

Standard Content Guide

ArcSight Express

ArcSight Express 4.0
with CORR-Engine

March 12, 2013



Copyright © 2013 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.

This document is confidential.

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI .
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Revision History

Date	Product Version	Description
03/12/2013	ArcSight Express Content for ArcSight Express 4.0 with CORR-Engine	Final revision for release.

Contents

Chapter 1: Overview	7
What is Standard Content?	7
Standard Content Documentation	8
Chapter 2: Installation and Configuration	9
Modeling the Network	10
Categorizing Assets	10
Configuring Notification Destinations	11
Configuring Notifications and Cases	11
Rules with Notifications to the CERT Team	11
Rules with Notifications to SOC Operators	12
Scheduling Reports	13
Using Trends	13
Viewing Use Case Resources	14
Viewing Resource URIs	14
Chapter 3: ArcSight Express Use Case	15
Resources	15
Chapter 4: Cisco Monitoring Use Cases	19
Cisco Overview	21
Configuration	21
Resources	21
Cisco Adaptive Security Appliance (ASA)	40
Configuration	40
Resources	40
Cisco Cross-Device	51
Devices	51
Configuration	51
Resources	51
Cisco Firewall Services Module (FWSM)	61
Configuration	61
Resources	61
Cisco Generic Firewall	71

Devices	71
Configuration	71
Resources	71
Cisco Generic Intrusion Prevention System (IPS)	83
Devices	83
Configuration	83
Resources	84
Cisco Intrusion Prevention System (IPS) Sensor	91
Configuration	91
Resources	91
Cisco IOS Intrusion Prevention System (IOS IPS)	97
Configuration	97
Resources	97
Cisco Ironport Email Security Appliance (ESA)	102
Configuration	102
Resources	102
Cisco Ironport Web Security Appliance (WSA)	108
Configuration	108
Resources	108
Cisco Network	113
Configuration	113
Resources	113
Cisco Wireless	119
Configuration	119
Resources	119
Chapter 5: Devices Use Cases	123
Devices	124
Configuration	124
Resources	124
Anti-Virus	132
Resources	132
BlueCoat	139
Resources	139
Database	140
Resources	140
Firewall	144
Configuration	144
Resources	144
Identity Management	156
Resources	156
IDS - IPS	165
Configuration	165

Resources	165
Network	172
Resources	172
Operating System	183
Resources	183
VPN	191
Resources	191
Chapter 6: Microsoft Windows Monitoring Use Cases	203
Microsoft Windows Monitoring	204
Resources	204
Account Management	207
Applicable Events	207
Configuration	208
Resources	208
Authentication	221
Applicable Events	221
Configuration	221
Resources	222
Policy Changes	227
Applicable Events	227
Configuration	227
Resources	227
System Services and Auditing	230
Applicable Events	230
Configuration	230
Resources	231
Chapter 7: NetFlow Monitoring Use Case	239
Devices	240
Configuration	240
Resources	240
Chapter 8: Operations Use Cases	247
Operations	248
Resources	248
Case Tracking and Escalation	251
Resources	251
Configuration Changes	260
Resources	260
Logins	266
Resources	266
System Notifications and Escalation	270

- Resources270
- Traffic Monitoring273
 - Resources273
- Chapter 9: Security and Threat Use Cases 279**
 - Security and Threat279
 - Configuration279
 - Resources280
 - Vulnerabilities296
 - Resources296
- Index..... 299**

Chapter 1

Overview

This chapter discusses the following topics.

["What is Standard Content?" on page 7](#)

["Standard Content Documentation" on page 8](#)

What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the-box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

Standard content is pre-installed on the ArcSight Express appliance to provide essential system health and status operations. Standard content consists of the following:

- **ArcSight Administration** provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of the content and system components.
- **ArcSight System** is required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.
- **ArcSight Express** is organized into the topics listed below. To provide easy access, the most valuable content from each of these topics is linked directly under the ArcSight Express group. Content in each topic is also grouped in a use case resource, for easy access through the use case home page.
 - ◆ **Cisco Monitoring** provides both a broad overview of your Cisco infrastructure and visibility into specific Cisco devices. Powerful analysis tools allow you to monitor activity, configuration changes, availability, and threats across Cisco devices in your environment. A comprehensive and easily customizable set of dashboards, active channels, and reports allows you to measure and report on the status of devices and a variety of other activities taking place in your network.
 - ◆ **Devices** provides resources that monitor the devices in your environment, such as firewalls, Intrusion Detection Systems (IDS), and virtual private networks (VPN), as well as cross-device functions such as logins and configuration management.
 - ◆ **NetFlow Monitoring** is designed specifically for NetFlow; a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting

IP traffic information. In addition to Cisco IOS, NetFlow also supports Juniper routers and Linux. Using ArcSight Express to leverage session-level data provided by NetFlow can help you monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

- ◆ **Operations** provides resources for monitoring operations in your environment, including traffic monitoring and case management.
- ◆ **Security and Threat** provides resources for monitoring the security of your environment, including malware and reconnaissance attempts.
- ◆ **Microsoft Windows Monitoring** provides resources for monitoring network activity specific to Windows operating systems. The resources help you monitor additions, modifications, and deletions to user accounts and computer accounts, login activity and failed authentications. You can also monitor policy changes and violations, new and removed system services, and the status of critical services.
- **ArcSight Solutions** contains the HP Reputation Security Monitor solution (RepSM) that uses data received from TippingPoint DVLabs about malicious domains and addresses to detect malware infection, zero day attacks, and dangerous browsing on your network.

Standard Content Documentation

This guide describes the ArcSight Express content. For information about the ArcSight System and ArcSight Administration content, refer to the ArcSight System and ArcSight Administration Standard Content Guide. For information about the RepSM solution, refer to the HP Reputation Security Monitor Solution Guide.

ArcSight documentation is available on Protect 724 (<https://protect724.arcsight.com>).



Certain resources described in this guide are visible to the ArcSight Administrator only. As an ArcSight Administrator, you can view resources that are not available to other users and can edit resources to tailor the content to your environment.

Chapter 2

Installation and Configuration

ArcSight Express content is required for basic functionality and is pre-installed on the ArcSight Express appliance. You do not have to perform any additional installation tasks. However, some basic configuration is recommended to tailor the content for your operating environment.



You need to perform the configuration tasks in this section as the ArcSight Administrator. As the Administrator, you can view resources that are not available to other users and can edit resources to tailor the content to your environment.

This chapter discusses the following topics:

- ["Modeling the Network" on page 10](#)
- ["Categorizing Assets" on page 10](#)
- ["Configuring Notification Destinations" on page 11](#)
- ["Configuring Notifications and Cases" on page 11](#)
- ["Scheduling Reports" on page 13](#)
- ["Using Trends" on page 13](#)
- ["Viewing Use Case Resources" on page 14](#)

Modeling the Network

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

There are several ways to model your network. For information about populating the network model, see the ArcSight Console User's Guide. To learn more about the architecture of the network modeling tools, see the ESM 101 guide.

Categorizing Assets

After you have populated your network model with assets, apply the standard asset categories to activate standard content that uses these categories so that you can apply criticality and business context to events.

- Categorize all assets (or the zones to which the assets belong) that are internal to the network with the `/Site Asset Categories/Address Spaces/Protected` asset category.

Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as *Protected*.



Assets with a private IP address (such as 192.168.0.0) are considered as Protected by the system, even if they are not categorized as such.

- Categorize all assets that are considered critical to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with the `/System Asset Categories/Criticality/High or Very High` asset category.

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

You can assign asset categories to assets, zones, asset groups, or zone groups. If assigned to a group, all resources under that group inherit the categories.

You can assign asset categories individually using the Asset editor or in a batch using the Network Modeling wizard. For information about how to assign asset categories using the ArcSight Console tools, see the ArcSight Console User's Guide.

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, see the ArcSight Console User's Guide or the ESM 101 guide.

Configuring Notification Destinations

Configure notification destinations if you want to be notified when certain rules are triggered. By default, the notifications are disabled in the standard content rules. However, ArcSight Administrators can configure the destinations *and* enable the notification in the rules. For more information about enabling the notifications in rules, see [Configuring Notifications and Cases](#), below.

The ArcSight Express and ArcSight Administration rules reference two notification destination groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. See the ArcSight Console User's Guide for more details.

Configuring Notifications and Cases

Standard content depends on rules to send notifications and open cases when conditions are met. Notifications and cases are the tools used to track and resolve the security issues that the content is designed to find. By default, notifications to the CERT Team and SOC Operators notification destination groups, and create case actions are disabled in the standard content rules.

To configure rules to send notifications and open cases, first configure notification destinations, then enable the send notification and open case actions in the rules. See the ArcSight Console User's Guide for details about enabling notifications and opening cases.

Rules with Notifications to the CERT Team

The following security-related rules send notifications to the **CERT Team** notification destination group. In these rules, both the send notification and open case actions are disabled by default. Assign cases created by these rules to the appropriate user or user group in your organization.

Rule Name	Rule URI
High Number of IDS Alerts for DoS	ArcSight Express/Security and Threat/Attack Monitoring/DoS/
SYN Flood Detected by IDS or Firewall	ArcSight Express/Security and Threat/Attack Monitoring/DoS/
High Number of IDS Alerts for Backdoor	ArcSight Express/Security and Threat/Attack Monitoring/Malware Activity/
Warning - Insecure Configuration	ArcSight Express/Security and Threat/Vulnerabilities/
Warning - Vulnerable Software	ArcSight Express/Security and Threat/Vulnerabilities/
Notify on Successful Attack	ArcSight Express/Security and Threat/Attack Monitoring/
High Number of Connections	ArcSight Express/Operations/Traffic Monitoring/
High Number of Denied Connections for A Source Host	ArcSight Express/Operations/Traffic Monitoring/
High Number of Denied Inbound Connections	ArcSight Express/Operations/Traffic Monitoring/
Blaster Infected Host	ArcSight Express/Security and Threat/Worm Outbreak/

Rules with Notifications to SOC Operators

The following rules send notifications to the **SOC Operators** notification destination group. In these rules, the send notification actions are disabled by default.

Rule Name	Rule URI
Case Deleted	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Case Escalation	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Account Locked Out	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Account Locked Out Multiple Times in 24 Hours	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Lockout Attempt Failed	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Privileged Account Locked Out	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Authentication Attempted to Disabled Account	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Authentication Attempted to Non-Existing Account	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Failed Authentication - Windows Domain Account	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Failed Authentication - Windows Workstation	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Lockout Policy Changed	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
Password Policy Changed	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
System Audit Policy Changed	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
CrashOnAuditFail Modified	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Request Start	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Request Stop	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Started	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Stopped	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Install Service Attempt	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Unable to Log Events	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Rule Name	Rule URI
Windows Audit Events Discarded	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows Security Audit Log Cleared	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Starting	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Time Changed	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Scheduling Reports

You can schedule reports based on cases, notifications, assets, or events to run automatically or on a regular schedule. By default, the reports are not scheduled to run automatically.

Evaluate the reports and schedule the ones that are of interest to your organization and business objectives. For instructions about how to schedule reports, see the ArcSight Console User's Guide.



Note

You cannot run non-event-based reports for the previous day or the previous week; their output is always the *current* state.

Using Trends

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

ArcSight Express content includes trends, which are enabled by default. These enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m. when network traffic is usually less busy than during peak daytime business hours. You can customize these schedules to suit your needs using the Trend scheduler in the ArcSight Console.

To disable a trend, go to the Navigator panel, right-click the trend and select **Disable Trend**.



Caution

To enable a disabled trend, you must first **change the default start date** in the Trend editor.

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

For more information about trends, refer to the the ArcSight Console User's Guide.

Viewing Use Case Resources

The ArcSight Express resources are grouped together in the ArcSight Console using use case resources. A use case resource provides a way to group a set of resources that help address a specific security issue or business requirement.

To view the resources associated with a use case resource:

- 1 In the Navigator panel, select the **Use Cases** tab.
- 2 Browse for an ArcSight Express use case resource such as ArcSight Express/Microsoft Windows Monitoring/Account Management.
- 3 Right-click the use case resource and select the **Open Use Case** option, or double-click the use case resource.

The resources that make up a use case resource are displayed in the Viewer. The use case resource tables listed in the following chapters contain all the resources that have been explicitly assigned to the use case.

Viewing Resource URIs

Certain resources in ArcSight Express are linked from other content groups, such as ArcSight Foundation or ArcSight Administration. For such resources, the ArcSight Console and this guide show the parent URIs; for example All Dashboards/ArcSight Foundation/NetFlow Monitoring/NetFlow Bandwidth Usage Overview instead of All Dashboards/ArcSight Express/NetFlow Monitoring/NetFlow Bandwidth Usage Overview.

You can see the parent URI for a resource on the ArcSight Console either from the Inspect/Edit panel when you edit a resource or by hovering your mouse cursor on the resource in a use case. If the parent URI points to content for which you do not have permissions (for example, ArcSight Foundation content is available to ArcSight Administrators but not to Express users), the **Find Resource in Navigator** command does not display the resource in the Navigator. Use the use case resource to run reports, see dashboards, and so on.

Chapter 3

ArcSight Express Use Case

The ArcSight Express use case serves as a container that groups other ArcSight Express use cases. This use case also provides easy access to the most valuable resources from each of the other use cases.

Resources

The following table lists all the resources explicitly assigned to the ArcSight Express use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 3-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Monitor Resources			
Case Events	This active channel shows case audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Last 5 Minutes	This active channel shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.	Active Channel	ArcSight Express
Live	This active channel shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.	Active Channel	ArcSight System/Core
Reconnaissance Activity	This active channel shows reconnaissance events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

Resource	Description	Type	URI
Correlated Alerts	This active channel shows all the rules that triggered within the last two hours.	Active Channel	ArcSight Express/
Security Activity Statistics	This dashboard displays an overview of common attackers, targets, protocols, and activity by time.	Dashboard	ArcSight Express/
Security Activity	This dashboard displays an overview of security activity, including suspicious network activity, failed logins, and common attacks on the network.	Dashboard	ArcSight Express/
Interesting Mail	This dashboard shows event information related to large email messages.	Dashboard	ArcSight Express/
Traffic Monitoring	This dashboard shows well-known port activity for sources and destinations outside the United States.	Dashboard	ArcSight Express/
Threat View	This dashboard displays information about events that have a High or Very High priority, or have been correlated.	Dashboard	ArcSight Express/
Anti-Virus Overview	This dashboard shows an overview of the top infections, the top infected systems, and the most recent and top anti-virus error events.	Dashboard	ArcSight Express/
IDS - IPS Overview	This dashboard shows an overview of IDS signatures. The dashboard shows the Top 10 Signature Destinations, Top 10 Signature Sources, Top 10 Signature Types, and Top 10 Signatures data monitors.	Dashboard	ArcSight Express/
Firewall Connection Overview	This dashboard shows an overview of all the denied connection events originating from firewalls.	Dashboard	ArcSight Express/
Blue Coat	This dashboard displays information related to web browser activity as reported by Blue Coat web security devices.	Dashboard	ArcSight Express/
Cisco Event Statistics	This dashboard displays an overview of protocols and activities recorded by Cisco devices in recent hours.	Dashboard	ArcSight Express/
Windows Monitoring	This dashboard monitors the top Microsoft Windows users, top Windows event types, and top Windows devices.	Dashboard	ArcSight Express/

Resource	Description	Type	URI
Malware	This dashboard displays information regarding events that can be correlated with malware activity.	Dashboard	ArcSight Express/
Login Information	This dashboard displays an overview of logins, both failures and successes, for privileged and non-privileged accounts.	Dashboard	ArcSight Express/
Security Intelligence Status Report	This report displays four charts and six tables. The first chart gives an hourly breakdown of the event counts by agent severity. The three tables below the Event Count by Agent Severity chart show the top events, top attacks and top triggering rules. The three charts below the tables show the top attackers, top targets, and top target ports. The three tables at the bottom of the page show the number of cases added and notifications sent, along with a list of assets and the vulnerabilities used to compromise them.	Report	ArcSight Express/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
admin	This destination is pre-defined for SOC operators. Add additional information, such as email addresses.	Destination	SOC Operators/1
admincert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	Destination	CERT Team/1
Vulnerabilities	The Vulnerabilities use case provides several resources for monitoring security assessment and vulnerability activity, as well as a way to configure some of the resources.	Use Case	ArcSight Express/Security and Threat/
NetFlow Monitoring	This use case provides resources that help you monitor events from NetFlow related systems.	Use Case	ArcSight Foundation/NetFlow Monitoring/
Security and Threat	This use case provides resources to monitor common security events on a network.	Use Case	ArcSight Express/Security and Threat/

Resource	Description	Type	URI
Microsoft Windows Monitoring	This use case provides a set of use cases that help you monitor important events in Microsoft Windows systems. The use cases focus on account management, authentication, policy changes, and monitoring critical services.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
Devices	The Devices use case provides several resources to help you monitor various devices. This is a master use case that contains other device monitoring use cases. You can configure common elements used by all of the related use cases.	Use Case	ArcSight Express/Devices/
Operations	This use case provides resources for monitoring cases, tracking logins and accounts, and monitoring configuration changes and network traffic.	Use Case	ArcSight Express/Operations/
Cisco Overview	This use case provides high-level reports showing logins, configuration changes, and other events from Cisco firewalls and Cisco Intrusion Prevention Systems in your environment.	Use Case	ArcSight Foundation/Cisco Monitoring/

Chapter 4

Cisco Monitoring Use Cases

Cisco Monitoring provides both a broad overview of your Cisco infrastructure and visibility into specific Cisco devices. Powerful analysis tools allow you to monitor activity, configuration changes, availability, and threats across Cisco devices in your environment. A comprehensive and easily customizable set of dashboards, active channels, and reports allows you to measure and report on the status of devices and a variety of other activities taking place in your network.

The Cisco Monitoring resources are grouped together using use cases, which help address a specific issue or function. The Cisco Monitoring use cases are listed in the following table.

Use Case	Description
"Cisco Overview" on page 21	The Cisco Overview use case provides high-level reports describing logins, configuration changes, and other events involving Cisco Firewalls and Cisco Intrusion Prevention Systems in your environment.
"Cisco Adaptive Security Appliance (ASA)" on page 40	The Cisco Adaptive Security Appliance (ASA) use case provides firewall information based on events reported by Cisco Adaptive Security Appliances.
"Cisco Cross-Device" on page 51	The Cisco Cross-Device use case provides information about logins, configuration changes, and bandwidth consumption across all Cisco devices in your environment.
"Cisco Firewall Services Module (FWSM)" on page 61	The Cisco Firewall Services Module (FWSM) use case provides firewall information reports and dashboards based on events generated by Cisco Firewall Services Modules present in your network.
"Cisco Generic Firewall" on page 71	The Cisco Generic Firewall use case identifies and provides firewall information based on events reported by any Cisco Firewall device or module in your network.
"Cisco Generic Intrusion Prevention System (IPS)" on page 83	The Cisco Generic Intrusion Prevention System (IPS) use case provides reports and dashboards based on alerts generated by any Cisco IDS/IPS devices or modules.

Use Case	Description
"Cisco Intrusion Prevention System (IPS) Sensor" on page 91	The Cisco Intrusion Prevention System (IPS) Sensor use case provides event statistics and configuration changes reported by Cisco Intrusion Prevention Systems Sensors such as the Cisco IPS 4200 series appliance, Cisco Catalyst 6500 series Intrusion Detection System Services Module (ISDM), and Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM).
"Cisco IOS Intrusion Prevention System (IOS IPS)" on page 97	The Cisco IOS Intrusion Prevention System (IOS IPS) use case provides event statistics and configuration change information reported by Cisco IOS Intrusion Prevention System devices present in your network.
"Cisco Ironport Email Security Appliance (ESA)" on page 102	The Cisco Ironport Email Security Appliance (ESA) use case identifies and provides email traffic information based on events reported by Cisco Ironport Email Security Appliances.
"Cisco Ironport Web Security Appliance (WSA)" on page 108	The Cisco Ironport Web Security Appliance (WSA) use case identifies and provides web traffic information based on events reported by Cisco Ironport Web Security Appliances present in your network.
"Cisco Network" on page 113	The Cisco Network use case identifies and provides information based on events reported by Cisco network equipment.
"Cisco Wireless" on page 119	The Cisco Wireless use case provides information about wireless traffic recorded by Cisco Aironet wireless access points present in your network.

Cisco Overview

The Cisco Overview use case provides high-level reports describing logins, configuration changes, and other events involving Cisco Firewalls and Cisco Intrusion Prevention Systems in your environment.

Configuration

The Cisco Overview use case relies on having one or more of the following use cases properly configured for your environment:

- [“Cisco Generic Firewall” on page 71](#)
- [“Cisco Generic Intrusion Prevention System \(IPS\)” on page 83](#)

Resources

The following table lists all the resources explicitly assigned to the Overview use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-1 Resources that Support the Cisco Overview Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco Event Statistics	This dashboard displays an overview of protocols and activities recorded by Cisco devices in recent hours.	Dashboard	ArcSight Express/
Cisco Current Event Sources	This dashboard displays information about the status of reporting Cisco devices, as well as the top Cisco devices currently contributing events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Login Overview	This dashboard shows an overview of login attempts collected by Cisco devices within the last two hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco IPS Sensor Event Overview	This dashboard shows an overview of all the events originating from Cisco IPS devices. The dashboard displays the overall top IPS event type, the top IPS products, and the event moving average per data product.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /
Cisco ASA Event Overview	This dashboard shows an overview of all the events originating from Cisco ASA devices. The dashboard displays the overall top ASA devices with the most events, the event moving average per device, and the recent configuration modification events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
Cisco Configuration Changes Overview	This dashboard shows an overview of successful configuration changes on Cisco WSA, ESA, IPS, and firewall systems.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Web Transactions	This dashboard shows information about web traffic through all Cisco WSAs and includes the top request hosts, blocked and allowed traffic, and the top requested sites.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Cisco IOS IPS Event Overview	This dashboard shows an overview of all the events originating from Cisco IOS IPS devices. The dashboard displays the overall top IPS event type, the top IPS products, and the event moving average per device.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS) /
Sender and Recipient Overview	This dashboard shows the top senders and recipients with the most messages and most bandwidth consumption within the last two hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Cisco FWSM Event Overview	This dashboard shows an overview of all the events originating from Cisco FWSM devices. The dashboard displays the top FWSM devices with the most events, the event moving average per device, and the recent configuration modification events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Recipients in the Last 2 Hours	This query viewer shows the top recipients with the most successful transactions within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Cisco Network Equipment Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco network devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco IPS Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco IPS devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Hosts with Most Web Traffic	This query viewer shows information about the top hosts with the most web traffic within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /

Resource	Description	Type	URI
Cisco Configuration Change Detail (Trend Based)	This query viewer shows all configuration changes recorded by Cisco devices within the last seven days, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Hosts Accessed Most Sites	This query viewer shows information about the top 10 source hosts that accessed the highest number of sites over the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
IPS Sensor Hourly Event Count	This query viewer shows the count of IPS Sensor events within the last six hours. It provides drilldowns to all events in a particular hour, as well as to all hourly events by a particular device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco ASA Hourly Event Count	This query viewer shows the count of events from all Cisco ASA systems within the last six hours. It provides drilldowns to a particular hour, from which another drilldown to hourly event counts per a particular device is provided.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Firewall Configuration Changes in Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco firewall devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
IPS Sensor Hourly Event Count per Device	This query viewer shows the count of IPS Sensor events per device within the last six hours. It provides drilldowns to a specific device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Failed Logins by User in the Last 2 Hours	This query viewer shows users with failed login attempts within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Sites with Most Request Errors	This query viewer shows information about the top ten sites with the most request errors (for example, to a file) over the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Login Details in the Last 7 Days (Trend Based)	This query viewer shows all logins recorded by Cisco devices within the last seven days, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco FWSM Hourly Event Count	This query viewer shows the count of events from all Cisco FWSM systems within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/

Resource	Description	Type	URI
Top Users with Most Failed Logins	This query viewer shows the top ten users with most failed login attempts across all devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Senders with Most Bandwidth in the Last 2 Hours	This query viewer shows the top senders with the most bandwidth consumption within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco IOS IPS Hourly Event Count	This query viewer shows the count of IOS IPS events within the last six hours. It provides drilldowns to all events in a particular hour, from which another drilldown to all hourly events by a particular device is provided.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Successful Logins by User in the Last 2 Hours	This query viewer shows users with successful login attempts within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Recipients with Most Bandwidth in the Last 2 Hours	This query viewer shows the top recipients with the most bandwidth consumption within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco WSA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport WSA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Event Count by Hour	This query viewer shows the total number of Cisco events per hour within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco ESA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport ESA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Successful Requests	This query viewer shows all successful requests within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco IOS IPS Hourly Event Count per Device	This query viewer shows the count of IOS IPS events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco FWSM Hourly Event per Device	This query viewer shows the count of FWSM events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/

Resource	Description	Type	URI
Message Transaction Details	This query viewer shows all message transactions in the previous day.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ASA Hourly Event per Device	This query viewer shows the count of ASA events per device within the last six hours, and provides drilldowns to a particular device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Accessed Sites with Most Traffic	This query viewer shows information about the top accessed sites with the most traffic within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Senders in the Last 2 Hours	This query viewer shows the top senders with the most successful transactions within the last two hours. It also provides drilldowns to a particular sender.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Accessed Sites	This query viewer shows information about the top accessed sites within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Source Addresses with Most Failed Logins	This query viewer shows the top sources with most failed authentication attempts within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Overview of Cisco Configuration Changes	This report displays a summary of configuration changes to Cisco devices. The information includes the change count per day and per hour, the top affected device, and the top users.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Cisco Firewall Overview - Top Allowed Systems	This report displays a summary of the top allowed systems reported by Cisco firewall devices within the last 24 hours, and includes the top inbound (outbound) sources and destinations.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Cisco Firewall Overview - Top Denied Systems	This report displays a summary of the top denied systems reported by Cisco firewall devices within the last 24 hours, and includes the top inbound (outbound) blocked sources and destinations.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Overview of Logins Reported by Cisco Devices - Systems	This report displays a summary of the login attempts recorded by Cisco devices, and includes the top successful and failed login sources and destinations.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/

Resource	Description	Type	URI
Overview of Logins Reported by Cisco Devices - Trend and Users	This report shows a summary of login attempts recorded by Cisco devices, such as the attempt count per day, per product, and the top users with successful and failed logins.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Cisco Intrusion Prevention System Overview	This report displays a summary of alerts reported by Cisco IPS devices within the last 24 hours and includes the alerts per day, the top alerts, the top attackers, and the targets involved.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Cisco Firewall Overview - Trend and Port	This report displays a summary of firewall events from Cisco devices, and includes the inbound (outbound) connections per day and the top inbound (outbound) blocked ports.	Report	ArcSight Foundation/Cisco Monitoring/Overview Reports/
Library Resources			
Cisco Firewall Message Types	This active list contains the mapping of Cisco firewall syslog message types.	Active List	ArcSight Express/Cisco Monitoring/
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Cisco ASA Event Flow Statistics by Device	This data monitor shows the total number of Cisco ASA events per device for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Transport Protocols	This data monitor shows the top transport protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top IOS IPS Event Types	This data monitor shows the distribution of Cisco IPS event types from IOS IPS devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top Event Sources by Device Group	This data monitor shows the top 20 Cisco device groups with the most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top FWSM Event Sources by Message Types	This data monitor shows the top ten Cisco select categories from FWSM devices with most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/

Resource	Description	Type	URI
Cisco Top IOS IPS Devices	This data monitor shows the top 20 event-generating Cisco IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IPS Sensor Devices	This data monitor shows the top 20 event-generating Cisco IPS Sensor devices in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Top Event Sources by Product	This data monitor shows the top 20 event-generating Cisco products within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco FWSM Event Flow Statistics by Device	This data monitor shows the total number of Cisco FWSM events per device for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Top Application Protocols	This data monitor shows the top application protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top ASA Event Sources by Message Types	This data monitor shows the top ten Cisco select categories from ASA devices with most events in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco IPS Sensor Event Flow Statistics by Device	This data monitor shows the total number of events from Cisco IPS Sensor devices per device product for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Most Frequent Ports	This data monitor shows the top target ports recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top Event Sources by Device	This data monitor shows the top 50 Cisco specific devices with most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Last 10 Cisco IOS IPS Successful Configuration Changes	This data monitor shows the last ten successful Cisco IOS IPS configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/

Resource	Description	Type	URI
Cisco IOS IPS Event Flow Statistics by Device	This data monitor shows the total number of events from Cisco IOS IPS devices per device product for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top ASA Sources	This data monitor shows the top 20 event-generating Cisco ASA devices in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Categories	This data monitor displays the top categories of web browser activity based on Blue Coat categories.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Cisco IPS Sensor Event Types	This data monitor shows the distribution of Cisco IPS event types from IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Top FWSM Sources	This data monitor shows the top 20 event-generating Cisco FWSM devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Last 10 Cisco IPS Sensor Successful Configuration Changes	This data monitor shows the last ten successful Cisco IPS Sensor configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Event Flow Statistics by Device in Last 2 Hours (Cisco WSA)	This data monitor shows the total number of Cisco WSA events per device for the last two hours. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Last 10 Cisco FWSM Successful Configuration Changes	This data monitor shows the last ten successful Cisco ASA configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Cisco Events with Protocols	This field set contains fields for evaluating events from Cisco devices.	Field Set	ArcSight Foundation/Cisco Monitoring/
Cisco Device Interface Notifications	This field set focuses on common fields specific to device interface notification events from Cisco network systems.	Field Set	ArcSight Foundation/Cisco Monitoring/
Categories	This field set shows all the categorization fields for events.	Field Set	ArcSight Express/

Resource	Description	Type	URI
Cisco IOS IPS Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco IOS IPS module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Web Requests	This filter selects all web requests to Cisco WSAs.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall-Categorized Events	This filter passes events with the category device group of Firewall from a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Sensor Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco IPS Sensor.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Cisco FWSM Systems	This filter identifies events from Cisco Firewall Services Module (FWSM) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Email Message Transaction (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems, where an (successful or dropped) email transaction is recorded.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Ironport WSA Systems	This filter selects events from Cisco Ironport Web Security Appliance (WSA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Application Protocol Present	This filter selects all Cisco events where the application protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Ironport ESA Systems	This filter identifies events from Cisco Ironport Email Security Appliance (ESA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Successful Web Transactions	This filter selects successful web server requests.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Attacker and Target Address Present	This filter identifies events in which both the attacker and target address fields are populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Windows Events with a Non-Machine User	This filters identifies Microsoft Windows events that have a non-machine/system user in either the attacker or the target fields.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Unsuccessful Logins	This filter identifies failed logins by both administrative and non-administrative users.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Common IPS Event Types	This filter selects all IPS events where the field deviceEventCategory starts with ev.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Systems	This filter identifies events from all Cisco IPS-IDS devices (or modules). Modify this filter to include all IPS products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker User Present	This filter identifies events that have the Attacker User Name event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Select Category Present	This filter selects all Cisco events where at least one of the Category Object, Behavior, Technique and Significance fields is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Unsuccessful Web Server Requests	This filter identifies all requests made to the Cisco WSA returned with client side errors.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Transportation Protocol Present	This filter selects all Cisco events where the transportation protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Internal Targets	This filter looks for events targeting systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Target Port Present	This filter selects all Cisco events where the target port is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco IPS Sensor Systems	This filter selects events from Cisco Intrusion Detection/Prevention Systems that are based on Cisco IPS Sensor Software (not IOS IPS). Configure this filter to include all such systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/

Resource	Description	Type	URI
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco FWSM Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco FWSM device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Failed Logins by Destination Address	This query returns failed login attempts recorded by Cisco devices.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Recipients with Most Bandwidth	This query returns the top recipients with most bandwidth consumption.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
IOS IPS Event Counts by Hour per Device	This query selects the count of IOS IPS events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Top Senders with Most Bandwidth	This query returns the top senders with most bandwidth consumption.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Configuration Changes per Hour in the Previous Day	This query returns the number of configuration change events to the system per hour in the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Overall Outbound Connections per Day	This query returns the count of outbound connections per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Daily Message Transactions - Base	This query returns the number of message transactions grouped by the hour, sender/recipient pair, policy and engine decision.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Event Count by Hour	This query counts the total number of Cisco events per hour within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/

Resource	Description	Type	URI
Failed Logins by Source Address	This query returns failed authentication events recorded by Cisco devices, grouped by the source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Successful Logins by Destination Address	This query returns successful authentication events recorded by Cisco devices, grouped by destination address.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
IPS Sensor Event Counts by Hour per Device	This query returns the count of IPS Sensor events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /
Cisco IPS Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco IPS devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Denied Outbound Connections by Source Host	This query returns the count of denied outbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Alerts per Day	This query returns the count of alerts per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Detail Successful Requests	This query returns all successful requests within the last two hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Logins per Day in the Last 7 Days	This query returns the number of login events to the system and their outcomes per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco WSA Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco Ironport WSA devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Cisco Overall Denied Inbound Connections by Source Host	This query returns the count of denied inbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Top Hosts with Most Web Traffic	This query returns information about the top hosts with most web traffic over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /

Resource	Description	Type	URI
Cisco Overall Denied Inbound Connections by Destination Host	This query returns the count of denied inbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Network Equipment Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco network devices per hour within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco ESA Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco Ironport ESA devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Overall Denied Outbound Connections by Port	This query returns the count of denied outbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Failed Logins by User	This query returns all failed login attempts and the involved users.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Source Hosts Accessed Most Sites	This query returns information about the top source hosts that accessed the highest number of sites over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Cisco Login Detail (Trend Based)	This query returns all logins recorded by Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco FWSM Event Counts by Hour	This query returns the count of events from all Cisco FWSM systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Attackers in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts, grouped by source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Allowed Inbound Connections by Source Host	This query returns the count of allowed inbound connections by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Firewall Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco firewall devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Successful Login by Source Address	This query returns all successful authentication events, grouped by source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
IPS Sensor Event Counts by Hour	This query returns the count of IPS Sensor events within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Overall Denied Inbound Connections by Port	This query returns the count of denied inbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Top Accessed Sites with Most Traffic	This query returns information about the top 100 accessed sites with most traffic over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Overall Inbound Connections per Day	This query returns the count of inbound connections per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Daily Logins per Product	This query tracks login attempts into the system recorded by a Cisco device, grouped by the reporting product.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Message Transaction Details	This query returns the total number of message transactions by hour and engine decision in the previous day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ASA Event Counts by Hour in Last 6 Hours	This query returns the count of events from all Cisco ASA systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Overall Allowed Outbound Connections by Source Host	This query returns the count of allowed outbound connections by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Top Senders with Most Transactions	This query returns the top senders with most transactions.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Resource	Description	Type	URI
Top Sites with Most Request Errors	This query returns information about the top 100 sites with most request errors over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Accessed Sites	This query returns information about the top 100 accessed sites over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Cisco Overall Allowed Outbound Connections by Destination Host	This query returns the count of allowed outbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Successful Logins by User	This query returns all successful login attempts and the users involved.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Users with Successful Logins	This query returns the top users with successful login attempts.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Configuration Changes per Day in the Last 7 Days	This query returns the number of configuration change events to the system per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Targets in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts, grouped by destination host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Users with Most Failed Logins	This query returns the top users with most failed login attempts.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
IOS IPS Event Counts by Hour	This query returns the count of IOS IPS events within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS) /
Cisco Overall Allowed Inbound Connections by Destination Host	This query returns the count of allowed inbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Top Recipients with Most Transactions	This query returns the top recipients with most transactions.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Top Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Daily Connection Setup Attempts - Base	This query tracks inbound and outbound connection attempts to and from the network. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Configuration Change Detail (Trend Based)	This query returns all configuration changes recorded by Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Alerts - Base	This query tracks all alerts by Cisco IPS devices or modules. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Denied Outbound Connections by Destination Host	This query returns the count of denied outbound connections by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco ASA Event Counts by Hour per Device	This query returns the count of ASA events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco FWSM Event Counts by Hour per Device	This query returns the count of FWSM events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Daily Logins - Base	This query tracks login attempts into the system recorded by a Cisco device. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Daily Connection Setup Attempts	This trend stores information about connection establishment attempts to and from the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Daily Alerts	This trend stores all alerts collected by Cisco IPS devices in the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Email Transactions	This trend stores the email message transactions grouped by hour, sender and recipient pair, policy and engine decision.	Trend	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Daily Logins	This trend stores daily login attempts tracked by Cisco devices.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco IOS Intrusion Prevention System (IOS IPS)	This use case provides event statistics and configuration change information reported by Cisco IOS Intrusion Prevention System devices present in your network.	Use Case	ArcSight Foundation/Cisco Monitoring/

Resource	Description	Type	URI
Cisco Ironport Email Security Appliance (ESA)	This use case identifies and provides email traffic information based on events reported by Cisco Ironport Email Security Appliances (ESAs).	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Firewall Services Module (FWSM)	This use case provides firewall information based on events generated by Cisco Firewall Services Modules present in your network.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Ironport Web Security Appliance (WSA)	This use case identifies and provides web traffic information based on events reported by Cisco Ironport Web Security Appliances present in your network.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Network	This use case identifies and provides information based on events reported by Cisco Network Equipment.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Generic Intrusion Prevention System (IPS)	This use case provides IPS information based on alerts generated by any Cisco IDS/IPS device or module.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Generic Firewall	This use case identifies and provides firewall information based on events reported by any Cisco Firewall device or module in your network.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Cross-Device	This use case provides information about logins, configuration changes, and bandwidth consumption across all Cisco devices in your environment.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Wireless	This use case provides information about wireless traffic recorded by Cisco Aironet wireless access points present in your network.	Use Case	ArcSight Foundation/Cisco Monitoring/
Cisco Intrusion Prevention System (IPS) Sensor	This use case provides event statistics and configuration changes reported by Cisco Intrusion Prevention System Sensors, such as the Cisco IPS 4200 series appliance, Cisco Catalyst 6500 series Intrusion Detection System Services Module (ISDM), and Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM).	Use Case	ArcSight Foundation/Cisco Monitoring/

Resource	Description	Type	URI
Cisco Adaptive Security Appliance (ASA)	This use case provides firewall information based on events reported by Cisco Adaptive Security Appliances.	Use Case	ArcSight Foundation/Cisco Monitoring/

Cisco Adaptive Security Appliance (ASA)

The Cisco Adaptive Security Appliance (ASA) use case provides firewall information based on events reported by Cisco Adaptive Security Appliances.

Configuration

The Cisco Adaptive Security Appliance (ASA) use case requires the following configuration for your environment.

- Verify that the [Cisco ASA Systems](#) filter includes all the Cisco ASA systems present in your network. If necessary, the ArcSight Administrator can update the filter to include missing devices.

Resources

The following table lists all the resources explicitly assigned to the Cisco Adaptive Security Appliance (ASA) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-2 Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco ASA Events	This active channel shows all events originating from Cisco Adaptive Security Appliance (ASA) systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Alert, Critical and Error Events from Cisco ASA Systems	This active channel shows all alert, critical and error events originating from Cisco ASA systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
IPS Syslog Events from Cisco ASA Systems	This active channel shows all IPS alert events originating from Cisco ASA systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA Denied Connections Overview	This dashboard shows an overview of all the denied connection events coming from Cisco ASA firewalls.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA Event Overview	This dashboard shows an overview of all the events originating from Cisco ASA devices. The dashboard displays the overall top ASA devices with the most events, the event moving average per device, and the recent configuration modification events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
Cisco ASA Allowed Connections Overview	This dashboard shows an overview of all the allowed connection events coming from Cisco ASA firewalls.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top ports across allowed outbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top sources with the most denied inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top destinations with the most allowed inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top destination hosts across Denied Outbound Connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top sources with the most denied outbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top ten ports of allowed inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top ports across denied outbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top destinations with the most denied inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/

Resource	Description	Type	URI
Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top sources with the most allowed outbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA Hourly Event Count	This query viewer shows the count of events from all Cisco ASA systems within the last six hours. It provides drilldowns to a particular hour, from which another drilldown to hourly event counts per a particular device is provided.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top ten ports of denied inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top destinations with most allowed outbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA Hourly Event per Device	This query viewer shows the count of ASA events per device within the last six hours, and provides drilldowns to a particular device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA)	This query viewer shows the top sources with the most allowed inbound connections by Cisco ASA devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Denied Inbound Connections by Address (Cisco ASA)	This report shows a summary of the denied inbound traffic blocked by Cisco ASA devices. The traffic is grouped by foreign address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
Denied Outbound Connections by Port (Cisco ASA)	This report shows a summary of the denied outbound traffic blocked by Cisco ASA devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
VPN Connections Accepted by Address (Cisco ASA)	This report shows successful VPN connection data to a Cisco ASA system. A chart summarizes the top VPN device addresses with successful connections. A table shows details of the successful connections.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Outbound Connection Setup Attempts per Day (Cisco ASA)	This report shows a summary of the outbound connection setup attempts reported by Cisco ASA devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Configuration Changes by Type (Cisco ASA)	This report displays all successful configuration changes to Cisco ASA devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Configuration Changes by User (Cisco ASA)	This report displays all successful configuration changes to Cisco ASA devices. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
VPN Connection Counts by User (Cisco ASA)	This report shows count information about VPN connections to a Cisco ASA system for each user. A summary of the top users by connection count is provided. Details of the connection counts for each user are also provided, including connection count and systems accessed.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Inbound Connection Setup Attempts per Day (Cisco ASA)	This report shows a summary of the inbound connection setup attempts reported by Cisco ASA devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
VPN Authentication Errors (Cisco ASA)	This report shows errors generated by a VPN connection attempt to a Cisco ASA system. The address is the IP address of the VPN connection source. This report can be used to see which users are having difficulties using or setting up their VPN clients.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/

Resource	Description	Type	URI
Top Bandwidth Target Hosts (Cisco ASA)	This report shows a summary of the bandwidth usage, recorded by a Cisco ASA device, grouped by the top target hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Denied Inbound Connections by Port (Cisco ASA)	This report shows a summary of the denied inbound traffic blocked by Cisco ASA devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Bandwidth Usage by Protocol (Cisco ASA)	This report shows a summary of the bandwidth usage recorded by a Cisco ASA device, grouped by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage. This report shows you the applications that are consuming the most bandwidth.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Bandwidth Usage by Hour (Cisco ASA)	This report shows a summary of the bandwidth usage per hour, recorded by a Cisco ASA device. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
VPN Connections Denied by Address (Cisco ASA)	This report shows denied VPN connection data from a Cisco ASA system. A chart summarizes the top VPN device addresses with denied connections. A table shows details of the denied connections.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /VPN/
Denied Outbound Connections by Address (Cisco ASA)	This report shows a summary of the denied outbound traffic, blocked by Cisco ASA devices, grouped by local address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
Top Bandwidth Source Hosts (Cisco ASA)	This report shows a summary of the bandwidth usage recorded by a Cisco ASA device, grouped by the top source hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Library Resources			
Cisco Firewall Message Types	This active list contains the mapping of Cisco firewall syslog message types.	Active List	ArcSight Express/Cisco Monitoring/
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Cisco ASA Event Flow Statistics by Device	This data monitor shows the total number of Cisco ASA events per device for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Top ASA Sources	This data monitor shows the top 20 event-generating Cisco ASA devices in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Top ASA Event Sources by Message Types	This data monitor shows the top ten Cisco select categories from ASA devices with most events in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall-Categorized Events	This filter passes events with the category device group of /Firewall from a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Failed VPN Connection Events (Cisco ASA)	This filter selects unsuccessful VPN events from a Cisco ASA system where the behavior is /Access/Start.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/

Resource	Description	Type	URI
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco FWSM Systems	This filter identifies events from Cisco Firewall Services Module (FWSM) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker and Target Address Present	This filter identifies events in which both the attacker and target address fields are populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Internal Targets	This filter looks for events targeting systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco ASA Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco ASA device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA IPS Alert Events	This filter selects IPS alert events from Cisco ASA Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
VPN Authentication Errors (Cisco ASA)	This filter selects VPN authentication error events from Cisco ASA devices, where an authentication error event is defined as having the category behavior of /Authentication/Verify and the category significance of /Informational/Error.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Successful VPN Connection Events (Cisco ASA)	This filter selects successful VPN events from a Cisco ASA system where the behavior is /Access/Start.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Allowed Inbound Connections by Destination Address (Cisco ASA)	This query returns the count of allowed inbound connections by Cisco ASA devices, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Allowed Inbound Connections by Source Address (Cisco ASA)	This query returns the count of allowed inbound connections by Cisco ASA devices, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/

Resource	Description	Type	URI
Allowed Outbound Connections by Destination Address (Cisco ASA)	This query returns the count of allowed outbound connections by Cisco ASA devices, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Connections Denied by Address (Cisco ASA)	This query returns the device zone, address, host name and a count of VPN devices with denied connections.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Denied Inbound Connections by Port (Cisco ASA)	This query returns the count of denied inbound connections by Cisco ASA devices, grouped by port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Overall Denied Inbound Connections by Port	This query returns the count of denied inbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Authentication Errors (Cisco ASA)	This query returns VPN authentication events from Cisco ASA systems where there has been an error. It returns the user information, the host information, the error, the time (within an hour) and the number of times the error occurred in the hour.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Allowed Inbound Connections by Port (Cisco ASA)	This query returns the count of allowed inbound connections by Cisco ASA devices, grouped by port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Connections Accepted by Address (Cisco ASA)	This query returns the device zone, address, host name, and a count of VPN devices with successful connections through a Cisco ASA system.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Cisco ASA Outbound Connections per Day	This query returns the count of outbound connections per day reported by Cisco ASA devices for the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Overall Denied Outbound Connections by Source Host	This query returns the count of denied outbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco ASA Event Counts by Hour in Last 6 Hours	This query returns the count of events from all Cisco ASA systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Allowed Outbound Connections by Source Address (Cisco ASA)	This query returns the count of allowed outbound connections by Cisco ASA devices, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Denied Outbound Connections by Port (Cisco ASA)	This query returns the count of denied outbound connections by Cisco ASA devices, grouped by port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Users by Connection Count (Cisco ASA)	This query returns VPN events from Cisco ASA systems where the Category Behavior is /Access/Start, /Authentication/Verify or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Denied Outbound Connections by Destination Address (Cisco ASA)	This query returns the count of denied outbound connections by Cisco ASA devices, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Top Bandwidth Source Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each source host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Denied Inbound Connections by Destination Address (Cisco ASA)	This query returns the count of denied inbound connections by Cisco ASA devices, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Overall Denied Inbound Connections by Source Host	This query returns the count of denied inbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Denied Inbound Connections by Source Address (Cisco ASA)	This query returns the count of denied inbound connections by Cisco ASA devices, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Denied Outbound Connections by Source Address (Cisco ASA)	This query returns the count of denied outbound connections by Cisco ASA devices, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Daily Connection Setup Attempts - Base	This query tracks inbound and outbound connection attempts to and from the network. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Top Bandwidth Destination Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each destination host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco ASA Inbound Connections per Day	This query returns the count of inbound connections per day recorded by Cisco ASA devices for the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco Overall Denied Outbound Connections by Port	This query returns the count of denied outbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Allowed Outbound Connections by Port (Cisco ASA)	This query returns the count of allowed outbound connections by Cisco ASA devices, grouped by port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Cisco ASA Event Counts by Hour per Device	This query returns the count of ASA events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Daily Connection Setup Attempts	This trend stores information about connection establishment attempts to and from the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Cisco Cross-Device

The Cisco Cross-Device use case provides information about logins, configuration changes, and bandwidth consumption across all Cisco devices in your environment.

