages of this reference if more pages are available.
- Use the browser's **Back** button to return.

Chapter 10

Setting Preferences

Options Menu

In any display, click **Options** in the toolbar to set or change your preferences for date formatting, locale, active channel startup, and password.

Click the **Formats** tab to choose the style and punctuation to use for date and time values. Click **Update** to apply your changes before moving to another tab.

Click the **Locale** tab to choose the time zone you work in. Click **Update** to apply your changes before moving to another tab.

Click the **Channels** tab to set, or bypass setting, the parameters for active channels, each time you open one. The check box is clear by default, which means that you see the channel setup options. Select the check box to avoid setup and to go directly to the channel display. There is also an option to hide (collapse) the channel tree on the left panel when a channel is already running. By default, this tree remains in view. Click **Update** to apply your changes before moving to another tab.

Click the **Password** tab to change your current password. Enter your old password first. Then enter your new password and repeat it to confirm. Click **Update** to put your change into effect. For information on password restrictions see the Administrator's Guide, chapter 2 on "Configuration," topic called "Managing Password Configurations."

Hide Exception Reporting Details

ArcSight Web returns detailed exceptions messages and stack traces to the web client when an operational error occurs. Error messages occur either when invalid user input is provided or when exceptions occur during normal operation.

When there is an exception in the code, ArcSight Web displays the exception stack trace. If you are concerned about the level of detail exposed to users in these messages, you can turn off the display of the exception stack as follows:

- 1 In the `webserver.properties` file, add the following line:

```
web.display.exception.stack=false
```
- 2 Clear the browser cache.

Chapter 11

Custom Branding and Styling

You can change logo images, colors, and styles for ArcSight Web by creating and editing the file `<ArcSightWeb_HOME>/config/web/styles.properties`. This file doesn't exist by default, but you can create it by copying either `example.styles.properties` or `full.styles.properties` and renaming it to **styles.properties**.



Do not modify the file `<ArcSightWeb_HOME>/config/web/styles.defaults.properties`. This file contains the default settings. It is overridden by your custom `styles.properties` file. (All default property files are overwritten during upgrades.)

To add custom branding or styles:

- 1 Modify the properties in `styles.properties` as needed to fit your custom branding and style requirements, and remove the comment tags from the lines that contain property settings you want to apply.
- 2 If you want to add one or more custom logo images as part of your re-branding effort, you need to both both modify the relevant property settings and add the image(s) to the `webapp/images` directory:
 - ◆ Modify the properties file to call your custom image file(s) and un-comment the relevant lines (e.g., `navbarLogoImg=MyCustomLogo.gif` and `loginLogoImg=logo-login-MyCustomLogo.gif`). You might also want to modify and un-comment the logo image size property and navigation bar text colors to make the proper customizations.
 - ◆ Add the image file to the directory `<ArcSightWeb_HOME>/webapp/images`.
- 3 Restart ArcSight Web to see the effects of your custom changes.

These branding changes are visible to anyone using that instance of ArcSight Web.

To add a custom login banner message:

- 1 Create a file called `loginbanner.txt` in the `<ArcSightWeb_HOME>/config` folder.
- 2 Edit the file to add the new Login banner text message you want to appear at login.
- 3 Restart the ArcSight Web server and log in again. The new login message appears.

Index

A

- active channel 15
 - grids 18
 - headers 17
 - inline filters 19
 - open 15
 - view in ArcSight Web 17
- archived reports 102, 103
- ArcSight Web
 - about 7
 - home page 9
- audit event
 - in active channel 69

B

- branding 115

C

- case
 - attachments 96
 - chapter 89
 - columns 90
 - create 91
 - events 96
 - Final tab 94
 - Follow Up tab 94
 - Initial tab 92
 - notes 97
 - security classification codes 90
- channel 15
 - preferences 113

D

- dashboard
 - audit events 75
 - monitoring 107
- data fields 28

E

- events
 - audit events 69
 - data fields 28
 - event categories 21
 - in cases 96
 - inspecting 19

F

- format
 - preferences 113

H

- home page, ArcSight Web 11

I

- inline filters 19
- inspecting events 19

K

- knowledge base
 - ArcSight Web 109

L

- locale, preferences 113
- logo, customizing, in ArcSight Web 115

M

- monitoring
 - inspecting events 19

N

- notifications
 - audit events 79
 - categories 99

O

- options 113

P

- partitions
 - audit events 81
- passwords
 - change 113
- pattern discovery
 - audit events 81
- preferences, ArcSight Web 113

Q

- query viewers
 - audit events 82

R

reference pages, event 111

reports

- archived reports 102
- audit events 82
- configuration 104
- in ArcSight Web 101
- parameters 102
- viewing archived reports 103

resources

- audit events 69

S

schedules

audit events 85

session list

audit events 85

styles.properties 115

T

trends

audit events 86

U

users

audit events 88