Devices

The following Cisco device types can supply events that apply to the Cisco Cross-Device use case:

- Cisco Intrusion Detection System/Intrusion Prevention System
- Operating System
- Cisco Firewall devices or modules
- Virtual Private Network
- Cisco Network Equipment (routers or switches)
- Cisco Wireless (Aironet Access Points only)
- Cisco Web Security Appliance
- Cisco Email Security Appliance

Configuration

The Cisco Cross-Device use case relies on having one or more of the following use cases properly configured for your environment:

- ["Cisco Generic Intrusion Prevention System \(IPS\)" on page 83](#)
- ["Cisco Generic Firewall" on page 71](#)
- ["Cisco Ironport Email Security Appliance \(ESA\)" on page 102](#)
- ["Cisco Ironport Web Security Appliance \(WSA\)" on page 108](#)
- ["Cisco Network" on page 113](#)

Resources

The following table lists all the resources explicitly assigned to the Cisco Cross-Device use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-3 Resources that Support the Cisco Cross-Device Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco Event Statistics	This dashboard displays an overview of protocols and activities recorded by Cisco devices in recent hours.	Dashboard	ArcSight Express/
Cisco Current Event Sources	This dashboard displays information about the status of reporting Cisco devices, as well as the top Cisco devices currently contributing events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/

Resource	Description	Type	URI
Login Overview	This dashboard shows an overview of login attempts collected by Cisco devices within the last two hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Configuration Changes Overview	This dashboard shows an overview of successful configuration changes on Cisco WSA, ESA, IPS, and firewall systems.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Event Count by Hour	This query viewer shows the total number of Cisco events per hour within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Failed Logins by User in the Last 2 Hours	This query viewer shows users with failed login attempts within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco ESA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport ESA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Cisco Network Equipment Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco network devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco IPS Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco IPS devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Login Details in the Last 7 Days (Trend Based)	This query viewer shows all logins recorded by Cisco devices within the last seven days, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Configuration Change Detail (Trend Based)	This query viewer shows all configuration changes recorded by Cisco devices within the last seven days, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Users with Most Failed Logins	This query viewer shows the top ten users with most failed login attempts across all devices within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Firewall Configuration Changes in Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco firewall devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Successful Logins by User in the Last 2 Hours	This query viewer shows users with successful login attempts within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Source Addresses with Most Failed Logins	This query viewer shows the top sources with most failed authentication attempts within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco WSA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport WSA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Logins per Day	This report shows the summary of logins per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Configuration Changes per Hour in the Previous Day	This report shows a summary of the configuration changes per hour in the previous day.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Logins per Hour in the Previous Day	This report shows the summary of all login attempts to the system and their outcomes per hour in the previous day.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Bandwidth Source Hosts	This report shows a summary of the bandwidth usage by the top source hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Top Bandwidth Destination Hosts	This report shows a summary of the bandwidth usage by the top destination hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Configuration Changes by User	This report displays all configuration changes to Cisco devices. Events are grouped by user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Configuration Changes per Day	This report shows a summary of the configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Cisco Configuration Changes by Type	This report displays all configuration changes to Cisco devices. Events are grouped by type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Top Transport Protocols	This data monitor shows the top transport protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Top Categories	This data monitor displays the top categories of web browser activity based on Blue Coat categories.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Cisco Top Event Sources by Device Group	This data monitor shows the top 20 Cisco device groups with the most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top Event Sources by Product	This data monitor shows the top 20 event-generating Cisco products within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Top Application Protocols	This data monitor shows the top application protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Most Frequent Ports	This data monitor shows the top target ports recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Top Event Sources by Device	This data monitor shows the top 50 Cisco specific devices with most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Cisco Events with Protocols	This field set contains fields for evaluating events from Cisco devices.	Field Set	ArcSight Foundation/Cisco Monitoring/
Cisco Device Interface Notifications	This field set focuses on common fields specific to device interface notification events from Cisco network systems.	Field Set	ArcSight Foundation/Cisco Monitoring/
Categories	This field set shows all the categorization fields for events.	Field Set	ArcSight Express/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Login Attempts	This filter selects any attempts at logging into systems. It excludes machine logins into Microsoft Windows systems.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco FWSM Systems	This filter identifies events from Cisco Firewall Services Module (FWSM) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Ironport WSA Systems	This filter selects events from Cisco Ironport Web Security Appliance (WSA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Application Protocol Present	This filter selects all Cisco events where the application protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Ironport ESA Systems	This filter identifies events from Cisco Ironport Email Security Appliance (ESA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Windows Events with a Non-Machine User	This filter identifies Microsoft Windows events that have a non-machine/system user in either the attacker or the target fields.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Unsuccessful Logins	This filter identifies failed logins by both administrative and non-administrative users.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Cisco IPS Systems	This filter identifies events from all Cisco IPS-IDS devices (or modules). Modify this filter to include all IPS products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker User Present	This filter identifies events that have the Attacker User Name event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Select Category Present	This filter selects all Cisco events where at least one of the Category Object, Behavior, Technique and Significance fields is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Transportation Protocol Present	This filter selects all Cisco events where the transportation protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco Target Port Present	This filter selects all Cisco events where the target port is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco IPS Sensor Systems	This filter selects events from Cisco Intrusion Detection/Prevention Systems that are based on Cisco IPS Sensor Software (not IOS IPS). Configure this filter to include all such systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Failed Logins by Destination Address	This query returns failed login attempts recorded by Cisco devices.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Login Detail (Trend Based)	This query returns all logins recorded by Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Configuration Changes per Hour in the Previous Day	This query returns the number of configuration change events to the system per hour in the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Event Count by Hour	This query counts the total number of Cisco events per hour within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Successful Login by Source Address	This query returns all successful authentication events, grouped by source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Failed Logins by Source Address	This query returns failed authentication events recorded by Cisco devices, grouped by the source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Cisco Firewall Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco firewall devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Successful Logins by Destination Address	This query returns successful authentication events recorded by Cisco devices, grouped by destination address.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Logins per Hour in the Previous Day	This query shows the number of login events to the system and their outcomes per hour in the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco IPS Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco IPS devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Logins per Day in the Last 7 Days	This query returns the number of login events to the system and their outcomes per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Successful Logins by User	This query returns all successful login attempts and the users involved.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Users with Successful Logins	This query returns the top users with successful login attempts.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Configuration Changes per Day in the Last 7 Days	This query returns the number of configuration change events to the system per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Users with Most Failed Logins	This query returns the top users with most failed login attempts.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Bandwidth Source Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each source host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco WSA Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco Ironport WSA devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Daily Connection Setup Attempts - Base	This query tracks inbound and outbound connection attempts to and from the network. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Network Equipment Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco network devices per hour within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco ESA Configuration Changes in the Last 6 Hours	This query returns all configuration changes recorded by Cisco Ironport ESA devices within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Resource	Description	Type	URI
Top Bandwidth Destination Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each destination host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Alerts - Base	This query tracks all alerts by Cisco IPS devices or modules. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Configuration Change Detail (Trend Based)	This query returns all configuration changes recorded by Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Failed Logins by User	This query returns all failed login attempts and the involved users.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Daily Logins - Base	This query tracks login attempts into the system recorded by a Cisco device. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Daily Connection Setup Attempts	This trend stores information about connection establishment attempts to and from the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Daily Alerts	This trend stores all alerts collected by Cisco IPS devices in the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Logins	This trend stores daily login attempts tracked by Cisco devices.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Cisco Firewall Services Module (FWSM)

The Cisco Firewall Services Module (FWSM) use case provides firewall information reports and dashboards based on events generated by Cisco Firewall Services Modules present in your network.

Configuration

The Cisco Firewall Services Module (FWSM) use case requires the following configuration for your environment:

- Verify that the [Cisco FWSM Systems](#) filter includes all the Cisco Firewall Services Modules present in your network. If necessary, the ArcSight Administrator can modify the filter to include any missing modules.

Resources

The following table lists all the resources explicitly assigned to the Cisco Firewall Services Module (FWSM) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-4 Resources that Support the Cisco Firewall Services Module (FWSM) Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco FWSM Events	This active channel shows events originating from Cisco Firewall Service Modules (FWSM) within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Alert, Critical and Error Events from Cisco FWSM Systems	This active channel shows all alert, critical, and error events coming from Cisco FWSM systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Allowed Connections Overview	This dashboard shows an overview of all the denied connection events coming from Cisco FWSM modules.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Denied Connections Overview	This dashboard shows an overview of all the denied connection events originating from Cisco FWSM modules.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Event Overview	This dashboard shows an overview of all the events originating from Cisco FWSM devices. The dashboard displays the top FWSM devices with the most events, the event moving average per device, and the recent configuration modification events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top source hosts across allowed outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top ports across all allowed inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top ports across all denied inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Hourly Event Count	This query viewer shows the count of events from all Cisco FWSM systems within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top destination hosts across denied outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top ports across allowed outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top destination hosts across allowed outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top source hosts across denied outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top source hosts across allowed inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Hourly Event per Device	This query viewer shows the count of FWSM events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top destination hosts across denied inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top ports across denied outbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top destination hosts across allowed inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM)	This query viewer shows the top source hosts across denied inbound connections by Cisco FWSM modules within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Outbound Connections by Port (Cisco FWSM)	This report shows a summary of the denied outbound traffic blocked by Cisco FWSM modules, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Outbound Connections by Address (Cisco FWSM)	This report shows a summary of the denied outbound traffic, blocked by Cisco FWSM modules, grouped by local address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Denied Inbound Connections by Port (Cisco FWSM)	This report shows a summary of the denied inbound traffic blocked by Cisco FWSM modules, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Inbound Connection Setup Attempts per Day (Cisco FWSM)	This report shows a summary of the inbound connection setup attempts reported by Cisco FWSM devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Inbound Connections per Hour (Cisco FWSM)	This report shows a summary of the denied inbound traffic per hour by Cisco FWSM modules. A chart shows the total number of denied connections per hour for the last day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Bandwidth Source Hosts (Cisco FWSM)	This report shows a summary of the bandwidth usage recorded by a Cisco FWSM module, grouped by the top source hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Bandwidth Destination Hosts (Cisco FWSM)	This report shows a summary of the bandwidth usage, recorded by a Cisco FWSM module, grouped by the top target (destination) hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Outbound Connection Setup Attempts per Day (Cisco FWSM)	This report shows a summary of the outbound connection setup attempts reported by Cisco FWSM devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Configuration Changes by Type (Cisco FWSM)	This report displays all successful configuration changes to Cisco FWSM modules. Events are grouped by type and then user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Bandwidth Usage by Protocol (Cisco FWSM)	This report shows a summary of the bandwidth usage recorded by a Cisco FWSM module, grouped by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage. Use this report to identify the applications that are consuming the most bandwidth.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Bandwidth Usage by Hour (Cisco FWSM)	This report shows a summary of the bandwidth usage per hour, recorded by a Cisco FWSM module. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Configuration Changes by User (Cisco FWSM)	This report displays all successful configuration changes to Cisco FWSM modules. Events are grouped by user and then type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Inbound Connections by Address (Cisco FWSM)	This report shows a summary of the denied inbound traffic, blocked by Cisco FWSM modules. The traffic is grouped by foreign address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Outbound Connections per Hour (Cisco FWSM)	This report shows a summary of the denied outbound traffic per hour by Cisco FWSM modules. A chart shows the total number of denied connections per hour for the last day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Library Resources			
Cisco Firewall Message Types	This active list contains the mapping of Cisco firewall syslog message types.	Active List	ArcSight Express/Cisco Monitoring/
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Cisco Top FWSM Event Sources by Message Types	This data monitor shows the top ten Cisco select categories from FWSM devices with most events within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Cisco Top FWSM Sources	This data monitor shows the top 20 event-generating Cisco FWSM devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Event Flow Statistics by Device	This data monitor shows the total number of Cisco FWSM events per device for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Last 10 Cisco FWSM Successful Configuration Changes	This data monitor shows the last ten successful Cisco ASA configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker and Target Address Present	This filter identifies events in which both the attacker and target address fields are populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Internal Targets	This filter looks for events targeting systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall-Categorized Events	This filter passes events with the category device group of /Firewall from a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco FWSM Systems	This filter identifies events from Cisco Firewall Services Module (FWSM) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco FWSM Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco FWSM device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Denied Inbound Connections by Port (Cisco FWSM)	This query returns the count of denied inbound connections by Cisco FWSM modules, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Inbound Connections by Source Address (Cisco FWSM)	This query returns the count of denied inbound connections by Cisco FWSM modules, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco FWSM Event Counts by Hour	This query returns the count of events from all Cisco FWSM systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Denied Inbound Connections by Destination Address (Cisco FWSM)	This query returns the count of denied inbound connections by Cisco FWSM modules, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco FWSM Outbound Connections per Day	This query returns the count of outbound connections per day reported by Cisco devices with FWSM for the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Overall Denied Inbound Connections by Port	This query returns the count of denied inbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Allowed Inbound Connections by Source Address (Cisco FWSM)	This query returns the count of allowed inbound connections by Cisco FWSM modules, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Overall Denied Outbound Connections by Source Host	This query returns the count of denied outbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Denied Outbound Connections by Port (Cisco FWSM)	This query returns the count of denied outbound connections by Cisco FWSM modules, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Allowed Inbound Connections by Destination Address (Cisco FWSM)	This query returns the count of allowed inbound connections by Cisco FWSM modules, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
Allowed Outbound Connections by Port (Cisco FWSM)	This query returns the count of allowed outbound connections by Cisco FWSM modules, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Top Bandwidth Source Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each source host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco FWSM Inbound Connections per Day	This query returns the count of inbound connections per day recorded by Cisco devices with FWSM for the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Overall Denied Inbound Connections by Source Host	This query returns the count of denied inbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Denied Outbound Connections by Destination Address (Cisco FWSM)	This query returns the count of denied outbound connections by Cisco FWSM modules, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Denied Outbound Connections by Source Address (Cisco FWSM)	This query returns the count of denied outbound connections by Cisco FWSM modules, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Daily Connection Setup Attempts - Base	This query tracks inbound and outbound connection attempts to and from the network. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Allowed Inbound Connections by Port (Cisco FWSM)	This query returns the count of allowed inbound connections by Cisco FWSM modules, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Overall Denied Inbound Connections per Hour - Event Based	This query returns the count of denied inbound connections per hour for each source zone within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Top Bandwidth Destination Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each destination host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Allowed Outbound Connections by Destination Address (Cisco FWSM)	This query returns the count of allowed outbound connections by Cisco FWSM modules, grouped by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Allowed Outbound Connections by Source Address (Cisco FWSM)	This query returns the count of allowed outbound connections by Cisco FWSM modules, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Overall Denied Outbound Connections by Port	This query returns the count of denied outbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections per Hour - Event Based	This query returns the count of denied outbound connections per hour for each source zone within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco FWSM Event Counts by Hour per Device	This query returns the count of FWSM events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Daily Connection Setup Attempts	This trend stores information about connection establishment attempts to and from the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Cisco Generic Firewall

The Cisco Generic Firewall use case identifies and provides firewall information based on events reported by any Cisco Firewall device or module in your network.

Devices

The following Cisco device types can supply events that apply to the Cisco Generic Firewall use case:

- Cisco Firewall devices or modules

Configuration

The Cisco Generic Firewall use case requires the following configuration for your environment:

- If Cisco Adaptive Security Appliances or Cisco Firewall Services Modules are present in your network, configure the [Cisco Intrusion Prevention System \(IPS\) Sensor](#) use case.
- Verify that the [Cisco Firewall Systems](#) filter includes all the Cisco firewall devices or modules present in your network. If necessary, the ArcSight Administrator can modify the filter to include missing devices.

Resources

The following table lists all the resources explicitly assigned to the Cisco Generic Firewall use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-5 Resources that Support the Cisco Generic Firewall Use Case

Resource	Description	Type	URI
Monitor Resources			
Events from Cisco Firewall Systems	This active channel shows all the events coming from Cisco firewall systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Alert, Critical and Error Events from Cisco Firewall Systems	This active channel shows all alert, critical and error events originating from Cisco firewall systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Allowed Connections in Last 2 Hours	This dashboard shows an overview of all the denied connection events coming from firewalls. The dashboard displays the Top 10 Denied Ports (Inbound), Top 10 Denied Ports (Outbound), Top 10 Hosts With Denied Inbound Connections, and Top 10 Hosts With Denied Outbound Connections data monitors.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Firewall Denied Connections in Last 2 Hours	This dashboard shows an overview of all denied connection events originating from Cisco firewalls.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Generic Firewall Event Overview	This dashboard shows an overview of all the events coming from Cisco firewall devices. The dashboard displays the overall top firewall products with most events, event moving average per data product and the hourly event count within the last six hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Ports across Allowed Outbound Connections in Last 2 Hours	This query viewer shows the top ports across all allowed outbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Ports across Allowed Inbound Connections in Last 2 Hours	This query viewer shows the top ports across allowed inbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Destination Hosts across Denied Inbound Connections in Last 2 Hours	This query viewer shows the top destination hosts (target zone, address, and hostname) across denied inbound connections within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Hourly Event Count	This query viewer shows the count of events from all Cisco firewall systems within the last six hours. It also provides drilldowns to ASA and FWSM devices.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Source Hosts across Denied Outbound Connections in Last 2 Hours	This query viewer shows the top source addresses across denied outbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Ports across Denied Outbound Connections in Last 2 Hours	This query viewer shows the top ports across all denied outbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours	This query viewer shows the top destination hosts across allowed inbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Top Destination Hosts across Denied Outbound Connections in Last 2 Hours	This query viewer shows the top destination hosts (target zone, address, and hostname) across denied outbound connections within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Source Hosts across Allowed Outbound Connections in Last 2 Hours	This query viewer shows the top source hosts across allowed outbound connections within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall
Top Source Hosts across Denied Inbound Connections in Last 2 Hours	This query viewer shows the top source addresses across denied inbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Ports across Denied Inbound Connections in Last 2 Hours	This query viewer shows the top ports across denied inbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco FWSM Hourly Event per Device	This query viewer shows the count of FWSM events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco ASA Hourly Event per Device	This query viewer shows the count of ASA events per device within the last six hours, and provides drilldowns to a particular device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours	This query viewer shows the top destination hosts across allowed outbound connections by Cisco firewalls within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Source Hosts across Allowed Inbound Connections in Last 2 Hours	This query viewer shows the top source hosts (attacker zone, address, and hostname) across allowed inbound connections within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Inbound Connection Setup Attempts per Day	This report shows a summary of the inbound connection setup attempts per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Overall Allowed Outbound Connections by Source Host	This report shows a summary of the allowed outbound traffic by Cisco firewall devices, grouped by source address. A chart shows the top ten addresses with the highest event count. A report lists all the addresses sorted by event count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Top Bandwidth Source Hosts (Cisco Firewall)	This report shows a summary of the bandwidth usage recorded by a Cisco firewall device, grouped by the top source hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Outbound Connections by Destination Host	This report shows a summary of the allowed outbound traffic by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest event count. A report lists all the addresses sorted by event count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections by Destination Port	This report shows a summary of the denied inbound traffic, blocked by Cisco firewall devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Inbound Connections by Destination Host	This report shows a summary of the allowed inbound traffic by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest event count. A report lists all the addresses sorted by event count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Bandwidth Usage by Protocol (Cisco Firewall)	This report shows a summary of the bandwidth usage recorded by a Cisco firewall device, grouped by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage. Use this report to see the applications that are consuming the most bandwidth.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Summary of Denied Traffic by Specific Cisco Firewall	This report shows a summary of the denied traffic by a specific Cisco firewall. A chart shows the top denied source hosts, destination hosts, and target ports.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Summary of Allowed Traffic by Specific Cisco Firewall	This report shows a summary of the allowed traffic by a specific Cisco firewall. A chart shows the top allowed source hosts, destination hosts, and target ports.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections per Hour in the Previous Day	This report shows a summary of the denied inbound traffic per hour in the previous day. A chart shows the total number of denied connections per hour for the last day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections by Source Host	This report shows a summary of the denied outbound traffic, blocked by Cisco firewall devices, grouped by source address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes by Type	This report displays all successful configuration changes to Cisco firewall devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Outbound Connection Setup Attempts per Day	This report shows a summary of the outbound connection setup attempts per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes by User	This report displays all successful configuration changes to Cisco firewall devices. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Bandwidth Usage by Hour (Cisco Firewall)	This report shows a summary of the bandwidth usage per hour, recorded by a Cisco firewall device. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections by Source Host	This report shows a summary of the denied inbound traffic, blocked by Cisco firewall devices, grouped by source address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Overall Denied Outbound Connections per Hour in the Previous Day	This report shows a summary of the denied outbound traffic per hour in the previous day. A chart shows the total number of denied connections per hour for the last day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections by Destination Host	This report shows a summary of the denied inbound traffic, blocked by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes by Device	This report displays all successful configuration changes to Cisco firewall devices. Events are grouped by reporting device, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes per Day	This report shows a summary of the Cisco firewall configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections by Destination Host	This report shows a summary of the denied outbound traffic, blocked by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections by Destination Port	This report shows a summary of the denied outbound traffic blocked by Cisco firewall devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Inbound Connections by Source Host	This report shows a summary of the allowed inbound traffic by Cisco firewall devices, grouped by source address. A chart shows the top ten addresses with the highest event count. A report lists all the addresses sorted by event count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Top Bandwidth Destination Hosts (Cisco Firewall)	This report shows a summary of the bandwidth usage, recorded by a Cisco firewall device, grouped by the top target hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Top Activities across Cisco Firewall Devices	This data monitor shows the top 20 Cisco device groups with the most events in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Event Flow by Cisco Firewall Products in the Last 2 Hours	This data monitor shows the number of Cisco firewall events per device product within the last two hours. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Top Firewall Product Sources	This data monitor shows the top 20 event-generating Cisco Firewall device products within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Events	This field set focuses on common fields specific to Cisco firewall events.	Field Set	ArcSight Foundation/Cisco Monitoring/
Attacker and Target Address Present	This filter identifies events in which both the attacker and target address fields are populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Internal Targets	This filter looks for events targeting systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall Category Device Group Present	This filter selects all events from a Cisco firewall device where the Category Device Group field is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall-Categorized Events	This filter passes events with the category device group of /Firewall from a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco FWSM Systems	This filter identifies events from Cisco Firewall Services Module (FWSM) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Successful Configuration Changes	This filter selects all successful configuration changes recorded by Cisco firewalls.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Cisco Denied Connections by Destination Host - Template	This query returns the count of denied connections by a particular firewall, grouped by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes per Day in the Last 7 Days	This query returns the number of Cisco firewall configuration changes per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Event Counts by Hour	This query returns the count of events from all Cisco firewall systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Outbound Connections per Hour in the Previous Day	This query returns the count of denied outbound connections per hour in the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Overall Outbound Connections per Day	This query returns the count of outbound connections per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Inbound Connections by Port	This query returns the count of allowed inbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Denied Connections by Port - Template	This query returns the count of denied connections by a particular firewall, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Overall Allowed Inbound Connections by Source Host	This query returns the count of allowed inbound connections by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Allowed Connections by Source Host - Template	This query returns the count of allowed connections by a particular firewall, grouped by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections by Port	This query returns the count of denied inbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Inbound Connections per Day	This query returns the count of inbound connections per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Cisco Overall Denied Outbound Connections by Source Host	This query returns the count of denied outbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Outbound Connections by Source Host	This query returns the count of allowed outbound connections by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Allowed Connections by Port - Template	This query returns the count of allowed connections by a particular firewall, grouped by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Outbound Connections by Destination Host	This query returns the count of allowed outbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Cisco Overall Allowed Outbound Connections by Port	This query returns the count of allowed outbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Bandwidth Source Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each source host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Overall Denied Inbound Connections by Source Host	This query returns the count of denied inbound connections by source host (source zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Inbound Connections by Destination Host	This query returns the count of allowed inbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Denied Connections by Source Host - Template	This query returns the count of denied connections by a particular firewall, grouped by source host (attacker zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections per Hour in the Previous Day	This query returns the count of denied inbound connections per day in the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Inbound Connections by Destination Host	This query returns the count of denied inbound connections by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Daily Connection Setup Attempts - Base	This query tracks inbound and outbound connection attempts to and from the network. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Bandwidth Destination Hosts	This query returns the count of TotalBytes (Bytes In + Bytes Out) for each destination host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Overall Denied Outbound Connections by Port	This query returns the count of denied outbound connections by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections by Destination Host	This query returns the count of denied outbound connections by destination address (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco Allowed Connections by Destination Host - Template	This query returns the count of allowed connections by a particular firewall, grouped by destination host (target zone, address, and hostname).	Query	ArcSight Express/Cisco Monitoring/Functionality/Firewall/
Cisco FWSM Event Counts by Hour per Device	This query returns the count of FWSM events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco ASA Event Counts by Hour per Device	This query returns the count of ASA events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Daily Connection Setup Attempts	This trend stores information about connection establishment attempts to and from the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

Cisco Generic Intrusion Prevention System (IPS)

The Cisco Generic Intrusion Prevention System (IPS) use case provides reports and dashboards based on alerts generated by any Cisco IDS/IPS devices or modules.

The Cisco Generic Intrusion Prevention System (IPS) use case provides reports based on all Cisco IPS alerts being generated in your network. The following use cases focus on particular Cisco products and provide extra product-specific information such as reports on configuration changes, or dashboards showing event statistics:

- ["Cisco Intrusion Prevention System \(IPS\) Sensor" on page 91](#)
- ["Cisco IOS Intrusion Prevention System \(IOS IPS\)" on page 97](#)

Devices

The following Cisco device types can supply events that apply to the Cisco Generic Intrusion Prevention System (IPS) use case:

- Cisco Firewalls
- Cisco Intrusion Prevention Systems
- Cisco Intrusion Detection Systems

Configuration

The Cisco Generic Intrusion Prevention System (IPS) use case requires the following configuration for your environment:

- If IPS sensors and IOS IPS devices are present in your network, configure the following use cases:
 - ◆ ["Cisco Intrusion Prevention System \(IPS\) Sensor" on page 91](#)
 - ◆ ["Cisco IOS Intrusion Prevention System \(IOS IPS\)" on page 97](#)
- Verify that the Cisco IPS Systems filter includes all Cisco IPS devices present in your network. If necessary, the ArcSight Administrator can modify the filter to include missing devices and verify that the following filters capture all alert, error, and status events from those systems:
 - ◆ [Cisco IPS Alert Events](#)
 - ◆ [Cisco IPS Error Events](#)
 - ◆ [Cisco IPS Status Events](#)

Resources

The following table lists all the resources explicitly assigned to the Cisco Generic Intrusion Prevention System (IPS) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-6 Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case

Resource	Description	Type	URI
Monitor Resources			
Error Events from Cisco IPS Systems	This active channel shows all the error events originating from Cisco IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Status Events from Cisco IPS Systems	This active channel shows all status events originating from Cisco IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Events from Cisco IPS Systems	This active channel shows all events originating from Cisco IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Alert Events from Cisco IPS Systems	This active channel shows all alert events originating from Cisco IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Generic IPS Event Overview	This dashboard shows an overview of all the events originating from Cisco IPS devices. The dashboard displays the overall top IPS event type, top IPS products, and event moving average per data product.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Generic IPS Alert Overview	This dashboard shows an overview of all the alerts originating from Cisco IPS devices. The dashboard displays the top alerts, top source and destination alerted, top alert ports, alert technique, and alert severity distribution.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Targets in Cisco Alerts over the Last 2 Hours	This query viewer shows the count of Cisco IDS and IPS alerts, grouped by destination host within the last two hours. It provides drilldowns to all alerts with a target host here as well as the attacker or target in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Top Attackers in Cisco Alerts over the Last 2 Hours	This query viewer shows the count of Cisco IDS and IPS alerts, grouped by source host within the last two hours. It provides drilldowns to all alerts with a particular source here as well the attacker or target in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Details (Trend Based)	This query viewer returns the count of alerts and the alert details per hour for the previous day.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Severity in the Last 2 Hours	This query viewer shows the count of Cisco IDS and IPS alerts by severity (agent severity) within the last two hours. It provides drilldowns to all alerts of a particular severity in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Port in the Last 2 Hours	This query viewer shows the count of IDS and IPS alerts by destination port within the last two hours. It also provides drilldowns to all alerts to a particular destination port in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Configuration Changes by Type	This report displays all successful configuration changes to Cisco IPS devices in a day. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Alert Count by Type	This report shows the count of Cisco IDS and IPS alerts by type.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Targets in Cisco Alerts over a Month	This report shows the top targets in alerts from Cisco IPS devices within the last 30 days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alerts per Hour in the Previous Day	This report shows a summary of the Cisco IPS alerts per hour in the previous day.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Configuration Changes by User	This report displays all successful configuration changes to Cisco IPS devices in a day. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alerts	This report shows the top alerts from Cisco IPS devices within the last 24 hours.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Top Attackers in Cisco Alerts	This report shows the top attackers in alerts from Cisco IPS devices within the last 24 hours.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Alert Count by Port	This report shows the count of Cisco IDS and IPS alerts by port.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Configuration Changes per Day	This report shows a summary of the IPS configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Attackers in Cisco Alerts over a Month	This report shows the top targets in alerts from Cisco IPS devices over the last 30 days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Alert Count by Device	This report shows the count of Cisco IDS and IPS alerts by device.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Configuration Changes by Device	This report displays all successful configuration changes to Cisco IPS devices. Events are grouped by reporting device, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alerts in a Month	This report shows the top alerts from Cisco IPS devices within the last 30 days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Targets in Cisco Alerts	This report shows the top targets in alerts from Cisco IPS devices within last 24 hours.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alerts per Day	This report shows a summary of the Cisco IPS alerts per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Overall Alert Count by Severity	This report shows the count of Cisco IDS and IPS alerts by severity.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Cisco Top IPS Alerts	This data monitor shows the top 20 Cisco IPS alerts (name and the corresponding signature ID) within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Cisco IPS Event Flow Statistics by Device Product	This data monitor shows the total number of events from Cisco IPS devices per device product for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Top IPS Alert Techniques	This data monitor shows the top 20 Cisco IPS alerts within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Sensor Event Types	This data monitor shows the distribution of Cisco IPS event types from IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /
Cisco Top IOS IPS Event Types	This data monitor shows the distribution of Cisco IPS event types from IOS IPS devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS Event Types	This data monitor shows the distribution of Cisco IPS event types within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Top IPS Products	This data monitor shows the top 20 event-generating Cisco IPS device products within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Error Events	This filter selects error events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco IPS device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Cisco IPS Status Events	This filter selects status events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Common IPS Event Types	This filter selects all IPS events where the field deviceEventCategory starts with ev.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Systems	This filter identifies events from all Cisco IPS-IDS devices (or modules). Modify this filter to include all IPS products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Sensor Systems	This filter selects events from Cisco Intrusion Detection/Prevention Systems that are based on Cisco IPS Sensor Software (not IOS IPS). Configure this filter to include all such systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Cisco Alert Counts by Port	This query returns the count of IDS and IPS alerts by destination port.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Reporting Device	This query returns the count of Cisco IDS and IPS alerts by device product, zone, address, and hostname.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Top Attackers and Reporting Devices in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts, grouped by source address, zone, and reporting device information.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Attackers in Cisco Alerts (Trend Based)	This query returns the top targets in Cisco IDS and IPS alerts over the last 30 days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Details (Trend Based)	This query returns the count of alerts and the alert details per hour for the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Port and Device	This query returns the count of IDS and IPS alerts by destination port and reporting device.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Targets and Reporting Devices in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts by destination address, zone, and reporting device information.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Attackers in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts, grouped by source host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Type and Device	This query returns the count of Cisco IDS and IPS alerts by type (category technique) and reporting device.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Targets in Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts, grouped by destination host.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Severity and Device	This query returns the count of Cisco IDS and IPS alerts by severity (agent severity), and reporting device information.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alerts (Trend Based)	This query returns the top Cisco IDS and IPS alerts over the last 30 days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

Resource	Description	Type	URI
Top Targets in Cisco Alerts (Trend Based)	This query returns the top targets in Cisco IDS and IPS alerts over the last 30 days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alerts	This query returns the count of Cisco IDS and IPS alerts within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
IPS Configuration Changes per Day in the Last 7 Days	This query returns the number of IPS configuration changes events to the system per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alert Counts by Severity	This query returns the count of Cisco IDS and IPS alerts by severity (agent severity).	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Alerts - Base	This query tracks all alerts by Cisco IPS devices or modules. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alerts per Hour in the Previous Day	This query returns the count of alerts per hour for the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco Alerts per Day	This query returns the count of alerts per day for the previous week.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Alerts	This trend stores all alerts collected by Cisco IPS devices in the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Cisco Intrusion Prevention System (IPS) Sensor

The Cisco Intrusion Prevention System (IPS) Sensor use case provides event statistics and configuration changes reported by Cisco Intrusion Prevention Systems Sensors such as the Cisco IPS 4200 series appliance, Cisco Catalyst 6500 series Intrusion Detection System Services Module (ISDM), and Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM).

The Cisco Intrusion Prevention System (IPS) Sensor use case provides reports based on all Cisco IPS alerts being generated in your network. For more information, see [“Cisco Generic Intrusion Prevention System \(IPS\)” on page 83](#).

Configuration

The Cisco Intrusion Prevention System (IPS) Sensor use case requires the following configuration for your environment:

- Verify that the [Cisco IPS Sensor Systems](#) filter includes all sensor-based IPS devices present in your network. If necessary, the ArcSight Administrator can modify the filter to include any missing systems and verify that the following filters capture all alert, error, and status events from those systems:
 - ◆ [Cisco IPS Alert Events](#)
 - ◆ [Cisco IPS Error Events](#)
 - ◆ [Cisco IPS Status Events](#)

Resources

The following table lists all the resources explicitly assigned to the Cisco Intrusion Prevention System (IPS) Sensor use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-7 Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco IPS Sensor Events	This active channel shows events originating from Cisco Intrusion Detection/Prevention Sensor systems within the last two hours.	Active Channel	<code>ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /</code>
Status Events from Cisco IPS Sensor Systems	This active channel shows all status events originating from Cisco IPS Sensor systems within the last two hours.	Active Channel	<code>ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /</code>
Alert Events from Cisco IPS Sensor Systems	This active channel shows all alert events originating from Cisco IPS Sensor systems within the last two hours.	Active Channel	<code>ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /</code>

Resource	Description	Type	URI
Error Events from Cisco IPS Sensor Systems	This active channel shows all error events originating from Cisco IPS Sensor systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco IPS Sensor Event Overview	This dashboard shows an overview of all the events originating from Cisco IPS devices. The dashboard displays the overall top IPS event type, the top IPS products, and the event moving average per data product.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco IPS Sensor Alert Overview	This dashboard shows an overview of all the alerts originating from Cisco IPS devices. The dashboard displays the top alerts, top source and destination alerted, top alert ports, alert technique, and alert severity distribution.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Top Cisco Alert Destinations Observed by IPS Sensor	This query viewer shows the count of Cisco IDS and IPS alerts by destination host as observed by IPS Sensor devices within the last two hours. It provides drilldowns to all alerts to and from a particular destination host in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
IPS Sensor Hourly Event Count	This query viewer shows the count of IPS Sensor events within the last six hours. It provides drilldowns to all events in a particular hour, as well as to all hourly events by a particular device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Alert Details (Trend Based)	This query viewer returns the count of alerts and the alert details per hour for the previous day.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alert Sources Observed by IPS Sensor	This query viewer shows the count of Cisco IDS and IPS alerts by source host as observed by IPS Sensor devices within the last two hours. It provides drilldowns to all alerts to and from a particular source in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
IPS Sensor Hourly Event Count per Device	This query viewer shows the count of IPS Sensor events per device within the last six hours. It provides drilldowns to a specific device.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/

Resource	Description	Type	URI
Cisco IPS Sensor Configuration Changes by Type	This report displays all successful configuration changes to Cisco IPS Sensor devices. Events are grouped by type and then user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco IPS Sensor Configuration Changes by User	This report displays all successful configuration changes to Cisco IPS Sensor devices. Events are grouped by user and then type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Cisco Top IPS Sensor Alerts by Device	This data monitor shows the top 20 alert-reporting Cisco IPS Sensor devices along with their alert count within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Top IPS Sensor Alert Techniques	This data monitor shows the top 20 Cisco IPS Sensor alerts within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco IPS Sensor Event Types	This data monitor shows the distribution of Cisco IPS event types from IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Top IPS Sensor Devices	This data monitor shows the top 20 event-generating Cisco IPS Sensor devices in the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Last 10 Cisco IPS Sensor Successful Configuration Changes	This data monitor shows the last ten successful Cisco IPS Sensor configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco IPS Sensor Event Flow Statistics by Device	This data monitor shows the total number of events from Cisco IPS Sensor devices per device product for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Top IPS Sensor Alerts	This data monitor shows the top 20 Cisco IPS alerts (name and the corresponding signature ID) from IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/

Resource	Description	Type	URI
Cisco IPS Error Events	This filter selects error events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS Status Events	This filter selects status events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Cisco IPS-Categorized IPS Sensor Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events from IPS Sensor systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Systems	This filter identifies events from all Cisco IPS-IDS devices (or modules). Modify this filter to include all IPS products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS Sensor Alert Events	This filter selects alert events from Cisco IPS Sensor systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/

Resource	Description	Type	URI
Cisco IPS Sensor Systems	This filter selects events from Cisco Intrusion Detection/Prevention Systems that are based on Cisco IPS Sensor Software (not IOS IPS). Configure this filter to include all such systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Cisco IPS Sensor Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco IPS Sensor.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
IPS Sensor Event Counts by Hour	This query returns the count of IPS Sensor events within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
IPS Sensor Event Counts by Hour per Device	This query returns the count of IPS Sensor events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Alert Details (Trend Based)	This query returns the count of alerts and the alert details per hour for the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Alerts - Base	This query tracks all alerts by Cisco IPS devices or modules. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Top Cisco Alert Sources Observed by IPS Sensor	This query returns the count of Cisco IDS and IPS alerts by source host, observed by IPS Sensor devices.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Cisco Alert Destinations Observed by IPS Sensor	This query returns the count of Cisco IDS and IPS alerts by destination host, observed by IPS Sensor devices.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/

Resource	Description	Type	URI
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Alerts	This trend stores all alerts collected by Cisco IPS devices in the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Cisco IOS Intrusion Prevention System (IOS IPS)

The Cisco IOS Intrusion Prevention System (IOS IPS) use case provides event statistics and configuration change information reported by Cisco IOS Intrusion Prevention System devices present in your network.

The Cisco IOS Intrusion Prevention System (IOS IPS) use case provides reports based on all Cisco IPS alerts being generated in your network. For more information, see "[Cisco Generic Intrusion Prevention System \(IPS\)](#)" on page 83.

Configuration

The Cisco IOS Intrusion Prevention System (IOS IPS) use case requires the following configuration for your environment:

- Verify that the [Cisco IOS IPS Systems](#) filter includes all Cisco IOS IPS devices present in your network. If necessary, the ArcSight Administrator can modify the filter to include these devices and verify that the following filters capture all alert, error, and status events from those systems:
 - ◆ [Cisco IPS Alert Events](#)
 - ◆ [Cisco IPS Error Events](#)
 - ◆ [Cisco IPS Status Events](#)

Resources

The following table lists all the resources explicitly assigned to the Cisco IOS Intrusion Prevention System (IOS IPS) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-8 Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case

Resource	Description	Type	URI
Monitor Resources			
Alert Events from Cisco IOS IPS Systems	This active channel shows all alert events originating from Cisco IOS IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Error Events from Cisco IOS IPS Systems	This active channel shows all the error events coming from Cisco IOS IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IOS IPS Events	This active channel shows events originating from Cisco IOS Intrusion Detection/Prevention systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Status Events from Cisco IOS IPS Systems	This active channel shows all the status events originating from Cisco IPS systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/

Resource	Description	Type	URI
Cisco IOS IPS Alert Overview	This dashboard shows an overview of all the alerts originating from Cisco IPS devices. The dashboard displays the top alerts, top source and destination alerted, top alert ports, alert technique, and alert severity distribution.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IOS IPS Event Overview	This dashboard shows an overview of all the events originating from Cisco IOS IPS devices. The dashboard displays the overall top IPS event type, the top IPS products, and the event moving average per device.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IOS IPS Hourly Event Count per Device	This query viewer shows the count of IOS IPS events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Top Targets in Cisco IOS IPS Alerts	This query viewer shows the top targets alerted by Cisco IOS IPS devices within the last two hours. It provides drilldowns to all alerts with a particular destination host for the attacker or target in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Alert Details (Trend Based)	This query viewer returns the count of alerts and the alert details per hour for the previous day.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IOS IPS Hourly Event Count	This query viewer shows the count of IOS IPS events within the last six hours. It provides drilldowns to all events in a particular hour, from which another drilldown to all hourly events by a particular device is provided.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Top Attackers in Cisco IOS IPS Alerts	This query viewer shows the top attackers alerted by IOS IPS devices within the last two hours. It provides drilldowns to all alerts with a particular source for both the attacker or target in the recent past.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IOS IPS Configuration Changes by User	This report displays all successful configuration changes to Cisco IOS IPS devices. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/

Resource	Description	Type	URI
Cisco IOS IPS Configuration Changes by Type	This report displays all successful configuration changes to Cisco IOS IPS devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Cisco IOS IPS Event Flow Statistics by Device	This data monitor shows the total number of events from Cisco IOS IPS devices per device product for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IOS IPS Alert Techniques	This data monitor shows the top 20 Cisco IOS IPS alerts within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IOS IPS Event Types	This data monitor shows the distribution of Cisco IPS event types from IOS IPS devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IOS IPS Devices	This data monitor shows the top 20 event-generating Cisco IPS Sensor devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IOS IPS Alerts by Device	This data monitor shows the top 20 Cisco alert-reporting IOS IPS devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Top IOS IPS Alerts	This data monitor shows the top 20 Cisco IOS IPS alerts (name and the corresponding signature ID) within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Last 10 Cisco IOS IPS Successful Configuration Changes	This data monitor shows the last ten successful Cisco IOS IPS configuration changes.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IOS IPS Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco IOS IPS module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS Error Events	This filter selects error events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS Status Events	This filter selects status events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Common IPS Event Types	This filter selects all IPS events where the field deviceEventCategory starts with ev.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS Systems	This filter identifies events from all Cisco IPS-IDS devices (or modules). Modify this filter to include all IPS products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Cisco IOS IPS Alert Events	This filter selects alert events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco IPS-Categorized IOS IPS Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events from IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/

Resource	Description	Type	URI
Cisco IPS Sensor Systems	This filter selects events from Cisco Intrusion Detection/Prevention Systems that are based on Cisco IPS Sensor Software (not IOS IPS). Configure this filter to include all such systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Top Attackers in Cisco IOS IPS Alerts	This query returns the count of IDS and IPS alerts generated by Cisco IOS IPS devices, grouped by source host.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
IOS IPS Event Counts by Hour per Device	This query selects the count of IOS IPS events per device within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Top Targets in Cisco IOS IPS Alerts	This query returns the count of IDS and IPS alerts generated by Cisco IOS IPS devices, grouped by target host.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Alert Details (Trend Based)	This query returns the count of alerts and the alert details per hour for the previous day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
Daily Alerts - Base	This query tracks all alerts by Cisco IPS devices or modules. This query serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Intrusion Prevention System/
IOS IPS Event Counts by Hour	This query returns the count of IOS IPS events within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Alerts	This trend stores all alerts collected by Cisco IPS devices in the network.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Cisco Ironport Email Security Appliance (ESA)

The Cisco Ironport Email Security Appliance (ESA) use case identifies and provides email traffic information based on events reported by Cisco Ironport Email Security Appliances.

Configuration

The Cisco Ironport Email Security Appliance (ESA) use case requires the following configuration for your environment:

- Verify that the [Cisco Ironport ESA Systems](#) filter includes all the Cisco Ironport Email Security Appliances present in your network. If necessary, the ArcSight Administrator can modify the filter to include any missing devices.

Resources

The following table lists all the resources explicitly assigned to the Cisco Ironport Email Security Appliance (ESA) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-9 Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco Ironport ESA Events	This active channel shows events originating from Cisco Ironport Email Security Appliances within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Transaction Connections Overview	This dashboard shows the information about SMTP connections to and from Cisco ESA systems within the last two hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Sender and Recipient Overview	This dashboard shows the top senders and recipients with the most messages and most bandwidth consumption within the last two hours.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Injection Connections by Hour	This query viewer shows the count of delivery connections from all Cisco Email Security Appliance (ESA) systems (to other SMTP servers) within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /
Top Recipients in the Last 2 Hours	This query viewer shows the top recipients with the most successful transactions within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA) /

Resource	Description	Type	URI
Top Systems with Most Delivery Connections	This query viewer returns the top hosts (mail transfer agent servers) receiving the most delivery connections from Cisco ESA systems in the network within the last two hours. It also provides various drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Systems with Most Injection Connections	This query viewer shows the top systems (mail transfer agent servers) sending the most injection connections to Cisco ESA systems within the last two hours. It also provides various drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Injection Connections	This query viewer shows information about injection connections, such as the Sender Group and the corresponding SenderBase Score. It also provides various drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Message Transaction Details	This query viewer shows all message transactions in the previous day.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders with Most Bandwidth in the Last 2 Hours	This query viewer shows the top senders with the most bandwidth consumption within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Delivery Connections by Hour	This query viewer shows the count of delivery connections to all Cisco Email Security Appliance (ESA) systems within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Delivery Connections	This query viewer shows events related to delivery connections. It also provides various drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Recipients with Most Bandwidth in the Last 2 Hours	This query viewer shows the top recipients with the most bandwidth consumption within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders in the Last 2 Hours	This query viewer shows the top senders with the most successful transactions within the last two hours. It also provides drilldowns to a particular sender.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders with Most Bandwidth Consumption (Cisco ESA)	This report shows a summary of top senders with most bandwidth consumption.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Resource	Description	Type	URI
Top Recipients with Most Transactions (Cisco ESA)	This report shows a summary of top recipients with most transactions.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ESA Configuration Changes per Day	This report shows a summary of the Cisco ESA configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ESA Configuration Changes by User	This report displays all successful configuration changes to Cisco ESA devices. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders with Most Transactions (Cisco ESA)	This report shows a summary of top senders with most transactions.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Message Transaction per Hour in the Previous Day (Cisco ESA)	This report shows a summary of the email message transactions per hour in the previous day.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Message Transactions per Day (Cisco ESA)	This report shows a summary of the email message transactions per hour within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Connection Overview (Cisco ESA)	This report shows a summary of top email servers with most delivery connections, injection connections, and rejected injection connections.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ESA Configuration Changes by Type	This report displays all successful configuration changes to Cisco ESA devices. Events are grouped by type and then user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Recipients with Most Bandwidth Consumption (Cisco ESA)	This report shows a summary of top recipients with most bandwidth consumption.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Library Resources			
Top Systems with Most Rejected Injection Connections	This data monitor shows the top systems with most rejected injection connections by Cisco ESA systems within the last two hours.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Resource	Description	Type	URI
Event Flow Statistics by Device in Last 2 Hours (Cisco ESA)	This data monitor shows the total number of Cisco ESA events per device for the last two hours. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Rejected Injection Connection (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems related to related injection connections.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Ironport ESA Systems	This filter identifies events from Cisco Ironport Email Security Appliance (ESA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Delivery Connection (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems related to delivery connections.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes (Cisco ESA)	This filter selects all successful Cisco ESA configuration changes.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Email Message Transaction (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems, where an (successful or dropped) email transaction is recorded.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Injection Connection (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems related to injection connections.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/

Resource	Description	Type	URI
Top Recipients with Most Bandwidth	This query returns the top recipients with most bandwidth consumption.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders with Most Bandwidth	This query returns the top senders with most bandwidth consumption.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Senders with Most Transactions	This query returns the top senders with most transactions.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Systems Receiving Most Delivery Connections	This query returns the top systems (mail transfer agent servers) receiving most delivery connections from Cisco ESA systems in the network.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Delivery Connections	This query returns information around delivery connections, such as status and ID.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Systems Sending Most Rejected Injection Connections	This query returns the top systems (mail transfer agent servers) with most rejected injection connections by Cisco ESA systems.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Systems Sending Most Injection Connections	This query returns the top systems (mail transfer agent servers) sending most injection connections to Cisco ESA systems in the network.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Injection Connections	This query returns information about injection connections such as their Sender Group, corresponding SenderBase Score.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Daily Message Transactions - Base	This query returns the number of message transactions grouped by the hour, sender/recipient pair, policy and engine decision.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco ESA Injection Connection Count by Hour	This query selects the count of injection connections to all Cisco Email Security Appliance (ESA) systems (from other SMTP servers) within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Resource	Description	Type	URI
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco ESA Delivery Connection Count by Hour	This query returns the count of delivery connections from all Cisco Email Security Appliance (ESA) systems (to other SMTP servers) within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Message Transactions per Hour in the Previous Day	This query returns the total number of message transactions by hour and engine decision in the previous day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Top Recipients with Most Transactions	This query returns the top recipients with most transactions.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco ESA Configuration Changes per Day in the Last 7 Days	This query returns the number of Cisco ESA configuration change events to the system per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Message Transaction Details	This query returns the total number of message transactions by hour and engine decision in the previous day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Message Transactions per Day in the Previous Week	This query returns the total number of message transactions by day and engine decision in the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Daily Email Transactions	This trend stores the email message transactions grouped by hour, sender and recipient pair, policy and engine decision.	Trend	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

Cisco Ironport Web Security Appliance (WSA)

The Cisco Ironport Web Security Appliance (WSA) use case identifies and provides web traffic information based on events reported by Cisco Ironport Web Security Appliances present in your network.

Configuration

The Cisco Ironport Web Security Appliance (WSA) use case requires the following configuration for your environment:

- Verify that the [Cisco Ironport WSA Systems](#) filter includes all the Cisco Ironport Web Security Appliances present in your network. If necessary, the ArcSight Administrator can modify the filter to include any missing devices.

Resources

The following table lists all the resources explicitly assigned to the Cisco Ironport Web Security Appliance (WSA) use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-10 Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case

Resource	Description	Type	URI
Monitor Resources			
Cisco Ironport WSA Events	This active channel shows events originating from Cisco Ironport Web Security Appliances (WSA) within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Web Transactions	This dashboard shows information about web traffic through all Cisco WSAs and includes the top request hosts, blocked and allowed traffic, and the top requested sites.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Sites with Most Request Errors	This query viewer shows information about the top ten sites with the most request errors (for example, to a file) over the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Successful Requests	This query viewer shows all successful requests within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Hosts with Most Web Traffic	This query viewer shows information about the top hosts with the most web traffic within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Accessed Sites with Most Traffic	This query viewer shows information about the top accessed sites with the most traffic within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /

Resource	Description	Type	URI
Top Accessed Sites	This query viewer shows information about the top accessed sites within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Unsuccessful Requests	This query viewer shows all unsuccessful requests within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Hosts Accessed Most Sites	This query viewer shows information about the top 10 source hosts that accessed the highest number of sites over the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Accessed Sites (Cisco WSA)	This report shows a summary of the top accessed sites.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco WSA Configuration Changes by Type	This report displays all successful configuration changes to Cisco WSA devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Accessed Sites with Most Traffic (Cisco WSA)	This report shows a summary of the top accessed sites with most traffic.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Sources with Most Request Errors (Cisco WSA)	This report shows a summary of the top source hosts with most web request errors.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco WSA Configuration Changes per Day	This report shows a summary of the Cisco WSA configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Hosts with Most Web Traffic (Cisco WSA)	This report shows a summary of the top source hosts with the most web bandwidth consumption.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Denied Sites (Cisco WSA)	This report shows a summary of the top sites denied by Cisco WSA systems.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Hosts Accessed Most (Distinct) Sites (Cisco WSA)	This report shows a summary of the top hosts that accessed most sites.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Web Requests per Day in the Previous Week (Cisco WSA)	This report shows a summary of the web requests per day in the previous week.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/

Resource	Description	Type	URI
Web Requests per Hour in the Previous Day (Cisco WSA)	This report shows a summary of the web requests per hour in the previous day.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Request Error Statistics (Cisco WSA)	This report shows several aspects of request error codes such as distribution and number of distinct sources.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Sites with Most Request Errors (Cisco WSA)	This report shows a summary of the top sites with most request errors.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Cisco WSA Configuration Changes by User	This report displays all successful configuration changes to Cisco WSA devices. Events are grouped by user and type, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Top Sources with Most Denied Requests (Cisco WSA)	This report shows a summary of the top source hosts with the most denied web requests.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Library Resources			
HTTP Status Code Classes	This active list stores the HTTP return status code classes.	Active List	ArcSight Express/Cisco Monitoring/
Event Flow Statistics by Device in Last 2 Hours (Cisco WSA)	This data monitor shows the total number of Cisco WSA events per device for the last two hours. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Successful Web Transactions	This filter selects successful web server requests.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Successful WSA Configuration Changes	This filter selects successful Cisco WSA configuration changes.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Web Requests	This filter selects all web requests to Cisco WSAs.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Cisco Ironport WSA Systems	This filter selects events from Cisco Ironport Web Security Appliance (WSA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Unsuccessful Web Server Requests	This filter identifies all requests made to the Cisco WSA returned with client side errors.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Denied Web Server Requests	This filter identifies all web requests denied by Cisco WSA systems according to access policies.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Cisco WSA Configuration Changes per Day in the Last 7 Days	This query returns the number of Cisco WSA configuration change events to the system per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Sites with Most Request Errors	This query returns information about the top 100 sites with most request errors over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Accessed Sites	This query returns information about the top 100 accessed sites over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Source Hosts with Most Request Errors	This query gets information about the top source hosts with most web request errors over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Web Requests - Base	This query returns all web requests and their HTTP statuses per hour in a day. This is a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

Resource	Description	Type	URI
Top Hosts with Most Web Traffic	This query returns information about the top hosts with most web traffic over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Web Requests per Hour in the Previous Day	This query returns the total number of web requests by hour and web engine decision in the previous day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Detail Unsuccessful Requests	This query returns all unsuccessful requests.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Source Hosts with Most Denied Requests	This query returns the top source hosts with most denied web requests over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Accessed Sites with Most Traffic	This query returns information about the top 100 accessed sites with most traffic over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Request Errors	This query returns the request errors and the requesting sources in the past 24 hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Web Requests per Day in the Previous Week	This query returns the total number of web requests per day in the previous week.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Detail Successful Requests	This query returns all successful requests within the last two hours.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Denied Sites	This query returns the top 100 sites denied by Cisco WSA systems over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Source Hosts Accessed Most Sites	This query returns information about the top source hosts that accessed the highest number of sites over the past day.	Query	ArcSight Express/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Daily Web Requests	This trend stores web requests in a day.	Trend	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/

Cisco Network

The Cisco Network use case identifies and provides information based on events reported by Cisco network equipment.

Configuration

The Cisco Network use case requires the following configuration for your environment:

Resources

The following table lists all the resources explicitly assigned to the Cisco Network use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-11 Resources that Support the Cisco Network Use Case

Resource	Description	Type	URI
Monitor Resources			
Device Interface Notifications	This active channel shows all the events on device interfaces from Cisco network systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Network Events	This active channel shows all network events reported by Cisco network equipment (routers, switches).	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Network/
Events from Cisco Network Systems	This active channel shows all the events originating from Cisco network systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Network/
Device Interface Status	This dashboard shows the status of inbound and outbound interfaces of Cisco network devices based on events reported by this equipment.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Event Overview	This dashboard shows an overview of all the events originating from Cisco IPS devices. The dashboard displays the overall top IPS event type, top IPS products, and event moving average per data product.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Event Count by Hour	This query viewer shows the count of events from all Cisco network systems within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Network/

Resource	Description	Type	URI
Cisco Device Critical Events	This report shows information about critical events on Cisco network devices. These critical events might be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Changes per Day	This report shows a summary of all Cisco network equipment configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Trend of Daily Cisco SNMP Access	This report shows daily SNMP access among all the Cisco traffic.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network SNMP Authentication Failures	This report shows summaries of SNMP failed authentication attempts to a Cisco network device by device or by user. A table details the failed user SNMP authentication attempts for the devices. Two charts provide an overview of the users or devices with the most SNMP authentication failures. Use this report to help determine whether SNMP accounts are targets of brute force attacks and which devices are exhibiting the most SNMP authentication failure activity.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Changes by Device	This report displays all successful configuration changes to Cisco network devices. Events are grouped by reporting device and type.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Changes by User	This report displays all successful configuration changes to Cisco network devices. Events are grouped by user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Top Target Cisco SNMP Access in a Week	This report shows the top Cisco network equipment with the most SNMP access in a week.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Device Errors	This report shows information regarding device errors on Cisco network devices. These events might be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Device Interface Status Messages	This report displays the Cisco network devices reporting link status changes.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/

Resource	Description	Type	URI
Trend of Daily SNMP Access on Specific Cisco Target	This report shows daily SNMP access trend among all the Cisco traffic on a particular target address.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Changes by Type	This report displays all successful configuration changes to Cisco network devices. Events are grouped by event type, and then reporting device.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Library Resources			
Device Outbound Interface Status	This data monitor shows the status of outbound interfaces of Cisco network devices based on events reported by these equipment.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Network/
Device Inbound Interface Status	This data monitor shows the status of inbound interfaces of Cisco network devices based on events reported by this equipment.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Network Event Flow Statistics by Device	This data monitor shows the total number of events from Cisco network devices per device for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Top Network Devices	This data monitor shows the top 20 event-generating Cisco network devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Device Interface Notifications	This field set focuses on common fields specific to device interface notification events from Cisco network systems.	Field Set	ArcSight Foundation/Cisco Monitoring/
Target Host or Address Present	This filter identifies events that have either the Target Host Name or Target Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Network Events	This filter passes events where the category object starts with /Network or the category device group starts with /Network Equipment and that were recorded by a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Error Events	This filter selects Cisco events related to network device errors.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/

Resource	Description	Type	URI
SNMP Authentication Failed	This filter selects all events from Cisco network systems reporting SNMP authentication or authorization failures.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
SNMP Events	This filter looks for SNMP events reported by Cisco devices.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Cisco Critical Network Events	This filter selects critical events related to Cisco network devices.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Device Inbound Interface Status Events	This filter selects events from Cisco devices related to device inbound interfaces, ports, or links. VPN events are excluded.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Device Interface Status Events	This filter selects events from Cisco devices related to device interfaces, ports, or links. VPN events are excluded.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Device Outbound Interface Status Events	This filter selects events from Cisco devices related to device outbound interfaces, ports, or links. VPN events are excluded.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Network Device Interface Down Messages	This filter selects device interface events from Cisco devices stating that an interface, port, or link is down. VPN events are excluded.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Successful Network Configuration Changes	This filter selects successful configuration change events where the category object starts with /Network or the category device group starts with /Network Equipment and that were recorded by a Cisco device.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Cisco Device SNMP Authentication Failures	This query returns Cisco events where authentication or authorization failed using SNMP.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/Device SNMP Authentication Failures/

Resource	Description	Type	URI
Cisco Device Critical Events	This query returns critical base events from Cisco network devices where the device group is /Network Equipment or /Operating System, and the object starts with /Network.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco SNMP Authentication Failures by Device	This query returns Cisco events with an authentication or authorization failure using SNMP. It returns the device information sorted by count, from highest to lowest.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/Device SNMP Authentication Failures/
Cisco Device SNMP Authentication Failures by User	This query returns Cisco events with authentication or authorization failures using SNMP. It returns user information sorted by count, from highest to lowest.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/Device SNMP Authentication Failures/
Cisco Network Configuration Changes per Day in the Last 7 Days	This query returns the number of Cisco network equipment configuration changes per day within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Device Interface Status Messages	This query returns device information from Cisco network device events regarding network interfaces that are not VPN interfaces and where a link has been reported to be up or down, and the inbound or outbound interface is defined.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Daily SNMP Access - Base	This query returns all SNMP access to Cisco devices. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Configuration Changes by User (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours where either the attacker or target user name is present.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Cisco SNMP Access On Certain Target (Trend Based)	This query returns all SNMP Access recorded Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Top Target Weekly Cisco SNMP Access on Device	This query returns the Top Target SNMP access to Cisco devices.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Network Event Count by Hour	This query returns the count of events from all Cisco network systems within the last six hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/

Resource	Description	Type	URI
Cisco SNMP Access (Trend Based)	This query returns all SNMP Access recorded Cisco devices within the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Device Errors	This query returns error events from Cisco network systems where the device group is /Network Equipment or /Operating System, and the object starts with /Network.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Change By Event	This query returns all configuration changes recorded by Cisco network equipment within the last 24 hours.	Query	ArcSight Express/Cisco Monitoring/Functionality/Network/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily SNMP Access	This trend keeps track of all SNMP access on a daily basis.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Network/

Cisco Wireless

The Cisco Wireless use case provides information about wireless traffic recorded by Cisco Aironet wireless access points present in your network.

Configuration

The Cisco Wireless use case requires the following configuration for your environment:

- Verify that the [Cisco Aironet](#) filter captures all events from Aironet access points in your network.
- If necessary, the ArcSight Administrator can modify the [Cisco Wireless Systems](#) filter to include other Cisco aironet access points not captured by the Cisco Aironet filter. Events from these devices are shown in the [Events from Cisco Wireless Systems](#) active channel.

Resources

The following table lists all the resources explicitly assigned to the Cisco Wireless use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 4-12 Resources that Support the Cisco Wireless Use Case

Resource	Description	Type	URI
Monitor Resources			
Events from Cisco Wireless Systems	This active channel shows all the events originating from Cisco wireless systems within the last two hours.	Active Channel	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Access Points	This dashboard provides an overview of Cisco access points, such as the event flow, and the top access points with most associated or disassociated wireless devices.	Dashboard	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Associated Devices in a Day (Event Based)	This query viewer shows all devices that accessed the Wireless network through an Aironet AP within the last two hours. It provides various drilldowns from the wireless devices and APs listed.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Top Access Points with Most Distinct Associated Devices	This query viewer shows the top access points with the most distinct associated wireless devices within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Top Access Points with Most Distinct Disassociated Devices	This query viewer shows the count of wireless devices that disassociated with an AP, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/

Resource	Description	Type	URI
Disassociated Devices in a Day (Event Based)	This query viewer returns all devices that leave (disassociate with) an Aironet AP within the last two hours. It provides various drilldowns related to the wireless devices and APs listed.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Associations - Disassociations (Trend Based)	This query viewer shows all associations and disassociations within the last seven days, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Associations - Disassociations per Day (Cisco APs)	This report shows the number of association and disassociation events recorded by Cisco Aironet APs per day for the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Cisco Access Points and Associated Wireless Devices	This report shows a summary of the associated wireless devices per AP.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Associated Wireless Devices to Cisco APs	This report shows a summary of the wireless devices associated with an Cisco AP.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Library Resources			
Top Access Points with Most Association Events	This data monitor shows the top Access Points with most wireless device association events in the last hour. Note: This does not necessarily mean the Access Points associated with most distinct wireless devices.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Top Access Points with Most Disassociation Events	This data monitor shows the top Access Points with the most wireless device disassociation events in the last hour. Note: This does not mean these Access Points disassociated with most (distinct) wireless devices.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Cisco Wireless Event Flow Statistics by AP	This data monitor shows the total number of events per Cisco Access Point for the last 15 minutes. The sampling interval is one minute and a correlation event is generated when there is a 50 percent change in the moving average.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Cisco Wireless Events	This field set focuses on fields specific to Cisco wireless devices such as Aironet access points.	Field Set	ArcSight Foundation/Cisco Monitoring/
Cisco Wireless AP Device Disassociation	This filter selects events when a wireless device disassociates with a Cisco Access Point.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/

Resource	Description	Type	URI
Cisco Aironet	This filter selects events collected by Cisco Aironet access points.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Cisco Wireless Systems	This filter selects events collected by Cisco wireless systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Cisco Wireless AP Device Association	This filter selects events when a wireless device associates successfully with a Cisco Access Point.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/
Associated Devices per AP	This query returns the count of distinct devices that accessed the Wireless network per Access Point.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Disassociated Devices per AP	This query returns the count of wireless devices that disassociated with an Access Point.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Associated Devices in a Day - Event Based	This query returns all devices that accessed the wireless network through an Aironet Access Point.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Association - Disassociation per Day	This query returns the number of association/disassociation events recorded by Cisco Aironet Access Points per day for the last seven days.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Disassociated Devices	This query returns all devices that leave (disassociate with) an Aironet Access Point.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Association - Disassociation Details	This query returns all association or disassociation events grouped by hour within the last day.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Daily Configuration Changes - Base	This query looks for all attempts to change a configuration recorded by a Cisco device. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Daily Associations - Disassociations (Base)	This query returns all association-disassociation events recorded by a Cisco Aironet Access Point. This serves as a base query for a trend.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/
Associated APs per Device	This query returns all associated Access Points per wireless device.	Query	ArcSight Express/Cisco Monitoring/Functionality/Wireless/

Resource	Description	Type	URI
Daily Associations - Disassociations	This trend tracks all disassociation/association events related to Cisco Aironet Access Points.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/

Chapter 5

Devices Use Cases

The Devices resources monitor and report on the devices in your environment such as firewalls, Intrusion Detection Systems (IDS), and virtual private networks (VPN), as well as cross-device functions such as logins and configuration management. The resources are grouped together using use cases, which help address a specific issue or function. The Devices use cases are listed in the following table.

Use Case	Purpose
"Devices" on page 124	The Devices use case provides resources for monitoring various devices.
"Anti-Virus" on page 132	The Anti-Virus use case provides resources for monitoring anti-virus devices, virus, worm, and other malware activity.
"BlueCoat" on page 139	The BlueCoat use case provides resources for monitoring BlueCoat devices.
"Database" on page 140	The Database use case provides resources for monitoring database activity.
"Firewall" on page 144	The Firewall use case provides resources for monitoring firewall activity.
"Identity Management" on page 156	The Identity Management use case provides resources for monitoring Identity Management activity.
"IDS - IPS" on page 165	The IDS - IPS use case provides resources for monitoring Intrusion Detection/Prevention System activity.
"Network" on page 172	The Network use case provides resources for monitoring network device activity.
"Operating System" on page 183	The Operating System use case provides resources for monitoring Operating System activity.
"VPN" on page 191	The VPN use case provides resources for monitoring VPN activity.

Devices

The Devices use case provides resources for monitoring various devices.

Configuration

ArcSight Express content is designed to find activity for which the staff of your security operations center should be notified. If a situation is a benign or routine condition in your environment, use the [Event-based Rule Exclusions](#) active list to store event situations considered to be low or no risk.

The entries in the [Event-based Rule Exclusions](#) active list are ignored by the rules that reference it. The entries list specific events from a specific source (attacker) address and zone to a specific destination (target) address and zone. Other events from the same device originating from a different source or to a different destination are not ignored. Add to this list any events that occur very frequently between two systems, causing a rule to fire too much. The [Event-based Rule Exclusions](#) active list is referenced by the following event-based rules:

- [High Number of Connections](#)
- [High Number of Denied Inbound Connections](#)
- [High Number of Denied Connections for A Source Host](#)

For information about how to add entries to active lists, see the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the Devices use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-1 Resources that Support the Devices Use Case

Resource	Description	Type	URI
Monitor Resources			
VPN Events	This active channel shows all VPN activity within the last two hours.	Active Channel	ArcSight Express/Devices/Channel
X-OS-Traffic	This active channel displays operating system events that are not related to Microsoft, Cisco, Nortel, or ArcSight products.	Active Channel	ArcSight Express/Devices/Channel
Operating System Events	This active channel shows all events originating from operating systems within the last two hours.	Active Channel	ArcSight Express/Devices/Channel
IDS - IPS Events	This active channel shows all events originating from Intrusion Detection Systems (IDS) within the last two hours.	Active Channel	ArcSight Express/Devices/Channel
Firewall Events	This active channel shows all events originating from firewalls within the last two hours.	Active Channel	ArcSight Express/Devices/Channel

Resource	Description	Type	URI
Identity Management Events	This active channel shows all events originating from Identity Management Systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Anti-Virus Events	This active channel shows all the events coming from Anti-Virus Systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Database Events	This active channel shows all events originating from databases within the last two hours.	Active Channel	ArcSight Express/Devices/
Network Events	This active channel shows all events originating from networking systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Configuration Changes Overview	This dashboard shows an overview of the successful configuration changes for databases, firewalls, VPNs, and network devices.	Dashboard	ArcSight Express/Devices/ Cross-Device/
Current Event Sources	This dashboard displays information about the status of your connectors, as well as the top devices (vendor and product) that are contributing events.	Dashboard	ArcSight Administration/Connectors /System Health/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage by top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find hosts with the highest bandwidth.	Report	ArcSight Express/Devices/ Cross-Device/Bandwidth Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/ Cross-Device/User Change Tracking/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/ Cross-Device/User Change Tracking/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/ Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Bandwidth Usage by Hour	This report shows a summary of bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/

Library - Correlation Resources

High Number of Denied Connections for A Source Host	This rule detects firewall deny events. The rule triggers when ten events originating from the same source host occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Connections	This rule detects firewall accept events for MSSQL, Terminal Services, and TFTP connections (default destination ports: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule triggers when ten events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Denied Inbound Connections	This rule detects inbound firewall deny events. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
User VPN Session Stopped	This rule detects VPN user session stop (or terminate) events, defined as a VPN access stop event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/VPN/
User VPN Session Started	This rule detects VPN user session start events, defined as a VPN access start event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/VPN/

Library Resources

Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight Express/Tuning
-----------------------------	--	-------------	-------------------------

Resource	Description	Type	URI
Protected	This is a site asset category.	Asset Category	Site Asset Categories/ Address Spaces
Last 10 Firewall Configuration Changes	This data monitor shows the last ten successful firewall configuration changes.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Configuration Changes Overview/
Last 10 Database Configuration Changes	This data monitor shows the last ten successful database configuration changes.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Configuration Changes Overview/
Top Event Sources	This data monitor shows the most common event generating products and displays a listing of the top 20.	Data Monitor	ArcSight Administration/ Connectors/System Health/Current Event Sources/
Last 10 VPN Configuration Changes	This data monitor shows the last ten successful VPN configuration changes.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Configuration Changes Overview/
Last 10 Network Configuration Changes	This data monitor shows the last ten successful configuration changes on network devices.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Configuration Changes Overview/
IDS	This field set displays useful fields for evaluating events from various firewall devices.	Field Set	ArcSight Express/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
Virus Information	This field set displays useful fields for evaluating anti-virus events.	Field Set	ArcSight Express/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	ArcSight Foundation/Cisco Monitoring/Products/ Cisco Adaptive Security Appliance (ASA) /
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Express/Devices/Network/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/ Cross-Device/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/ Common/Network Filters/ Boundary Filters/

Resource	Description	Type	URI
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Express/ Devices/Database/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Network Configuration Changes	This filter identifies successful configuration change events that match the Network Events filter.	Filter	ArcSight Express/ Devices/Network/
Firewall Configuration Changes	This filter identifies successful configuration change events that match the Firewall Events filter.	Filter	ArcSight Express/ Devices/Firewall/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/ Common/Network Filters/ Boundary Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/ Common/Network Filters/ Boundary Filters/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Express/ Devices/IDS - IPS/
Anti-Virus Events	This filter identifies events in which the category device group is /IDS/Host/Antivirus.	Filter	ArcSight Express/ Devices/Anti-Virus/
Operating System Events	This filter identifies events in which the category device group is Operating System.	Filter	ArcSight Express/ Devices/Operating System/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	Filter	ArcSight Express/ Devices/Identity Management/
VPN Configuration Changes	This filter identifies successful configuration change events that match the VPN Events filter.	Filter	ArcSight Express/ Devices/VPN/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Database Configuration Changes	This filter identifies successful configuration change events that match the Database Events filter.	Filter	ArcSight Express/Devices/Database/
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Express/Devices/Cross-Device/
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Express/Devices/Firewall/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
User VPN Sessions	This session list tracks VPN user session starts and stops (or terminations), for purposes of tracking user session durations. The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	Session List	ArcSight Foundation/ Intrusion Monitoring/ User Tracking/VPN/
Operating System	The Operating System use case provides several resources for monitoring Operating System activity, as well as a way to configure some of the resources.	Use Case	ArcSight Express/Devices/
Database	The Database use case provides several resources for monitoring database activity, as well as a way to configure some of these resources.	Use Case	ArcSight Express/Devices/
VPN	The VPN use case provides several resources for monitoring VPN activity, as well as a way to configure some of the resources.	Use Case	ArcSight Express/Devices/
BlueCoat	This use case provides resources that monitor events from Blue Coat devices.	Use Case	ArcSight Express/Devices/
Network	The Network use case provides several resources for monitoring Network device activity, as well as a way to configure some of the resources.	Use Case	ArcSight Express/Devices/
IDS - IPS	The IDS - IPS use case provides several resources for monitoring Intrusion Detection/Prevention System activity, as well as a way to configure some of these resources.	Use Case	ArcSight Express/Devices/
Firewall	The Firewall use case provides several useful resources for monitoring firewall activity, as well as a way to configure some of these resources.	Use Case	ArcSight Express/Devices/
Anti-Virus	The Anti-Virus use case provides several resources for monitoring anti-virus devices, virus, worm, and other malware activity, as well as a way to configure some of these resources.	Use Case	ArcSight Express/Devices/

Resource	Description	Type	URI
Identity Management	The Identity Management use case provides several resources for monitoring Identity Management activity, as well as a way to configure some of these resources.	Use Case	ArcSight Express/Devices/

Anti-Virus

The Anti-Virus use case provides resources for monitoring anti-virus devices, virus, worm, and other malware activity.

Resources

The following table lists all the resources explicitly assigned to the Anti-Virus use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
Monitor Resources			
Anti Virus Information	This active channel displays anti-virus events.	Active Channel	ArcSight Express/Devices
Anti-Virus Events	This active channel shows all the events coming from Anti-Virus Systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Anti-Virus Information	This dashboard displays information about infected systems and anti-virus updates.	Dashboard	ArcSight Express/Devices/Anti-Virus/
Virus Activity Statistics	This dashboard displays data monitors showing virus activity by zone and by host.	Dashboard	ArcSight Express/Devices/Anti-Virus/
Anti-Virus Overview	This dashboard shows an overview of the top infections, the top infected systems, and the most recent and top anti-virus error events.	Dashboard	ArcSight Express/
Errors Detected in Anti-Virus Deployment	This report displays the hosts reporting the most anti-virus errors for the previous day and includes the anti-virus product, host details, error information, and the number of errors.	Report	ArcSight Express/Devices/Anti-Virus/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Top Infected Systems	This report displays summaries of the systems reporting the most infections during the previous day.	Report	ArcSight Express/Devices/Anti-Virus/

Resource	Description	Type	URI
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Failed Anti-Virus Updates	This report displays a table with the anti-virus vendor and product name as well as the hostname, zone, and IP address of the host on which the update failed. The time (EndTime) at which the update failed is also displayed. This report runs against events that occurred yesterday.	Report	ArcSight Express/Devices/Anti-Virus/
Virus Activity by Time	This report displays malware activity by hour for the previous day by hour and priority.	Report	ArcSight Express/Devices/Anti-Virus/
Update Summary	This report displays a summary of the results of anti-virus update activity by zones since yesterday.	Report	ArcSight Express/Devices/Anti-Virus/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Top 10 Infected Systems	This data monitor shows the top ten systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Overview/
Infected Systems	This data monitor displays the last 20 events related to infected systems.	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Information/
Top 10 Anti-Virus Errors	This data monitor shows the top ten systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Failure, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Overview/

Resource	Description	Type	URI
Top 10 Infections	This data monitor shows the top ten infections with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Overview/
Virus Activity by Host	This data monitor shows the most active hosts with virus activity on the network.	Data Monitor	ArcSight Express/Devices/Anti-Virus/Virus Activity Statistics/
Virus Activity by Zone	This data monitor shows the most active zones with virus activity on the network.	Data Monitor	ArcSight Express/Devices/Anti-Virus/Virus Activity Statistics/
Anti-Virus Updates	This data monitor shows the last 20 anti-virus update events.	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Information/
Last 10 Anti-Virus Errors	This data monitor tracks the last anti-virus error events, displaying the time of occurrence, the priority, the vendor information, and the device information.	Data Monitor	ArcSight Express/Devices/Anti-Virus/Anti-Virus Overview/
Virus Information	This field set displays useful fields for evaluating anti-virus events.	Field Set	ArcSight Express/
All Anti Virus	This filter selects events from various anti-virus devices.	Filter	ArcSight Foundation/Intrusion Monitoring/Devices/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Update Events	This filter identifies events related to anti-virus product data file updates.	Filter	ArcSight Express/Devices/Anti-Virus/
All Events	This filter matches all events.	Filter	ArcSight System/Core

Resource	Description	Type	URI
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Anti-Virus Infection	This filter selects anti-virus events related to infected systems.	Filter	ArcSight Foundation/ Intrusion Monitoring/ Devices/
Anti-Virus Update Status	This filter selects events related to anti-virus updates.	Filter	ArcSight Foundation/ Intrusion Monitoring/ Devices/
Anti-Virus Events	This filter identifies events in which the category device group is /IDS/Host/Antivirus.	Filter	ArcSight Express/Devices/ Anti-Virus/
Virus Activity	This filter detects virus activity reported by either an IDS or a anti-virus application. The filter classifies virus events in two ways: The Category Object starts With /Vector/Virus or /Host/Infection/Virus, or the Category Behavior is /Found/Vulnerable, starts with /Modify/Content or /Modify/Attribute, and has a Category Device Group of /IDS/Host/Antivirus and the Device Custom String1 is set to some value.	Filter	ArcSight Express/Devices/ Anti-Virus/
AV - Found Infected	This filter identifies all events where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable.	Filter	ArcSight Express/Devices/ Anti-Virus/
Anti-Virus Errors	This filter identifies events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational.	Filter	ArcSight Express/Devices/ Anti-Virus/
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/ Common/Conditional Variable Filters/Host/

Resource	Description	Type	URI
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
AV - Failed Updates	This filter identifies all anti-virus update events (based on the Update Events filter), where the Category Outcome is Failure.	Filter	ArcSight Express/Devices/Anti-Virus/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Infected Systems	This query identifies data matching the AV - Found Infected filter where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable.	Query	ArcSight Express/Devices/Anti-Virus/Top Infected Systems/
Failed Anti-Virus Updates	This query identifies the device vendor, device product, target zone name, target host name, target address, and time (EndTime) from events that match the AV - Failed Updates filter.	Query	ArcSight Express/Devices/Anti-Virus/
Failed Anti-Virus Updates Chart	This query identifies the target zone name and the sum of the aggregated event count from events that match the AV - Failed Updates filter.	Query	ArcSight Express/Devices/Anti-Virus/
Virus Activity by Hour	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Express/Devices/Anti-Virus/Virus Activity by Time/

Resource	Description	Type	URI
Top Zones with Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational. The query returns the zone and the number of times the error occurred.	Query	ArcSight Express/Devices/Anti-Virus/Errors/
Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational. The query returns the priority, vendor information, host information, error name, and the number of times the error occurred.	Query	ArcSight Express/Devices/Anti-Virus/Errors/
Update Summary Chart	This query identifies the target zone name, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Express/Devices/Anti-Virus/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Top Infected Systems	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Express/Devices/Anti-Virus/Top Infected Systems/
Top Anti-Virus Errors	This query identifies data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not Success, and the Category Significance starts with Informational. The query returns the error name and the number of times the error occurred.	Query	ArcSight Express/Devices/Anti-Virus/Errors/

Resource	Description	Type	URI
Update Summary	This query identifies the target zone name, target host name, target address, device vendor, device product, category outcome, and the sum of the aggregated event count from events that match the Update Events filter.	Query	ArcSight Express/Devices/Anti-Virus/

BlueCoat

The BlueCoat use case provides resources for monitoring BlueCoat devices.

Resources

The following table lists all the resources explicitly assigned to the BlueCoat use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-3 Resources that Support the BlueCoat Use Case

Resource	Description	Type	URI
Monitor Resources			
BlueCoat	This active channel displays events from Blue Coat products.	Active Channel	ArcSight Express/Devices/
Blue Coat	This dashboard displays information related to web browser activity as reported by Blue Coat web security devices.	Dashboard	ArcSight Express/
Library Resources			
Top Browsers	This data monitor displays the top users per source IP address based on events from Blue Coat devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Top Actions	This data monitor displays the top actions taken by Blue Coat devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Top Web Sites	This data monitor displays the top requested URL hosts reported by Blue Coat devices.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Top Categories	This data monitor displays the top categories of web browser activity based on Blue Coat categories.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Blue Coat	This field set contains fields for evaluating events from Blue Coat devices.	Field Set	ArcSight Express/
Blue Coat	This filter identifies events from Blue Coat devices.	Filter	ArcSight Express/Devices/

Database

The Database use case provides resources for monitoring database activity.

Resources

The following table lists all the resources explicitly assigned to the Database use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-4 Resources that Support the Database Use Case

Resource	Description	Type	URI
Monitor Resources			
Database Events	This active channel shows all events originating from databases within the last two hours.	Active Channel	ArcSight Express/Devices/
Database Errors	This dashboard shows the most recent and the top errors affecting database applications on the network.	Dashboard	ArcSight Express/Devices/Database/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Database Errors and Warnings	This report shows recent database errors and warnings. A chart shows the top ten errors and warnings. A table lists all the errors and warnings chronologically.	Report	ArcSight Express/Devices/Database/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Password Changes	This report shows password changes for the previous day and groups the password changes by user, sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces

Resource	Description	Type	URI
Last 10 Database Errors	This data monitor displays the most recent database error events.	Data Monitor	ArcSight Express/Devices/Database/Database Errors/
Top 10 Database Errors	This data monitor shows the top ten systems with events matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure, and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Devices/Database/Database Errors/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Express/Devices/Database/
Successful Password Changes	This filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success.	Filter	ArcSight Express/Devices/Cross-Device/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Database Errors	This filter identifies events where the category device group is Application, the category object is /Host/Application/Database, and the category significance is /Informational/Warning or /Informational/Error.	Filter	ArcSight Express/Devices/Database/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Database Configuration Changes	This filter identifies successful configuration change events that match the Database Events filter.	Filter	ArcSight Express/Devices/Database/

Resource	Description	Type	URI
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Express/Devices/Database/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Database Errors and Warnings (Chart)	This query returns the count of database errors and warnings by event name.	Query	ArcSight Express/Devices/Database/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Password Changes	This query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success.	Query	ArcSight Express/Devices/Cross-Device/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Database Errors and Warnings	This query retrieves all the database error and warning events. The query returns the time, event name, result, user name, and category significance.	Query	ArcSight Express/Devices/Database/

Firewall

The Firewall use case provides resources for monitoring firewall activity.

Configuration

ArcSight Express content is designed to find activity for which the staff of your security operations center should be notified. If a situation is a benign or routine condition in your environment, you can use the [Event-based Rule Exclusions](#) active list to store event situations considered to be low or no risk.

The entries in the [Event-based Rule Exclusions](#) active list are ignored by the rules that reference it. The entries list specific events from a specific source (attacker) address and zone to a specific destination (target) address and zone. Other events from the same device originating from a different source or to a different destination are not ignored. Add to this list any events that occur very frequently between two systems, causing a rule to fire too much. The [Event-based Rule Exclusions](#) active list is referenced by the following event-based rules:

- [SYN Flood Detected by IDS or Firewall](#)
- [High Number of Connections](#)
- [High Number of Denied Inbound Connections](#)
- [High Number of Denied Connections for A Source Host](#)

For information about how to add entries to active lists, see the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the Firewall use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
Monitor Resources			
Firewall Events	This active channel shows all events originating from firewalls within the last two hours.	Active Channel	ArcSight Express/Devices/
Firewall Connection Overview	This dashboard shows an overview of all the denied connection events originating from firewalls.	Dashboard	ArcSight Express/
Firewall Login Overview	This dashboard shows an overview of firewall logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Denied Outbound Connections by Port	This report shows a summary of the denied outbound traffic by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Express/Devices/Firewall/
Denied Outbound Connections per Hour	This report shows a summary of the denied outbound traffic per hour. A chart shows the total number of denied connections per hour for the previous day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Denied Inbound Connections per Hour	This report shows a summary of the denied inbound traffic per hour. A chart shows the total number of denied connections per hour for the previous day (by default). A table shows the connection count per hour grouped by source zone.	Report	ArcSight Express/Devices/Firewall/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Denied Outbound Connections by Address	This report shows a summary of the denied outbound traffic by local address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Denied Inbound Connections by Address	This report shows a summary of the denied inbound traffic by foreign address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Express/Devices/Firewall/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage by top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find hosts with the highest bandwidth.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Bandwidth Usage by Hour	This report shows a summary of bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/
Denied Inbound Connections by Port	This report shows a summary of the denied inbound traffic by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Express/Devices/Firewall/
Top Hosts by Number of Connections	This report shows a summary of the number of connections by the top hosts in a chart. By default, the chart shows the number of connections by host for the previous day.	Report	ArcSight Express/Devices/Cross-Device/Top Activity/
Library - Correlation Resources			
High Number of Denied Connections for A Source Host	This rule detects firewall deny events. The rule triggers when ten events originating from the same source host occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Connections	This rule detects firewall accept events for MSSQL, Terminal Services, and TFTP connections (default destination ports: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule triggers when ten events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Denied Inbound Connections	This rule detects inbound firewall deny events. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
SYN Flood Detected by IDS or Firewall	This rule detects SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/DoS/

Resource	Description	Type	URI
Library Resources			
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight Express/Tuning
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top 10 Hosts With Denied Outbound Connections	This data monitor shows the top ten hosts with denied outbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/
Top 10 Hosts With Denied Inbound Connections	This data monitor shows the top ten hosts with denied inbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/
Top 10 Accepted Ports (Outbound)	This data monitor shows the top ten ports with accepted outbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/
Top 10 Accepted Ports (Inbound)	This data monitor shows the top ten ports with accepted inbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/
Top 10 Denied Ports (Outbound)	This data monitor shows the top ten ports with denied outbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top 10 Denied Ports (Inbound)	This data monitor shows the top ten ports with denied inbound connections.	Data Monitor	ArcSight Express/ArcSight Express/Firewall Connection Overview/

Resource	Description	Type	URI
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight Express/
Login Events	This filter identifies events where the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/Cross-Device/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Denied Outbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies outbound events.	Filter	ArcSight Express/Devices/Firewall/
Successful Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Failed Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/Cross-Device/
Denied Inbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Failure. The filter identifies inbound events.	Filter	ArcSight Express/Devices/Firewall/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Accepted Outbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Success. The filter looks for outbound events.	Filter	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Express/Devices/Firewall/
Failed Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/Firewall/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Firewall Configuration Changes	This filter identifies successful configuration change events that match the Firewall Events filter.	Filter	ArcSight Express/Devices/Firewall/
Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/Firewall/
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Express/Devices/IDS - IPS/
Accepted Inbound Connections	This filter identifies firewall events in which the category behavior is /Access and the category outcome is /Success. The filter identifies inbound events.	Filter	ArcSight Express/Devices/Firewall/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/

Resource	Description	Type	URI
Successful Firewall Login Events	This filter identifies firewall events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/Firewall/
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Express/Devices/Cross-Device/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall connections by the top hosts. By default, a chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the previous day (by default). Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Express/Devices/Firewall/
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage reported by firewalls by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/

Resource	Description	Type	URI
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Denied Outbound Connections by Address	This query identifies the count of denied outbound connections by local address (source zone, address, and hostname).	Query	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Denied Outbound Connections by Port	This query identifies the count of denied outbound connections by destination port.	Query	ArcSight Express/Devices/Firewall/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Top Hosts by Number of Connections	This query returns host information and the number of events in which the category behavior is /Access/Start and the category outcome is not Failure.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Denied Outbound Connections per Hour	This query identifies the count of denied outbound connections per hour for each source zone.	Query	ArcSight Express/Devices/Firewall/
Denied Inbound Connections per Hour	This query identifies the count of denied inbound connections per hour for each source zone.	Query	ArcSight Express/Devices/Firewall/
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Denied Inbound Connections by Address	This query identifies the count of denied inbound connections by foreign address (source zone, address, and hostname).	Query	ArcSight Express/Devices/Firewall/
Denied Inbound Connections by Port	This query identifies the count of denied inbound connections by destination port.	Query	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Denied Outbound Connections per Hour (Chart)	This query identifies the count of denied outbound connections per hour.	Query	ArcSight Express/Devices/Firewall/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Denied Inbound Connections per Hour (Chart)	This query identifies the count of denied inbound connections per hour.	Query	ArcSight Express/Devices/Firewall/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/

Identity Management

The Identity Management use case provides resources for monitoring Identity Management activity.

Resources

The following table lists all the resources explicitly assigned to the Identity Management use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
Monitor Resources			
Identity Management Events	This active channel shows all events originating from Identity Management Systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Identity Management Overview	This dashboard displays information reported by Identity Management devices, such as the top users by number of connections and authentication failures by source and destination.	Dashboard	ArcSight Express/Devices/Identity Management/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Connection Counts by User	This report shows count information about connections for each user reported by Identity Management devices. A summary of the top users by connection count is provided.	Report	ArcSight Express/Devices/Identity Management/

Resource	Description	Type	URI
Failed Login Attempts	This report shows the count of authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Connection Durations by User	This report shows duration information about VPN connections for each user. A summary of the top VPN connection duration by user is provided. Details of the connection durations for each user are also provided, including minimum, average, maximum, and total connection minutes. Also included are details of connections that are currently open at the time the report is run. By default, this report shows user VPN duration information for the previous day.	Report	ArcSight Express/Devices/Identity Management/
Password Changes	This report shows password changes for the previous day and groups the password changes by user, sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Library - Correlation Resources			
User Session (Administrative User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Cisco Secure ACS.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/
User Session (Accounting User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/
User Session (Normal User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/
User Session (Accounting User) Stopped	This rule detects user session stop events reported by identity management devices, defined as an identity management access stop event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Juniper Steel-Belted Radius.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/

Resource	Description	Type	URI
User Session (Administrative User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports Cisco Secure ACS.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/
User Session (Normal User) Started	This rule detects user session start events reported by identity management devices, defined as an identity management access start event with user ID and session information. The rule then updates the Identity Management's User Sessions session list. This rule supports ActivCard AAA Server Accounting and Cisco VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/Identity Management/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Authentication Failures by Destination	This data monitor displays the destination information of failed authentication attempts within five-minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	ArcSight Express/Devices/Identity Management/Identity Management Overview/
Authentication Failures by Source	This data monitor displays the source information of failed authentication attempts within five-minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	ArcSight Express/Devices/Identity Management/Identity Management Overview/
Top Users by Connection Count	This data monitor shows the top users by the number of connections in five-minute intervals for the last hour, as reported by Identity Management devices.	Data Monitor	ArcSight Express/Devices/Identity Management/Identity Management Overview/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight Express/

Resource	Description	Type	URI
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User/
Identity Management Connection Start Events	This filter identifies events where an Identity Management system has seen an access start event with valid user information.	Filter	ArcSight Express/Devices/Identity Management/
Failed Identity Management Login Attempts	This filter identifies events where an authentication attempt failed.	Filter	ArcSight Express/Devices/Identity Management/
Identity Management Events	This filter identifies events in which the Category Device Group starts with Identity Management.	Filter	ArcSight Express/Devices/Identity Management/
Successful Password Changes	This filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success.	Filter	ArcSight Express/Devices/Cross-Device/
All Events	This filter matches all events.	Filter	ArcSight System/Core
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Failed Login Attempts	This report shows the count of authentication failures from login attempts reported by identity management systems by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Express/Devices/Identity Management/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
Users with Open Connections	This query returns the user ID and the Identity Management device for each user in the User Sessions list where the user entry has not been terminated (logged out or timed out) or expired (by default).	Query	ArcSight Express/Devices/Identity Management/Connection Durations by User/
Closed Connection Durations	This query returns the user ID and the minimum, average, maximum, and total durations (in minutes) for all user IDs with closed or terminated sessions in the User Sessions list.	Query	ArcSight Express/Devices/Identity Management/Connection Durations by User/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Users by Connection Count	This query returns events in which the category behavior is /Access/Start, /Authentication/Verify or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	ArcSight Express/Devices/Identity Management/Connection Counts by User/
Failed Login Attempts (Chart)	This query returns the count of authentication failures from login attempts by hour.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Top Connection Durations	This query returns the user ID and average duration from the User Identity Management Sessions list and sorts them by the top duration.	Query	ArcSight Express/Devices/Identity Management/Connection Durations by User/
Failed Login Attempts	This query returns all authentication failures from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Password Changes	This query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Top Users by Connection Count	This query identifies VPN events in which the Category Behavior is /Access/Start, /Authentication/Verify, or /Authorization/Verify, with user information available, returning the number of VPN connections per user.	Query	ArcSight Express/Devices/VPN/Connection Counts by User/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/ Cross-Device/
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/ Cross-Device/
User Sessions	This session list tracks Identity Management user session starts and stops (or terminations). The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, increase the Entry Expiration Time. The sessions are maintained by the User Session (Identity Management) Started and User Session (Identity Management) Stopped rules.	Session List	ArcSight Foundation/ Intrusion Monitoring/User Tracking/Identity Management/

IDS - IPS

The IDS - IPS use case provides resources for monitoring Intrusion Detection/Prevention System activity.

Configuration

ArcSight Express content is designed to find activity for which the staff of your security operations center should be notified. If a situation is a benign or routine condition in your environment, you can use the [Event-based Rule Exclusions](#) active list to store event situations considered to be low or no risk.

The entries in the [Event-based Rule Exclusions](#) active list are ignored by the rules that reference it. The entries list specific events from a specific source (attacker) address and zone to a specific destination (target) address and zone. Other events from the same device originating from a different source or to a different destination are not ignored. Add to this list any events that occur very frequently between two systems, causing a rule to fire too much. The [Event-based Rule Exclusions](#) active list is referenced by the following event-based rules:

- [High Number of IDS Alerts for DoS](#)
- [SYN Flood Detected by IDS or Firewall](#)
- [High Number of IDS Alerts for Backdoor](#)

For information about how to add entries to active lists, see the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the IDS - IPS use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-7 Resources that Support the IDS - IPS Use Case

Resource	Description	Type	URI
Monitor Resources			
IDS - IPS Events	This active channel shows all events originating from Intrusion Detection Systems (IDS) within the last two hours.	Active Channel	ArcSight Express/Devices/
IDS - IPS Overview	This dashboard shows an overview of IDS signatures. The dashboard shows the Top 10 Signature Destinations, Top 10 Signature Sources, Top 10 Signature Types, and Top 10 Signatures data monitors.	Dashboard	ArcSight Express/
Worm Outbreak Overview	This dashboard provides a view of worm activity across the network.	Dashboard	ArcSight Express/Security and Threat/

Resource	Description	Type	URI
Top Alerts from IDS and IPS	This report shows the top alerts coming from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	Report	ArcSight Express/Devices/Cross-Device/Top Activity/
Top Alert Sources	This report shows the top IDS and IPS alert sources per day. A chart shows the top ten IDS and IPS alert source IP addresses. A table shows the top alert source IP addresses and zones, as well as the device vendor and product of the reporting device.	Report	ArcSight Express/Devices/IDS - IPS/
Alert Counts per Hour	This report shows the total count of IDS and IPS alerts per hour during the past 24 hours (by default).	Report	ArcSight Express/Devices/IDS - IPS/
Worm Infected Systems	This report presents a table of systems that have been infected by a worm. The table is sorted by the Attacker Zone Name, then by the Attacker Host Name and finally by the Attacker Address (for cases where the system does not have a host name). You can change the start and end times of the event query, and the row limit (to show more or fewer systems). You can also use the Filter By parameter to create an additional filter to limit the report to specific systems. Changing the Filter By parameter causes the query to select events that match both the selected filter and the Worm Traffic filter (Worm Traffic AND <selected filter>).	Report	ArcSight Express/Devices/IDS - IPS/
Alert Counts by Device	This report shows the count of IDS and IPS alerts by device. A chart shows the top ten device addresses with the highest counts. A table shows the list of all the devices, grouped by device vendor and product, then sorted by count.	Report	ArcSight Express/Devices/IDS - IPS/
Alert Counts by Port	This report shows the count of IDS and IPS alerts by destination port. A chart shows the top ten ports with the highest counts. A table shows the list of all the counts sorted in descending order.	Report	ArcSight Express/Devices/IDS - IPS/
Top Attackers	This report displays a chart of the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile.	Report	ArcSight Express/Devices/Cross-Device/Top Activity/

Resource	Description	Type	URI
Alert Counts by Severity	This report shows the total count of IDS and IPS alerts by agent severity. A chart shows the count of alerts by severity. A table shows the count of alerts by severity, device vendor, and device product.	Report	ArcSight Express/Devices/IDS - IPS/
Alert Counts by Type	This report shows the count of IDS and IPS alerts by type (category technique). A chart shows the top ten alert counts. A table shows the list of all the counts sorted in descending order.	Report	ArcSight Express/Devices/IDS - IPS/
Top Alert Destinations	This report shows the top IDS and IPS alert destinations per day.	Report	ArcSight Express/Devices/IDS - IPS/
Top Targets	This report displays the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter.	Report	ArcSight Express/Devices/Cross-Device/Top Activity/
Library - Correlation Resources			
Worm Outbreak Detected	This rule is looking for both the Possible Network Sweep rule to trigger and the Target Port Activity by Attacker data monitor to trigger a correlation event that indicates an increase in target port activity by one attacker of more than 100%. Joining the attackers and target ports from these two correlation events determines that the attacker has shown an increase in target port traffic to multiple hosts, not just a two-way communication with a single host. This behavior is indicative of a worm infected system.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/
High Number of IDS Alerts for DoS	This rule detects Denial of Service (DoS) alerts from Intrusion Detection Systems (IDS). The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/DoS/
SYN Flood Detected by IDS or Firewall	This rule detects SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/DoS/

Resource	Description	Type	URI
High Number of IDS Alerts for Backdoor	This rule detects backdoor alerts from Intrusion Detection Systems (IDS). The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/Malware Activity/
Library Resources			
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight Express/Tuning
Worm Infected Systems	This active list is automatically populated by rules that have detected worm activity on a given system.	Active List	ArcSight Express/Security and Threat/Worm Outbreak/
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Domain Name Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Proxy	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Worm Infected Systems	This data monitor displays the status of systems that have been infected in the course of a worm outbreak.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Top 10 Alert Types	This data monitor shows the top ten IDS alert types.	Data Monitor	ArcSight Express/Devices/IDS - IPS/IDS Overview/
Top 10 Alert Destinations	This data monitor shows the top ten destination hosts with IDS alert counts.	Data Monitor	ArcSight Express/Devices/IDS - IPS/IDS Overview/
Top 10 Alert Sources	This data monitor shows the top ten source hosts with IDS alert counts.	Data Monitor	ArcSight Express/Devices/IDS - IPS/IDS Overview/
Target Port Activity by Attacker	This data monitor is used in conjunction with the Worm Outbreak detected rule and the possible network sweep rule to detect worm outbreaks before an IDS signature is released.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Worm Activity Status	This data monitor shows the most recent events related to worm activity in the network zones.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/

Resource	Description	Type	URI
Top 10 Alerts	This data monitor shows the top ten IDS alerts.	Data Monitor	ArcSight Express/Devices/IDS - IPS/IDS Overview/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
IDS	This field set displays useful fields for evaluating events from various firewall devices.	Field Set	ArcSight Express/
Worm Outbreak	This filter retrieves events with the name Worm Outbreak Detected and type Correlation.	Filter	ArcSight Express/Security and Threat/
Target Port Activity By Attacker	This filter selects events where the source address is available, the target (destination) port is available but is not the ArcSight port (8443), and the source is not a DNS, email, or proxy server.	Filter	ArcSight Express/Security and Threat/
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Express/Devices/IDS - IPS/
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Express/Security and Threat/
Worm Traffic	This filter selects events related to successful worm activity on a network.	Filter	ArcSight Express/Security and Threat/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Express/Devices/Firewall/
Worm Activity	This filter selects events related to all worm activity on a network.	Filter	ArcSight Express/Security and Threat/
Top 10 Targets	This report shows the top ten targets in a chart.	Focused Report	ArcSight Express/Devices/IDS - IPS/
Top 10 Alerts	This report shows the top alerts that originate from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).	Focused Report	ArcSight Express/Devices/IDS - IPS/
Top 10 Attackers	This report shows the top ten attackers.	Focused Report	ArcSight Express/Devices/IDS - IPS/
Top Alert Sources	This query identifies the count of IDS and IPS alerts by source address, zone, device vendor, and device product.	Query	ArcSight Express/Devices/IDS - IPS/

Resource	Description	Type	URI
Alert Counts by Severity (Chart)	This query returns the count of IDS and IPS alerts by severity (agent severity).	Query	ArcSight Express/Devices/IDS - IPS/
Alert Counts by Port	This query returns the count of IDS and IPS alerts by destination port.	Query	ArcSight Express/Devices/IDS - IPS/
Alert Counts by Type	This query selects the count of IDS and IPS alerts by type (category technique).	Query	ArcSight Express/Devices/IDS - IPS/
Top IDS and IPS Alerts	This query returns IDS and IPS alert events, selecting the device event class ID, event name, device vendor, device product, and a count on the end time of the event.	Query	ArcSight Express/Devices/Cross-Device/
Alert Counts by Severity	This query returns the count of IDS and IPS alerts by severity (agent severity), device vendor, and device product.	Query	ArcSight Express/Devices/IDS - IPS/
Top 10 Attackers	This query identifies the attacker zone name, attacker address, and the count of events where the category significance starts with Compromise or Hostile. The query uses the sum of the aggregated event count instead of counting the EventID so that attackers are not split by the attack type.	Query	ArcSight Foundation/ Intrusion Monitoring/ Detail/Attack Monitoring/ Attackers/Top and Bottom 10/
Top Alert Destinations	This query returns the count of IDS and IPS alerts by destination address, zone, device vendor, and device product.	Query	ArcSight Express/Devices/IDS - IPS/
Top 10 Targets	This query returns the target zone name, target address, and the sum of the aggregated event count for events matching the Attack Events filter used in the following reports: Top N Targets, Top N Targets (3D Pie Chart), Top N Targets (Bar Chart), Top N Targets (Inverted Bar Chart), Top N Targets (Pie Chart), Top N Targets (Table and Chart), and Top N Targets (Table).	Query	ArcSight Foundation/ Intrusion Monitoring/ Detail/Attack Monitoring/ Targets/Top and Bottom 10/
Alert Counts by Device	This query returns the count of IDS and IPS alerts by device vendor, product, zone, address, and hostname.	Query	ArcSight Express/Devices/IDS - IPS/
Worm Infected Systems	This query returns the attacker zone name, attacker host name, and attacker address from events matching the Worm Traffic filter.	Query	ArcSight Express/Devices/IDS - IPS/

Resource	Description	Type	URI
Alert Counts per Hour	This query returns the count of IDS and IPS alerts per hour.	Query	ArcSight Express/Devices/IDS - IPS/

Network

The Network use case provides resources for monitoring network device activity.

Resources

The following table lists all the resources explicitly assigned to the Network use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Monitor Resources			
Network Events	This active channel shows all events originating from networking systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Network Login Overview	This dashboard shows an overview of logins on network devices. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and the Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Express/Devices/Network/
Network Status Overview	This dashboard displays data monitors related to network device errors, network interfaces, and critical network events.	Dashboard	ArcSight Express/Devices/Network/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Device SNMP Authentication Failures	This report shows summaries of SNMP authentication failures by device or by user. A table details the failed user SNMP authentication attempts for the devices. Two charts give an overview of the users or devices with the most SNMP authentication failures. Use this report to help determine if SNMP accounts are targets of brute force attacks and which devices are exhibiting the most SNMP authentication failure activity.	Report	ArcSight Express/Devices/Network/

Resource	Description	Type	URI
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Device Interface Down Notifications	This report displays the network devices that report a down link.	Report	ArcSight Express/Devices/Network/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Device Interface Status Messages	This report shows the network devices reporting link status changes.	Report	ArcSight Express/Devices/Network/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage by top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find hosts with the highest bandwidth.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Device Events	This report shows information about events on network devices.	Report	ArcSight Express/Devices/Network/
Device Errors	This report shows information about system errors on network devices. These events might be an indication of hardware failures, resource exhaustion, configuration issues, or attacks.	Report	ArcSight Express/Devices/Network/
Bandwidth Usage by Hour	This report shows a summary of bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/
Top Hosts by Number of Connections	This report shows a summary of the number of connections by the top hosts in a chart. By default, the chart shows the number of connections by host for the previous day.	Report	ArcSight Express/Devices/Cross-Device/Top Activity/
Device Critical Events	This report shows information about critical events on network devices. These critical events might be an indication of hardware failures, resource exhaustion, configuration issues, or attacks.	Report	ArcSight Express/Devices/Network/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces

Resource	Description	Type	URI
Last 10 Interface Status Messages	This data monitor displays the last ten events reported by network devices related to network interfaces, ports, or links.	Data Monitor	ArcSight Express/Devices/Network/Network Status Overview/
Last 10 Critical Network Events	This data monitor displays the last ten events reported by network devices with an agent severity of High or Very High.	Data Monitor	ArcSight Express/Devices/Network/Network Status Overview/
Devices with High Error Rates	This data monitor tracks network device error rates over the last hour. The devices listed when this data monitor is displayed in a dashboard or in the resulting correlation events, have reported at least three errors within a five minute period.	Data Monitor	ArcSight Express/Devices/Network/Network Status Overview/
Top Users by Login Activity	This data monitor shows the users with the most network login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Last 10 Interface Down Messages	This data monitor displays the last ten events reported by network devices related to down network interfaces, ports, or links.	Data Monitor	ArcSight Express/Devices/Network/Network Status Overview/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/

Resource	Description	Type	URI
Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify and the category device group starts with Network.	Filter	ArcSight Express/Devices/Network/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Express/Devices/Network/
Login Events	This filter identifies events where the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/Cross-Device/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Successful Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Failed Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/Cross-Device/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Failed Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify, the category outcome is Failure, and the category object starts with Network.	Filter	ArcSight Express/Devices/Network/

Resource	Description	Type	URI
Critical Network Events	This filter identifies critical events related to network devices.	Filter	ArcSight Express/Devices/Network/
Successful Network Login Events	This filter identifies events in which the category behavior is /Authentication/Verify, the category outcome is Success, and the category object starts with Network.	Filter	ArcSight Express/Devices/Network/
Network Device Interface Status Events	This filter identifies events related to device interfaces, ports, or links. VPN events are excluded.	Filter	ArcSight Express/Devices/Network/
Network Error Events	This filter identifies events related to network device errors.	Filter	ArcSight Express/Devices/Network/
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Express/Devices/Cross-Device/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Network Device Interface Down Messages	This filter identifies device interface events stating that an interface, port, or link is down. VPN events are excluded.	Filter	ArcSight Express/Devices/Network/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/

Resource	Description	Type	URI
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall connections by the top hosts. By default, a chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/Devices/Firewall/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage reported by firewalls by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Express/Devices/Firewall/
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/

Resource	Description	Type	URI
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the previous day (by default). Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Top Device System Authentication Events	This query retrieves base authentication events in which the device group is Network Equipment, or the device group is Operating System and the object starts with Network.	Query	ArcSight Express/Devices/Network/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Device Interface Down Notifications	This query returns device information from network device events for network interfaces that are not VPN interfaces, where a link has been reported to be down and the inbound or outbound interface is defined.	Query	ArcSight Express/Devices/Network/

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Device Critical Events	This query returns critical base events where the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Express/Devices/Network/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Device Interface Status Messages	This query returns device information from network device events where the network interfaces are not VPN interfaces, where a link has been reported to be up or down and the inbound or outbound interface is defined.	Query	ArcSight Express/Devices/Network/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
Device Errors	This query returns base error events in which the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Express/Devices/Network/
Top Hosts by Number of Connections	This query returns host information and the number of events in which the category behavior is /Access/Start and the category outcome is not Failure.	Query	ArcSight Express/Devices/Cross-Device/
Device Events	This query returns base events in which the device group is Network Equipment or Operating System, and the object starts with Network.	Query	ArcSight Express/Devices/Network/
SNMP Authentication Failures by Device	This query returns events with authentication or authorization failures using SNMP. The query returns the device information sorted by count, from highest to lowest.	Query	ArcSight Express/Devices/Network/Device SNMP Authentication Failures/
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Device SNMP Authentication Failures by User	This query returns events with authentication or authorization failures using SNMP. The query returns user information sorted by count, from highest to lowest.	Query	ArcSight Express/Devices/Network/Device SNMP Authentication Failures/

Resource	Description	Type	URI
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Device SNMP Authentication Failures	This query returns events with authentication or authorization failures using SNMP.	Query	ArcSight Express/Devices/Network/Device SNMP Authentication Failures/

Operating System

The Operating System use case provides resources for monitoring Operating System activity.

Resources

The following table lists all the resources explicitly assigned to the Operating System use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
Monitor Resources			
Operating System Events	This active channel shows all events originating from operating systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Operating System Login Overview	This dashboard shows an overview of operating system logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Express/Devices/Operating System/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Failed Login Attempts	This report shows the count of authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Password Changes	This report shows password changes for the previous day and groups the password changes by user, sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
User Administration	This report shows a summary of user and user group creation, modification, and deletion.	Report	ArcSight Express/Devices/Operating System/
Login Errors by User	This report shows a summary of the operating system login errors by username. A chart shows the top ten users with failed logins. A table shows details of the failed logins for each username (time, event name, source, destination).	Report	ArcSight Express/Devices/Operating System/

Resource	Description	Type	URI
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/ Address Spaces
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last ten failed firewall logins.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Firewall Login Overview/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed firewall logins.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Firewall Login Overview/
Last 10 Successful Login Events	This data monitor shows the last ten successful firewall logins.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Firewall Login Overview/
Top Users by Login Activity	This data monitor shows the users with the most network login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Network Login Overview/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/ Cross-Device/
Login Events	This filter identifies events where the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/ Cross-Device/
Successful Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/ Cross-Device/
Failed Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/ Cross-Device/
Operating System Events	This filter identifies events in which the category device group is Operating System.	Filter	ArcSight Express/Devices/ Operating System/

Resource	Description	Type	URI
Successful Password Changes	This filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success.	Filter	ArcSight Express/Devices/Cross-Device/
Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/Operating System/
Failed Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/Operating System/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Successful Operating System Login Events	This filter identifies operating system events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/Operating System/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/

Resource	Description	Type	URI
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Login Attempts	This report shows the count of authentication failures from login attempts reported by identity management systems by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Express/Devices/Identity Management/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
User Administration (Chart)	This query returns the count of user (and user group) creations, modifications, and deletions.	Query	ArcSight Express/Devices/Operating System/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login Attempts (Chart)	This query returns the count of authentication failures from login attempts by hour.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login Attempts	This query returns all authentication failures from login attempts.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Password Changes	This query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
User Administration	This query returns the user (and user group), creation, modification, and deletion events.	Query	ArcSight Express/Devices/Operating System/
Login Errors by User	This query returns operating system login errors. The query returns the user name, event name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Operating System/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Login Errors by User (Chart)	This query returns the count of operating system login errors by username.	Query	ArcSight Express/Devices/Operating System/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/

VPN

The VPN use case provides resources for monitoring VPN activity.

Resources

The following table lists all the resources explicitly assigned to the VPN use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 5-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Monitor Resources			
VPN Events	This active channel shows all VPN activity within the last two hours.	Active Channel	ArcSight Express/Devices/
VPN Login Overview	This dashboard shows an overview of VPN logins. The dashboard displays the Last 10 Failed Login Events, Last 10 Successful Login Events, Login Results, and Top 10 Users With Failed Logins data monitors.	Dashboard	ArcSight Express/Devices/VPN/
VPN Connection Statistics	This dashboard displays data monitors related to VPN servers, including connection status counts and authentication errors.	Dashboard	ArcSight Express/Devices/VPN/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Users by Average Session Length	This report shows duration information about VPN connections for each user. A summary of the top VPN connection duration by user is provided. Details of the connection durations for each user are also provided, including minimum, average, maximum, and total connection minutes. Also included are details of connections that are open at the time the report is run.	Report	ArcSight Express/Devices/VPN/

Resource	Description	Type	URI
Connection Counts by User	This report shows count information about connections for each user reported by Identity Management devices. A summary of the top users by connection count is provided.	Report	ArcSight Express/Devices/Identity Management/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Connections Denied by Address	This report shows denied VPN connection data. A chart summarizes the top VPN device addresses with denied connections. A table shows details of the denied connections.	Report	ArcSight Express/Devices/VPN/
Connections Denied by Hour	This report shows denied VPN connection data. A chart summarizes the number of denied connections for each hour. A table shows details of the denied connections by hour.	Report	ArcSight Express/Devices/VPN/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Password Changes	This report shows password changes for the previous day and groups the password changes by user, sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage by top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find hosts with the highest bandwidth.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Authentication Errors	This report shows errors generated by a VPN connection attempt. The address is the IP address of the VPN connection source. Use this report to see which users are having difficulties using or setting up their VPN clients.	Report	ArcSight Express/Devices/VPN/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Connections Accepted by Address	This report shows successful VPN connection data. A chart summarizes the top VPN device addresses with successful connections. A table shows details of the successful connections.	Report	ArcSight Express/Devices/VPN/
Bandwidth Usage by Hour	This report shows a summary of bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Express/Devices/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Top Hosts by Number of Connections	This report shows a summary of the number of connections by the top hosts in a chart. By default, the chart shows the number of connections by host for the previous day.	Report	ArcSight Express/Devices/Cross-Device/Top Activity/
Library - Correlation Resources			
User VPN Session Stopped	This rule detects VPN user session stop (or terminate) events, defined as a VPN access stop event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/VPN/
User VPN Session Started	This rule detects VPN user session start events, defined as a VPN access start event with user ID information. The rule then updates the User VPN Sessions session list. This rule supports Cisco VPN products, the Nokia Security Platform, and Nortel VPN products.	Rule	ArcSight Express/Security and Threat/Session Monitoring/VPN/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Last 10 Failed Login Events	This data monitor shows the last ten failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top Users by Login Activity	This data monitor shows the users with the most network login activity within the last 60 minutes.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Network Login Overview/
Top VPN Users with Authentication Errors	This data monitor tracks the number of VPN authentication error events for each VPN user (including the VPN server), every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Last 10 Successful Login Events	This data monitor shows the last ten successful firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/

Resource	Description	Type	URI
Top VPN Servers with Denied Connections	This data monitor tracks the number of failed VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Top 10 Users With Failed Logins	This data monitor shows the top ten users with failed firewall logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top VPN Servers with Authentication Errors	This data monitor tracks the number of VPN authentication error events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure).	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Firewall Login Overview/
Top VPN Servers with Successful Connections	This data monitor tracks the number of successful VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Foundation/Network Monitoring/Device Activity/VPN Connection Statistics/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Login Events	This filter identifies events where the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/Cross-Device/
Target User ID is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Target User ID is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/User/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Successful Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Failed Login Events	This filter identifies events where the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/Cross-Device/
VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify.	Filter	ArcSight Express/Devices/VPN/
Successful Password Changes	This filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success.	Filter	ArcSight Express/Devices/Cross-Device/
Failed VPN Connection Events	This filter identifies unsuccessful VPN events in which the behavior is /Access/Start.	Filter	ArcSight Express/Devices/VPN/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Successful VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify and the category outcome is Success.	Filter	ArcSight Express/Devices/VPN/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Failed VPN Login Events	This filter identifies VPN events in which the category behavior is /Authentication/Verify and the category outcome is Failure.	Filter	ArcSight Express/Devices/VPN/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
VPN Configuration Changes	This filter identifies successful configuration change events that match the VPN Events filter.	Filter	ArcSight Express/Devices/VPN/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Successful VPN Connection Events	This filter identifies successful VPN events in which the behavior is /Access/Start.	Filter	ArcSight Express/Devices/VPN/
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Express/Devices/Cross-Device/
VPN Authentication Errors	This filter identifies VPN authentication error events in which an authentication error event is defined as having the category behavior of /Authentication/Verify and the category significance of /Informational/Error.	Filter	ArcSight Express/Devices/VPN/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Failed Logins by User	This report shows authentication failures from firewall login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with failed login attempts. A table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour. A chart shows the average bandwidth usage per hour for the previous day (by default). Use this report to find high bandwidth usage hours during the day.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address. A chart shows the top ten source addresses with successful login attempts. A table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/Devices/Firewall/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall connections by the top hosts. By default, a chart shows the number of connections by host for the previous day.	Focused Report	ArcSight Express/Devices/Firewall/
Login Event Audit	This report shows all the successful and failed database login events in a table sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Password Changes	This report shows database password changes for the previous day and groups the password changes by user, sorted chronologically.	Focused Report	ArcSight Express/Devices/Database/
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Configuration Changes by User	This report displays anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes made by a specific user.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Top Bandwidth Hosts	This report shows a summary of bandwidth usage reported by firewalls by the top hosts. A chart shows the average bandwidth usage by host for the previous day (by default). Use this report to find the highest bandwidth hosts.	Focused Report	ArcSight Express/Devices/Firewall/
Successful Logins by User	This report shows authentication successes from firewall login attempts by user. A chart shows the top ten users with successful login attempts. A table shows details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Configuration Changes by Type	This report displays the configuration change name, the user making the change, device information, and the time of the change for anti-virus configuration change events reported the previous day. Use this report to find all the configuration changes of a certain type.	Focused Report	ArcSight Express/Devices/Anti-Virus/
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Devices/Firewall/
Connections Accepted by Address	This query returns the device zone, address, host name, and a count of VPN devices with successful connections.	Query	ArcSight Express/Devices/VPN/Connections Accepted by Address/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Authentication Errors	This query returns VPN authentication events in which there has been an error. The query returns the user information, the host information, the error, the time (within an hour), and the number of times the error occurred within the hour.	Query	ArcSight Express/Devices/VPN/
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Closed VPN Connection Durations	This query returns the user ID and the minimum, average, maximum, and total durations (in minutes) for all user IDs with closes or terminated VPN sessions in the User VPN Sessions list.	Query	ArcSight Express/Devices/VPN/Connection Durations by User/
Password Changes	This query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Top Connections Accepted by Address	This query returns the device zone, address, and a count to show the top VPN devices with successful connections.	Query	ArcSight Express/Devices/VPN/Connections Accepted by Address/
Connections Denied by Address	This query returns the device zone, address, host name, and a count of VPN devices with denied connections.	Query	ArcSight Express/Devices/VPN/Connections Denied by Address/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Connections Denied by Hour	This query returns the device zone, address, host name, and a count of VPN devices with denied connections.	Query	ArcSight Express/Devices/VPN/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
Users by Connection Count	This query returns events in which the category behavior is /Access/Start, /Authentication/Verify or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	ArcSight Express/Devices/Identity Management/Connection Counts by User/
Top VPN Connection Durations	This query identifies the user ID and the average duration from the User VPN Sessions list, sorted by the top duration.	Query	ArcSight Express/Devices/VPN/Connection Durations by User/
Top Connections Denied by Address	This query returns the device zone, address, and a count to show the top VPN devices with denied connections.	Query	ArcSight Express/Devices/VPN/Connections Denied by Address/
Top Hosts by Number of Connections	This query returns host information and the number of events in which the category behavior is /Access/Start and the category outcome is not Failure.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Top Users by Connection Count	This query identifies VPN events in which the Category Behavior is /Access/Start, /Authentication/Verify, or /Authorization/Verify, with user information available, returning the number of VPN connections per user.	Query	ArcSight Express/Devices/VPN/Connection Counts by User/
Users with Open VPN Connections	This query identifies the user ID and the VPN device for each user in the User VPN Sessions list where the user entry has not been terminated (logged out or timed out) or expired (by default).	Query	ArcSight Express/Devices/VPN/Connection Durations by User/
User VPN Sessions	This session list tracks VPN user session starts and stops (or terminations), for purposes of tracking user session durations. The default expiration time for a session is five days, at which point the session is automatically considered terminated. If a majority of the sessions are showing a duration of five days, consider increasing the Entry Expiration Time. The sessions are maintained by the User VPN Session Started and User VPN Session Stopped rules.	Session List	ArcSight Foundation/Intrusion Monitoring/User Tracking/VPN/

Chapter 6

Microsoft Windows Monitoring Use Cases

The Microsoft Windows Monitoring content provides a series of coordinated resources that monitor and report on system activities on the Microsoft Windows operating system.



The Microsoft Windows Monitoring content is triggered by Microsoft Windows events from the Microsoft Windows Event Log- Unified SmartConnector with parser version 1. Make sure this SmartConnector is installed and configured. Make sure that the system running the Microsoft Windows Event Log – Unified SmartConnector is configured to use the same DNS servers as the Active Directory. This ensures consistency between host names and addresses.

The Microsoft Windows Monitoring resources are grouped together using use cases, which help address a specific issue or function. The Microsoft Windows Monitoring use cases are listed in the following table.

Use Case	Purpose
"Microsoft Windows Monitoring" on page 204	The Microsoft Windows Monitoring use case includes several resources that provide an overview of events being monitored through the Account Management, Authentication, Policy Changes, and System Services and Auditing use cases.
"Account Management" on page 207	The Account Management use case provides resources that monitor changes to the status of Windows accounts, including accounts that become locked out as a result of multiple login failures, changes to administrator privileges or other access permissions, and creation or disabling of user accounts.
"Authentication" on page 221	The Authentication use case provides resources that monitor login activity in Windows. These resources can provide information such as the number of failed logins per user and host, or attempted authentications against disabled or non-existent accounts. Rules categorize user accounts for which failed authentications occur and enable you to view the authentication failures by category.
"Policy Changes" on page 227	The Policy Changes use case provides resources that monitor changes to policies in your Windows environment, including policies related to password updates, lockouts, and audits.
"System Services and Auditing" on page 230	The System Services and Auditing use case provides resources that monitor Windows activity related to clearing the audit log, and starting or stopping critical operating system services.

Microsoft Windows Monitoring

The Microsoft Windows Monitoring use case includes several resources that provide an overview of events being monitored through the Account Management, Authentication, Policy Changes, and System Services and Auditing use cases.

Resources

The following table lists all the resources explicitly assigned to the Microsoft Windows Monitoring use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 6-1 Resources that Support the Microsoft Windows Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
Windows Monitoring Events	This active channel shows events received during the past two hours and displays all Microsoft Windows events.	Active Channel	ArcSight Express/Microsoft Windows Monitoring/
Windows Monitoring Correlation Events	This active channel shows the correlation events from Microsoft Windows Monitoring content within the last two hours.	Active Channel	ArcSight Express/Microsoft Windows Monitoring/
Windows Monitoring	This dashboard monitors the top Microsoft Windows users, top Windows event types, and top Windows devices.	Dashboard	ArcSight Express/
Top Windows Devices by Event Count	This query viewer displays the top Microsoft Windows devices by event count.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Top Windows Devices by Event Count	This report displays a table showing the top Microsoft Windows devices by event count. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Top 10 Event Types last Hour	This data monitor displays the top ten Microsoft Windows event types within the last hour.	Data Monitor	ArcSight Express/Microsoft Windows Monitoring/Windows Monitoring/
Top 10 Windows Users Last Hour	This data monitor displays the top ten Microsoft Windows users within the last hour.	Data Monitor	ArcSight Express/Microsoft Windows Monitoring/Windows Monitoring/

Resource	Description	Type	URI
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	Destination	SOC Operators/1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_HostName	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight Express/
Windows Monitoring Correlation	This field set is used to display relevant information when investigating Microsoft Windows correlation events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Monitoring	This field set is used to display relevant information when investigating Microsoft Windows events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Events	This filter identifies Microsoft Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Target User with Domain Information	This filter is designed for conditional expression variables and passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/

Resource	Description	Type	URI
EventID.net	This integration command runs a search with the external ID and the device event category in the selected event.	Integration Command	ArcSight Foundation/Microsoft Windows Monitoring/
MS - Event Lookup	This integration configuration configures the EventID.net command. You can run the command on any cell selected in the viewer.	Integration Configuration	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Events by Device Trend	This query returns the device address, device event class ID, and device hostname of Microsoft Windows events.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/For Trends/
Top Windows Devices by Event Count - Trend	This query returns Microsoft Windows events by Device. The query selects the device host name, the device address, and the number of events.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows Events by Event and Device	This trend tracks the number of Microsoft Windows events by device and stores the number of Windows events, the device address, device event class id, and device host name.	Trend	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Authentication	This use case monitors user logon activity in Microsoft Windows, focusing on multiple failed logins and logins to disabled and non-existing accounts.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
Policy Changes	This use case monitors changes to the audit, password, and account lockout policies in Microsoft Windows.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
System Services and Auditing	This use case monitors the starting and stopping of critical services on Microsoft Windows systems, changes to system times, and clearing of audit logs.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/
Account Management	This use case monitors changes to Microsoft Windows user accounts, including account lockouts and modifications to user and privileged accounts.	Use Case	ArcSight Foundation/Microsoft Windows Monitoring/

Account Management

The Account Management use case provides resources that monitor changes to the status of Windows accounts, including accounts that become locked out as a result of multiple login failures, changes to administrator privileges or other access permissions, and creation or disabling of user accounts.

Applicable Events

The following events apply to this use case.

Windows 2003 family:

- Security:528
- Security:540
- Security:624
- Security:626
- Security:627
- Security:628
- Security:629
- Security:630
- Security:632
- Security:633
- Security:636
- Security:637
- Security:642
- Security:644
- Security:645
- Security:646
- Security:647
- Security:660
- Security:661
- Security:671

Windows 2008 family:

- Microsoft-Windows-Security-Auditing:4624
 - Microsoft-Windows-Security-Auditing:4720
 - Microsoft-Windows-Security-Auditing:4722
 - Microsoft-Windows-Security-Auditing:4723
 - Microsoft-Windows-Security-Auditing:4724
 - Microsoft-Windows-Security-Auditing:4725
 - Microsoft-Windows-Security-Auditing:4726
 - Microsoft-Windows-Security-Auditing:4728
 - Microsoft-Windows-Security-Auditing:4729
 - Microsoft-Windows-Security-Auditing:4732
 - Microsoft-Windows-Security-Auditing:4733
 - Microsoft-Windows-Security-Auditing:4738
 - Microsoft-Windows-Security-Auditing:4740
 - Microsoft-Windows-Security-Auditing:4741
 - Microsoft-Windows-Security-Auditing:4742
 - Microsoft-Windows-Security-Auditing:4743
 - Microsoft-Windows-Security-Auditing:4756
 - Microsoft-Windows-Security-Auditing:4757
 - Microsoft-Windows-Security-Auditing:4767
 - Microsoft-Windows-Security-Auditing:6279
 - SAM:12294
-

Configuration

The Account Management use case requires the following configuration for your environment. You must have ArcSight Administrator privileges to perform the configuration.

- Configure the following active lists. These active lists are referenced by rules.
 - ◆ Populate the [Privileged Accounts](#) active list with all the privileged accounts in your environment.



Use lower case for the User Name and Domain fields.

- ◆ Populate the [Privileged Groups](#) active list with the group names of all Windows privileged groups.

For information on how to configure active lists, refer to the ArcSight Console User's Guide.

- *Optional:* Enable the notification action for the following rules, if appropriate for your organization.
 - ◆ [Account Locked Out Multiple Times in 24 Hours](#)
 - ◆ [Privileged Account Locked Out](#)
 - ◆ [Lockout Attempt Failed](#)
 - ◆ [Account Locked Out](#)

For information on how to enable notification actions, refer to the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the Account Management use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 6-2 Resources that Support the Account Management Use Case

Resource	Description	Type	URI
Monitor Resources			
Account Management	This dashboard shows an overview of Microsoft Windows account management events. The dashboard displays the User Accounts Created, Deleted, Disabled or Enabled, Windows Account Lockouts, Modified Windows Privileged Accounts, and Privileged Accounts Modified data monitors or query viewers.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Windows Account Lockouts	This query viewer displays Microsoft Windows user accounts that have been locked out today.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/

Resource	Description	Type	URI
Privileged Accounts Modified - Drilldown	This query viewer is used for drilldown purposes to display detailed information about privileged group member modifications.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Modified Windows Privileged Accounts	This query viewer displays modifications to a Microsoft Windows privileged account such as enabling or disabling, deleting, or changing the password.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Accounts Modified	This query viewer displays modifications to a Microsoft Windows privileged account, such as being added to or removed from a privileged group.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Computer Accounts Deleted Weekly	This report displays a table showing the Microsoft Windows computer accounts that have been deleted. The report also displays a chart showing the number of deleted computer accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Deleted Weekly	This report displays a table showing Microsoft Windows user accounts that have been deleted. The report also displays a chart showing the number of deleted user accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Daily Accounts Locked Out	This report displays a table showing the Microsoft Windows user accounts that have been locked out. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Modified Windows Privileged Group Members	This report displays a table showing additions or removals of users in Microsoft Windows privileged groups. The report also displays a chart showing the number of additions or removals per group.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Enabled Weekly	This report displays a table showing the Microsoft Windows user accounts that have been enabled. It also displays a chart showing the number of enabled user accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Computer Accounts Modified Weekly	This report displays a table showing the Microsoft Windows computer accounts that have been modified. The report also displays a chart showing the number of modified computer accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Disabled Weekly	This report displays a table showing the Microsoft Windows user accounts that have been disabled. The report also displays a chart showing the number of disabled user accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Modified Windows Privileged Accounts	This report displays a table showing the Microsoft Windows privileged accounts that have been modified. This table includes any accounts that have been enabled, disabled, deleted, had the password changed, or any other type of modification. The report also displays a chart showing the count per change type.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Weekly Accounts Locked Out	This report displays a table showing the Microsoft Windows user accounts that have been locked out. It also displays a chart showing the number of lockout events per day. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Computer Accounts Created Weekly	This report displays a table showing the Microsoft Windows computer accounts that have been created. The report also displays a chart showing the number of created computer accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Created Weekly	This report displays a table showing Microsoft Windows user accounts that have been created. The report also displays a chart showing the number of created user accounts per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Library - Correlation Resources			
Locked Account Re-enabled	This rule detects Microsoft Windows user account logon successful and user account unlocked events. On each event, the rule terminates the existing session entry (if any) in the Locked Out Accounts session list. The device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Computer Account Changed	This rule detects changes to Microsoft Windows computer accounts. On every event, the account is added in the Modified Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Lockout Attempt Failed	This rule detects a failure to lock out a Microsoft Windows account. This event might indicate a possible brute force attack against the default Administrator account. Because this account does not lock out by default, the system event log records SAM event 12294 instead. Investigate even a single occurrence of this event immediately; this condition can also indicate the presence of an unauthorized operating system. Check the Domain Name field for unknown domains. On each event, a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Account Removed from Privileged Group	This rule detects Microsoft Windows user accounts that are removed from a privileged group. Edit the Privileged Groups active list to define which groups are considered privileged in your environment. On every event, the user account and group is added to the Privileged Group Members Modified active list and removed from the Privileged Accounts active list, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/

Resource	Description	Type	URI
Privileged Account Enabled	This rule detects Microsoft Windows account enabled events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Account Disabled	This rule detects Microsoft Windows account disabled events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Account Deleted	This rule detects Microsoft Windows user account deleted events. On every event, the user account is added in the Deleted User Accounts session list, the entry in the Created User Accounts session list is terminated if it exists, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Privileged Account Modified	This rule detects Microsoft Windows account changed events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Account Added to Privileged Group	This rule detects Microsoft Windows user accounts that are in a privileged group. Edit the Privileged Groups active list to define which groups are considered privileged in your environment. On every event, the user account and group are added to the Privileged Group Members Modified and Privileged Accounts active lists, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/

Resource	Description	Type	URI
Computer Account Deleted	This rule detects Microsoft Windows computer account deleted events. On every event, the account is added to the Deleted Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Account Enabled	This rule detects Microsoft Windows user account enabled events. On every event, the user account is added in the Enabled User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
User Account Disabled	This rule detects Microsoft Windows user account disabled events. On every event, the user account is added to the Disabled User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Account Created	This rule detects Microsoft Windows computer account creation events. On every event, the account is added in the Created Computer Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Privileged Account Deleted	This rule detects Microsoft Windows account deleted events in which the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list and removed from the Privileged Accounts active list. The device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Account Locked Out	This rule detects Microsoft Windows user account locked out events. On each event, the user account is added to the Accounts Locked Out Multiple Times in 24 Hours session list, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. If the user account is already in the session list, the Locked Count is incremented. The account is also added to the Locked Out Accounts session list for historical purposes.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/

Resource	Description	Type	URI
User Account Created	This rule detects Microsoft Windows user account creation events. On every event, the user account is added to the Created User Accounts session list, and the device and agent severity values are set to Low.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Privileged Account Locked Out	This rule detects Microsoft Windows privileged account lockout events. The rule uses the Privileged Accounts active list to determine which users have special privileges. On each event, a notification is sent to the SOC Operators team (by default, the notification is disabled) and the device and agent severity values are set to High.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Privileged Account Password Changed	This rule detects Microsoft Windows password changed events where the user name is present in the Privileged Accounts active list. On every event, the user account is added to the Privileged Accounts Modified active list, and the device and agent severity values are set to Medium.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Account Locked Out Multiple Times in 24 Hours	This rule detects Microsoft Windows user accounts that have been locked out multiple times in 24 hours using the Accounts Locked Out Multiple Times in 24 Hours session list where the Locked Count is greater than 1. On each event, a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Library Resources			
Privileged Accounts Modified	This active list stores the target account name, target domain, caller user name, caller domain, and the event name (type of modification) when a Microsoft Windows privileged account is modified. The TTL is set to seven days by default.	Active List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Accounts	This active list stores all privileged accounts in the environment as defined by the user.	Active List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/

Resource	Description	Type	URI
Privileged Group Members Modified	This active list stores the account name, group name, target IP address, target zone, target host name, caller user name, caller domain, and the category behavior (type of modification) when a Microsoft Windows user account is added or removed from a privileged group. The TTL is set to seven days by default.	Active List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Privileged Groups	This active list stores the group name of all the Microsoft Windows privileged groups. Configure the active list to correspond to the privileged groups in your environment. By default, the entries in this list do not expire. After this active list is populated, the following rules need to be enabled: Account Added to Privileged Group, Account Removed from Privileged Group, Privileged Account Deleted, Privileged Account Disabled, Privileged Account Enabled, Privileged Account Modified, and Privileged Account Password Changed.	Active List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Created, Deleted, Disabled, or Enabled	This data monitor displays the last 20 created, deleted, disabled, or enabled events for a Microsoft Windows user account. The data monitor shows the affected user name, the affected user's domain, the caller user name, the caller user's domain, and the event name. The caller user name is mapped to the attacker user name. The caller domain is mapped to attacker domain.	Data Monitor	ArcSight Express/Microsoft Windows Monitoring/Account Management/
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	Destination	SOC Operators/1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_Host Name	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Privileged Account	This field set is used to display relevant information when a privileged account is created, deleted, disabled, or enabled.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
User Accounts Created, Deleted, Disabled, or Enabled	This filter provides only created, deleted, disabled, or enabled events for Microsoft Windows user accounts.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Account Management/
LockedCount is NULL	This filter is designed for conditional expression variables. The filter passes events where the LockedCount is NULL. LockedCount is a variable used in the Account Locked Out rule and retrieves the number of times a Microsoft Windows account has been locked out from the Accounts Locked Out Multiple Times in 24 Hours session list.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Windows Events	This filter identifies Microsoft Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Target User with Domain Information	This filter is designed for conditional expression variables and passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
User Accounts Deleted Weekly - Table	This query retrieves Microsoft Windows user accounts that have been deleted. The query selects the deleted account name, deleted account domain, deleted account target host, subject account name, subject account domain, and the time the account was deleted.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Weekly Account Lockouts - Chart	This query retrieves account lockouts over the last seven days. The query selects the day the lockout occurred and the number of lockouts that occurred each day.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
User Accounts Created Weekly - Chart	This query retrieves Microsoft Windows user accounts that have been created. The query selects the domain and the number of created accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Created Weekly - Table	This query retrieves Microsoft Windows computer accounts that have been created. The query selects the new account name, new account domain, new account host, subject account name, subject account domain, and the time the account was created.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Deleted Weekly - Chart	This query retrieves Microsoft Windows user accounts that have been deleted. The query selects the domain and the number of deleted accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Modified Windows Privileged Group Members - Table	This query selects the group name, user name, caller user name, caller domain, and category behavior.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Created Weekly - Table	This query retrieves Microsoft Windows user accounts that have been created. The query selects the new account name, new account domain, new account target host, subject account name, subject account domain, and the time the account was created.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Deleted Weekly - Chart	This query retrieves Microsoft Windows computer accounts that have been deleted. It selects the domain and the number of deleted accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Enabled Weekly - Chart	This query retrieves Microsoft Windows user accounts that have been enabled. The query selects the domain and the number of enabled accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/

Resource	Description	Type	URI
Daily Account Lockouts	This query retrieves account lockouts over the previous day. The query selects the user name, the hostname, the user's domain, and the timestamp for the lockout occurred, and queries against the Locked Out Accounts session list.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Modified Privileged Accounts - Table	This query selects the target account name, target domain, caller user, caller domain, event name, and count.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
User Accounts Disabled Weekly - Chart	This query retrieves Microsoft Windows user accounts that have been disabled. The query selects the domain and the number of disabled accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Created Weekly - Chart	This query retrieves Microsoft Windows computer accounts that have been created. The query selects the domain and the number of created accounts.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Computer Accounts Modified Weekly - Chart	This query retrieves Microsoft Windows computer accounts that have been modified. The query selects the domain and the number of domain.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
User Accounts Disabled Weekly - Table	This query retrieves Microsoft Windows user accounts that have been disabled. The query selects the disabled account name, disabled account domain, disabled account target host, subject account name, subject account domain, and the time the account was disabled.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
User Accounts Enabled Weekly - Table	This query retrieves Microsoft Windows user accounts that have been enabled. The query selects the enabled account name, enabled account domain, enabled account target host, subject account name, subject account domain, and the time the account was enabled.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Computer Accounts Deleted Weekly - Table	This query retrieves Microsoft Windows computer accounts that have been deleted. It selects the deleted account name, NT domain controller, deleted account domain, subject account name, subject account domain, and the time the account was deleted.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Resource	Description	Type	URI
Weekly Account Lockouts - Table	This query retrieves account lockouts over the last seven days. The query selects the user name, the hostname, the user's domain, the timestamp, and the day that the lockout occurred.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Computer Accounts Modified Weekly - Table	This query retrieves Microsoft Windows computer accounts that have been modified. The query selects the modified account name, modified account domain, NT domain controller, subject account name, subject account domain, and the time the account was modified.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Modified Windows Privileged Group Members - Chart	This query selects the group name, category behavior, and the number of membership changes.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Modified Privileged Accounts - Chart	This query retrieves the name (type of change) and the count.	Query	ArcSight Express/Microsoft Windows Monitoring/Account Management/Privileged Account Monitoring/
Deleted User Accounts	This session list stores the deleted account name, deleted account domain, delete account target host, subject account name, and subject account domain when a Microsoft Windows user account is deleted.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Created Computer Accounts	This session list stores the new account name, new account domain, new account host, subject account name, and subject account domain when a Microsoft Windows computer account is created.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/
Enabled User Accounts	This session list stores the enabled account name, enabled account domain, enabled account target host, subject account name, and subject account domain when a Microsoft Windows user account is enabled.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Modified Computer Accounts	This session list stores the modified account name, modified account domain, NT Domain Controller, subject account name, and subject account domain when a Microsoft Windows computer account is modified.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Resource	Description	Type	URI
Locked Out Accounts	This session list stores the user name, domain, and host information when a Microsoft Windows account has been locked out. The Account Locked Out rule adds user accounts to the list for historical tracking and reporting. The Locked Account Re-enabled rule terminates the session entry.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Created User Accounts	This session list stores the new account name, new account domain, new account target host, subject account name, and subject account domain when a Microsoft Windows user account is created.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Accounts Locked Out Multiple Times in 24 Hours	This session list stores the user name, target host, domain, and number of times a Microsoft Windows account was locked out in last 24 hours. By default, the entry expires in one day.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Account Locked Out/
Disabled User Accounts	This session list stores the disabled account name, disabled account domain, disabled account target host, subject account name, and subject account domain when a Microsoft Windows user account is disabled.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/User Account Monitoring/
Deleted Computer Accounts	This session list stores the deleted account name, NT domain controller, deleted account domain, subject account name, and subject account domain when a Microsoft Windows computer account is deleted.	Session List	ArcSight Express/Microsoft Windows Monitoring/Account Management/Computer Account Monitoring/

Authentication

The Authentication use case provides resources that monitor login activity in Windows. These resources can provide information such as the number of failed logins per user and host, or attempted authentications against disabled or non-existent accounts. Rules categorize user accounts for which failed authentications occur and enable you to view the authentication failures by category.

Applicable Events

The following events apply to this use case.

Windows 2003 family:

- Security:529
- Security:530
- Security:531
- Security:532
- Security:533
- Security:534
- Security:535
- Security:536
- Security:537
- Security:539
- Security:672
- Security:673
- Security:675
- Security:676
- Security:677
- Security:680
- Security:681

Windows 2008 family:

- Microsoft-Windows-Security-Auditing:4625
 - Microsoft-Windows-Security-Auditing:4768
 - Microsoft-Windows-Security-Auditing:4769
 - Microsoft-Windows-Security-Auditing:4771
 - Microsoft-Windows-Security-Auditing:4772
 - Microsoft-Windows-Security-Auditing:4773
 - Microsoft-Windows-Security-Auditing:4776
-

Configuration

The Authentication use case requires the following configuration for your environment. You must have ArcSight Administrator privileges to perform the configuration.

- *Optional:* Enable the notification action for the following rules, if appropriate for your organization.
 - ◆ [Failed Authentication - Windows Domain Account](#)
 - ◆ [Authentication Attempted to Non-Existing Account](#)
 - ◆ [Authentication Attempted to Disabled Account](#)
 - ◆ [Failed Authentication - Windows Workstation](#)

For information on how to enable notification actions, refer to the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the Authentication use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 6-3 Resources that Support the Authentication Use Case

Resource	Description	Type	URI
Monitor Resources			
Windows Failed Authentications - All	This active channel shows events received during the last day and displays all failed Microsoft Windows authentication events using the Failed Authentications field set.	Active Channel	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Windows Failed Authentications - Domain Accounts	This active channel shows events received during the last day and displays Microsoft Windows domain account failed authentication events using the Failed Authentications field set.	Active Channel	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Windows Failed Authentications - Workstations	This active channel shows events received during the last day and displays Microsoft Windows workstation failed authentication events using the Failed Authentications field set.	Active Channel	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Authentication Failed	This dashboard shows an overview of Microsoft Windows account authentication failures. The dashboard displays the Weekly Hosts With Multiple Failed Authentications, Weekly Users With Multiple Failed Authentications, Weekly User With Multiple Failed Authentications by Reason, and Weekly Users With Multiple Failed Authentications Detail query viewer.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Weekly Hosts With Multiple Failed Authentications	This query viewer displays the number of failed authentications by IP address.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications Detail	This query viewer displays the user name with multiple failed authentications in detail. It shows the target user name, target domain, target IP address, target zone name, failure reason, and number of time failure.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Weekly Users With Multiple Failed Authentications	This query viewer displays the number of failed authentications by user name.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications by Reason	This query viewer displays the number of failed authentications by reason.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Hosts With Multiple Failed Authentications	This report displays a table showing Microsoft Windows hosts with multiple failed authentication attempts. The report also displays a chart showing the top ten hosts with failed authentication attempts by zone name. By default, this report runs over the last seven days and the threshold is five failures.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications	This report displays a table showing Microsoft Windows users with multiple failed authentication attempts. The report also displays a chart showing the number of failed attempts by user name. By default, this report runs over the last seven days, and the threshold is five failures.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Library - Correlation Resources			
Failed Authentication - Windows Domain Account	This rule detects failed authentication attempts to Microsoft Windows domain accounts. On every event, the device and agent severity values are set to Medium, the event is added to the Failed Authentications session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Authentication Attempted to Non-Existing Account	This rule detects authentication attempts to non-existent Microsoft Windows user accounts. On every event, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Authentication Attempted to Disabled Account	This rule detects authentication attempts to disabled Microsoft Windows user accounts. On every event, the device and agent severity values are set to Medium and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Failed Authentication - Windows Workstation	This rule detects failed authentication attempts to Microsoft Windows workstations. On every event, the device and agent severity values are set to Medium, the event is added to the Failed Authentications session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Library Resources			
Logon Types	This active list stores a mapping from encoded logon types to their string equivalents. This list is pre-populated and the entries never expire by default.	Active List	ArcSight Express/Microsoft Windows Monitoring/Authentication/
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	Destination	SOC Operators/1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_HostName	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Failed Authentications	This field set displays relevant information when investigating Microsoft Windows failed authentication events.	Field Set	ArcSight Foundation/Microsoft Windows Monitoring/
WindowsLogonTypes.csv	This file provides the initial data for the Logon Types active list, which is part of the Microsoft Windows Monitoring/Authentication resources.	File	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Failed Authentication Events - All	This filter detects Microsoft Windows failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Failed Authentication Events - Workstation	This filter identifies Microsoft Windows workstation failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Windows Events	This filter identifies Microsoft Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Failed Authentication Events - Domain	This filter identifies Microsoft Windows domain account failed authentication events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Authentication/
Target User with Domain Information	This filter is designed for conditional expression variables and passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Weekly Users With Multiple Failed Authentications by Reason - Chart	This query returns Microsoft Windows failed authentications. It selects the number of failures and the reason for the failures. By default, the threshold is set to five failures.	Query	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Weekly Users With Multiple Failed Authentications - Chart	This query returns Microsoft Windows failed authentications. The query selects the target user name and the number of failures. By default, the threshold is set to five failures.	Query	ArcSight Express/Microsoft Windows Monitoring/Authentication/

Resource	Description	Type	URI
Weekly Users With Multiple Failed Authentications-Table	This query returns Microsoft Windows users with multiple failed authentications. The query selects the user name, domain, IP address, zone, failure reason, and the number of failures. By default, the threshold is set to five failures.	Query	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Weekly Hosts With Multiple Failed Authentications-Table	This query returns Microsoft Windows hosts with multiple failed authentications. The query selects the IP address, zone, reason, and number of failures. By default, the threshold is set to five failures.	Query	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Weekly Hosts With Multiple Failed Authentications - Chart	This query returns Microsoft Windows hosts with multiple failed authentications. The query selects the IP address, zone, and number of failures. By default, the threshold is set to five failures.	Query	ArcSight Express/Microsoft Windows Monitoring/Authentication/
Failed Authentications	This session list stores information about failed Microsoft Windows authentications, including the user and host information, failure reason, message, and logon type.	Session List	ArcSight Express/Microsoft Windows Monitoring/Authentication/

Policy Changes

The Policy Changes use case provides resources that monitor changes to policies in your Windows environment, including policies related to password updates, lockouts, and audits.

Applicable Events

The following events apply to this use case.

Windows 2003 family:	Windows 2008 family:
<ul style="list-style-type: none"> Security:612 Security:643 	<ul style="list-style-type: none"> Microsoft-Windows-Security-Auditing:4719 Microsoft-Windows-Security-Auditing:4739

Configuration

The Policy Changes use case requires the following configuration for your environment. You must have ArcSight Administrator privileges to perform the configuration.

- *Optional:* Enable the notification action for the following rules, if appropriate for your organization.
 - ◆ [System Audit Policy Changed](#)
 - ◆ [Lockout Policy Changed](#)
 - ◆ [Password Policy Changed](#)

For information on how to enable notification actions, refer to the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the the Policy Changes use case includes dependent resources. Dependent resources are not listed in a use case resource.

Table 6-4 Resources that Support the Policy Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Policy Changes	This dashboard shows an overview of Microsoft Windows policy change events. The dashboard displays the Policy Changes data monitor.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Weekly Policy Changes by Type	This report displays a table showing Microsoft Windows policy changes. It also displays a chart showing the number of changes per policy type, by domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/

Resource	Description	Type	URI
Library - Correlation Resources			
System Audit Policy Changed	This rule detects modifications to the Microsoft Windows system audit policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
Lockout Policy Changed	This rule detects modifications to the Microsoft Windows lockout policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
Password Policy Changed	This rule detects modifications to the Microsoft Windows password policy. On each event, agent and device severities are set to Medium, the change is added to the Policy Changes session list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
Library Resources			
Windows - Systems Starting Up	This active list stores Microsoft Windows systems that are starting up. It is used to reduce false positives in the System Audit Policy Changed rule, because many policy change events are generated by Windows when systems are starting. By default, the TTL is ten minutes.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Policy Changes	This data monitor displays the last ten Microsoft Windows policy change events, and shows the type of policy that was changed and the affected domain.	Data Monitor	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	Destination	SOC Operators/1
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_HostName	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Policy Changes	This filter identifies correlation events resulting from changes to Microsoft Windows policies.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Policy Changes/
Windows Events	This filter identifies Microsoft Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/
Target User with Domain Information	This filter is designed for conditional expression variables and passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Weekly Policy Changes	This query returns Microsoft Windows policy changes. It selects the policy, domain, host name, timestamp, attributes changed, and the number of changes.	Query	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/
Policy Changes	This session list stores Microsoft Windows policy change information. This list is populated by rules in the Microsoft Windows MonitoringPolicy Changes group.	Session List	ArcSight Express/Microsoft Windows Monitoring/Policy Changes/

System Services and Auditing

The System Services and Auditing use case provides resources that monitor Windows activity related to clearing the audit log, and starting or stopping critical operating system services.

Applicable Events

The following events apply to this use case.

Windows 2003 family:	Windows 2008 family:
<ul style="list-style-type: none">• Security:512• Security:516• Security:517• Security:520• Security:521• Security:601	<ul style="list-style-type: none">• Microsoft-Windows-Eventlog:1102• Microsoft-Windows-Security-Auditing:4608• Microsoft-Windows-Security-Auditing:4612• Microsoft-Windows-Security-Auditing:4616• Microsoft-Windows-Security-Auditing:4617• Microsoft-Windows-Security-Auditing:4697• Microsoft-Windows-Security-Auditing:4906• Service Control Manager:7035• Service Control Manager:7036

Configuration

The System Services and Auditing use case requires the following configuration for your environment. You must have ArcSight Administrator privileges to perform the configuration.

- Populate the [Critical Services](#) active list with the names of Windows services that you consider critical in your environment. For information on how to configure active lists, refer to the ArcSight Console User's Guide.
- Configure the [Critical Services](#) filter with the names of the critical Windows services that require alerts when those services are started or stopped.
- *Optional:* Enable the notification action for the following rules, if appropriate for your organization.
 - ◆ [Critical Service Stopped](#)
 - ◆ [Critical Service Started](#)
 - ◆ [Critical Service Request Start](#)
 - ◆ [Critical Service Request Stop](#)
 - ◆ [Windows System Time Changed](#)
 - ◆ [Windows Security Audit Log Cleared](#)
 - ◆ [Windows Audit Events Discarded](#)
 - ◆ [Windows System Starting](#)
 - ◆ [CrashOnAuditFail Modified](#)
 - ◆ [Install Service Attempt](#)
 - ◆ [Unable to Log Events](#)

For information on how to enable notification actions, refer to the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the System Services and Auditing use case, and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 6-5 Resources that Support the System Services and Auditing Use Case

Resource	Description	Type	URI
Monitor Resources			
System Services and Auditing	This dashboard shows an overview of Microsoft Windows critical services and auditing violation events. The dashboard displays the Windows System Services and Auditing Violations and the Critical Services Started or Stopped information.	Dashboard	ArcSight Foundation/Microsoft Windows Monitoring/
Critical Services Started or Stopped	This query viewer displays critical Microsoft Windows services that have been started or stopped in the last day.	Query Viewer	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Time Changes	This report displays a table showing Microsoft Windows system time-changed events. It also displays a chart showing the number of times the system time was changed per domain. By default, this report runs over the last seven days.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows Critical Services Started Or Stopped	This report displays a table showing critical Microsoft Windows services that have started or stopped. It also displays a chart showing the top ten start or stop events per service. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Windows Security Audit Logs Cleared	This report displays a table showing Microsoft Windows audit log cleared events. It also displays a chart showing the number of times the audit logs were cleared per domain. By default, this report runs over the previous day.	Report	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Library - Correlation Resources			
Windows Audit Events Discarded	This rule detects when Microsoft Windows audit events are discarded. On the first event, the device and agent severity values are set to High and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Windows System Starting	This rule detects when Microsoft Windows hosts are starting up. The rule adds host information to the Windows - Systems Starting Up active list, which is then used to reduce false positives in the Policy Changes rules. (Many policy change events are generated by Windows when systems are starting.) On every event, the agent and device severity values are set to Low and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Time Changed	This rule detects Microsoft Windows system time change events. On every event, the device and agent severities are set to Medium, the user name, host name, NT domain, previous times, new times, and changed times are added to the System Time Changes active list, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule is not designed to be activated on NTP time changes.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Request Start	This rule detects when critical Microsoft Windows services send a start control. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the Critical Services Started or Stopped active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. Enable this rule when the Critical Services active list is populated.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Unable to Log Events	This rule detects events that indicate Microsoft Windows is unable to write events to the security event log. If this behavior is detected on a high-value computer, investigate immediately. On the first event, the agent and device severity values are set to High and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Stopped	This rule detects when critical Microsoft Windows services stop. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information are added to the Critical Services Started or Stopped active list, the device and agent severity values are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. Enable this rule when the Critical Services active list is populated.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Install Service Attempt	This rule detects the installation of services which should be a rare event and not an everyday action. Investigate all successes and failures for this event. On every event, the agent and device severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
CrashOnAuditFail Modified	This rule detects changes to the Microsoft Windows 2008 family CrashOnAuditFail setting. On every event, the agent and device severity values are set to Medium and a notification is sent to the SOC Operators team. By default, the notification is disabled. This setting controls whether the host shuts down if it fails to write audit logs.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Windows Security Audit Log Cleared	This rule detects when Microsoft Windows audit logs are cleared. On every event, the device and agent severity values are set to Medium, the user and host information are added to the Audit Logs Cleared active list, and a notification is sent to the SOC Operators team. By default, the notification is disabled.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Request Stop	This rule detects when critical Microsoft Windows services send a stop control. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the Critical Services Started or Stopped active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. Enable this rule when the Critical Services active list is populated.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Service Started	This rule detects critical Microsoft Windows services that are starting. You can define which services are considered critical in your environment by editing the Critical Services active list or filter. On every event, the service, host, and user information is added to the Critical Services Started or Stopped active list, the device and agent severities are set to Medium, and a notification is sent to the SOC Operators team. By default, the notification is disabled. This rule requires collecting the Service Control Manager logs. Enable this rule when the Critical Services active list is populated.	Rule	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Library Resources			
System Time Changes	This active list stores the user name, NT domain, host name, previous time, new times, and change time when a Microsoft Windows host's system time changes. By default, the TTL is seven days.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

Resource	Description	Type	URI
Critical Services Started or Stopped	This active list stores the user name, domain, host, and service information when a critical Microsoft Windows system service is started or stopped. By default, the TTL is one day.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows - Systems Starting Up	This active list stores Microsoft Windows systems that are starting up. It is used to reduce false positives in the System Audit Policy Changed rule, because many policy change events are generated by Windows when systems are starting. By default, the TTL is ten minutes.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Services	This active list stores the service name for critical Microsoft Windows services that require alerts when started or stopped. Configured this active list with the critical Windows services in your environment. The service name stored in this list must match the Service Control Manager:7035 or Service Control Manager:7036 events from your Windows System logs. (The service name in the list must match the Target service name field of the base event.) After you populate this list with the services that are critical for your environment, enable the Critical Service Request Start, Critical Service Request Stop, Critical Service Stopped, and Critical Service Started rules.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared	This active list stores the user name, domain, host name, and timestamp when a Microsoft Windows audit log is cleared. By default, the TTL is one day.	Active List	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Windows System Services and Auditing Violations	This data monitor displays the last 20 Microsoft Windows events related to audit violations and shows the priority, user name, domain, host name, end time, and the event name.	Data Monitor	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
admin	This destination is pre-defined for SOC operators. Add additional information, such as email address.	Destination	SOC Operators/1
Target_HostName	This variable displays the Target Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Target_User	This variable displays the Target User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Target_NTDomain	This variable displays the Target NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_NTDomain	This variable displays the Attacker NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_Host Name	This variable displays the Attacker Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Attacker_User	This variable displays the Attacker User Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_NTDomain	This variable displays the Device NT Domain in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
Device_HostName	This variable displays the Device Host Name in lower case.	Global Variable	ArcSight Foundation/Microsoft Windows Monitoring/
CrashOnAuditFail is True	This filter is designed for a conditional evaluation and returns events in which the Microsoft Windows CrashOnAuditFail value is set to true. It is used in a conditional variable by the CrashOnAuditFail Modified rule. This filter is applicable only to Windows 2008 family events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Audit Log Cleared - pre-Win2k8	This filter is designed to provide only Microsoft Windows audit log cleared events. It identifies classic Windows 2003 family events and is used in a conditional variable by the Windows Security Audit Log Cleared rule.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
System Services and Auditing Violations	This filter provides correlation events only resulting from changes to Microsoft Windows system services or auditing violations.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Service Stopped Action Count is NULL	This filter is designed for conditional expression variables. It checks the Action Count value in the Critical Services Started or Stopped active list for Service Stopped is NULL.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Windows Events	This filter identifies Microsoft Windows events.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/

Resource	Description	Type	URI
Critical Services	This filter stores the service name for critical Microsoft Windows services that require alerts when started or stopped. Configure this filter with the critical Windows services in your environment.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/System Services and Auditing/
Target User with Domain Information	This filter is designed for conditional expression variables and passes events where the target user name contains the Domain information.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Service Started Action Count is NULL	This filter is designed for conditional expression variables. It checks the Action Count value in the Critical Services Started or Stopped active list for Service Started is NULL.	Filter	ArcSight Foundation/Microsoft Windows Monitoring/Conditional Variable Filters/
Critical Services Started or Stopped - Table	This query returns critical Microsoft Windows services that start or stop. It selects the service, user, and host information related to the service starting or stopping.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
System Time Changes - Table	This query returns Microsoft Windows system time-changed events. It selects the user name, NT domain, host name, new system time, previous system time, and the time at which the system time was changed.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared - Chart	This query returns Microsoft Windows audit log cleared events. It selects the domain and the number of times the logs were cleared.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
System Time Changes - Chart	This query returns Microsoft Windows system time-changed events. It selects the NT domain, host name, and the number of times the time was changed.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Audit Logs Cleared - Table	This query returns Microsoft Windows audit log cleared events. It selects the user, domain, host, and time that the log was cleared.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/
Critical Services Started or Stopped - Chart	This query returns critical Microsoft Windows services starting or stopping. It selects the service name and the number of times the service was started or stopped.	Query	ArcSight Express/Microsoft Windows Monitoring/System Services and Auditing/

NetFlow Monitoring Use Case

NetFlow is a network protocol developed by Cisco Systems to run on Cisco IOS-enabled equipment for collecting IP traffic information. It is proprietary, but supported by platforms other than Cisco IOS, such as Juniper routers and Linux. NetFlow provides session-level data. Leveraging this information using ArcSight can help to monitor network bandwidth usage and correlate it with other security logs (such as firewall, IDS, authentication logs, and so on).

The NetFlow Monitoring content provides resources to monitor and report on top bandwidth usage by source, destination and port. NetFlow Monitoring contains one use case with resources that:

- Monitor, investigate, and report on bandwidth usage by source, destination, and port.
- Monitor the bandwidth moving average and identify top bandwidth usage by source, destination, and port.
- Report on bandwidth usage in daily or weekly increments using trends and by source, destination, and port.

You can use this information to build correlation content; for example, you can build a rule that correlates NetFlow events with other security logs, such as firewall or IDS logs.

The NetFlow Monitoring content is triggered by NetFlow events from the following SmartConnectors. Make sure you have installed and configured these SmartConnectors.

SmartConnector	Device Version Supported
ArcSight IP Flow SmartConnector	<ul style="list-style-type: none">• Cisco NetFlow versions 5 and 9• Flexible NetFlow from IOS 15.0• Cisco ASA 8.2, and Juniper Networks J-Flow versions 5 and 9
ArcSight QoSient ARGUS SmartConnector	<ul style="list-style-type: none">• QoSient ARGUS versions 2 and 3

For information about how to obtain these SmartConnectors, contact your HP ArcSight sales representative.

Devices

Network devices with NetFlow enabled supply events that apply to the NetFlow Monitoring resources.

Configuration

NetFlow Monitoring contains five trends. Four of the trends are trend-on-trends, which all collect data from a single base trend (Top Bandwidth Usage Events). Do not schedule the four trend-on-trends to run before the base trend completes its daily query run. By default, the trends are scheduled to run daily at the times indicated below.

Trend Name	Scheduled run time
Top Bandwidth Usage by Destination	3:33:36 AM
Top Bandwidth Usage by Hour	2:40:34 AM
Top Bandwidth Usage by Port	3:15:50 AM
Top Bandwidth Usage by Source	3:07:08 AM
Top Bandwidth Usage Events (base trend)	1:15:09 AM

By default, each trend uses midnight of the date the package was installed as the date and time the trend will start collecting information. To adjust the schedule or start date/time for the trend, edit the values in the **Schedule** tab of the Inspect/Edit panel for the trend. For more information, refer to the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the NetFlow Monitoring use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 7-1 Resources in the NetFlow Monitoring

Resource	Description	Type	URI
Monitor Resources			
Top NetFlow Bandwidth Usage Monitoring	This dashboard shows the top bandwidth usage as reported by NetFlow events, showing top bandwidth usage by source, destination, well-known port, and non well-known port.	Dashboard	ArcSight Express/NetFlow Monitoring/
NetFlow Bandwidth Usage Overview	This dashboard shows an overview of bandwidth usage reported by NetFlow events. The report displays the top bandwidth usage events, and the inbound and outbound bandwidth moving average.	Dashboard	ArcSight Express/NetFlow Monitoring/

Resource	Description	Type	URI
List of Top Bandwidth Usage Events	This query viewer displays the top ten bandwidth usage events and contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Well-Known Port	This query viewer displays the top ten well-known destination ports, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	This query viewer displays the top ten source addresses, destination addresses, destination ports, counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This query viewer displays the top ten destination addresses, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Non-Well-Known Port	This query viewer displays the top ten non well-known destination ports, and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	This query viewer displays the top ten source addresses, destination addresses, and the total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This query viewer displays the top ten source addresses and the total bytes from NetFlow events, sorted by bytes. This query viewer contains several drilldowns for investigation.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source and Port	This query viewer displays the top ten source addresses, destination ports, flow counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination and Port	This query viewer displays the top ten destination addresses, destination ports, flow counts, and total bytes from NetFlow events, sorted by bytes.	Query Viewer	ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
Top Bandwidth Usage Weekly Report	This report displays the bandwidth usage, the top bandwidth usage by source, the top bandwidth usage by destination, and the top bandwidth usage by port. The default time range for this report is the past seven days.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination Port	This report displays top bandwidth usage by destination port. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This report displays top bandwidth usage by source. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This report displays top bandwidth usage by destination. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Daily Report	This report displays an hourly chart showing the bandwidth usage, a chart showing the top bandwidth usage by source, a chart showing the top bandwidth usage by destination, and a chart showing the top bandwidth usage by port. The default time range for this report is yesterday.	Report	ArcSight Foundation/NetFlow Monitoring/
Library Resources			
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Outbound Bandwidth (Bytes Per Second)	This data monitor shows the average outbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Express/NetFlow Monitoring/
Inbound Bandwidth (Bytes Per Second)	This data monitor shows the average inbound bandwidth (bytes/sec) for the last hour. The values are updated every five minutes.	Data Monitor	ArcSight Express/NetFlow Monitoring/
TotalBytes	This variable sums the values of Bytes In and Bytes Out for each event.	Global Variable	ArcSight Foundation/Variables Library/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/

Resource	Description	Type	URI
Inbound NetFlow Traffic	This filter identifies NetFlow events coming from external sources targeting the internal network.	Filter	ArcSight Foundation/NetFlow Monitoring/
Outbound Events	This filter identifies events originating from inside the company network, targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
Outbound NetFlow Traffic	This filter identifies NetFlow events coming from internal sources targeting the external network.	Filter	ArcSight Foundation/NetFlow Monitoring/
Bytes Out is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Bytes Out is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
QoSient Argus Events	This filter identifies events from Argus SmartConnectors.	Filter	ArcSight Foundation/NetFlow Monitoring/
Bytes In is NULL	This filter is designed for conditional expression variables. The filter identifies events in which the Bytes In is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Bytes/
NetFlow Traffic Reporting Devices	This filter identifies NetFlow traffic reporting devices. By default, the filter contains QoSient Argus, NetFlow V5, and NetFlow V9 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
NetFlow V9 Events	This filter identifies NetFlow version 9 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
Inbound Events	This filter identifies events coming from the outside network targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
Non-Well-Known Ports	This filter identifies events in which the Target Port is not NULL and is greater than 1024.	Filter	ArcSight Foundation/NetFlow Monitoring/

Resource	Description	Type	URI
NetFlow V5 Events	This filter identifies NetFlow version 5 events.	Filter	ArcSight Foundation/NetFlow Monitoring/
Well-Known Ports	This filter identifies events in which the Target Port is not NULL and is less than or equal to 1024.	Filter	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs	This query returns the source address, destination address, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Destination - Trend on Trend	This query identifies the destination address, destination zone, flow counts, and total bytes from the Top Bandwidth Usage by Destination trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source	This query returns the source address and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Hour - Trend on Trend	This query returns bandwidth usage information by hour from the Top Bandwidth Usage by Hour trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Source and Port	This query identifies the source address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This query identifies the destination address and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage Events	This query identifies the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour. This query is used by the Top Bandwidth Usage Events trend.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Day - Trend on Trend	This query identifies the bandwidth usage information by day from the Top Bandwidth Usage by Hour trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend	This query identifies the destination port, flow counts, and total bytes from the trend Top Bandwidth Usage Events.	Query	ArcSight Express/NetFlow Monitoring/Trend/

Resource	Description	Type	URI
Top Bandwidth Usage by Well-Known Port	This query returns the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour in which the destination port is well-known.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Hour - Trend	This query returns bandwidth usage information by hour from the Top Bandwidth Usage Events trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Port - Trend on Trend	This query identifies the target port, flow counts, and total bytes from the Top Bandwidth Usage by Port trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Destination and Port	This query identifies the destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Source - Trend	This query returns the source address, source zone, and total bytes from the Top Bandwidth Usage Events trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
Top Bandwidth Usage by Non-Well-Known Port	This query returns the destination port and total bytes (Bytes In + Bytes Out) from NetFlow events in which the destination port is not well-known within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Destination - Trend	This query identifies the destination address, destination zone, flow counts, and total bytes from the Top Bandwidth Usage Events trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/
List of Top Bandwidth Usage Events	This query returns the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Source-Destination Pairs and Port	This query identifies the source address, destination address, destination port, flow counts, and total bytes (Bytes In + Bytes Out) from NetFlow events within the last hour.	Query	ArcSight Express/NetFlow Monitoring/
Top Bandwidth Usage by Source - Trend on Trend	This query returns the source address, source zone, and total bytes from the Top Bandwidth Usage by Source trend.	Query	ArcSight Express/NetFlow Monitoring/Trend/

Resource	Description	Type	URI
Top Bandwidth Usage by Hour	This trend stores hourly information of top bandwidth usage, which includes the end time hour, flow counts, and total bytes. This trend depends on the Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage Events	This trend stores bandwidth usage information reported by NetFlow, which contains the end time hour, source address, source zone, destination address, destination zone, destination port, flow counts, and total bytes. This trend is the base trend, collecting a broad amount of aggregated NetFlow data for a short period of time, used by several other trends to further aggregate data and store for a longer period of time. The default retention period for this trend is eight days.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Source	This trend stores top bandwidth usage information by source, which includes source address, source zone, flow counts, and total bytes. This trend depends on the Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Destination	This trend stores top bandwidth usage information by destination, which includes destination address, destination zone, flow counts, and total bytes. This trend depends on the Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/
Top Bandwidth Usage by Port	This trend stores top bandwidth usage information by port, which includes destination port, flow counts, and total bytes. This trend depends on the Top Bandwidth Usage Events trend.	Trend	ArcSight Foundation/NetFlow Monitoring/

Chapter 8

Operations Use Cases

The Operations resources monitor and report on operations in your environment, such as traffic monitoring and case management.

The resources are grouped together using use cases, which help address a specific issue or function. The Operations use cases are listed in the following table.

Use Case	Purpose
"Operations" on page 248	The Operations use case contains resources for monitoring operations in your environment.
"Case Tracking and Escalation" on page 251	The Case Tracking and Escalation use case contains resources for monitoring case workflow activity, such as tracking the history of individual cases and being notified when a new case investigation has yet to be started within a policy time-frame.
"Configuration Changes" on page 260	The Configuration Changes use case contains resources for monitoring configuration changes made in your environment.
"Logins" on page 266	The Logins use case contains resources for monitoring logins to the systems in your environment.
"System Notifications and Escalation" on page 270	The System Notifications and Escalation use case monitors the response to incident notifications generated by the system.
"Traffic Monitoring" on page 273	The Traffic Monitoring use case contains resources for monitoring traffic in your environment.

Operations

The Operations use case contains resources for monitoring operations in your environment.

Resources

The following table lists all the resources explicitly assigned to the Operations use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-1 Resources that Support the Operations Use Case

Resource	Description	Type	URI
Monitor Resources			
Notification Events	This active channel shows notification audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/System Notifications and Escalation/
Traffic Statistics	This report displays the bytes in and out by hour, and bytes in and out by device. A table shows the hour, firewall zone and address, the transport protocol, and the bytes in and out.	Report	ArcSight Express/Operations/Traffic Monitoring/
Case Status Overview	This report shows the number of open cases by stage, consequence severity, operational impact, and associated impact. A table shows a list of recently closed cases.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
User Administration	This report shows a summary of user and user group creation, modification, and deletion.	Report	ArcSight Express/Devices/Operating System/
Library Resources			
Notifications	This field set tracks events related to the sending and acknowledgement of notifications.	Field Set	ArcSight Express/Active Channel/
Notification Event has Rule Name	This filter identifies notification events that have a Device Custom String 3 label set as Rule Name.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has User Name	This filter identifies notification events that have an attacker user name to represent the user who acknowledged or resolved a notification.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Destination Group	This filter identifies notification events that have a Device Custom String 4 label set as Group.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/

Resource	Description	Type	URI
Notification Event has Configuration Resource	This filter identifies notification events that have a Device Custom String 2 label set as Configuration Resource.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Acknowledgement Status	This filter identifies notification events that have a Device Custom String 6 label set as Acknowledgement Status.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Events	This filter identifies events that are related to sending and acknowledging notifications.	Filter	ArcSight Foundation/Workflow/System Notifications and Escalation/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Recently Closed Cases	This query on a case tracking session list selects the most recently closed cases for display in a query viewer. After a case is closed, if it is further modified, there might be multiple entries depending on the modifications. The Time Closed column shows the most recent modification of the closed case; this might not be the time when the case was initially closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Firewall Bandwidth Usage by Hour (chart)	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Usage by Firewall Address	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/
Open Cases by Associated Impact (Chart)	This query returns the number of open cases in the various associated impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Cases Open by Stage (Chart)	This query searches the cases for open cases and counts the number of them at each stage. Note: The stage for an open case is not Closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
User Administration (Chart)	This query returns the count of user (and user group) creations, modifications, and deletions.	Query	ArcSight Express/Devices/Operating System/
Firewall Bandwidth Usage per Hour	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/

Resource	Description	Type	URI
User Administration	This query returns the user (and user group), creation, modification, and deletion events.	Query	ArcSight Express/Devices/Operating System/
Open Cases by Consequence Severity (Chart)	This query returns the number of open cases in the various consequence severity ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Open Cases by Operational Impact (Chart)	This query returns the number of open cases in the various operational impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Case Tracking	This session list contains case history information, monitoring the changes of the attributes in a case as it flows through investigation and analysis.	Session List	ArcSight Express/Operations/Case Tracking and Escalation/
System Notifications and Escalation	The System Notification and Escalation use case monitors the response to incident notifications generated by the system.	Use Case	ArcSight Express/Operations/
Configuration Changes	This use case provides information about configuration changes for monitored devices on a network.	Use Case	ArcSight Express/Operations/
Case Tracking and Escalation	The Case Tracking and Escalation use case provides several resources for monitoring case workflow activity, from tracking the history of individual cases and being notified when a new case investigation has yet to be started within a policy time-frame.	Use Case	ArcSight Express/Operations/
Logins	This use case covers logins to monitored devices on a network.	Use Case	ArcSight Express/Operations/
Traffic Monitoring	This use case provides resources to monitor traffic across a network.	Use Case	ArcSight Express/Operations/

Case Tracking and Escalation

The Case Tracking and Escalation use case contains resources for monitoring case workflow activity, such as tracking the history of individual cases and being notified when a new case investigation has yet to be started within a policy time-frame.

Resources

The following table lists all the resources explicitly assigned to the Case Tracking and Escalation use case, and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-2 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
Monitor Resources			
Case Events	This active channel shows case audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Times to Resolution	This resource has no description.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Stages	This dashboard displays information about the current state of open cases, showing the case stages for each case owner. A table is also provided to show more detailed open case information for each owner.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Status	This dashboard displays information about the current status of open cases, showing their impact and severity ratings. A table of recently closed cases is also provided.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Open Cases by Stage	This query viewer shows the number of open cases at each stage.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Queued Stage Cases by Owner	This query viewer displays the number of cases in the Queued stage for each case owner.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/

Resource	Description	Type	URI
Recently Closed Cases	This query viewer displays the most recently closed cases. Note: After a case is closed, if it is further modified, there might be multiple entries depending on the modifications. The Time Closed column shows the most recent modification of the closed case; this might not be the time when the case was initially closed.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Average Time to Case Resolution - by Day	This query viewer displays the average time taken to resolve cases closed for each day of the reporting period.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
Open Cases by Consequence Severity	This query viewer shows the number of open cases at each Consequence Severity rating.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Final Stage Cases by Owner	This query viewer displays the number of cases in the Final stage for each case owner.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Follow-Up Stage Cases by Owner	This query viewer displays the number of cases in the Follow-Up stage for each case owner.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Initial Stage Cases by Owner	This query viewer displays the number of cases in the Initial stage for each case owner.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Average Time to Case Resolution - by User	This query viewer displays the average time taken to resolve cases that have been closed by each user during the reporting period.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
Average Time to Case Resolution - by Severity	This query viewer displays the severity and average time to resolution of all cases closed during the reporting period.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/

Resource	Description	Type	URI
Maximum Time to Case Resolution - by User	This query viewer displays the maximum time taken, in minutes, to resolve cases that have been closed since the start time (midnight, seven days ago by default), grouped by Operational Impact for each user who closed cases during this time period.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
Open Cases by Operational Impact	This query viewer shows the number of open cases at each operational impact rating.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Open Cases	This query viewer displays open case information in a table.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Open Cases by Associated Impact	This query viewer shows the number of open cases at each associated impact rating.	Query Viewer	ArcSight Express/Operations/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Average Time to Case Resolution - By User	This report shows the average time taken to resolve cases that have been closed by each user during the reporting period.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Average Time to Case Resolution - By Severity	This report shows the severity and average time to resolution of all cases closed during the reporting period.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Case Stages Overview	This report shows the number of open cases in each stage by owner and lists all open cases.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Average Time to Case Resolution - By Day	This report shows the average time taken to resolve cases closed for each day of the reporting period.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/

Resource	Description	Type	URI
Cases per Target	This report displays the attack target, case name, security classification, and consequence severity at each stage. Note: This report includes the count of all cases in the system, regardless of how long ago they were closed.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Status Overview	This report shows the number of open cases by stage, consequence severity, operational impact, and associated impact. A table shows a list of recently closed cases.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Open Cases	This report shows the name, creator, ticket type, stage, security classification, consequence severity, creation time, modification time, and attack target of all the open, non-system cases in the system.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Cases Created Today	This report shows the cases that have been generated since midnight this morning.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/
All Cases	This report shows the name, creator, ticket type, stage, security classification, and consequence severity of all the non-system cases in the system.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Max Time to Case Resolution - By User	This report shows the maximum time taken in minutes to resolve cases that have been closed since the start time (midnight, seven days ago by default), grouped by Operational Impact for each user who closed cases during this time period.	Report	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Library - Correlation Resources			
Case Deleted	This rule detects case audit events indicating that a case has been deleted without investigation. The rule removes the case from the active list for case tracking and escalation and sends a notification. This case is disabled by default.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Track Deleted Case	This rule detects case audit events generated when a case is deleted. The rule then updates the case entry in a case history tracking session list and marks it as deleted.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/

Resource	Description	Type	URI
Track New Case	This rule detects case audit events generated when a case is created. The rule then adds the case to a case history tracking session list.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Case Escalation	This rule tracks cases that have not yet been investigated when their entries expire from the case tracking and escalation active list. This case sends an escalation notification to the SOC Operators group and places the case information back on the active list.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Monitor New Case	This rule detects case audit events indicating that a case has been created. The rule adds the case to an active list for case tracking and escalation. This case is disabled by default.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Track Updated Case	This rule detects case audit events generated when a case is updated. If the case name, case owner, ticket type, stage, operational impact, security classification, consequence severity, or associated impact attribute changes, the rule adds the case to a case history tracking session list.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Track Closed Case	This rule detects case audit events generated when a case is closed. A case is closed when the stage is changed to Closed. The rule then updates the case entry in a case history tracking session list. Note: You can re-open a case by changing the stage attribute.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Case Investigation Started	This rule detects case audit events indicating that a case investigation has started. The rule then removes the case from the active list for case tracking and escalation.	Rule	ArcSight Express/Operations/Case Management/Case Tracking and Escalation/
Library Resources			
Case Escalation	This active list tracks case data on newly created cases that are still in the Queued stage. The default TTL is one day. If the case is not removed from the list, a rule will detect this, put it back on the list and send a notification.	Active List	ArcSight Express/Operations/Case Tracking and Escalation/

Resource	Description	Type	URI
DateTime	This variable returns the date and time in the year/month/day-hour:minute format. For example: 2009/10/03-00:43	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Month	This variable returns the numeric value of the month from the end time date field. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Minute	This variable returns the minute in a two-digit format. For example: 02	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
DateValue	This variable returns the date in the year/month/day format. For example: 2009/10/03.	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Hour	This variable returns the hour in a two-digit format. For example: 02	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Day	This variable returns the day in a two-digit format. For example: 03	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
EndTimeValue	This variable returns the hour and minute in the hour:minute format. For example: 00:10	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Year	This variable returns the year. For example: 2002	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Case	This field set contains several fields related to case information associated with case management events.	Field Set	ArcSight Express/Inspect - Edit/
Cases	This field set contains several fields related to case information associated with case management events.	Field Set	ArcSight Express/Active Channel/
Single-digit Minute	This filter supports the Minute variable by checking the end time to see if it is a single or double digit minute. The Minute variable prepends 0 to minutes with a single digit, so that the format is always mm.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Case Owner Value is null	This filter identifies the Device Custom String4 field in active list entry expired audit events for the case escalation active list where the owner of the case is not present.	Filter	ArcSight Foundation/Workflow/Case Tracking and Escalation/

Resource	Description	Type	URI
Case Events	This filter identifies events related to creating and updating cases.	Filter	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Single-digit Day	This filter identifies the Day variable by checking the end time to see if it is a single or double digit day. The Day variable prepends 0 to days with a single digit, so that the format is always DD (for example, the 1st displays as 01 instead of 1).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Single-digit Hour	This filter supports the Hour variable by checking the end time to see if it is a single or double digit hour. The Hour variable prepends 0 to hours with a single digit, so that the format is always HH (for example, 7:00 displays as 07 instead of 7).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Case Monitoring Entry Expiration	This filter identifies audit events for the case escalation active list where a case entry has expired (meets the TTL condition).	Filter	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case File Type	This filter identifies events in which the File Type field is Case.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Single-digit Month	This filter supports the Month variable by checking the end time to see if it is a single or double digit month. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Recently Closed Cases	This query on a case tracking session list selects the most recently closed cases for display in a query viewer. After a case is closed, if it is further modified, there might be multiple entries depending on the modifications. The Time Closed column shows the most recent modification of the closed case; this might not be the time when the case was initially closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Average Time to Case Resolution - By User	This query returns the case owner and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/

Resource	Description	Type	URI
Final Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Final.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Open Cases Details	This query returns case information for cases where the stage is not closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Follow-Up Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Follow-Up.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Open Cases by Associated Impact (Chart)	This query returns the number of open cases in the various associated impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Cases Open by Stage (Chart)	This query searches the cases for open cases and counts the number of them at each stage. Note: The stage for an open case is not Closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Cases Created Today	This query returns all cases created so far today that are not system cases.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Queued Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Queued.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
All Cases	This query returns the name, creator, ticket type, stage, security classification, and consequence severity, ordered by ticket type and stage, of all cases that are not system cases.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Open Cases by Consequence Severity (Chart)	This query returns the number of open cases in the various consequence severity ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Initial Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Initial.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Average Time to Case Resolution - By Severity	This query returns the consequence severity and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Cases per Target	This query retrieves the attack target, name, stage, security classification, and consequence severity, ordered by stage, of all cases that are not system cases.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/

Resource	Description	Type	URI
Average Time to Case Resolution - By Day	This query returns the day of the week and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Maximum Time to Case Resolution - By User	This query returns case statistics for cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Open Cases by Operational Impact (Chart)	This query returns the number of open cases in the various operational impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Trend on Case Audit Events	This query collects Time to Resolution (TTR) information from case audit events and stores them in a trend for case history reporting.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/
Maximum Time to Case Resolution - By User Chart	This query returns case statistics for cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Open Cases	This query returns the name, creator, ticket type, stage, security classification, consequence severity, create time, modification time and attack target, ordered by ticket type and stage, of all cases that are not system cases and not in the Closed Stage.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Tracking	This session list contains case history information, monitoring the changes of the attributes in a case as it flows through investigation and analysis.	Session List	ArcSight Express/Operations/Case Tracking and Escalation/
Case History Data	This trend stores case information from audit events resulting from case audit events for case history reporting.	Trend	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/

Configuration Changes

The Configuration Changes use case contains resources for monitoring configuration changes made in your environment.

Resources

The following table lists all the resources explicitly assigned to the Configuration Changes use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-3 Resources that Support the Configuration Changes Use Case

Resource	Description	Type	URI
Monitor Resources			
Configuration Changes Overview	This dashboard shows an overview of the successful configuration changes for databases, firewalls, VPNs, and network devices.	Dashboard	ArcSight Express/Devices/Cross-Device/
Host Problems Overview	This dashboard shows several data monitors that focus on host problem events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.	Dashboard	ArcSight Express/Operations/Configuration Changes/
Host Configuration Modifications	This dashboard shows three data monitors that focus on host configuration change events. The two Top Value Counts (Bucketized) data monitors show charts of the event counts by zone or the most common events. The Last N Events data monitor shows the last 20 events.	Dashboard	ArcSight Express/Operations/Configuration Changes/
User Configuration Modifications - Today	This query viewer shows configuration modification events related to users for the current day.	Query Viewer	ArcSight Express/Operations/Configuration Changes/
User Configuration Modifications - Yesterday	This query viewer shows configuration modification events related to users for the previous day.	Query Viewer	ArcSight Express/Operations/Configuration Changes/
Host Configuration Modifications - Today	This query viewer displays host related configuration modification events since midnight of the current day.	Query Viewer	ArcSight Express/Operations/Configuration Changes/

Resource	Description	Type	URI
Host Configuration Modifications - Yesterday	This query viewer displays host related configuration modification events since midnight of the previous day.	Query Viewer	ArcSight Express/Operations/Configuration Changes/
Configuration Changes by User	This report shows recent configuration changes grouped by user and type, and sorted chronologically. Use this report to find all the configuration changes made by a specific user.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Host Configuration Modifications by OS	This report shows the host configuration modifications by operating system.	Report	ArcSight Express/Operations/Configuration Changes/
Configuration Changes by Type	This report shows recent configuration changes, grouped by type and user, and sorted chronologically. Use this report to find all configuration changes of a certain type.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Password Changes	This report shows password changes for the previous day and groups the password changes by user, sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
By User Account - Accounts Created	This report generates a table of all user accounts created in the last day.	Report	ArcSight Express/Devices/Cross-Device/User Change Tracking/
Library Resources			
Operating System	This is a site asset category.	Asset Category	Site Asset Categories
Last 10 Firewall Configuration Changes	This data monitor shows the last ten successful firewall configuration changes.	Data Monitor	ArcSight Express/Operations/Configuration Changes/Configuration Changes Overview/
Last 10 Database Configuration Changes	This data monitor shows the last ten successful database configuration changes.	Data Monitor	ArcSight Express/Operations/Configuration Changes/Configuration Changes Overview/
Most Common Host Configuration Change Events	This data monitor displays the top ten most common host configuration changes. By default, the data monitor displays a pie chart.	Data Monitor	ArcSight Express/Operations/Configuration Changes/Host Configuration Modifications/
Last 10 VPN Configuration Changes	This data monitor shows the last ten successful VPN configuration changes.	Data Monitor	ArcSight Express/Operations/Configuration Changes/Configuration Changes Overview/

Resource	Description	Type	URI
Last 20 Host Problems	This data monitor shows the last 20 host issues noted by ArcSight. This data monitor is used in the Host Problems Overview data monitor.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Host Problems Overview/
Host Problem Event Counts by Zone	This data monitor shows host-specific problems noted by ArcSight, by zone. By default this data monitor displays a pie chart of the top ten zones by problem event volume.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Host Problems Overview/
Last 10 Network Configuration Changes	This data monitor shows the last ten successful configuration changes on network devices.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Configuration Changes Overview/
Host Configuration Change Event Counts by Zone	This data monitor displays the top ten zones with configuration changes. By default, the data monitor displays a pie chart.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Host Configuration Modifications/
Most Common Host Problem Events	This data monitor shows the top ten most common problems seen on your monitored hosts.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Host Problems Overview/
Last 20 Host Configuration Modification Events	This data monitor displays the last 20 host configuration events seen by the system. Events are noted by customer, system, and reporting device in addition to the change type information.	Data Monitor	ArcSight Express/ Operations/Configuration Changes/Host Configuration Modifications/
TargetHost	This variable returns available target information from an event. The format of the information is targetZoneName. <targetHostName> <targetAddress>:<targetPort> Information that is not in the event will not show a place-holder. Examples: RFC1918: 192.168.0.0-192.168.255.255 Itwiki.sv.arcsight.com 192.168.10.20:80 RFC1918: 192.168.0.0-192.168.255.255 192.168.10.30:53 RFC1918: 192.168.0.0-192.168.255.255:53 192.168.10.30:53 unknown	Global Variable	ArcSight Foundation/Variables Library/Host Information/
DeviceInfo	This variable returns the device information, including the device vendor, the device product, and the device version, if available within the event. The format is deviceVendor. <deviceProduct> or <deviceVendor> <deviceProduct> v. <deviceVersion>	Global Variable	ArcSight Foundation/Variables Library/

Resource	Description	Type	URI
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Network Events	This filter identifies events with the category object starts with Network or the category device group starts with Network Equipment.	Filter	ArcSight Express/Devices/Network/
Configuration Modifications	This filter identifies configuration modifications on any system or device. This resource is a part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Host Problems	This filter identifies host-related problems and errors. This filter is part of the Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Network Configuration Changes	This filter identifies successful configuration change events that match the Network Events filter.	Filter	ArcSight Express/Devices/Network/
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Successful Password Changes	This filter selects events related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of success.	Filter	ArcSight Express/Devices/Cross-Device/
Target Zone AND Host are NULL but Address is NOT NULL	This filter identifies events in which either the target zone or target address field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Database Events	This filter identifies events with the category object /Host/Application/Database.	Filter	ArcSight Express/Devices/Database/

Resource	Description	Type	URI
All Device Information is NULL	This filter identifies events in which there is no device information, meaning that the device vendor, device product, and device version fields are all NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor OR Product is NULL	This filter identifies events in which the device vendor or device product field is NULL, but not both.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Device Vendor AND Product are NULL	This filter identifies events in which the device vendor and device product fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/
Target Zone AND Host are NULL	This filter identifies events in which the target zone and target host name fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Successful Configuration Changes	This filter identifies events in which the category behavior is /Modify/Configuration and the category outcome is Success.	Filter	ArcSight Express/Devices/Cross-Device/
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Express/Devices/Firewall/
Firewall Configuration Changes	This filter identifies successful configuration change events that match the Firewall Events filter.	Filter	ArcSight Express/Devices/Firewall/
Target Information is NULL	This filter identifies events in which the target zone, target host name, and target address fields are NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
Target Port is NULL	This filter identifies events in which the target port field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Device Version is NULL	This filter identifies events in which the device product field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Device/

Resource	Description	Type	URI
VPN Configuration Changes	This filter identifies successful configuration change events that match the VPN Events filter.	Filter	ArcSight Express/Devices/VPN/
Host Configuration Modifications	This filter provides a more focused subset of configuration modification events for use when monitoring or reporting on host-specific configuration changes. This filter is a part of the host-specific Configuration Monitoring content.	Filter	ArcSight Express/Devices/Cross-Device/
Target Zone OR Host is NULL	This filter identifies events in which either the target zone or target host name field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Database Configuration Changes	This filter identifies successful configuration change events that match the Database Events filter.	Filter	ArcSight Express/Devices/Database/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
Host Configuration Modifications	This query retrieves host related configuration modification events since midnight of the current day.	Query	ArcSight Express/Operations/Configuration Changes/
Host Configuration Modifications by OS	This query retrieves host configuration modification data (restricted by the Host Configuration Modifications filter).	Query	ArcSight Express/Operations/Configuration Changes/
By User Account - Accounts Created	This query retrieves events meeting the conditions Category Behavior = /Authentication/Add and Category Outcome = /Success, selecting End Time, Target User Name, Attacker User Name, Name, Target Zone Name and Target Host Name for the By User Account - Accounts Created report.	Query	ArcSight Express/Devices/Cross-Device/
Password Changes	This query returns information related to successful password changes, defined as having the category behavior of /Authentication/Modify and the category outcome of Success.	Query	ArcSight Express/Devices/Cross-Device/
User Configuration Modifications	This query returns the previous day of configuration modification events related to users.	Query	ArcSight Express/Operations/Configuration Changes/
Configuration Changes	This query returns all the successful configuration changes made to devices. The query returns the name, the user, the device, and the time the change was made.	Query	ArcSight Express/Devices/Cross-Device/

Logins

The Logins use case contains resources for monitoring logins to the systems in your environment.

Resources

The following table lists all the resources explicitly assigned to the Logins use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-4 Resources that Support the Logins Use Case

Resource	Description	Type	URI
Monitor Resources			
Microsoft-Auth entication	This active channel displays authentication events from Microsoft products.	Active Channel	ArcSight Express/Devices/
Login Information	This dashboard displays an overview of logins, both failures and successes, for privileged and non-privileged accounts.	Dashboard	ArcSight Express/
Successful Logins by User	This report shows successful authentication events by user. A chart shows the top users with the most successful login attempts. A table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Login Event Audit	This report shows all the successful and failed login events in a table sorted chronologically.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user. A chart shows the top ten users with failed login attempts. A table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Login Attempts	This report shows the count of authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Failed Logins by Destination Address	This report shows failed logins by destination address. A chart shows the top ten destinations with the most failed logins. A table lists all failed logins grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address. A chart shows the top ten source addresses with failed login attempts. A table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Successful Logins by Source Address	This report shows all successful authentication events by source address. A chart shows the top ten sources. A table shows all successful events, grouped by source.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Login Errors by User	This report shows a summary of the operating system login errors by username. A chart shows the top ten users with failed logins. A table shows details of the failed logins for each username (time, event name, source, destination).	Report	ArcSight Express/Devices/Operating System/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address. A chart shows the top ten destination addresses with successful login attempts. A table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Devices/Cross-Device/Login Tracking/
Library Resources			
Non-Root-Adm in Failed Logins	This data monitor tracks the number of failed non-privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Non-Root-Adm in Logins	This data monitor tracks the number of successful non-privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Root-Admin Logins	This data monitor tracks the number of successful privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Root-Admin Failed Logins	This data monitor tracks the number of failed privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Microsoft	This field set displays useful fields for evaluating events from Microsoft products.	Field Set	ArcSight Express/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight Express/

Resource	Description	Type	URI
Root-Admin Failed Logins	This filter identifies failed login events where the user name is root or administrator.	Filter	ArcSight Express/Security and Threat/
Root-Admin Logins	This filter identifies login events where the user name is root or administrator.	Filter	ArcSight Express/Security and Threat/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Non-Root-Admin Failed Logins	This filter identifies failed logins to accounts that are not named root or administrator.	Filter	ArcSight Express/Security and Threat/
Non-Root-Admin Logins	This filter identifies login events that are not logins to root or administrator named accounts.	Filter	ArcSight Express/Security and Threat/
Successful Logins by Source Address (Chart)	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Source Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by source address.	Query	ArcSight Express/Devices/Cross-Device/
Login Event Audit	This query returns all the successful and failed login attempts. The query returns the source and destination addresses, hostnames, zones, user name, device group, and outcome.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Destination Address (Chart)	This query returns authentication failure events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login Attempts (Chart)	This query returns the count of authentication failures from login attempts by hour.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login by User (Chart)	This query returns the count of failed login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Failed Logins by Source-Destination Pair	This query returns authentication failure events from login attempts. The query returns the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	ArcSight Express/Devices/Cross-Device/
Failed Login Attempts	This query returns all authentication failures from login attempts.	Query	ArcSight Express/Devices/Cross-Device/

Resource	Description	Type	URI
Successful Logins by Source-Destination Pair	This query returns authentication success events from login attempts.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User	This query returns users with successful login attempts. The query returns the user name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Cross-Device/
Successful Login by User (Chart)	This query returns the count of successful login attempts per user.	Query	ArcSight Express/Devices/Cross-Device/
Login Errors by User	This query returns operating system login errors. The query returns the user name, event name, source and destination addresses, hostnames, and zones.	Query	ArcSight Express/Devices/Operating System/
Failed Login by User	This query returns users with failed login attempts. The query returns the user name, source and destination addresses, hostnames, zones, and the device group.	Query	ArcSight Express/Devices/Cross-Device/
Login Errors by User (Chart)	This query returns the count of operating system login errors by username.	Query	ArcSight Express/Devices/Operating System/
Successful Logins by Destination Address (Chart)	This query returns authentication success events from login attempts, including the count of failed login attempts by destination address.	Query	ArcSight Express/Devices/Cross-Device/

System Notifications and Escalation

The System Notifications and Escalation use case monitors the response to incident notifications generated by the system.

Resources

The following table lists all the resources explicitly assigned to the System Notifications and Escalation use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-5 Resources that Support the System Notifications and Escalation Use Case

Resource	Description	Type	URI
Monitor Resources			
Notification Events	This active channel shows notification audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/System Notifications and Escalation/
Notifications By Acknowledgment Status	This report displays a chart and a table showing the counts of the notifications created yesterday, by acknowledgment, status, and ArcSight severity.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Unacknowledged Level 3 Notifications	This report displays a table showing all the notifications by ArcSight severity groups responsible for them (including creation times and the notification (destination) that have not been acknowledged and are at escalation level 3.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Statistics Summary	This report shows three charts and a table. Two of the three charts show notifications by escalation level and acknowledgement status, the third shows notifications with an escalation level of 3 and the destination groups to which they were sent. The table shows notification details, such as the destination group, the escalation level, acknowledgement status, and the creation time and notification event name.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Overview	This report displays a chart showing the number of notifications, grouped by ArcSight severity, at each escalation level.	Report	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
All Level 3 Notifications	This report displays a table showing the event name, group name, create time, and ArcSight severity of all notifications with escalation level 3.	Report	ArcSight Foundation/Workflow/Details/
Notification Status Report	This report displays a table showing the notifications generated for each notification (Destination) group, including the notification creation time, escalation level, and acknowledgement status.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Library Resources			
Notifications	This field set tracks events related to the sending and acknowledgement of notifications.	Field Set	ArcSight Express/Active Channel/
Notification	This field set tracks events related to the sending and acknowledgement of notifications.	Field Set	ArcSight Express/Inspect - Edit/
Notification Event has Rule Name	This filter identifies notification events that have a Device Custom String 3 label set as Rule Name.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has User Name	This filter identifies notification events that have an attacker user name to represent the user who acknowledged or resolved a notification.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Destination Group	This filter identifies notification events that have a Device Custom String 4 label set as Group.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Configuration Resource	This filter identifies notification events that have a Device Custom String 2 label set as Configuration Resource.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Acknowledgement Status	This filter identifies notification events that have a Device Custom String 6 label set as Acknowledgement Status.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Events	This filter identifies events that are related to sending and acknowledging notifications.	Filter	ArcSight Foundation/Workflow/System Notifications and Escalation/
Notifications By Acknowledgement Status	This query returns the acknowledgement status, ArcSight severity, and the number of notifications (count of Notification ID), for all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Overview	This query returns the escalation level, ArcSight severity, and the number of notifications (count of Notification IDs), ordered by escalation level and ArcSight severity, of all notifications.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications Overview Chart	This query retrieves notification information (the destination group, severity, and count), for all notifications with an escalation level of 3.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Unacknowledged Level 3 Notifications	This query returns the event name, create time, ArcSight severity and group name, of all notifications with an escalation level of 3 and an acknowledgement status that is neither Acknowledged or Resolved.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications By Acknowledgement Status Chart	This query returns the acknowledgement status, ArcSight severity, and number of notifications (count of Notification ID), of all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/
All Level 3 Notifications	This query returns the event name, group name, create time, escalation level, and ArcSight severity, ordered by creation time, of all notifications with an escalation level of 3.	Query	ArcSight Foundation/Workflow/Details/
Notification Status Report	This query returns the group name, event name, creation time, escalation level, and acknowledgement status, ordered by the creation time, for all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Traffic Monitoring

The Traffic Monitoring use case contains resources for monitoring traffic in your environment.

Resources

The following table lists all the resources explicitly assigned to the Traffic Monitoring use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 8-6 Resources that Support the Traffic Monitoring Use Case

Resource	Description	Type	URI
Monitor Resources			
Traffic Moving Average	This dashboard shows a moving average of the ICMP, SYN, and UDP traffic. The dashboard contains three data monitors: Traffic Moving Average (ICMP), Traffic Moving Average (SYN), and Traffic Moving Average (UDP).	Dashboard	ArcSight Express/Operations/Traffic Monitoring/
Traffic Monitoring	This dashboard shows well-known port activity for sources and destinations outside the United States.	Dashboard	ArcSight Express/
Traffic Statistics	This report displays the bytes in and out by hour, and bytes in and out by device. A table shows the hour, firewall zone and address, the transport protocol, and the bytes in and out.	Report	ArcSight Express/Operations/Traffic Monitoring/
Inbound Traffic - Top Protocols	This report shows an operational summary of the inbound traffic usage by protocol.	Report	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Utilization - Last Hour	This report shows the bandwidth utilization for the last hour. A chart has two sets of values. The first set shows the number of bytes per second for the inbound traffic and the second set shows the number of bytes per second for the outbound traffic.	Report	ArcSight Express/Operations/Traffic Monitoring/
Traffic Snapshot	This report shows the top ten protocols, top ten attackers, and top ten targets.	Report	ArcSight Express/Operations/Traffic Monitoring/
Inbound Traffic - Top Source Hosts	This report shows an operational summary of the inbound traffic usage by source hosts.	Report	ArcSight Express/Operations/Traffic Monitoring/
Outbound Traffic - Top Source Hosts	This report shows an operational summary of the outbound traffic usage by source hosts.	Report	ArcSight Express/Operations/Traffic Monitoring/

Resource	Description	Type	URI
Bandwidth Utilization - Last 24 Hours	This report displays the bandwidth utilization for the last 24 hours. The first chart shows the number of bytes per second for inbound traffic and the second chart shows the number of bytes per second for outbound traffic.	Report	ArcSight Express/Operations/Traffic Monitoring/
Outbound Traffic - Top Protocols	This report shows an operational summary of the outbound traffic usage by protocol.	Report	ArcSight Express/Operations/Traffic Monitoring/
Library - Correlation Resources			
High Number of Denied Connections for A Source Host	This rule detects firewall deny events. The rule triggers when ten events originating from the same source host occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Connections	This rule detects firewall accept events for MSSQL, Terminal Services, and TFTP connections (default destination ports: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule triggers when ten events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
High Number of Denied Inbound Connections	This rule detects inbound firewall deny events. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Operations/Traffic Monitoring/
Library Resources			
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight Express/Tuning
Top Non-US Sources	This data monitor displays the top events and country codes for events originating outside the United States.	Data Monitor	ArcSight Express/Operations/Traffic Monitoring/
Top Non-US Sources - Graph	This data monitor displays events originating from systems outside the United States.	Data Monitor	ArcSight Express/Operations/Traffic Monitoring/
Traffic Moving Average (TCP)	This data monitor shows a moving average of the incoming UDP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/

Resource	Description	Type	URI
Traffic Moving Average (SYN)	This data monitor shows a moving average of the incoming SYN traffic (TCP connection requests) per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
Traffic Moving Average (ICMP)	This data monitor shows a moving average of the incoming ICMP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
Top Non-US Destinations - Graph	This data monitor shows events to destinations outside the United States.	Data Monitor	ArcSight Express/Operations/Traffic Monitoring/
Top Non-US Destinations	This data monitor displays the top destinations outside the United States.	Data Monitor	ArcSight Express/Operations/Traffic Monitoring/
Traffic Moving Average (UDP)	This data monitor shows a moving average of the incoming UDP traffic per minute for the last hour using 12 five-minute buckets.	Data Monitor	ArcSight Foundation/Network Monitoring/General/Traffic Moving Average/
admindcert	This destination is pre-defined for the CERT team. Add more information, such as email addresses.	Destination	CERT Team/1
Firewall	This field set displays useful fields for evaluating events from various IDS devices.	Field Set	ArcSight Express/
SYN Traffic	This filter identifies SYN (TCP transaction request) traffic.	Filter	ArcSight Express/Devices/Network/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Top Non-US Destinations	This filter selects events using well-known ports to destinations outside the United States.	Filter	ArcSight Express/Security and Threat/
TCP Traffic	This filter identifies TCP traffic.	Filter	ArcSight Express/Devices/Network/
UDP Traffic	This filter identifies UDP traffic.	Filter	ArcSight Express/Devices/Network/
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

Resource	Description	Type	URI
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Top Non-US Sources	This filter identifies events using well-known ports that originate outside the United States.	Filter	ArcSight Express/Security and Threat/
Target Port is NULL	This filter identifies events in which the target port field is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Qosient Argus	This filter identifies events originating from Argus connectors.	Filter	ArcSight Express/Devices/Network/
Outbound Traffic	This filter detects Argus events originating inside the company network and targeting the outside network.	Filter	ArcSight Express/Operations/Traffic Monitoring/
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Inbound Events	This filter looks for events coming from outside the company network targeting the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Bandwidth to or from External Systems	This filter detects events in which the source or destination of the event is internal to the network (but one of them is external), and at least one of Bytes In or Bytes Out values is present.	Filter	ArcSight Express/Devices/Cross-Device/
Network Traffic Reporting Devices	This filter identifies your network traffic reporting devices. The default network traffic reporting device is QoSient Argus.	Filter	ArcSight Express/Devices/Network/
Inbound Traffic	This filter identifies Argus events originating from the outside network, targeting inside the company network.	Filter	ArcSight Express/Operations/Traffic Monitoring/
ICMP Traffic	This filter identifies ICMP traffic.	Filter	ArcSight Express/Devices/Network/
Top Protocols	This query returns the protocol with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Express/Operations/Traffic Monitoring/

Resource	Description	Type	URI
Outbound Traffic by Source Host	This query returns outbound events (internal network to external network) and groups them by attacker address and attacker zone. The query selects the attacker address, the attacker zone name, and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/
Outbound Traffic by Transport Protocol	This query returns outbound events (internal network to external network) and groups them by transport protocol. The query selects the transport protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/
Inbound Traffic by Transport Protocol	This query retrieves inbound events (external network to internal network) and groups them by transport protocol. The query returns the transport protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/
Inbound Traffic by Application Protocol	This query returns inbound events (external network to internal network) and groups them by application protocol. The query selects the application protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/
Top Attackers	This query returns the attacker address or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events in which the Bytes In, Bytes Out, and Target Port fields are not empty, and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Top Targets	This query returns the target address or zone with the highest number of total bytes (Bytes In + Bytes Out) within the last hour.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Utilization - By Hour	This query returns the average number of bytes in and bytes out per second for inbound and outbound traffic, and groups the values by hour.	Query	ArcSight Express/Operations/Traffic Monitoring/

Resource	Description	Type	URI
Top Bandwidth Hosts	This query identifies the count of TotalBytes (Bytes In + Bytes Out) for each host, and sorts them so that the hosts with the highest totals are reported first. The query identifies events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Inbound Traffic by Source Host	This query returns inbound events (external network to internal network) and groups them by attacker address and attacker zone. The query selects the attacker address, the attacker zone, and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/
Firewall Bandwidth Usage by Hour (chart)	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Utilization - By Minute	This query returns the average number of bytes in and bytes out per second for the inbound and outbound traffic and groups the values by minute.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Usage by Firewall Address	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/
Firewall Bandwidth Usage per Hour	This query returns firewall events.	Query	ArcSight Express/Operations/Traffic Monitoring/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour. The query looks for events in which the Bytes In and Bytes Out fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	ArcSight Express/Devices/Cross-Device/
Outbound Traffic by Application Protocol	This query retrieves outbound events (internal network to external network) and groups them by application protocol. The query returns the application protocol and the corresponding sums of Bytes In and Bytes Out.	Query	ArcSight Express/Operations/Traffic Monitoring/

Chapter 9

Security and Threat Use Cases

The Security and Threat resources monitor and report on the security of your environment, including malware and reconnaissance attacks.

The resources are grouped together using use cases, which help address a specific issue or function. The Security and Threat use cases are listed in the following table.

Use Case	Purpose
"Security and Threat" on page 279	The Security and Threat use case provides resources for monitoring common security events on a network.
"Vulnerabilities" on page 296	The Vulnerabilities use case provides several resources for monitoring security assessment and vulnerability activity.

Security and Threat

The Security and Threat use case provides resources for monitoring common security events on a network.

Configuration

ArcSight Express content is designed to find activity for which the staff of your security operations center should be notified. If a situation is a benign or routine condition in your environment, you can use the [Event-based Rule Exclusions](#) active list to store event situations considered to be low or no risk.

The entries in the [Event-based Rule Exclusions](#) active list are ignored by the rules that reference it. The entries list specific events from a specific source (attacker) address and zone to a specific destination (target) address and zone. Other events from the same device originating from a different source or to a different destination are not ignored. Add to this list any events that occur very frequently between two systems, causing a rule to fire too much. The [Event-based Rule Exclusions](#) active list is referenced by the following event-based rules:

- [High Number of IDS Alerts for DoS](#)
- [SYN Flood Detected by IDS or Firewall](#)
- [High Number of IDS Alerts for Backdoor](#)

For information about how to add entries to active lists, see the ArcSight Console User's Guide.

Resources

The following table lists all the resources explicitly assigned to the Security and Threat use case, and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 9-1 Resources that Support the Security and Threat Use Case

Resource	Description	Type	URI
Monitor Resources			
Vulnerability Events	This active channel shows events received during the last two hours that are associated with a known vulnerability. The active channel includes a sliding window that displays the last two hours of event data.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Vulnerability View/
Reconnaissance Activity	This active channel shows reconnaissance events received during the last two hours. The active channel includes a sliding window that displays the last two hours of event data.	Active Channel	ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
DoS Channel	This active channel shows events received during the last two hours and includes a sliding window that displays the last two hours of event data. The active channel uses its own filter to limit the view to Denial of Service related events where the Category Technique is /DoS, the Category Significance is /Compromise, the Category Outcome is /Success, and the event MatchesFilter(Internal Target) .	Active Channel	ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Anti-Virus Events	This active channel shows all the events coming from Anti-Virus Systems within the last two hours.	Active Channel	ArcSight Express/Devices/
Reconnaissance in Progress	This dashboard displays the Top 10 Zones Scanned, the Last 10 Zones Scanned, the Last 10 Hosts Scanned, and the Last 10 Scanners data monitors to give an overview of the reconnaissance activity against the network.	Dashboard	ArcSight Express/Security and Threat/
Security Activity Statistics	This dashboard displays an overview of common attackers, targets, protocols, and activity by time.	Dashboard	ArcSight Express/

Resource	Description	Type	URI
Security Activity	This dashboard displays an overview of security activity, including suspicious network activity, failed logins, and common attacks on the network.	Dashboard	ArcSight Express/
Worm Outbreak Overview	This dashboard provides a view of worm activity across the network.	Dashboard	ArcSight Express/Security and Threat/
Interesting Mail	This dashboard shows event information related to large email messages.	Dashboard	ArcSight Express/
Threat View	This dashboard displays information about events that have a High or Very High priority, or have been correlated.	Dashboard	ArcSight Express/
Malware	This dashboard displays information regarding events that can be correlated with malware activity.	Dashboard	ArcSight Express/
Login Information	This dashboard displays an overview of logins, both failures and successes, for privileged and non-privileged accounts.	Dashboard	ArcSight Express/
Top Infected Systems	This report displays summaries of the systems reporting the most infections during the previous day.	Report	ArcSight Express/Devices/Anti-Virus/
Security Intelligence Status Report	This report displays four charts and six tables. The first chart gives an hourly breakdown of the event counts by agent severity. The three tables below the Event Count by Agent Severity chart show the top events, top attacks and top triggering rules. The three charts below the tables show the top attackers, top targets, and top target ports. The three tables at the bottom of the page show the number of cases added and notifications sent, along with a list of assets and the vulnerabilities used to compromise them.	Report	ArcSight Express/
Virus Activity by Time	This report displays malware activity by hour for the previous day by hour and priority.	Report	ArcSight Express/Devices/Anti-Virus/

Resource	Description	Type	URI
Library - Correlation Resources			
Worm Outbreak Detected	This rule is looking for both the Possible Network Sweep rule to trigger and the Target Port Activity by Attacker data monitor to trigger a correlation event that indicates an increase in target port activity by one attacker of more than 100%. Joining the attackers and target ports from these two correlation events determines that the attacker has shown an increase in target port traffic to multiple hosts, not just a two-way communication with a single host. This behavior is indicative of a worm infected system.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/
Blaster DDOS From Infected Host	This rule detects a Distributed Denial Of Service (DDOS) attack (Blaster) originating from an infected host. This rule detects DoS events targeting a windowsupdate.com host, either coming from a host in the Attackers/Untrusted List active list or from a host in the Targets/Compromised List active list. This means that a compromised target could be acting as an attacker. In this case, this host is infected. This rule only requires one such event, and the time frame is set to two minutes. After this rule is triggered, the categoryOutcome field is set to Success and the categorySignificance field is set to Hostile.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/
High Number of IDS Alerts for DoS	This rule detects Denial of Service (DoS) alerts from Intrusion Detection Systems (IDS). The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/DoS/

Resource	Description	Type	URI
Blaster Infected Host	This rule detects infected hosts by a Blaster worm. This rule looks for two events. The first event, the ExploitEvent, targets one of the following ports: 135, 139 or 445. The second event, the TftpEvent, targets the port 69 and uses UDP. Neither event comes from a host in the Attackers/Trusted List active list. To have a matching event, the Attacker-Target pair in the first event must match the swapped Target-Attacker pair in the second event. This rule requires one matching occurrence, and the time frame is set to two minutes. On the first occurrence, a notification is sent to the Analysts, the target of ExploitEvent is added to the Worm Infected Systems active list. The correlation event from the rule triggering is caught by the Hostile - Success rule.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/
SYN Flood Detected by IDS or Firewall	This rule detects SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/DoS/
Notify on Successful Attack	This rule detects successful attacks. This rule looks for high priority (≥ 8) successful attacks for which the attacker is not in the Attackers/Trusted list. This rule only requires one such event, and the time frame is set to ten minutes. After this rule is triggered, a notification is sent to the CERT team. The action to create a new case is available, but is disabled by default.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/
Possible Internal Network Sweep	This rule detects a single host trying to communicate with at least ten other hosts on the same target port within the network, within a minute. This rule, combined with a spike in target port activity by the same host, results in the worm outbreak detected rule being triggered.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/

Resource	Description	Type	URI
Possible Outbound Network Sweep	This rule detects a single host trying to communicate with at least ten other hosts on the same target port outside the network within a minute. This rule, combined with a spike in target port activity by the same host, results in the worm outbreak detected rule being triggered.	Rule	Real-time Rules/Intrusion Monitoring/Worm Outbreak/
High Number of IDS Alerts for Backdoor	This rule detects backdoor alerts from Intrusion Detection Systems (IDS). The rule triggers when 20 events from the same device occur within two minutes.	Rule	ArcSight Express/Security and Threat/Attack Monitoring/Malware Activity/
Library Resources			
Compromised List	This resource has no description.	Active List	ArcSight System/Threat Tracking
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from one system to another system that has been determined to be not relevant to the rules that would otherwise trigger on these events.	Active List	ArcSight Express/Tuning
Worm Infected Systems	This active list is automatically populated by rules that have detected worm activity on a given system.	Active List	ArcSight Express/Security and Threat/Worm Outbreak/
Untrusted List	This active list is to be manually populated with the addresses of known malicious systems.	Active List	ArcSight System/Attackers
Address Spaces	This is a site asset category.	Asset Category	Site Asset Categories
Email	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Domain Name Server	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces
Proxy	This is a site asset category.	Asset Category	Site Asset Categories/Application/Type

Resource	Description	Type	URI
Top Attacker IPs	This data monitor shows the counts of attack events and groups them by attacker IP address.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Malware Real-Time Tracking	This data monitor displays information from outbound events that use non-well known ports (destination port is > 1024). Initiation of connections with high port numbers can be correlated with malware activity.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Malware/
Events per Address Space	This data monitor shows the count of events for each type of address space, such as public, private, and so on.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Correlated Events	This data monitor displays the last ten correlated events generated by a rule.	Data Monitor	ArcSight Express/Security and Threat/Threat View/
Most Frequent Ports	This data monitor shows the top target ports recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/Cross-Device/
Last 10 Zones Scanned	This data monitor shows the time and the target zone of the last ten reconnaissance events, providing an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Root-Admin Logins	This data monitor tracks the number of successful privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Application Protocol Event Counts	This data monitor tracks the application protocol events by customer resource. The data monitor updates every 30 seconds. It uses 12 samples of five-minute intervals, for a time range of one hour. The data monitor requires a minimum of ten events to maintain a group (aggregated event counts are used when available).	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Recent Events	This data monitor shows the last 15 significant events.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Trojaned Machines	This data monitor shows the top systems exhibiting behavior of being compromised with a trojan system permitting inappropriate access by unauthorized users.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/

Resource	Description	Type	URI
Last 10 Scanners	This data monitor shows the attacker zone and address, along with the time, of the last ten reconnaissance events to give an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Reconnaissance/ Reconnaissance in Progress/
Last 10 Hosts Scanned	This data monitor shows the target zone and address, along with the time, of the last ten reconnaissance events, providing an overview of the most recent scanning activity against specific hosts.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Reconnaissance/Reco naissance in Progress/
Top 10 Users with Failed Logins	This data monitor shows users with the most failed login activity.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Security Activity/
Worm Infected Systems	This data monitor displays the status of systems that have been infected in the course of a worm outbreak.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Worm Outbreak/Worm Outbreak/
Outbound Mail over 20MB	This data monitor displays information about large, outbound email messages.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/User Tracking/ Interesting Mail/
Outbound High Port Traffic	This data monitor displays outbound event information using high ports. Use of high ports can be correlated with malware activity.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Virus/Malware/
Top Transport Protocols	This data monitor shows the top transport protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Express/Cisco Monitoring/Functionality/ Cross-Device/
Top Connectors	This data monitor provides a list of the top ten ArcSight SmartConnectors reporting events, minute-by-minute within the last 60 minutes, showing the connector name and ID (Agent Name and Agent ID fields), the total number of events reported, and a breakdown of the reported events by priority.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Worm Infected Machines	This data monitor shows the systems exhibiting the most worm-related traffic events.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/

Resource	Description	Type	URI
Top 10 Zones Scanned	This data monitor shows the target zone of the ten most frequent reconnaissance events within the last hour, providing an overview of the most recent scanning activity against the network.	Data Monitor	ArcSight Foundation/ Intrusion Monitoring/ Detail/Reconnaissance/ Reconnaissance in Progress/
Top Successful Attacks	This data monitor shows the top successful attack events.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Top Firewall Blocked Machines	This data monitor shows the systems with the most communication attempts blocked by a firewall.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Event Counts by Hour	This data monitor collects the count of events at each priority level for each hour for the last 24 hours.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
Last Failed Logins	This data monitor shows the last 15 failed logins.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Target Port Activity by Attacker	This data monitor is used in conjunction with the Worm Outbreak detected rule and the possible network sweep rule to detect worm outbreaks before an IDS signature is released.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Worm Activity Status	This data monitor shows the most recent events related to worm activity in the network zones.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Worm Outbreak/Worm Outbreak/
Root-Admin Failed Logins	This data monitor tracks the number of failed privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/ Login Information/
Very High Events	This data monitor displays the last ten events with a very high priority.	Data Monitor	ArcSight Express/Security and Threat/Threat View/
Top Target IPs	This data monitor shows the counts of attack events and groups them by the target IP address.	Data Monitor	ArcSight Express/Security and Threat/Security Activity Statistics/
High Events	This data monitor displays the last ten events with a high priority.	Data Monitor	ArcSight Express/Security and Threat/Threat View/
Port Monitor	This data monitor displays information about port activity and gives a status assessment for that port and zone based on the last event for that zone/port pair.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/

Resource	Description	Type	URI
Covert Channel	This data monitor displays event information indicating that there is a covert channel. Port 53 is a well-known port for DNS, but DNS activity is generally UDP. Such activity can be correlated with covert channels.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Malware/
Top Categories	This data monitor displays the top categories of web browser activity based on Blue Coat categories.	Data Monitor	ArcSight Foundation/Intrusion Monitoring/Detail/User Tracking/Blue Coat/
Non-Root-Admin Failed Logins	This data monitor tracks the number of failed non-privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Non-Root-Admin Logins	This data monitor tracks the number of successful non-privileged account logins.	Data Monitor	ArcSight Express/Operations/Logins/Login Information/
Standard	This field set contains several fields that are useful at a glance for selecting events for inspection. It uses the end time field for the timestamp.	Field Set	ArcSight Express/Active Channel/
IDS	This field set displays useful fields for evaluating events from various firewall devices.	Field Set	ArcSight Express/
Security	This field set contains several fields that are formatted to show more detailed information for security-related fields without needing to use the event inspector.	Field Set	ArcSight Express/Active Channel/
Virus Information	This field set displays useful fields for evaluating anti-virus events.	Field Set	ArcSight Express/
Vulnerability	This field set shows the following columns: End Time Name Attacker Address Target Address Priority Vulnerability Resource Device Vendor Device Product	Field Set	ArcSight Express/Active Channel/
Security Highlights	This field set is a modification to the Security field set with the custom Event Name field replaced with the (sortable) Name field.	Field Set	ArcSight Express/Active Channel/
ArcSight Express	This field set contains basic fields for reviewing events in an active channel to select which ones to investigate.	Field Set	ArcSight Express/

Resource	Description	Type	URI
Target Address is NULL	This filter is designed for conditional expression variables. The filter identifies events where the target address is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
Reconnaissance Events by Attacker	This filter identifies events where the attacker address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Express/Security and Threat/
Internal Source	This filter identifies events coming from inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Internal Target	This filter identifies events targeting inside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
All Events	This filter matches all events.	Filter	ArcSight System/Core
Worm Activity	This filter selects events related to all worm activity on a network.	Filter	ArcSight Express/Security and Threat/
Root-Admin Failed Logins	This filter identifies failed login events where the user name is root or administrator.	Filter	ArcSight Express/Security and Threat/
Internal to Internal Events	This filter retrieves events internal to the company network.	Filter	ArcSight Foundation/Common/Network Filters/Location Filters/
Backdoor Traffic	This filter selects events related to malware giving inappropriate access to a system.	Filter	ArcSight Express/Security and Threat/
Reconnaissance Events (Internal Targets)	This filter identifies events that match the Internal Target, Not Correlated and Not Closed and Not Hidden, and Non-ArcSight Internal Events filters and one or more conditions where the event name starts with Reconnaissance, the category significance is Recon, or the category technique starts with Scan. This is the foundation filter for the other Reconnaissance filters: Reconnaissance Events by Attacker, Reconnaissance Events by Target, and Reconnaissance Events by Target Zone.	Filter	ArcSight Express/Security and Threat/
Firewall Events	This filter retrieves events with the Firewall category device group.	Filter	ArcSight Express/Devices/Firewall/

Resource	Description	Type	URI
Failed Logins with Target Information	This filter selects events related to login failures where the target system information is available.	Filter	ArcSight Express/Security and Threat/
Top Non-US Destinations	This filter selects events using well-known ports to destinations outside the United States.	Filter	ArcSight Express/Security and Threat/
Large Mail-Outbound	This filter identifies email-related events (where the target port is 25), with an email size greater than 20,000 bytes.	Filter	ArcSight Express/Security and Threat/
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Root-Admin Logins	This filter identifies login events where the user name is root or administrator.	Filter	ArcSight Express/Security and Threat/
Very High Events	This filter selects all events with a priority of very high (9 or 10 out of 10).	Filter	ArcSight Express/Security and Threat/
Events with Vulnerabilities	This filter identifies events in which the vulnerability field has been populated. The vulnerability field is populated when an event that attempts to exploit the vulnerability targets an asset that has had that vulnerability reported by a security scanner.	Filter	ArcSight Express/Security and Threat/
Top Non-US Sources	This filter identifies events using well-known ports that originate outside the United States.	Filter	ArcSight Express/Security and Threat/
Non-Root-Admin Logins	This filter identifies login events that are not logins to root or administrator named accounts.	Filter	ArcSight Express/Security and Threat/
Malware-Outbound	This filter selects outbound events that use non-well known ports (the destination port is greater than 1024). Initiation of connections with high port numbers can be correlated with malware activity.	Filter	ArcSight Express/Security and Threat/

Resource	Description	Type	URI
Not Correlated and Not Closed and Not Hidden	This filter selects events that have not had their event annotation flags set to correlated (by a rule), close (by an analyst) or hidden (by system settings).	Filter	ArcSight System/Event Types
Anti-Virus Events	This filter identifies events in which the category device group is /IDS/Host/Antivirus.	Filter	ArcSight Express/Devices/Anti-Virus/
Failed Logins	This filter selects events related to failed login attempts, defined as having a category behavior of /Authentication/Verify and a category outcome of /Failure.	Filter	ArcSight Express/Security and Threat/
Non ArcSight Internal Event with TargetPort Set	This filter identifies events that have a category significance entry and a target port.	Filter	ArcSight Express/Security and Threat/
Target Port Activity By Attacker	This filter selects events where the source address is available, the target (destination) port is available but is not the ArcSight port (8443), and the source is not a DNS, email, or proxy server.	Filter	ArcSight Express/Security and Threat/
Worm Outbreak	This filter retrieves events with the name Worm Outbreak Detected and type Correlation.	Filter	ArcSight Express/Security and Threat/
Reconnaissance Events by Target	This filter identifies events where the target address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Express/Security and Threat/
Reconnaissance Events by Target Zone	This filter identifies events where the target zone is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	ArcSight Express/Security and Threat/
Correlated Events	This filter identifies events that have been correlated by a rule.	Filter	ArcSight Express/Security and Threat/
Covert Channels TCP port 53	This filter selects events indicating that there is a covert channel. Port 53 is a well-known port for DNS, but DNS activity is generally UDP. Such activity can be correlated with covert channels.	Filter	ArcSight Express/Security and Threat/
Target Host Name is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Host Name is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/

Resource	Description	Type	URI
ASM Events	This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment).	Filter	ArcSight System/Event Types
AV - Found Infected	This filter identifies all events where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Success, and the Category Behavior is /Found/Vulnerable.	Filter	ArcSight Express/Devices/Anti-Virus/
Non ArcSight Internal Event - Target Port Not Null	This resource has no description.	Filter	ArcSight Express/Security and Threat/
Target Zone is NULL	This filter is designed for conditional expression variables. The filter identifies events where the Target Zone is NULL.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Host/
High Events	This filter selects events with a high priority (7 or 8 out of 10).	Filter	ArcSight Express/Security and Threat/
Attack Events	This filter identifies events where the category significance starts with Compromise or Hostile.	Filter	ArcSight Express/Security and Threat/
External Source	This filter identifies events originating from outside the company network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Non-Root-Admin Failed Logins	This filter identifies failed logins to accounts that are not named root or administrator.	Filter	ArcSight Express/Security and Threat/
ArcSight Events	This filter captures all events generated by ArcSight, including events generated by ArcSight SmartConnectors. These events include system monitoring and health events, correlation events from rules, and data monitors. Note: Data from devices collected by SmartConnectors is not included.	Filter	ArcSight System/Event Types
IDS -IPS Events	This filter identifies Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	ArcSight Express/Devices/IDS - IPS/

Resource	Description	Type	URI
ArcSight Internal Events	This filter selects events that are internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
Non-ArcSight Internal Events	This filter selects events that are not internal events generated by the ArcSight ESM system.	Filter	ArcSight System/Event Types
External Target	This filter identifies events targeting the outside network.	Filter	ArcSight Foundation/Common/Network Filters/Boundary Filters/
Worm Traffic	This filter selects events related to successful worm activity on a network.	Filter	ArcSight Express/Security and Threat/
Successful Attacks	This filter detects events that have a significance of Compromise or Hostile, and an outcome of Success.	Filter	ArcSight Express/Security and Threat/
Non-ArcSight Events	This filter captures all events that are not generated by ArcSight or ArcSight SmartConnectors.	Filter	ArcSight System/Event Types
SIS-Top Firing Rules Table Query	This query returns the event name and sums the aggregated event count where the type is Correlation for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
Infected Systems	This query identifies data matching the AV - Found Infected filter where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable.	Query	ArcSight Express/Devices/Anti-Virus /Top Infected Systems/
Virus Activity by Hour	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Express/Devices/Anti-Virus /Virus Activity by Time/
SIS-Top Attacks Table Query	This query returns the event name and sums the aggregated event count for events that have a category significance of Compromise or Hostile, for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/

Resource	Description	Type	URI
SIS-Assets Compromised Table Query	This query returns the target asset name, vulnerability external ID (the vulnerability name), and a sum of the number of events reported for that asset/vulnerability pair for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
SIS-Top Attackers Chart Query	This query returns the attacker zone name, attacker address, and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
SIS-Event Count by Agent Severity Chart Query	This query returns the date, agent severity, and the number of events for each agent severity level for that day/hour for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
SIS-Cases Added Table Query	This query returns the stage, consequence severity, and a count of the cases with that pairing for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
Top Infected Systems	This query identifies data matching the AV - Found Infected filter (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is Success, and the Category Behavior is /Found/Vulnerable).	Query	ArcSight Express/Devices/Anti-Virus /Top Infected Systems/
SIS-Top Events Table Query	This query returns the event name and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
SIS-Top Targets Chart Query	This query returns the target zone name, target address, and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
SIS-Notifications Sent Table Query	This query returns the group name, escalation level, acknowledgement status, and a count of the notifications for these conditions for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/

Resource	Description	Type	URI
SIS-Top Target Ports Chart Query	This query returns the target port and sums the aggregated event count for use in the Security Intelligence Status Report.	Query	ArcSight Express/Security and Threat/Security Intelligence Status Report/
Security Intelligence Status Template	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	ArcSight Express/Security and Threat/Security Intelligence Status Template/

Vulnerabilities

The Vulnerabilities use case provides several resources for monitoring security assessment and vulnerability activity.

Resources

The following table lists all the resources explicitly assigned to the Vulnerabilities use case and includes dependent resources. Dependent resources are not listed in a use case resource.

Table 9-2 Resources that Support the Vulnerabilities Use Case

Resource	Description	Type	URI
Monitor Resources			
Exposed Vulnerabilities by Asset	This report shows a table of exposed vulnerabilities by asset.	Report	ArcSight Express/ Security and Threat/ Vulnerabilities/
Exposed Vulnerability Count by Asset	This report lists the count of vulnerabilities per asset and the ten assets with the most exposed vulnerabilities.	Report	ArcSight Express/ Security and Threat/ Vulnerabilities/
Library - Correlation Resources			
Warning - Vulnerable Software	This rule detects vulnerable software. The rule triggers whenever a vulnerable application or operating system is found. The vulnerability should not be a scan vulnerability. On the first event, a notification is sent to SOC operators.	Rule	Real-time Rules/ Configuration Monitoring/ Detail/Vulnerabilities/
Warning - Insecure Configuration	This rule detects insecure object configuration. The rule triggers whenever an insecure object is found or a security check fails. On the first event, a notification is sent to SOC operators.	Rule	Real-time Rules/ Configuration Monitoring/ Detail/Vulnerabilities/
Library Resources			
Trusted List	This active list is to be manually populated with the addresses of trusted systems that are typically used for security scanning.	Active List	ArcSight System/Attackers
Address Spaces	This is a site asset category.	Asset Category	Site Asset Categories
Criticality	This is a system asset category.	Asset Category	System Asset Categories
High	This is a system asset category.	Asset Category	System Asset Categories/Criticality
Protected	This is a site asset category.	Asset Category	Site Asset Categories/Address Spaces

Resource	Description	Type	URI
Exposed Vulnerability Count by Critical Asset	This report shows a table of exposed vulnerabilities on assets categorized as high criticality.	Focused Report	ArcSight Express/Security and Threat/Vulnerabilities/
Exposed Vulnerability Count by Asset	This query counts the vulnerabilities for each asset that is categorized under /All Asset Categories/System Asset Categories/Criticality.	Query	ArcSight Express/Devices/Vulnerabilities/
Top 10 Assets by Exposed Vulnerability Counts	This query counts the vulnerabilities for each asset that is categorized under /All Asset Categories/System Asset Categories/Criticality and returns the ten assets with with most vulnerabilities.	Query	ArcSight Express/Devices/Vulnerabilities/
Exposed Vulnerabilities by Asset	This query lists the vulnerabilities for each asset, up to 10,000 asset/vulnerability tuples.	Query	ArcSight Express/Devices/Vulnerabilities/

Index

A

- Accepted Inbound Connections filter 150
- Accepted Outbound Connections filter 149
- Access Points dashboard 119
- Account Added to Privileged Group rule 212
- Account Locked Out Multiple Times in 24 Hours rule 214
- Account Locked Out rule 213
- Account Management dashboard 208
- Account Management use case 206
- Account Removed from Privileged Group rule 211
- Accounts Locked Out Multiple Times in 24 Hours session list 220
- active channels
 - Alert Events from Cisco IOS IPS Systems 97
 - Alert Events from Cisco IPS Sensor Systems 91
 - Alert Events from Cisco IPS Systems 84
 - Alert, Critical and Error Events from Cisco ASA Systems 40
 - Alert, Critical and Error Events from Cisco Firewall Systems 71
 - Alert, Critical and Error Events from Cisco FWSM Systems 61
 - Anti Virus Information 132
 - Anti-Virus Events 125, 132, 280
 - BlueCoat 139
 - Case Events 15, 251
 - Cisco ASA Events 40
 - Cisco FWSM Events 61
 - Cisco IOS IPS Events 97
 - Cisco IPS Sensor Events 91
 - Cisco Ironport ESA Events 102
 - Cisco Ironport WSA Events 108
 - Cisco Network Events 113
 - Correlated Alerts 16
 - Database Events 125, 140
 - Device Interface Notifications 113
 - DoS Channel 280
 - Error Events from Cisco IOS IPS Systems 97
 - Error Events from Cisco IPS Sensor Systems 92
 - Error Events from Cisco IPS Systems 84
 - Events from Cisco Firewall Systems 71
 - Events from Cisco IPS Systems 84
 - Events from Cisco Network Systems 113
 - Events from Cisco Wireless Systems 119
 - Firewall Events 124, 144
 - Identity Management Events 125, 156
 - IDS - IPS Events 124, 165
 - IPS Syslog Events from Cisco ASA Systems 40
 - Last 5 Minutes 15
 - Live 15
 - Microsoft-Authentication 266
 - Network Events 125, 172
 - Notification Events 248, 270
 - Operating System Events 124, 183
 - Reconnaissance Activity 15, 280
 - Status Events from Cisco IOS IPS Systems 97
 - Status Events from Cisco IPS Sensor Systems 91
 - Status Events from Cisco IPS Systems 84
 - VPN Events 124, 191
 - Vulnerability Events 280
 - Windows Failed Authentications - All 222
 - Windows Failed Authentications - Domain Accounts 222
 - Windows Failed Authentications - Workstations 222
 - Windows Monitoring Correlation Events 204
 - Windows Monitoring Events 204
 - X-OS-Traffic 124
- active lists
 - Audit Logs Cleared 235
 - Case Escalation 255
 - Cisco Firewall Message Types 26, 45, 65
 - Compromised List 284
 - Critical Services 235
 - Critical Services Started or Stopped 235
 - Event-based Rule Exclusions 126, 148, 168, 274, 284
 - HTTP Status Code Classes 110
 - Logon Types 224
 - Privileged Accounts 214
 - Privileged Accounts Modified 214
 - Privileged Group Members Modified 215
 - Privileged Groups 215
 - System Time Changes 234
 - Trusted List 284, 296
 - Untrusted List 284
 - Windows - Systems Starting Up 228, 235
 - Worm Infected Systems 168, 284
- Address Spaces asset category 284, 296
- admin destination 17, 205, 215, 224, 228, 235
- admincert destination 17, 275
- Alert Counts by Device query 170
- Alert Counts by Device report 166
- Alert Counts by Port query 170
- Alert Counts by Port report 166
- Alert Counts by Severity (Chart) query 170
- Alert Counts by Severity query 170
- Alert Counts by Severity report 167
- Alert Counts by Type query 170
- Alert Counts by Type report 167
- Alert Counts per Hour query 171
- Alert Counts per Hour report 166
- Alert Events from Cisco IOS IPS Systems active channel

- 97
- Alert Events from Cisco IPS Sensor Systems active channel 91
- Alert Events from Cisco IPS Systems active channel 84
- Alert, Critical and Error Events from Cisco ASA Systems active channel 40
- Alert, Critical and Error Events from Cisco Firewall Systems active channel 71
- Alert, Critical and Error Events from Cisco FWSM Systems active channel 61
- All Anti Virus filter 134
- All Cases query 258
- All Cases report 254
- All Device Information is NULL filter 264
- All Events filter 128, 134, 141, 149, 160, 169, 176, 186, 196, 249, 263, 268, 289
- All Level 3 Notifications query 272
- All Level 3 Notifications report 271
- Allowed Inbound Connections by Destination Address (Cisco ASA) query 47
- Allowed Inbound Connections by Destination Address (Cisco FWSM) query 68
- Allowed Inbound Connections by Port (Cisco ASA) query 48
- Allowed Inbound Connections by Port (Cisco FWSM) query 69
- Allowed Inbound Connections by Source Address (Cisco ASA) query 47
- Allowed Inbound Connections by Source Address (Cisco FWSM) query 68
- Allowed Outbound Connections by Destination Address (Cisco ASA) query 48
- Allowed Outbound Connections by Destination Address (Cisco FWSM) query 70
- Allowed Outbound Connections by Port (Cisco ASA) query 50
- Allowed Outbound Connections by Port (Cisco FWSM) query 69
- Allowed Outbound Connections by Source Address (Cisco ASA) query 49
- Allowed Outbound Connections by Source Address (Cisco FWSM) query 70
- Anti Virus Information active channel 132
- Anti-Virus Errors filter 135
- Anti-Virus Errors query 137
- Anti-Virus Events active channel 125, 132, 280
- Anti-Virus Events filter 128, 135, 291
- Anti-Virus Infection filter 135
- Anti-Virus Information dashboard 132
- Anti-Virus Overview dashboard 16, 132
- Anti-Virus Update Status filter 135
- Anti-Virus Updates data monitor 134
- Anti-Virus use case 130
- applicable events
 - Account Management 207
 - Authentication 221
 - Policy Changes 227
 - System Services and Auditing 230
- Application Protocol Event Counts data monitor 285
- Application Protocol is NULL filter 46, 56, 66, 77, 128, 149, 176, 195, 275
- ArcSight Administration
 - overview 7
- ArcSight Events filter 128, 135, 142, 150, 160, 176, 186, 196, 264, 292
- ArcSight Express
 - scheduling reports 13
- ArcSight Express field set 149, 159, 205, 267, 288
- ArcSight Foundations overview 8
- ArcSight Internal Events filter 293
- ArcSight System
 - overview 7
- ASM Events filter 292
- asset categories
 - Address Spaces 284, 296
 - Business Impact Analysis 26, 45, 55, 65, 77, 86, 93, 99
 - Criticality 296
 - Domain Name Server 168, 284
 - Email 168, 284
 - High 296
 - Operating System 261
 - Protected 17, 26, 45, 65, 77, 127, 133, 140, 148, 159, 168, 174, 185, 194, 204, 242, 284, 296
 - Proxy 168, 284
- Associated APs per Device query 121
- Associated Devices in a Day - Event Based query 121
- Associated Devices in a Day (Event Based) query viewer 119
- Associated Devices per AP query 121
- Associated Wireless Devices to Cisco APs report 120
- Association - Disassociation Details query 121
- Association - Disassociation per Day query 121
- Associations - Disassociations (Trend Based) query viewer 120
- Associations - Disassociations per Day (Cisco APs) report 120
- Attack Events filter 169, 292
- Attacker and Target Address Present filter 30, 46, 66, 77
- Attacker Host or Address Present filter 29, 45, 55, 66, 78, 88, 94, 100, 105
- Attacker or Target User Present filter 30, 46, 56, 67, 79, 88, 95, 101, 105, 111, 116
- Attacker User Present filter 31, 57
- Attacker_HostName global variable 205, 216, 224, 229, 236
- Attacker_NTDomain global variable 205, 216, 224, 229, 236
- Attacker_User global variable 205, 216, 224, 229, 236
- Audit Log Cleared - pre-Win2k8 filter 236
- Audit Logs Cleared - Chart query 237
- Audit Logs Cleared - Table query 237
- Audit Logs Cleared active list 235
- Authentication Attempted to Disabled Account rule 224
- Authentication Attempted to Non-Existing Account rule 223
- Authentication Errors (Cisco ASA) query 48
- Authentication Errors query 200
- Authentication Errors report 193
- Authentication Failed dashboard 222
- Authentication Failures by Destination data monitor 159
- Authentication Failures by Source data monitor 159
- Authentication use case 206, 221
- AV - Failed Updates filter 136
- AV - Found Infected filter 135, 292
- Average Time to Case Resolution - By Day query 259
- Average Time to Case Resolution - by Day query viewer 252
- Average Time to Case Resolution - By Day report 253

Average Time to Case Resolution - By Severity query 258
 Average Time to Case Resolution - by Severity query viewer 252
 Average Time to Case Resolution - By Severity report 253
 Average Time to Case Resolution - By User query 257
 Average Time to Case Resolution - by User query viewer 252
 Average Time to Case Resolution - By User report 253

B

Backdoor Traffic filter 289
 Bandwidth to or from External Systems filter 129, 151, 177, 197, 276
 Bandwidth Usage by Firewall Address query 249, 278
 Bandwidth Usage by Hour (Cisco ASA) report 44
 Bandwidth Usage by Hour (Cisco Firewall) report 75
 Bandwidth Usage by Hour (Cisco FWSM) report 65
 Bandwidth Usage by Hour report 126, 147, 174, 193
 Bandwidth Usage by Protocol (Cisco ASA) report 44
 Bandwidth Usage by Protocol (Cisco Firewall) report 74
 Bandwidth Usage by Protocol (Cisco FWSM) report 65
 Bandwidth Usage by Protocol focused report 151, 178, 198
 Bandwidth Usage by Protocol query 47, 58, 68, 79, 129, 153, 180, 199, 277
 Bandwidth Usage by Protocol report 53, 125, 145, 173, 192
 Bandwidth Usage per Hour focused report 152, 179, 197
 Bandwidth Usage per Hour query 48, 58, 68, 80, 129, 155, 180, 200, 278
 Bandwidth Usage per Hour report 54
 Bandwidth Utilization - By Hour query 277
 Bandwidth Utilization - By Minute query 278
 Bandwidth Utilization - Last 24 Hours report 274
 Bandwidth Utilization - Last Hour report 273
 Blaster DDOS From Infected Host rule 282
 Blaster Infected Host rule 283
 Blue Coat dashboard 16, 139
 Blue Coat field set 139
 Blue Coat filter 139
 BlueCoat active channel 139
 BlueCoat use case 130
 Business Impact Analysis asset category 26, 45, 55, 65, 77, 86, 93, 99
 By User Account - Accounts Created query 265
 By User Account - Accounts Created report 261
 Bytes In is NULL filter 243
 Bytes Out is NULL filter 243

C

Case Deleted rule 254
 Case Escalation active list 255
 Case Escalation rule 255
 Case Events active channel 15, 251
 Case Events filter 257
 Case field set 256
 Case File Type filter 257
 Case History Data trend 259
 Case Investigation Started rule 255
 Case Monitoring Entry Expiration filter 257
 Case Owner Value is null filter 256
 Case Stages dashboard 251

Case Stages Overview report 253
 Case Status dashboard 251
 Case Status Overview report 248, 254
 Case Times to Resolution dashboard 251
 Case Tracking and Escalation use case 250
 Case Tracking session list 250, 259
 Cases Created Today query 258
 Cases Created Today report 254
 Cases field set 256
 Cases Open by Stage (Chart) query 249, 258
 Cases per Target query 258
 Cases per Target report 254
 Categories field set 28, 55
 Cisco Access Points and Associated Wireless Devices report 120
 Cisco Adaptive Security Appliance (ASA) use case 39
 Cisco Aironet filter 121
 Cisco Alert Counts by Port and Device query 89
 Cisco Alert Counts by Port in the Last 2 Hours query viewer 85
 Cisco Alert Counts by Port query 88
 Cisco Alert Counts by Reporting Device query 88
 Cisco Alert Counts by Severity and Device query 89
 Cisco Alert Counts by Severity in the Last 2 Hours query viewer 85
 Cisco Alert Counts by Severity query 90
 Cisco Alert Counts by Type and Device query 89
 Cisco Alert Details (Trend Based) query 89, 95, 101
 Cisco Alert Details (Trend Based) query viewer 85, 92, 98
 Cisco Alerts per Day query 33, 90
 Cisco Alerts per Day report 86
 Cisco Alerts per Hour in the Previous Day query 90
 Cisco Alerts per Hour in the Previous Day report 85
 Cisco Allowed Connections by Destination Host - Template query 82
 Cisco Allowed Connections by Port - Template query 80
 Cisco Allowed Connections by Source Host - Template query 80
 Cisco Application Protocol Present filter 30, 56
 Cisco ASA Allowed Connections Overview dashboard 41
 Cisco ASA Denied Connections Overview dashboard 40
 Cisco ASA Event Counts by Hour in Last 6 Hours query 35, 49
 Cisco ASA Event Counts by Hour per Device query 37, 50, 82
 Cisco ASA Event Flow Statistics by Device data monitor 26, 45
 Cisco ASA Event Overview dashboard 21, 40
 Cisco ASA Events active channel 40
 Cisco ASA Hourly Event Count query viewer 23, 42
 Cisco ASA Hourly Event per Device query viewer 25, 42, 73
 Cisco ASA Inbound Connections per Day query 50
 Cisco ASA IPS Alert Events filter 46
 Cisco ASA Outbound Connections per Day query 48
 Cisco ASA Successful Configuration Changes filter 46
 Cisco ASA Systems filter 32, 47, 57, 67, 79
 Cisco Configuration Change Detail (Trend Based) query 37, 60
 Cisco Configuration Change Detail (Trend Based) query viewer 23, 52
 Cisco Configuration Changes (Event Based) query 35, 47, 58, 68, 80, 89, 96, 101, 107, 111
 Cisco Configuration Changes by Type (Cisco ASA) report

- 43
- Cisco Configuration Changes by Type (Cisco FWSM) report 64
- Cisco Configuration Changes by Type report 54
- Cisco Configuration Changes by User (Cisco ASA) report 43
- Cisco Configuration Changes by User (Cisco FWSM) report 65
- Cisco Configuration Changes by User (Event Based) query 33, 49, 59, 69, 81, 89, 95, 101, 106, 111, 117
- Cisco Configuration Changes by User report 54
- Cisco Configuration Changes Overview dashboard 22, 52
- Cisco Configuration Changes per Day report 54
- Cisco Configuration Changes per Hour in the Previous Day report 53
- Cisco Critical Network Events filter 116
- Cisco Cross-Device use case 38
- Cisco Current Event Sources dashboard 21, 51
- Cisco Denied Connections by Destination Host - Template query 79
- Cisco Denied Connections by Port - Template query 79
- Cisco Denied Connections by Source Host - Template query 81
- Cisco Device Critical Events query 117
- Cisco Device Critical Events report 114
- Cisco Device Errors query 118
- Cisco Device Errors report 114
- Cisco Device Interface Notifications field set 28, 55, 115
- Cisco Device Interface Status Messages query 117
- Cisco Device Interface Status Messages report 114
- Cisco Device SNMP Authentication Failures by User query 117
- Cisco Device SNMP Authentication Failures query 116
- Cisco ESA Configuration Changes by Type report 104
- Cisco ESA Configuration Changes by User report 104
- Cisco ESA Configuration Changes in the Last 6 Hours query 34, 59
- Cisco ESA Configuration Changes in the Last 6 Hours query viewer 24, 52
- Cisco ESA Configuration Changes per Day in the Last 7 Days query 107
- Cisco ESA Configuration Changes per Day report 104
- Cisco ESA Delivery Connection Count by Hour query 107
- Cisco ESA Injection Connection Count by Hour query 106
- Cisco Event Count by Hour query 32, 58
- Cisco Event Count by Hour query viewer 24, 52
- Cisco Event Statistics dashboard 16, 21, 51
- Cisco Events filter 32, 47, 57, 67, 79, 88, 95, 101, 105, 111, 116, 121
- Cisco Events with Protocols field set 28, 55
- Cisco Firewall Allowed Connections in Last 2 Hours dashboard 71
- Cisco Firewall Category Device Group Present filter 78
- Cisco Firewall Configuration Changes by Device report 76
- Cisco Firewall Configuration Changes by Type report 75
- Cisco Firewall Configuration Changes by User report 75
- Cisco Firewall Configuration Changes in Last 6 Hours query viewer 23, 52
- Cisco Firewall Configuration Changes in the Last 6 Hours query 35, 58
- Cisco Firewall Configuration Changes per Day in the Last 7 Days query 79
- Cisco Firewall Configuration Changes per Day report 76
- Cisco Firewall Denied Connections in Last 2 Hours dashboard 72
- Cisco Firewall Event Counts by Hour query 79
- Cisco Firewall Events field set 77
- Cisco Firewall Hourly Event Count query viewer 72
- Cisco Firewall Message Types active list 26, 45, 65
- Cisco Firewall Overview - Top Allowed Systems report 25
- Cisco Firewall Overview - Top Denied Systems report 25
- Cisco Firewall Overview - Trend and Port report 26
- Cisco Firewall Services Module (FWSM) use case 38
- Cisco Firewall Successful Configuration Changes filter 78
- Cisco Firewall Systems filter 32, 47, 57, 67, 78
- Cisco Firewall-Categorized Events filter 29, 45, 67, 78
- Cisco FWSM Allowed Connections Overview dashboard 61
- Cisco FWSM Denied Connections Overview dashboard 61
- Cisco FWSM Event Counts by Hour per Device query 37, 70, 82
- Cisco FWSM Event Counts by Hour query 34, 67
- Cisco FWSM Event Flow Statistics by Device data monitor 27, 66
- Cisco FWSM Event Overview dashboard 22, 61
- Cisco FWSM Events active channel 61
- Cisco FWSM Hourly Event Count query viewer 23, 62
- Cisco FWSM Hourly Event per Device query viewer 24, 63, 73
- Cisco FWSM Inbound Connections per Day query 69
- Cisco FWSM Outbound Connections per Day query 68
- Cisco FWSM Successful Configuration Changes filter 32, 67
- Cisco FWSM Systems filter 29, 46, 56, 67, 78
- Cisco Generic Firewall Event Overview dashboard 72
- Cisco Generic Firewall use case 38
- Cisco Generic Intrusion Prevention System (IPS) use case 38
- Cisco Generic IPS Alert Overview dashboard 84
- Cisco Generic IPS Event Overview dashboard 84
- Cisco Intrusion Prevention System (IPS) Sensor use case 38
- Cisco Intrusion Prevention System Overview report 26
- Cisco IOS Intrusion Prevention System (IOS IPS) use case 37
- Cisco IOS IPS Alert Events filter 100
- Cisco IOS IPS Alert Overview dashboard 98
- Cisco IOS IPS Configuration Changes by Type report 99
- Cisco IOS IPS Configuration Changes by User report 98
- Cisco IOS IPS Event Flow Statistics by Device data monitor 28, 99
- Cisco IOS IPS Event Overview dashboard 22, 98
- Cisco IOS IPS Events active channel 97
- Cisco IOS IPS Hourly Event Count per Device query viewer 24, 98
- Cisco IOS IPS Hourly Event Count query viewer 24, 98
- Cisco IOS IPS Successful Configuration Changes filter 29, 99
- Cisco IOS IPS Systems filter 29, 55, 87, 94, 100
- Cisco IPS Alert Events filter 30, 56, 87, 94, 100
- Cisco IPS Configuration Changes by Device report 86
- Cisco IPS Configuration Changes by Type report 85
- Cisco IPS Configuration Changes by User report 85
- Cisco IPS Configuration Changes in the Last 6 Hours query 33, 58
- Cisco IPS Configuration Changes in the Last 6 Hours query viewer 22, 52
- Cisco IPS Configuration Changes per Day report 86
- Cisco IPS Error Events filter 87, 94, 99

- Cisco IPS Event Flow Statistics by Device Product data monitor 87
- Cisco IPS Event Types data monitor 87
- Cisco IPS Sensor Alert Events filter 94
- Cisco IPS Sensor Alert Overview dashboard 92
- Cisco IPS Sensor Configuration Changes by Type report 93
- Cisco IPS Sensor Configuration Changes by User report 93
- Cisco IPS Sensor Event Flow Statistics by Device data monitor 27, 93
- Cisco IPS Sensor Event Overview dashboard 21, 92
- Cisco IPS Sensor Event Types data monitor 28, 87, 93
- Cisco IPS Sensor Events active channel 91
- Cisco IPS Sensor Successful Configuration Changes filter 29, 95
- Cisco IPS Sensor Systems filter 31, 57, 88, 95, 101
- Cisco IPS Status Events filter 88, 94, 100
- Cisco IPS Successful Configuration Changes filter 87
- Cisco IPS Systems filter 31, 57, 88, 94, 100
- Cisco IPS-Categorized Events filter 29, 56, 88, 94, 100
- Cisco IPS-Categorized IOS IPS Events filter 100
- Cisco IPS-Categorized IPS Sensor Events filter 94
- Cisco Ironport Email Security Appliance (ESA) use case 38
- Cisco Ironport ESA Events active channel 102
- Cisco Ironport ESA Systems filter 30, 56, 105
- Cisco Ironport Web Security Appliance (WSA) use case 38
- Cisco Ironport WSA Events active channel 108
- Cisco Ironport WSA Systems filter 30, 56, 111
- Cisco Login Detail (Trend Based) query 34, 57
- Cisco Login Details in the Last 7 Days (Trend Based) query viewer 23, 52
- Cisco Network Configuration Changes per Day in the Last 7 Days query 117
- Cisco Network Device Inbound Interface Status Events filter 116
- Cisco Network Device Interface Down Messages filter 116
- Cisco Network Device Interface Status Events filter 116
- Cisco Network Device Outbound Interface Status Events filter 116
- Cisco Network Equipment Configuration Change By Event query 118
- Cisco Network Equipment Configuration Changes by Device report 114
- Cisco Network Equipment Configuration Changes by Type report 115
- Cisco Network Equipment Configuration Changes by User report 114
- Cisco Network Equipment Configuration Changes in the Last 6 Hours query 34, 59
- Cisco Network Equipment Configuration Changes in the Last 6 Hours query viewer 22, 52
- Cisco Network Equipment Configuration Changes per Day report 114
- Cisco Network Error Events filter 115
- Cisco Network Event Count by Hour query 117
- Cisco Network Event Count by Hour query viewer 113
- Cisco Network Event Flow Statistics by Device data monitor 115
- Cisco Network Event Overview dashboard 113
- Cisco Network Events active channel 113
- Cisco Network Events filter 115
- Cisco Network SNMP Authentication Failures report 114
- Cisco Network use case 38
- Cisco Overall Alert Count by Device report 86
- Cisco Overall Alert Count by Port report 86
- Cisco Overall Alert Count by Severity report 86
- Cisco Overall Alert Count by Type report 85
- Cisco Overall Allowed Inbound Connections by Destination Host query 36, 81
- Cisco Overall Allowed Inbound Connections by Destination Host report 74
- Cisco Overall Allowed Inbound Connections by Port query 79
- Cisco Overall Allowed Inbound Connections by Source Host query 34, 80
- Cisco Overall Allowed Inbound Connections by Source Host report 76
- Cisco Overall Allowed Outbound Connections by Destination Host query 36, 80
- Cisco Overall Allowed Outbound Connections by Destination Host report 74
- Cisco Overall Allowed Outbound Connections by Port query 81
- Cisco Overall Allowed Outbound Connections by Source Host query 35, 80
- Cisco Overall Allowed Outbound Connections by Source Host report 74
- Cisco Overall Denied Inbound Connections by Destination Host query 34, 81
- Cisco Overall Denied Inbound Connections by Destination Host report 76
- Cisco Overall Denied Inbound Connections by Destination Port report 74
- Cisco Overall Denied Inbound Connections by Port query 35, 48, 68, 80
- Cisco Overall Denied Inbound Connections by Source Host query 33, 49, 69, 81
- Cisco Overall Denied Inbound Connections by Source Host report 75
- Cisco Overall Denied Inbound Connections per Hour - Event Based query 69
- Cisco Overall Denied Inbound Connections per Hour in the Previous Day query 81
- Cisco Overall Denied Inbound Connections per Hour in the Previous Day report 75
- Cisco Overall Denied Outbound Connections by Destination Host query 37, 82
- Cisco Overall Denied Outbound Connections by Destination Host report 76
- Cisco Overall Denied Outbound Connections by Destination Port report 76
- Cisco Overall Denied Outbound Connections by Port query 34, 50, 70, 82
- Cisco Overall Denied Outbound Connections by Source Host query 33, 48, 68, 80
- Cisco Overall Denied Outbound Connections by Source Host report 75
- Cisco Overall Denied Outbound Connections per Hour - Event Based query 70
- Cisco Overall Denied Outbound Connections per Hour in the Previous Day report 76
- Cisco Overall Inbound Connection Setup Attempts per Day report 73
- Cisco Overall Inbound Connections per Day query 35, 80
- Cisco Overall Outbound Connection Setup Attempts per Day report 75

- Cisco Overall Outbound Connections per Day query 32, 79
- Cisco Overall Outbound Connections per Hour in the Previous Day query 79
- Cisco Overview use case 18
- Cisco Select Category Present filter 31, 57
- Cisco SNMP Access (Trend Based) query 118
- Cisco SNMP Access On Certain Target (Trend Based) query 117
- Cisco SNMP Authentication Failures by Device query 117
- Cisco Successful Network Configuration Changes filter 116
- Cisco Target Port Present filter 31, 57
- Cisco Top ASA Event Sources by Message Types data monitor 27, 45
- Cisco Top ASA Sources data monitor 28, 45
- Cisco Top Event Sources by Device data monitor 27, 55
- Cisco Top Event Sources by Device Group data monitor 26, 55
- Cisco Top Event Sources by Product data monitor 27, 55
- Cisco Top Firewall Product Sources data monitor 77
- Cisco Top FWSM Event Sources by Message Types data monitor 26, 65
- Cisco Top FWSM Sources data monitor 28, 66
- Cisco Top IOS IPS Alert Techniques data monitor 99
- Cisco Top IOS IPS Alerts by Device data monitor 99
- Cisco Top IOS IPS Alerts data monitor 99
- Cisco Top IOS IPS Devices data monitor 27, 99
- Cisco Top IOS IPS Event Types data monitor 26, 87, 99
- Cisco Top IPS Alert Techniques data monitor 87
- Cisco Top IPS Alerts data monitor 86
- Cisco Top IPS Products data monitor 87
- Cisco Top IPS Sensor Alert Techniques data monitor 93
- Cisco Top IPS Sensor Alerts by Device data monitor 93
- Cisco Top IPS Sensor Alerts data monitor 93
- Cisco Top IPS Sensor Devices data monitor 27, 93
- Cisco Top Network Devices data monitor 115
- Cisco Transportation Protocol Present filter 31, 57
- Cisco Wireless AP Device Association filter 121
- Cisco Wireless AP Device Disassociation filter 120
- Cisco Wireless Event Flow Statistics by AP data monitor 120
- Cisco Wireless Events field set 120
- Cisco Wireless Systems filter 121
- Cisco Wireless use case 38
- Cisco WSA Configuration Changes by Type report 109
- Cisco WSA Configuration Changes by User report 110
- Cisco WSA Configuration Changes in the Last 6 Hours query 33, 59
- Cisco WSA Configuration Changes in the Last 6 Hours query viewer 24, 53
- Cisco WSA Configuration Changes per Day in the Last 7 Days query 111
- Cisco WSA Configuration Changes per Day report 109
- Closed Connection Durations query 162
- Closed VPN Connection Durations query 200
- Common IPS Event Types filter 31, 88, 100
- Compromised List active list 284
- Computer Account Changed rule 211
- Computer Account Created rule 213
- Computer Account Deleted rule 213
- Computer Accounts Created Weekly - Chart query 218
- Computer Accounts Created Weekly - Table query 217
- Computer Accounts Created Weekly report 210
- Computer Accounts Deleted Weekly - Chart query 217
- Computer Accounts Deleted Weekly - Table query 218
- Computer Accounts Deleted Weekly report 209
- Computer Accounts Modified Weekly - Chart query 218
- Computer Accounts Modified Weekly - Table query 219
- Computer Accounts Modified Weekly report 210
- configuration
 - Account Management 208
 - Authentication 221
 - Policy Changes 227
 - scheduling reports 13
 - System Services and Auditing 230
- Configuration Changes by Type focused report 136, 142, 152, 161, 177, 186, 199
- Configuration Changes by Type report 125, 133, 140, 147, 157, 174, 184, 193, 261
- Configuration Changes by User focused report 136, 142, 151, 162, 177, 186, 198
- Configuration Changes by User report 125, 132, 140, 146, 156, 173, 184, 193, 261
- Configuration Changes Overview dashboard 125, 260
- Configuration Changes per Day in the Last 7 Days query 36, 59
- Configuration Changes per Hour in the Previous Day query 32, 58
- Configuration Changes query 129, 137, 143, 155, 163, 180, 189, 201, 265
- Configuration Changes use case 250
- Configuration Modifications filter 127, 134, 141, 149, 160, 176, 185, 195, 263
- Connection Counts by User report 156, 192
- Connection Durations by User report 157
- Connection Overview (Cisco ESA) report 104
- Connections Accepted by Address (Cisco ASA) query 48
- Connections Accepted by Address query 199
- Connections Accepted by Address report 193
- Connections Denied by Address (Cisco ASA) query 48
- Connections Denied by Address query 200
- Connections Denied by Address report 192
- Connections Denied by Hour query 201
- Connections Denied by Hour report 192
- Correlated Alerts active channel 16
- Correlated Events data monitor 285
- Correlated Events filter 291
- Covert Channel data monitor 288
- Covert Channels TCP port 53 filter 291
- CrashOnAuditFail is True filter 236
- CrashOnAuditFail Modified rule 233
- Created Computer Accounts session list 219
- Created User Accounts session list 220
- Critical Network Events filter 177
- Critical Service Request Start rule 232
- Critical Service Request Stop rule 234
- Critical Service Started rule 234
- Critical Service Stopped rule 233
- Critical Services active list 235
- Critical Services filter 237
- Critical Services Started or Stopped - Chart query 237
- Critical Services Started or Stopped - Table query 237
- Critical Services Started or Stopped active list 235
- Critical Services Started or Stopped query viewer 231
- Criticality asset category 296
- Current Event Sources dashboard 125

D

- Daily Account Lockouts query 218
- Daily Accounts Locked Out report 209
- Daily Alerts - Base query 37, 60, 90, 95, 101
- Daily Alerts trend 37, 60, 90, 96, 101
- Daily Associations - Disassociations (Base) query 121
- Daily Associations - Disassociations trend 122
- Daily Configuration Changes - Base query 34, 60, 82, 90, 107, 112, 118, 121
- Daily Connection Setup Attempts - Base query 37, 50, 59, 69, 81
- Daily Connection Setup Attempts trend 37, 50, 60, 70, 82
- Daily Email Transactions trend 37, 107
- Daily Logins - Base query 37, 60
- Daily Logins per Product query 35
- Daily Logins trend 37, 60
- Daily Message Transactions - Base query 32, 106
- Daily SNMP Access - Base query 117
- Daily SNMP Access trend 118
- Daily Web Requests - Base query 111
- Daily Web Requests trend 112
- dashboards
 - Access Points 119
 - Account Management 208
 - Anti-Virus Information 132
 - Anti-Virus Overview 16, 132
 - Authentication Failed 222
 - Blue Coat 16, 139
 - Case Stages 251
 - Case Status 251
 - Case Times to Resolution 251
 - Cisco ASA Allowed Connections Overview 41
 - Cisco ASA Denied Connections Overview 40
 - Cisco ASA Event Overview 21, 40
 - Cisco Configuration Changes Overview 22, 52
 - Cisco Current Event Sources 21, 51
 - Cisco Event Statistics 16, 21, 51
 - Cisco Firewall Allowed Connections in Last 2 Hours 71
 - Cisco Firewall Denied Connections in Last 2 Hours 72
 - Cisco FWSM Allowed Connections Overview 61
 - Cisco FWSM Denied Connections Overview 61
 - Cisco FWSM Event Overview 22, 61
 - Cisco Generic Firewall Event Overview 72
 - Cisco Generic IPS Alert Overview 84
 - Cisco Generic IPS Event Overview 84
 - Cisco IOS IPS Alert Overview 98
 - Cisco IOS IPS Event Overview 22, 98
 - Cisco IPS Sensor Alert Overview 92
 - Cisco IPS Sensor Event Overview 21, 92
 - Cisco Network Event Overview 113
 - Configuration Changes Overview 125, 260
 - Current Event Sources 125
 - Database Errors 140
 - Device Interface Status 113
 - Firewall Connection Overview 16, 144
 - Firewall Login Overview 144
 - Host Configuration Modifications 260
 - Host Problems Overview 260
 - Identity Management Overview 156
 - IDS - IPS Overview 16, 165
 - Interesting Mail 16, 281
 - Login Information 17, 266, 281
 - Login Overview 21, 52
 - Malware 17, 281
 - NetFlow Bandwidth Usage Overview 240
 - Network Login Overview 172
 - Network Status Overview 172
 - Operating System Login Overview 183
 - Policy Changes 227
 - Reconnaissance in Progress 280
 - Security Activity 16, 281
 - Security Activity Statistics 16, 280
 - Sender and Recipient Overview 22, 102
 - System Services and Auditing 231
 - Threat View 16, 281
 - Top NetFlow Bandwidth Usage Monitoring 240
 - Traffic Monitoring 16, 273
 - Traffic Moving Average 273
 - Transaction Connections Overview 102
 - Virus Activity Statistics 132
 - VPN Connection Statistics 191
 - VPN Login Overview 191
 - Web Transactions 22, 108
 - Windows Monitoring 16, 204
 - Worm Outbreak Overview 165, 281
- data monitors
 - Anti-Virus Updates 134
 - Application Protocol Event Counts 285
 - Authentication Failures by Destination 159
 - Authentication Failures by Source 159
 - Cisco ASA Event Flow Statistics by Device 26, 45
 - Cisco FWSM Event Flow Statistics by Device 27, 66
 - Cisco IOS IPS Event Flow Statistics by Device 28, 99
 - Cisco IPS Event Flow Statistics by Device Product 87
 - Cisco IPS Event Types 87
 - Cisco IPS Sensor Event Flow Statistics by Device 27, 93
 - Cisco IPS Sensor Event Types 28, 87, 93
 - Cisco Network Event Flow Statistics by Device 115
 - Cisco Top ASA Event Sources by Message Types 27, 45
 - Cisco Top ASA Sources 28, 45
 - Cisco Top Event Sources by Device 27, 55
 - Cisco Top Event Sources by Device Group 26, 55
 - Cisco Top Event Sources by Product 27, 55
 - Cisco Top Firewall Product Sources 77
 - Cisco Top FWSM Event Sources by Message Types 26, 65
 - Cisco Top FWSM Sources 28, 66
 - Cisco Top IOS IPS Alert Techniques 99
 - Cisco Top IOS IPS Alerts 99
 - Cisco Top IOS IPS Alerts by Device 99
 - Cisco Top IOS IPS Devices 27, 99
 - Cisco Top IOS IPS Event Types 26, 87, 99
 - Cisco Top IPS Alert Techniques 87
 - Cisco Top IPS Alerts 86
 - Cisco Top IPS Products 87
 - Cisco Top IPS Sensor Alert Techniques 93
 - Cisco Top IPS Sensor Alerts 93
 - Cisco Top IPS Sensor Alerts by Device 93
 - Cisco Top IPS Sensor Devices 27, 93
 - Cisco Top Network Devices 115
 - Cisco Wireless Event Flow Statistics by AP 120
 - Correlated Events 285

- Covert Channel 288
- Device Inbound Interface Status 115
- Device Outbound Interface Status 115
- Devices with High Error Rates 175
- Event Counts by Hour 287
- Event Flow by Cisco Firewall Products in the Last 2 Hours 77
- Event Flow Statistics by Device in Last 2 Hours (Cisco ESA) 105
- Event Flow Statistics by Device in Last 2 Hours (Cisco WSA) 28, 110
- Events per Address Space 285
- High Events 287
- Host Configuration Change Event Counts by Zone 262
- Host Problem Event Counts by Zone 262
- Inbound Bandwidth (Bytes Per Second) 242
- Infected Systems 133
- Last 10 Anti-Virus Errors 134
- Last 10 Cisco FWSM Successful Configuration Changes 28, 66
- Last 10 Cisco IOS IPS Successful Configuration Changes 27, 99
- Last 10 Cisco IPS Sensor Successful Configuration Changes 28, 93
- Last 10 Critical Network Events 175
- Last 10 Database Configuration Changes 127, 261
- Last 10 Database Errors 141
- Last 10 Failed Login Events 148, 175, 185, 194
- Last 10 Firewall Configuration Changes 127, 261
- Last 10 Hosts Scanned 286
- Last 10 Interface Down Messages 175
- Last 10 Interface Status Messages 175
- Last 10 Network Configuration Changes 127, 262
- Last 10 Scanners 286
- Last 10 Successful Login Events 148, 175, 185, 194
- Last 10 VPN Configuration Changes 127, 261
- Last 10 Zones Scanned 285
- Last 20 Host Configuration Modification Events 262
- Last 20 Host Problems 262
- Last Failed Logins 287
- Login Results 148, 175, 185, 195
- Malware Real-Time Tracking 285
- Most Common Host Configuration Change Events 261
- Most Common Host Problem Events 262
- Most Frequent Ports 27, 55, 285
- Non-Root-Admin Failed Logins 267, 288
- Non-Root-Admin Logins 267, 288
- Outbound Bandwidth (Bytes Per Second) 242
- Outbound High Port Traffic 286
- Outbound Mail over 20MB 286
- Policy Changes 228
- Port Monitor 287
- Recent Events 285
- Root-Admin Failed Logins 267, 287
- Root-Admin Logins 267, 285
- Target Port Activity by Attacker 168, 287
- Top 10 Accepted Ports (Inbound) 148
- Top 10 Accepted Ports (Outbound) 148
- Top 10 Alert Destinations 168
- Top 10 Alert Sources 168
- Top 10 Alert Types 168
- Top 10 Alerts 169
- Top 10 Anti-Virus Errors 133
- Top 10 Database Errors 141
- Top 10 Denied Ports (Inbound) 148
- Top 10 Denied Ports (Outbound) 148
- Top 10 Event Types last Hour 204
- Top 10 Hosts With Denied Inbound Connections 148
- Top 10 Hosts With Denied Outbound Connections 148
- Top 10 Infected Systems 133
- Top 10 Infections 134
- Top 10 Users With Failed Logins 148, 175, 185, 195
- Top 10 Users with Failed Logins 286
- Top 10 Windows Users Last Hour 204
- Top 10 Zones Scanned 287
- Top Access Points with Most Association Events 120
- Top Access Points with Most Disassociation Events 120
- Top Actions 139
- Top Activities across Cisco Firewall Devices 77
- Top Application Protocols 27, 55
- Top Attacker IPs 285
- Top Browsers 139
- Top Categories 28, 55, 139, 288
- Top Connectors 286
- Top Event Sources 127
- Top Firewall Blocked Machines 287
- Top Non-US Destinations 275
- Top Non-US Destinations - Graph 275
- Top Non-US Sources 274
- Top Non-US Sources - Graph 274
- Top Successful Attacks 287
- Top Systems with Most Rejected Injection Connections 104
- Top Target IPs 287
- Top Transport Protocols 26, 55, 286
- Top Users by Connection Count 159
- Top Users by Login Activity 175, 185, 194
- Top VPN Servers with Authentication Errors 195
- Top VPN Servers with Denied Connections 195
- Top VPN Servers with Successful Connections 195
- Top VPN Users with Authentication Errors 194
- Top Web Sites 139
- Traffic Moving Average (ICMP) 275
- Traffic Moving Average (SYN) 275
- Traffic Moving Average (TCP) 274
- Traffic Moving Average (UDP) 275
- Trojaned Machines 285
- User Accounts Created, Deleted, Disabled, or Enabled 215
- Very High Events 287
- Virus Activity by Host 134
- Virus Activity by Zone 134
- Windows System Services and Auditing Violations 235
- Worm Activity Status 168, 287
- Worm Infected Machines 286
- Worm Infected Systems 168, 286
- Database Configuration Changes filter 129, 141, 265
- Database Errors and Warnings (Chart) query 142
- Database Errors and Warnings query 143
- Database Errors and Warnings report 140
- Database Errors dashboard 140
- Database Errors filter 141
- Database Events active channel 125, 140

- Database Events filter 128, 141, 142, 263
 - Database use case 130
 - DateTime global variable 256
 - DateValue global variable 256
 - Day global variable 256
 - Deleted Computer Accounts session list 220
 - Deleted User Accounts session list 219
 - Delivery Connection (Cisco ESA) filter 105
 - Delivery Connections by Hour query viewer 103
 - Delivery Connections query 106
 - Delivery Connections query viewer 103
 - Denied Inbound Connections by Address (Cisco ASA) report 42
 - Denied Inbound Connections by Address (Cisco FWSM) report 65
 - Denied Inbound Connections by Address query 154
 - Denied Inbound Connections by Address report 146
 - Denied Inbound Connections by Destination Address (Cisco ASA) query 49
 - Denied Inbound Connections by Destination Address (Cisco FWSM) query 68
 - Denied Inbound Connections by Port (Cisco ASA) query 48
 - Denied Inbound Connections by Port (Cisco ASA) report 44
 - Denied Inbound Connections by Port (Cisco FWSM) query 67
 - Denied Inbound Connections by Port (Cisco FWSM) report 64
 - Denied Inbound Connections by Port query 154
 - Denied Inbound Connections by Port report 147
 - Denied Inbound Connections by Source Address (Cisco ASA) query 50
 - Denied Inbound Connections by Source Address (Cisco FWSM) query 67
 - Denied Inbound Connections filter 149
 - Denied Inbound Connections per Hour (Chart) query 155
 - Denied Inbound Connections per Hour (Cisco FWSM) report 64
 - Denied Inbound Connections per Hour query 154
 - Denied Inbound Connections per Hour report 145
 - Denied Outbound Connections by Address (Cisco ASA) report 44
 - Denied Outbound Connections by Address (Cisco FWSM) report 63
 - Denied Outbound Connections by Address query 153
 - Denied Outbound Connections by Address report 145
 - Denied Outbound Connections by Destination Address (Cisco ASA) query 49
 - Denied Outbound Connections by Destination Address (Cisco FWSM) query 69
 - Denied Outbound Connections by Port (Cisco ASA) query 49
 - Denied Outbound Connections by Port (Cisco ASA) report 43
 - Denied Outbound Connections by Port (Cisco FWSM) query 68
 - Denied Outbound Connections by Port (Cisco FWSM) report 63
 - Denied Outbound Connections by Port query 153
 - Denied Outbound Connections by Port report 145
 - Denied Outbound Connections by Source Address (Cisco ASA) query 50
 - Denied Outbound Connections by Source Address (Cisco FWSM) query 69
 - Denied Outbound Connections filter 149
 - Denied Outbound Connections per Hour (Chart) query 155
 - Denied Outbound Connections per Hour (Cisco FWSM) report 65
 - Denied Outbound Connections per Hour query 154
 - Denied Outbound Connections per Hour report 145
 - Denied Web Server Requests filter 111
 - destinations
 - admin 17, 205, 215, 224, 228, 235
 - admindcert 17, 275
 - Detail Successful Requests query 33, 112
 - Detail Unsuccessful Requests query 112
 - Device Critical Events query 180
 - Device Critical Events report 174
 - Device Errors query 181
 - Device Errors report 174
 - Device Events query 181
 - Device Events report 174
 - Device Inbound Interface Status data monitor 115
 - Device Interface Down Notifications query 179
 - Device Interface Down Notifications report 173
 - Device Interface Notifications active channel 113
 - Device Interface Status dashboard 113
 - Device Interface Status Messages query 181
 - Device Interface Status Messages report 173
 - Device Outbound Interface Status data monitor 115
 - Device SNMP Authentication Failures by User query 181
 - Device SNMP Authentication Failures query 182
 - Device SNMP Authentication Failures report 172
 - Device Vendor AND Product are NULL filter 264
 - Device Vendor OR Product is NULL filter 264
 - Device Version is NULL filter 264
 - Device_HostName global variable 205, 216, 225, 229, 236
 - Device_NTDomain global variable 205, 216, 225, 229, 236
 - DeviceInfo global variable 262
 - Devices use case 18
 - Devices with High Error Rates data monitor 175
 - Disabled User Accounts session list 220
 - Disassociated Devices in a Day (Event Based) query viewer 120
 - Disassociated Devices per AP query 121
 - Disassociated Devices query 121
 - Domain Name Server asset category 168, 284
 - DoS Channel active channel 280
- ## E
- Email asset category 168, 284
 - Email Message Transaction (Cisco ESA) filter 30, 105
 - Enabled User Accounts session list 219
 - EndTimeValue global variable 256
 - Error Events from Cisco IOS IPS Systems active channel 97
 - Error Events from Cisco IPS Sensor Systems active channel 92
 - Error Events from Cisco IPS Systems active channel 84
 - Errors Detected in Anti-Virus Deployment report 132
 - Event Counts by Hour data monitor 287
 - Event Flow by Cisco Firewall Products in the Last 2 Hours data monitor 77
 - Event Flow Statistics by Device in Last 2 Hours (Cisco ESA) data monitor 105

Event Flow Statistics by Device in Last 2 Hours (Cisco WSA) data monitor 28, 110
 Event-based Rule Exclusions active list 126, 148, 168, 274, 284
 EventID.net integration command 206
 Events from Cisco Firewall Systems active channel 71
 Events from Cisco IPS Systems active channel 84
 Events from Cisco Network Systems active channel 113
 Events from Cisco Wireless Systems active channel 119
 Events per Address Space data monitor 285
 Events with Vulnerabilities filter 290
 events, applicable
 Account Management 207
 Authentication 221
 Policy Changes 227
 System Services and Auditing 230
 Exposed Vulnerabilities by Asset query 297
 Exposed Vulnerabilities by Asset report 296
 Exposed Vulnerability Count by Asset query 297
 Exposed Vulnerability Count by Asset report 296
 Exposed Vulnerability Count by Critical Asset focused report 297
 External Source filter 127, 150, 242, 275, 292
 External Target filter 150, 243, 276, 293

F

Failed Anti-Virus Updates Chart query 136
 Failed Anti-Virus Updates query 136
 Failed Anti-Virus Updates report 133
 Failed Authentication - Windows Domain Account rule 223
 Failed Authentication - Windows Workstation rule 224
 Failed Authentication Events - All filter 225
 Failed Authentication Events - Domain filter 225
 Failed Authentication Events - Workstation filter 225
 Failed Authentications field set 225
 Failed Authentications session list 226
 Failed Firewall Login Events filter 150
 Failed Identity Management Login Attempts filter 160
 Failed Login Attempts (Chart) query 162, 188, 268
 Failed Login Attempts focused report 161, 187
 Failed Login Attempts query 163, 188, 268
 Failed Login Attempts report 157, 183, 266
 Failed Login by User (Chart) query 153, 163, 180, 188, 199, 268
 Failed Login by User query 155, 164, 180, 189, 201, 269
 Failed Login Events filter 149, 176, 185, 196
 Failed Logins by Destination Address (Chart) query 153, 162, 179, 188, 199, 268
 Failed Logins by Destination Address focused report 151, 160, 179, 187, 197
 Failed Logins by Destination Address query 32, 57
 Failed Logins by Destination Address report 54, 145, 157, 173, 183, 192, 266
 Failed Logins by Source Address (Chart) query 153, 162, 181, 188, 201, 268
 Failed Logins by Source Address focused report 151, 161, 178, 187, 199
 Failed Logins by Source Address query 33, 58
 Failed Logins by Source Address report 54, 146, 157, 174, 184, 193, 267
 Failed Logins by Source-Destination Pair query 154, 163, 181, 189, 202, 268

Failed Logins by User focused report 153, 162, 178, 187, 197
 Failed Logins by User in the Last 2 Hours query viewer 23, 52
 Failed Logins by User query 34, 60
 Failed Logins by User report 53, 146, 156, 173, 184, 193, 266
 Failed Logins filter 291
 Failed Logins with Target Information filter 290
 Failed Network Login Events filter 176
 Failed Operating System Login Events filter 186
 Failed VPN Connection Events (Cisco ASA) filter 45
 Failed VPN Connection Events filter 196
 Failed VPN Login Events filter 196
 field sets
 ArcSight Express 149, 159, 205, 267, 288
 Blue Coat 139
 Case 256
 Cases 256
 Categories 28, 55
 Cisco Device Interface Notifications 28, 55, 115
 Cisco Events with Protocols 28, 55
 Cisco Firewall Events 77
 Cisco Wireless Events 120
 Failed Authentications 225
 Firewall 275
 IDS 127, 169, 288
 Microsoft 267
 Notification 271
 Notifications 248, 271
 Privileged Account 216
 Security 288
 Security Highlights 288
 Standard 127, 141, 149, 159, 169, 175, 185, 195, 263, 288
 Virus Information 127, 134, 288
 Vulnerability 288
 Windows Monitoring 205
 Windows Monitoring Correlation 205

files

WindowsLogonTypes.csv 225

filters

Accepted Inbound Connections 150
 Accepted Outbound Connections 149
 All Anti Virus 134
 All Device Information is NULL 264
 All Events 128, 134, 141, 149, 160, 169, 176, 186, 196, 249, 263, 268, 289
 Anti-Virus Errors 135
 Anti-Virus Events 128, 135, 291
 Anti-Virus Infection 135
 Anti-Virus Update Status 135
 Application Protocol is NULL 46, 56, 66, 77, 128, 149, 176, 195, 275
 ArcSight Events 128, 135, 142, 150, 160, 176, 186, 196, 264, 292
 ArcSight Internal Events 293
 ASM Events 292
 Attack Events 169, 292
 Attacker and Target Address Present 30, 46, 66, 77
 Attacker Host or Address Present 29, 45, 55, 66, 78, 88, 94, 100, 105
 Attacker or Target User Present 30, 46, 56, 67, 79, 88, 95, 101, 105, 111, 116
 Attacker User Present 31, 57

- Audit Log Cleared - pre-Win2k8 236
- AV - Failed Updates 136
- AV - Found Infected 135, 292
- Backdoor Traffic 289
- Bandwidth to or from External Systems 129, 151, 177, 197, 276
- Blue Coat 139
- Bytes In is NULL 243
- Bytes Out is NULL 243
- Case Events 257
- Case File Type 257
- Case Monitoring Entry Expiration 257
- Case Owner Value is null 256
- Cisco Aironet 121
- Cisco Application Protocol Present 30, 56
- Cisco ASA IPS Alert Events 46
- Cisco ASA Successful Configuration Changes 46
- Cisco ASA Systems 32, 47, 57, 67, 79
- Cisco Critical Network Events 116
- Cisco Events 32, 47, 57, 67, 79, 88, 95, 101, 105, 111, 116, 121
- Cisco Firewall Category Device Group Present 78
- Cisco Firewall Successful Configuration Changes 78
- Cisco Firewall Systems 32, 47, 57, 67, 78
- Cisco Firewall-Categorized Events 29, 45, 67, 78
- Cisco FWSM Successful Configuration Changes 32, 67
- Cisco FWSM Systems 29, 46, 56, 67, 78
- Cisco IOS IPS Alert Events 100
- Cisco IOS IPS Successful Configuration Changes 29, 99
- Cisco IOS IPS Systems 29, 55, 87, 94, 100
- Cisco IPS Alert Events 30, 56, 87, 94, 100
- Cisco IPS Error Events 87, 94, 99
- Cisco IPS Sensor Alert Events 94
- Cisco IPS Sensor Successful Configuration Changes 29, 95
- Cisco IPS Sensor Systems 31, 57, 88, 95, 101
- Cisco IPS Status Events 88, 94, 100
- Cisco IPS Successful Configuration Changes 87
- Cisco IPS Systems 31, 57, 88, 94, 100
- Cisco IPS-Categorized Events 29, 56, 88, 94, 100
- Cisco IPS-Categorized IOS IPS Events 100
- Cisco IPS-Categorized IPS Sensor Events 94
- Cisco Ironport ESA Systems 30, 56, 105
- Cisco Ironport WSA Systems 30, 56, 111
- Cisco Network Device Inbound Interface Status Events 116
- Cisco Network Device Interface Down Messages 116
- Cisco Network Device Interface Status Events 116
- Cisco Network Device Outbound Interface Status Events 116
- Cisco Network Error Events 115
- Cisco Network Events 115
- Cisco Select Category Present 31, 57
- Cisco Successful Network Configuration Changes 116
- Cisco Target Port Present 31, 57
- Cisco Transportation Protocol Present 31, 57
- Cisco Wireless AP Device Association 121
- Cisco Wireless AP Device Disassociation 120
- Cisco Wireless Systems 121
- Common IPS Event Types 31, 88, 100
- Configuration Modifications 127, 134, 141, 149, 160, 176, 185, 195, 263
- Correlated Events 291
- Covert Channels TCP port 53 291
- CrashOnAuditFail is True 236
- Critical Network Events 177
- Critical Services 237
- Database Configuration Changes 129, 141, 265
- Database Errors 141
- Database Events 128, 141, 142, 263
- Delivery Connection (Cisco ESA) 105
- Denied Inbound Connections 149
- Denied Outbound Connections 149
- Denied Web Server Requests 111
- Device Vendor AND Product are NULL 264
- Device Vendor OR Product is NULL 264
- Device Version is NULL 264
- Email Message Transaction (Cisco ESA) 30, 105
- Events with Vulnerabilities 290
- External Source 127, 150, 242, 275, 292
- External Target 150, 243, 276, 293
- Failed Authentication Events - All 225
- Failed Authentication Events - Domain 225
- Failed Authentication Events - Workstation 225
- Failed Firewall Login Events 150
- Failed Identity Management Login Attempts 160
- Failed Login Events 149, 176, 185, 196
- Failed Logins 291
- Failed Logins with Target Information 290
- Failed Network Login Events 176
- Failed Operating System Login Events 186
- Failed VPN Connection Events 196
- Failed VPN Connection Events (Cisco ASA) 45
- Failed VPN Login Events 196
- Firewall Accepts 31, 47, 67, 78
- Firewall Access Events 31, 46, 57, 66, 78
- Firewall Configuration Changes 128, 150, 264
- Firewall Deny 31, 46, 66, 78, 292
- Firewall Events 129, 150, 169, 264, 289
- Firewall Login Events 150
- High Events 292
- Host Configuration Modifications 265
- Host Problems 263
- ICMP Traffic 276
- Identity Management Connection Start Events 160
- Identity Management Events 128, 160
- IDS -IPS Events 128, 150, 169, 292
- Inbound Events 29, 45, 66, 78, 128, 150, 243, 276
- Inbound NetFlow Traffic 243
- Inbound Traffic 276
- Injection Connection (Cisco ESA) 105
- Internal Attackers 32, 47, 67, 78
- Internal Source 128, 149, 176, 196, 243, 276, 289
- Internal Target 128, 149, 176, 196, 243, 276, 289
- Internal Targets 31, 46, 66, 78
- Internal to Internal Events 289
- Large Mail-Outbound 290
- LockedCount is NULL 216
- Login Attempts 29, 56
- Login Events 149, 176, 185, 195
- Malware-Outbound 290
- NetFlow Traffic Reporting Devices 243
- NetFlow V5 Events 244
- NetFlow V9 Events 243
- Network Configuration Changes 128, 263

- Network Device Interface Down Messages 177
- Network Device Interface Status Events 177
- Network Error Events 177
- Network Events 127, 176, 263
- Network Login Events 176
- Network Traffic Reporting Devices 276
- Non ArcSight Internal Event - Target Port Not Null 292
- Non ArcSight Internal Event with TargetPort Set 291
- Non-ArcSight Events 129, 136, 142, 151, 160, 177, 186, 197, 265, 293
- Non-ArcSight Internal Events 293
- Non-Root-Admin Failed Logins 268, 292
- Non-Root-Admin Logins 268, 290
- Non-Well-Known Ports 243
- Not Correlated and Not Closed and Not Hidden 291
- Notification Event has Acknowledgement Status 249, 271
- Notification Event has Configuration Resource 249, 271
- Notification Event has Destination Group 248, 271
- Notification Event has Rule Name 248, 271
- Notification Event has User Name 248, 271
- Notification Events 249, 271
- Operating System Events 128, 185
- Operating System Login Events 186
- Outbound Events 30, 46, 67, 78, 150, 243, 275, 290
- Outbound NetFlow Traffic 243
- Outbound Traffic 276
- Policy Changes 229
- QoSient Argus 276
- QoSient Argus Events 243
- Reconnaissance Events (Internal Targets) 289
- Reconnaissance Events by Attacker 289
- Reconnaissance Events by Target 291
- Reconnaissance Events by Target Zone 291
- Rejected Injection Connection (Cisco ESA) 105
- Root-Admin Failed Logins 268, 289
- Root-Admin Logins 268, 290
- Service Started Action Count is NULL 237
- Service Stopped Action Count is NULL 236
- Single-digit Day 257
- Single-digit Hour 257
- Single-digit Minute 256
- Single-digit Month 257
- SNMP Authentication Failed 116
- SNMP Events 116
- Successful Attacks 293
- Successful Configuration Changes 30, 46, 66, 77, 88, 94, 100, 105, 110, 116, 129, 141, 150, 196, 264
- Successful Configuration Changes (Cisco ESA) 105
- Successful Firewall Login Events 151
- Successful Login Events 149, 176, 185, 196
- Successful Logins 29, 55
- Successful Network Login Events 177
- Successful Operating System Login Events 186
- Successful Password Changes 141, 160, 186, 196, 263
- Successful VPN Connection Events 197
- Successful VPN Connection Events (Cisco ASA) 47
- Successful VPN Login Events 196
- Successful Web Transactions 30, 110
- Successful WSA Configuration Changes 110
- SYN Traffic 275
- System Services and Auditing Violations 236
- Target Address is NULL 134, 263, 289
- Target Host Name is NULL 134, 263, 291
- Target Host or Address Present 29, 45, 55, 66, 77, 87, 94, 100, 105, 115
- Target Information is NULL 264
- Target Port Activity By Attacker 169, 291
- Target Port is NULL 264, 276
- Target User ID is NULL 160, 195
- Target User Present 30, 46, 56, 116
- Target User with Domain Information 205, 216, 225, 229, 237
- Target Zone AND Host are NULL 264
- Target Zone AND Host are NULL but Address is NOT NULL 263
- Target Zone is NULL 135, 264, 292
- Target Zone OR Host is NULL 265
- TCP Traffic 275
- Top Non-US Destinations 275, 290
- Top Non-US Sources 276, 290
- UDP Traffic 275
- Unsuccessful Logins 30, 56
- Unsuccessful Web Server Requests 31, 111
- Update Events 134
- User Accounts Created, Deleted, Disabled, or Enabled 216
- Very High Events 290
- Virus Activity 135
- VPN Authentication Errors 197
- VPN Authentication Errors (Cisco ASA) 47
- VPN Configuration Changes 128, 196, 265
- VPN Events 46, 127, 195, 263
- VPN Login Events 196
- Web Requests 29, 110
- Well-Known Ports 244
- Windows Events 205, 216, 225, 229, 236
- Windows Events with a Non-Machine User 30, 56
- Worm Activity 169, 289
- Worm Outbreak 169, 291
- Worm Traffic 169, 293
- Final Stage Cases by Owner (Chart) query 258
- Final Stage Cases by Owner query viewer 252
- Firewall Accepts filter 31, 47, 67, 78
- Firewall Access Events filter 31, 46, 57, 66, 78
- Firewall Bandwidth Usage by Hour (chart) query 249, 278
- Firewall Bandwidth Usage per Hour query 249, 278
- Firewall Configuration Changes filter 128, 150, 264
- Firewall Connection Overview dashboard 16, 144
- Firewall Deny filter 31, 46, 66, 78, 292
- Firewall Events active channel 124, 144
- Firewall Events filter 129, 150, 169, 264, 289
- Firewall field set 275
- Firewall Login Events filter 150
- Firewall Login Overview dashboard 144
- Firewall use case 130
- focused reports
 - Bandwidth Usage by Protocol 151, 178, 198
 - Bandwidth Usage per Hour 152, 179, 197
 - Configuration Changes by Type 136, 142, 152, 161, 177, 186, 199
 - Configuration Changes by User 136, 142, 151, 162, 177, 186, 198

Exposed Vulnerability Count by Critical Asset 297
 Failed Login Attempts 161, 187
 Failed Logins by Destination Address 151, 160, 179, 187, 197
 Failed Logins by Source Address 151, 161, 178, 187, 199
 Failed Logins by User 153, 162, 178, 187, 197
 Login Event Audit 142, 152, 178, 186, 198
 Password Changes 142, 161, 188, 198
 Successful Logins by Destination Address 152, 161, 179, 188, 198
 Successful Logins by Source Address 152, 161, 177, 187, 197
 Successful Logins by User 152, 161, 178, 187, 198
 Top 10 Alerts 169
 Top 10 Attackers 169
 Top 10 Targets 169
 Top Bandwidth Hosts 152, 178, 198
 Top Hosts by Number of Connections 151, 178, 198
 Follow-Up Stage Cases by Owner (Chart) query 258
 Follow-Up Stage Cases by Owner query viewer 252

G

global variables

Attacker_HostName 205, 216, 224, 229, 236
 Attacker_NTDomain 205, 216, 224, 229, 236
 Attacker_User 205, 216, 224, 229, 236
 DateTime 256
 DateValue 256
 Day 256
 Device_HostName 205, 216, 225, 229, 236
 Device_NTDomain 205, 216, 225, 229, 236
 DeviceInfo 262
 EndTimeValue 256
 Hour 256
 Minute 256
 Month 256
 Target_HostName 205, 215, 224, 229, 235
 Target_NTDomain 205, 215, 224, 229, 236
 Target_User 205, 215, 224, 228, 236
 TargetHost 262
 TotalBytes 242
 Year 256

H

High asset category 296
 High Events data monitor 287
 High Events filter 292
 High Number of Connections rule 126, 147, 274
 High Number of Denied Connections for A Source Host rule 126, 147, 274
 High Number of Denied Inbound Connections rule 126, 147, 274
 High Number of IDS Alerts for Backdoor rule 168, 284
 High Number of IDS Alerts for DoS rule 167, 282
 Host Configuration Change Event Counts by Zone data monitor 262
 Host Configuration Modifications - Today query viewer 260
 Host Configuration Modifications - Yesterday query viewer 261
 Host Configuration Modifications by OS query 265

Host Configuration Modifications by OS report 261
 Host Configuration Modifications dashboard 260
 Host Configuration Modifications filter 265
 Host Configuration Modifications query 265
 Host Problem Event Counts by Zone data monitor 262
 Host Problems filter 263
 Host Problems Overview dashboard 260
 Hour global variable 256
 HTTP Status Code Classes active list 110

I

ICMP Traffic filter 276
 Identity Management Connection Start Events filter 160
 Identity Management Events active channel 125, 156
 Identity Management Events filter 128, 160
 Identity Management Overview dashboard 156
 Identity Management use case 131
 IDS - IPS Events active channel 124, 165
 IDS - IPS Overview dashboard 16, 165
 IDS - IPS use case 130
 IDS field set 127, 169, 288
 IDS -IPS Events filter 128, 150, 169, 292
 Inbound Bandwidth (Bytes Per Second) data monitor 242
 Inbound Connection Setup Attempts per Day (Cisco ASA) report 43
 Inbound Connection Setup Attempts per Day (Cisco FWSM) report 64
 Inbound Events filter 29, 45, 66, 78, 128, 150, 243, 276
 Inbound NetFlow Traffic filter 243
 Inbound Traffic - Top Protocols report 273
 Inbound Traffic - Top Source Hosts report 273
 Inbound Traffic by Application Protocol query 277
 Inbound Traffic by Source Host query 278
 Inbound Traffic by Transport Protocol query 277
 Inbound Traffic filter 276
 Infected Systems data monitor 133
 Infected Systems query 136, 293
 Initial Stage Cases by Owner (Chart) query 258
 Initial Stage Cases by Owner query viewer 252
 Injection Connection (Cisco ESA) filter 105
 Injection Connections by Hour query viewer 102
 Injection Connections query 106
 Injection Connections query viewer 103
 Install Service Attempt rule 233
 integration commands
 EventID.net 206
 integration configurations
 MS - Event Lookup 206
 Interesting Mail dashboard 16, 281
 Internal Attackers filter 32, 47, 67, 78
 Internal Source filter 128, 149, 176, 196, 243, 276, 289
 Internal Target filter 128, 149, 176, 196, 243, 276, 289
 Internal Targets filter 31, 46, 66, 78
 Internal to Internal Events filter 289
 IOS IPS Event Counts by Hour per Device query 32, 101
 IOS IPS Event Counts by Hour query 36, 101
 IPS Configuration Changes per Day in the Last 7 Days query 90
 IPS Sensor Event Counts by Hour per Device query 33, 95
 IPS Sensor Event Counts by Hour query 35, 95
 IPS Sensor Hourly Event Count per Device query viewer

23, 92
IPS Sensor Hourly Event Count query viewer 23, 92
IPS Syslog Events from Cisco ASA Systems active channel 40

L

Large Mail-Outbound filter 290
Last 10 Anti-Virus Errors data monitor 134
Last 10 Cisco FWSM Successful Configuration Changes data monitor 28, 66
Last 10 Cisco IOS IPS Successful Configuration Changes data monitor 27, 99
Last 10 Cisco IPS Sensor Successful Configuration Changes data monitor 28, 93
Last 10 Critical Network Events data monitor 175
Last 10 Database Configuration Changes data monitor 127, 261
Last 10 Database Errors data monitor 141
Last 10 Failed Login Events data monitor 148, 175, 185, 194
Last 10 Firewall Configuration Changes data monitor 127, 261
Last 10 Hosts Scanned data monitor 286
Last 10 Interface Down Messages data monitor 175
Last 10 Interface Status Messages data monitor 175
Last 10 Network Configuration Changes data monitor 127, 262
Last 10 Scanners data monitor 286
Last 10 Successful Login Events data monitor 148, 175, 185, 194
Last 10 VPN Configuration Changes data monitor 127, 261
Last 10 Zones Scanned data monitor 285
Last 20 Host Configuration Modification Events data monitor 262
Last 20 Host Problems data monitor 262
Last 5 Minutes active channel 15
Last Failed Logins data monitor 287
Level 3 Notifications Overview Chart query 272
List of Top Bandwidth Usage Events query 245
List of Top Bandwidth Usage Events query viewer 241
Live active channel 15
Locked Account Re-enabled rule 211
Locked Out Accounts session list 220
LockedCount is NULL filter 216
Lockout Attempt Failed rule 211
Lockout Policy Changed rule 228
Login Attempts filter 29, 56
Login Errors by User (Chart) query 189, 269
Login Errors by User query 189, 269
Login Errors by User report 184, 267
Login Event Audit focused report 142, 152, 178, 186, 198
Login Event Audit query 142, 153, 179, 188, 199, 268
Login Event Audit report 140, 145, 172, 183, 191, 266
Login Events filter 149, 176, 185, 195
Login Information dashboard 17, 266, 281
Login Overview dashboard 21, 52
Login Results data monitor 148, 175, 185, 195
Logins per Day in the Last 7 Days query 33, 59
Logins per Day report 53
Logins per Hour in the Previous Day query 58
Logins per Hour in the Previous Day report 53
Logins use case 250

Logon Types active list 224

M

Malware dashboard 17, 281
Malware Real-Time Tracking data monitor 285
Malware-Outbound filter 290
Max Time to Case Resolution - By User report 254
Maximum Time to Case Resolution - By User Chart query 259
Maximum Time to Case Resolution - By User query 259
Maximum Time to Case Resolution - by User query viewer 253
Message Transaction Details query 35, 107
Message Transaction Details query viewer 25, 103
Message Transaction per Hour in the Previous Day (Cisco ESA) report 104
Message Transactions per Day (Cisco ESA) report 104
Message Transactions per Day in the Previous Week query 107
Message Transactions per Hour in the Previous Day query 107
Microsoft field set 267
Microsoft Windows Event Log- Unified SmartConnector 203
Microsoft Windows Monitoring use case 18
Microsoft-Authentication active channel 266
Minute global variable 256
Modified Computer Accounts session list 219
Modified Privileged Accounts - Chart query 219
Modified Privileged Accounts - Table query 218
Modified Windows Privileged Accounts query viewer 209
Modified Windows Privileged Accounts report 210
Modified Windows Privileged Group Members - Chart query 219
Modified Windows Privileged Group Members - Table query 217
Modified Windows Privileged Group Members report 209
Monitor New Case rule 255
Month global variable 256
Most Common Host Configuration Change Events data monitor 261
Most Common Host Problem Events data monitor 262
Most Frequent Ports data monitor 27, 55, 285
MS - Event Lookup integration configuration 206

N

NetFlow Bandwidth Usage Overview dashboard 240
NetFlow Monitoring use case 17
NetFlow Traffic Reporting Devices filter 243
NetFlow V5 Events filter 244
NetFlow V9 Events filter 243
Network Configuration Changes filter 128, 263
Network Device Interface Down Messages filter 177
Network Device Interface Status Events filter 177
Network Error Events filter 177
Network Events active channel 125, 172
Network Events filter 127, 176, 263
Network Login Events filter 176
Network Login Overview dashboard 172
Network Status Overview dashboard 172
Network Traffic Reporting Devices filter 276
Network use case 130
Non ArcSight Internal Event - Target Port Not Null filter

292

Non ArcSight Internal Event with TargetPort Set filter 291

Non-ArcSight Events filter 129, 136, 142, 151, 160, 177, 186, 197, 265, 293

Non-ArcSight Internal Events filter 293

Non-Root-Admin Failed Logins data monitor 267, 288

Non-Root-Admin Failed Logins filter 268, 292

Non-Root-Admin Logins data monitor 267, 288

Non-Root-Admin Logins filter 268, 290

Non-Well-Known Ports filter 243

Not Correlated and Not Closed and Not Hidden filter 291

Notification Event has Acknowledgement Status filter 249, 271

Notification Event has Configuration Resource filter 249, 271

Notification Event has Destination Group filter 248, 271

Notification Event has Rule Name filter 248, 271

Notification Event has User Name filter 248, 271

Notification Events active channel 248, 270

Notification Events filter 249, 271

Notification field set 271

Notification Overview query 272

Notification Overview report 270

Notification Statistics Summary report 270

Notification Status Report query 272

Notification Status Report report 271

Notifications By Acknowledgement Status Chart query 272

Notifications By Acknowledgement Status query 271

Notifications By Acknowledgement Status report 270

Notifications field set 248, 271

Notify on Successful Attack rule 283

O

Open Cases by Associated Impact (Chart) query 249, 258

Open Cases by Associated Impact query viewer 253

Open Cases by Consequence Severity (Chart) query 250, 258

Open Cases by Consequence Severity query viewer 252

Open Cases by Operational Impact (Chart) query 250, 259

Open Cases by Operational Impact query viewer 253

Open Cases by Stage query viewer 251

Open Cases Details query 258

Open Cases query 259

Open Cases query viewer 253

Open Cases report 254

Operating System asset category 261

Operating System Events active channel 124, 183

Operating System Events filter 128, 185

Operating System Login Events filter 186

Operating System Login Overview dashboard 183

Operating System use case 130

Operations use case 18

Outbound Bandwidth (Bytes Per Second) data monitor 242

Outbound Connection Setup Attempts per Day (Cisco ASA) report 43

Outbound Connection Setup Attempts per Day (Cisco FWSM) report 64

Outbound Events filter 30, 46, 67, 78, 150, 243, 275, 290

Outbound High Port Traffic data monitor 286

Outbound Mail over 20MB data monitor 286

Outbound NetFlow Traffic filter 243

Outbound Traffic - Top Protocols report 274

Outbound Traffic - Top Source Hosts report 273

Outbound Traffic by Application Protocol query 278

Outbound Traffic by Source Host query 277

Outbound Traffic by Transport Protocol query 277

Outbound Traffic filter 276

Overview of Cisco Configuration Changes report 25

Overview of Logins Reported by Cisco Devices - Systems report 25

Overview of Logins Reported by Cisco Devices - Trend and Users report 26

P

Parent URIs 14

Password Changes focused report 142, 161, 188, 198

Password Changes query 143, 163, 189, 200, 265

Password Changes report 140, 157, 183, 192, 261

Password Policy Changed rule 228

Policy Changes dashboard 227

Policy Changes data monitor 228

Policy Changes filter 229

Policy Changes session list 229

Policy Changes use case 206, 227

Port Monitor data monitor 287

Possible Internal Network Sweep rule 283

Possible Outbound Network Sweep rule 284

Privileged Account Deleted rule 213

Privileged Account Disabled rule 212

Privileged Account Enabled rule 212

Privileged Account field set 216

Privileged Account Locked Out rule 214

Privileged Account Modified rule 212

Privileged Account Password Changed rule 214

Privileged Accounts active list 214

Privileged Accounts Modified - Drilldown query viewer 209

Privileged Accounts Modified active list 214

Privileged Accounts Modified query viewer 209

Privileged Group Members Modified active list 215

Privileged Groups active list 215

Protected asset category 17, 26, 45, 65, 77, 127, 133, 140, 148, 159, 168, 174, 185, 194, 204, 242, 284, 296

Proxy asset category 168, 284

Q

QoSient Argus Events filter 243

QoSient Argus filter 276

queries

- Alert Counts by Device 170
- Alert Counts by Port 170
- Alert Counts by Severity 170
- Alert Counts by Severity (Chart) 170
- Alert Counts by Type 170
- Alert Counts per Hour 171
- All Cases 258
- All Level 3 Notifications 272
- Allowed Inbound Connections by Destination Address (Cisco ASA) 47
- Allowed Inbound Connections by Destination

- Address (Cisco FWSM) 68
- Allowed Inbound Connections by Port (Cisco ASA) 48
- Allowed Inbound Connections by Port (Cisco FWSM) 69
- Allowed Inbound Connections by Source Address (Cisco ASA) 47
- Allowed Inbound Connections by Source Address (Cisco FWSM) 68
- Allowed Outbound Connections by Destination Address (Cisco ASA) 48
- Allowed Outbound Connections by Destination Address (Cisco FWSM) 70
- Allowed Outbound Connections by Port (Cisco ASA) 50
- Allowed Outbound Connections by Port (Cisco FWSM) 69
- Allowed Outbound Connections by Source Address (Cisco ASA) 49
- Allowed Outbound Connections by Source Address (Cisco FWSM) 70
- Anti-Virus Errors 137
- Associated APs per Device 121
- Associated Devices in a Day - Event Based 121
- Associated Devices per AP 121
- Association - Disassociation Details 121
- Association - Disassociation per Day 121
- Audit Logs Cleared - Chart 237
- Audit Logs Cleared - Table 237
- Authentication Errors 200
- Authentication Errors (Cisco ASA) 48
- Average Time to Case Resolution - By Day 259
- Average Time to Case Resolution - By Severity 258
- Average Time to Case Resolution - By User 257
- Bandwidth Usage by Firewall Address 249, 278
- Bandwidth Usage by Protocol 47, 58, 68, 79, 129, 153, 180, 199, 277
- Bandwidth Usage per Hour 48, 58, 68, 80, 129, 155, 180, 200, 278
- Bandwidth Utilization - By Hour 277
- Bandwidth Utilization - By Minute 278
- By User Account - Accounts Created 265
- Cases Created Today 258
- Cases Open by Stage (Chart) 249, 258
- Cases per Target 258
- Cisco Alert Counts by Port 88
- Cisco Alert Counts by Port and Device 89
- Cisco Alert Counts by Reporting Device 88
- Cisco Alert Counts by Severity 90
- Cisco Alert Counts by Severity and Device 89
- Cisco Alert Counts by Type and Device 89
- Cisco Alert Details (Trend Based) 89, 95, 101
- Cisco Alerts per Day 33, 90
- Cisco Alerts per Hour in the Previous Day 90
- Cisco Allowed Connections by Destination Host - Template 82
- Cisco Allowed Connections by Port - Template 80
- Cisco Allowed Connections by Source Host - Template 80
- Cisco ASA Event Counts by Hour in Last 6 Hours 35, 49
- Cisco ASA Event Counts by Hour per Device 37, 50, 82
- Cisco ASA Inbound Connections per Day 50
- Cisco ASA Outbound Connections per Day 48
- Cisco Configuration Change Detail (Trend Based) 37, 60
- Cisco Configuration Changes (Event Based) 35, 47, 58, 68, 80, 89, 96, 101, 107, 111
- Cisco Configuration Changes by User (Event Based) 33, 49, 59, 69, 81, 89, 95, 101, 106, 111, 117
- Cisco Denied Connections by Destination Host - Template 79
- Cisco Denied Connections by Port - Template 79
- Cisco Denied Connections by Source Host - Template 81
- Cisco Device Critical Events 117
- Cisco Device Errors 118
- Cisco Device Interface Status Messages 117
- Cisco Device SNMP Authentication Failures 116
- Cisco Device SNMP Authentication Failures by User 117
- Cisco ESA Configuration Changes in the Last 6 Hours 34, 59
- Cisco ESA Configuration Changes per Day in the Last 7 Days 107
- Cisco ESA Delivery Connection Count by Hour 107
- Cisco ESA Injection Connection Count by Hour 106
- Cisco Event Count by Hour 32, 58
- Cisco Firewall Configuration Changes in the Last 6 Hours 35, 58
- Cisco Firewall Configuration Changes per Day in the Last 7 Days 79
- Cisco Firewall Event Counts by Hour 79
- Cisco FWSM Event Counts by Hour 34, 67
- Cisco FWSM Event Counts by Hour per Device 37, 70, 82
- Cisco FWSM Inbound Connections per Day 69
- Cisco FWSM Outbound Connections per Day 68
- Cisco IPS Configuration Changes in the Last 6 Hours 33, 58
- Cisco Login Detail (Trend Based) 34, 57
- Cisco Network Configuration Changes per Day in the Last 7 Days 117
- Cisco Network Equipment Configuration Change By Event 118
- Cisco Network Equipment Configuration Changes in the Last 6 Hours 34, 59
- Cisco Network Event Count by Hour 117
- Cisco Overall Allowed Inbound Connections by Destination Host 36, 81
- Cisco Overall Allowed Inbound Connections by Port 79
- Cisco Overall Allowed Inbound Connections by Source Host 34, 80
- Cisco Overall Allowed Outbound Connections by Destination Host 36, 80
- Cisco Overall Allowed Outbound Connections by Port 81
- Cisco Overall Allowed Outbound Connections by Source Host 35, 80
- Cisco Overall Denied Inbound Connections by Destination Host 34, 81
- Cisco Overall Denied Inbound Connections by Port 35, 48, 68, 80
- Cisco Overall Denied Inbound Connections by Source Host 33, 49, 69, 81
- Cisco Overall Denied Inbound Connections per Hour - Event Based 69

- Cisco Overall Denied Inbound Connections per Hour in the Previous Day 81
- Cisco Overall Denied Outbound Connections by Destination Host 37, 82
- Cisco Overall Denied Outbound Connections by Port 34, 50, 70, 82
- Cisco Overall Denied Outbound Connections by Source Host 33, 48, 68, 80
- Cisco Overall Denied Outbound Connections per Hour - Event Based 70
- Cisco Overall Inbound Connections per Day 35, 80
- Cisco Overall Outbound Connections per Day 32, 79
- Cisco Overall Outbound Connections per Hour in the Previous Day 79
- Cisco SNMP Access (Trend Based) 118
- Cisco SNMP Access On Certain Target (Trend Based) 117
- Cisco SNMP Authentication Failures by Device 117
- Cisco WSA Configuration Changes in the Last 6 Hours 33, 59
- Cisco WSA Configuration Changes per Day in the Last 7 Days 111
- Closed Connection Durations 162
- Closed VPN Connection Durations 200
- Computer Accounts Created Weekly - Chart 218
- Computer Accounts Created Weekly - Table 217
- Computer Accounts Deleted Weekly - Chart 217
- Computer Accounts Deleted Weekly - Table 218
- Computer Accounts Modified Weekly - Chart 218
- Computer Accounts Modified Weekly - Table 219
- Configuration Changes 129, 137, 143, 155, 163, 180, 189, 201, 265
- Configuration Changes per Day in the Last 7 Days 36, 59
- Configuration Changes per Hour in the Previous Day 32, 58
- Connections Accepted by Address 199
- Connections Accepted by Address (Cisco ASA) 48
- Connections Denied by Address 200
- Connections Denied by Address (Cisco ASA) 48
- Connections Denied by Hour 201
- Critical Services Started or Stopped - Chart 237
- Critical Services Started or Stopped - Table 237
- Daily Account Lockouts 218
- Daily Alerts - Base 37, 60, 90, 95, 101
- Daily Associations - Disassociations (Base) 121
- Daily Configuration Changes - Base 34, 60, 82, 90, 107, 112, 118, 121
- Daily Connection Setup Attempts - Base 37, 50, 59, 69, 81
- Daily Logins - Base 37, 60
- Daily Logins per Product 35
- Daily Message Transactions - Base 32, 106
- Daily SNMP Access - Base 117
- Daily Web Requests - Base 111
- Database Errors and Warnings 143
- Database Errors and Warnings (Chart) 142
- Delivery Connections 106
- Denied Inbound Connections by Address 154
- Denied Inbound Connections by Destination Address (Cisco ASA) 49
- Denied Inbound Connections by Destination Address (Cisco FWSM) 68
- Denied Inbound Connections by Port 154
- Denied Inbound Connections by Port (Cisco ASA) 48
- Denied Inbound Connections by Port (Cisco FWSM) 67
- Denied Inbound Connections by Source Address (Cisco ASA) 50
- Denied Inbound Connections by Source Address (Cisco FWSM) 67
- Denied Inbound Connections per Hour 154
- Denied Inbound Connections per Hour (Chart) 155
- Denied Outbound Connections by Address 153
- Denied Outbound Connections by Destination Address (Cisco ASA) 49
- Denied Outbound Connections by Destination Address (Cisco FWSM) 69
- Denied Outbound Connections by Port 153
- Denied Outbound Connections by Port (Cisco ASA) 49
- Denied Outbound Connections by Port (Cisco FWSM) 68
- Denied Outbound Connections by Source Address (Cisco ASA) 50
- Denied Outbound Connections by Source Address (Cisco FWSM) 69
- Denied Outbound Connections per Hour 154
- Denied Outbound Connections per Hour (Chart) 155
- Detail Successful Requests 33, 112
- Detail Unsuccessful Requests 112
- Device Critical Events 180
- Device Errors 181
- Device Events 181
- Device Interface Down Notifications 179
- Device Interface Status Messages 181
- Device SNMP Authentication Failures 182
- Device SNMP Authentication Failures by User 181
- Disassociated Devices 121
- Disassociated Devices per AP 121
- Exposed Vulnerabilities by Asset 297
- Exposed Vulnerability Count by Asset 297
- Failed Anti-Virus Updates 136
- Failed Anti-Virus Updates Chart 136
- Failed Login Attempts 163, 188, 268
- Failed Login Attempts (Chart) 162, 188, 268
- Failed Login by User 155, 164, 180, 189, 201, 269
- Failed Login by User (Chart) 153, 163, 180, 188, 199, 268
- Failed Logins by Destination Address 32, 57
- Failed Logins by Destination Address (Chart) 153, 162, 179, 188, 199, 268
- Failed Logins by Source Address 33, 58
- Failed Logins by Source Address (Chart) 153, 162, 181, 188, 201, 268
- Failed Logins by Source-Destination Pair 154, 163, 181, 189, 202, 268
- Failed Logins by User 34, 60
- Final Stage Cases by Owner (Chart) 258
- Firewall Bandwidth Usage by Hour (chart) 249, 278
- Firewall Bandwidth Usage per Hour 249, 278
- Follow-Up Stage Cases by Owner (Chart) 258
- Host Configuration Modifications 265
- Host Configuration Modifications by OS 265
- Inbound Traffic by Application Protocol 277
- Inbound Traffic by Source Host 278
- Inbound Traffic by Transport Protocol 277
- Infected Systems 136, 293

- Initial Stage Cases by Owner (Chart) 258
- Injection Connections 106
- IOS IPS Event Counts by Hour 36, 101
- IOS IPS Event Counts by Hour per Device 32, 101
- IPS Configuration Changes per Day in the Last 7 Days 90
- IPS Sensor Event Counts by Hour 35, 95
- IPS Sensor Event Counts by Hour per Device 33, 95
- Level 3 Notifications Overview Chart 272
- List of Top Bandwidth Usage Events 245
- Login Errors by User 189, 269
- Login Errors by User (Chart) 189, 269
- Login Event Audit 142, 153, 179, 188, 199, 268
- Logins per Day in the Last 7 Days 33, 59
- Logins per Hour in the Previous Day 58
- Maximum Time to Case Resolution - By User 259
- Maximum Time to Case Resolution - By User Chart 259
- Message Transaction Details 35, 107
- Message Transactions per Day in the Previous Week 107
- Message Transactions per Hour in the Previous Day 107
- Modified Privileged Accounts - Chart 219
- Modified Privileged Accounts - Table 218
- Modified Windows Privileged Group Members - Chart 219
- Modified Windows Privileged Group Members - Table 217
- Notification Overview 272
- Notification Status Report 272
- Notifications By Acknowledgement Status 271
- Notifications By Acknowledgement Status Chart 272
- Open Cases 259
- Open Cases by Associated Impact (Chart) 249, 258
- Open Cases by Consequence Severity (Chart) 250, 258
- Open Cases by Operational Impact (Chart) 250, 259
- Open Cases Details 258
- Outbound Traffic by Application Protocol 278
- Outbound Traffic by Source Host 277
- Outbound Traffic by Transport Protocol 277
- Password Changes 143, 163, 189, 200, 265
- Queued Stage Cases by Owner (Chart) 258
- Recently Closed Cases 249, 257
- Request Errors 112
- SIS-Assets Compromised Table Query 294
- SIS-Cases Added Table Query 294
- SIS-Event Count by Agent Severity Chart Query 294
- SIS-Notifications Sent Table Query 294
- SIS-Top Attackers Chart Query 294
- SIS-Top Attacks Table Query 293
- SIS-Top Events Table Query 294
- SIS-Top Firing Rules Table Query 293
- SIS-Top Target Ports Chart Query 295
- SIS-Top Targets Chart Query 294
- SNMP Authentication Failures by Device 181
- Successful Login by Source Address 35, 58
- Successful Login by User 154, 163, 180, 189, 200, 269
- Successful Login by User (Chart) 154, 163, 182, 189, 202, 269
- Successful Logins by Destination Address 33, 58
- Successful Logins by Destination Address (Chart) 155, 164, 181, 190, 201, 269
- Successful Logins by Source Address (Chart) 153, 162, 179, 188, 199, 268
- Successful Logins by Source-Destination Pair 154, 163, 182, 189, 202, 269
- Successful Logins by User 36, 59
- System Time Changes - Chart 237
- System Time Changes - Table 237
- Top 10 Assets by Exposed Vulnerability Counts 297
- Top 10 Attackers 170
- Top 10 Targets 170
- Top Accessed Sites 36, 111
- Top Accessed Sites with Most Traffic 35, 112
- Top Alert Destinations 170
- Top Alert Sources 169
- Top Anti-Virus Errors 137
- Top Attackers 277
- Top Attackers and Reporting Devices in Cisco Alerts 89
- Top Attackers in Cisco Alerts 34, 89
- Top Attackers in Cisco Alerts (Trend Based) 89
- Top Attackers in Cisco IOS IPS Alerts 101
- Top Bandwidth Destination Hosts 50, 60, 70, 82
- Top Bandwidth Hosts 129, 154, 180, 200, 278
- Top Bandwidth Source Hosts 49, 59, 69, 81
- Top Bandwidth Usage by Day - Trend on Trend 244
- Top Bandwidth Usage by Destination 244
- Top Bandwidth Usage by Destination - Trend 245
- Top Bandwidth Usage by Destination - Trend on Trend 244
- Top Bandwidth Usage by Destination and Port 245
- Top Bandwidth Usage by Hour - Trend 245
- Top Bandwidth Usage by Hour - Trend on Trend 244
- Top Bandwidth Usage by Non-Well-Known Port 245
- Top Bandwidth Usage by Port - Trend 244
- Top Bandwidth Usage by Port - Trend on Trend 245
- Top Bandwidth Usage by Source 244
- Top Bandwidth Usage by Source - Trend 245
- Top Bandwidth Usage by Source - Trend on Trend 245
- Top Bandwidth Usage by Source and Port 244
- Top Bandwidth Usage by Source-Destination Pairs 244
- Top Bandwidth Usage by Source-Destination Pairs and Port 245
- Top Bandwidth Usage by Well-Known Port 245
- Top Bandwidth Usage Events 244
- Top Cisco Alert Destinations Observed by IPS Sensor 95
- Top Cisco Alert Sources Observed by IPS Sensor 95
- Top Cisco Alerts 36, 90
- Top Cisco Alerts (Trend Based) 89
- Top Connection Durations 163
- Top Connections Accepted by Address 200
- Top Connections Denied by Address 201
- Top Denied Sites 112
- Top Device System Authentication Events 179
- Top Hosts by Number of Connections 153, 181, 201
- Top Hosts with Most Web Traffic 33, 112
- Top IDS and IPS Alerts 170
- Top Infected Systems 137, 294
- Top Protocols 276

- Top Recipients with Most Bandwidth 32, 106
- Top Recipients with Most Transactions 36, 107
- Top Senders with Most Bandwidth 32, 106
- Top Senders with Most Transactions 35, 106
- Top Sites with Most Request Errors 36, 111
- Top Source Hosts Accessed Most Sites 34, 112
- Top Source Hosts with Most Denied Requests 112
- Top Source Hosts with Most Request Errors 111
- Top Systems Receiving Most Delivery Connections 106
- Top Systems Sending Most Injection Connections 106
- Top Systems Sending Most Rejected Injection Connections 106
- Top Target Weekly Cisco SNMP Access on Device 117
- Top Targets 277
- Top Targets and Reporting Devices in Cisco Alerts 89
- Top Targets in Cisco Alerts 36, 89
- Top Targets in Cisco Alerts (Trend Based) 90
- Top Targets in Cisco IOS IPS Alerts 101
- Top Users by Connection Count 163, 202
- Top Users with Most Failed Logins 36, 59
- Top Users with Successful Logins 36, 59
- Top VPN Connection Durations 201
- Top Windows Devices by Event Count - Trend 206
- Top Zones with Anti-Virus Errors 137
- Trend on Case Audit Events 259
- Unacknowledged Level 3 Notifications 272
- Update Summary 138
- Update Summary Chart 137
- User Accounts Created Weekly - Chart 217
- User Accounts Created Weekly - Table 217
- User Accounts Deleted Weekly - Chart 217
- User Accounts Deleted Weekly - Table 216
- User Accounts Disabled Weekly - Chart 218
- User Accounts Disabled Weekly - Table 218
- User Accounts Enabled Weekly - Chart 217
- User Accounts Enabled Weekly - Table 218
- User Administration 189, 250
- User Administration (Chart) 188, 249
- User Configuration Modifications 265
- Users by Connection Count 162, 201
- Users by Connection Count (Cisco ASA) 49
- Users with Open Connections 162
- Users with Open VPN Connections 202
- Virus Activity by Hour 136, 293
- Web Requests per Day in the Previous Week 112
- Web Requests per Hour in the Previous Day 112
- Weekly Account Lockouts - Chart 217
- Weekly Account Lockouts - Table 219
- Weekly Hosts With Multiple Failed Authentications - Chart 226
- Weekly Hosts With Multiple Failed Authentications-Table 226
- Weekly Policy Changes 229
- Weekly Users With Multiple Failed Authentications - Chart 225
- Weekly Users With Multiple Failed Authentications by Reason - Chart 225
- Weekly Users With Multiple Failed Authentications-Table 226
- Windows Events by Device Trend 206
- Worm Infected Systems 170
- query viewers
 - Associated Devices in a Day (Event Based) 119
 - Associations - Disassociations (Trend Based) 120
 - Average Time to Case Resolution - by Day 252
 - Average Time to Case Resolution - by Severity 252
 - Average Time to Case Resolution - by User 252
 - Cisco Alert Counts by Port in the Last 2 Hours 85
 - Cisco Alert Counts by Severity in the Last 2 Hours 85
 - Cisco Alert Details (Trend Based) 85, 92, 98
 - Cisco ASA Hourly Event Count 23, 42
 - Cisco ASA Hourly Event per Device 25, 42, 73
 - Cisco Configuration Change Detail (Trend Based) 23, 52
 - Cisco ESA Configuration Changes in the Last 6 Hours 24, 52
 - Cisco Event Count by Hour 24, 52
 - Cisco Firewall Configuration Changes in Last 6 Hours 23, 52
 - Cisco Firewall Hourly Event Count 72
 - Cisco FWSM Hourly Event Count 23, 62
 - Cisco FWSM Hourly Event per Device 24, 63, 73
 - Cisco IOS IPS Hourly Event Count 24, 98
 - Cisco IOS IPS Hourly Event Count per Device 24, 98
 - Cisco IPS Configuration Changes in the Last 6 Hours 22, 52
 - Cisco Login Details in the Last 7 Days (Trend Based) 23, 52
 - Cisco Network Equipment Configuration Changes in the Last 6 Hours 22, 52
 - Cisco Network Event Count by Hour 113
 - Cisco WSA Configuration Changes in the Last 6 Hours 24, 53
 - Critical Services Started or Stopped 231
 - Delivery Connections 103
 - Delivery Connections by Hour 103
 - Disassociated Devices in a Day (Event Based) 120
 - Failed Logins by User in the Last 2 Hours 23, 52
 - Final Stage Cases by Owner 252
 - Follow-Up Stage Cases by Owner 252
 - Host Configuration Modifications - Today 260
 - Host Configuration Modifications - Yesterday 261
 - Initial Stage Cases by Owner 252
 - Injection Connections 103
 - Injection Connections by Hour 102
 - IPS Sensor Hourly Event Count 23, 92
 - IPS Sensor Hourly Event Count per Device 23, 92
 - List of Top Bandwidth Usage Events 241
 - Maximum Time to Case Resolution - by User 253
 - Message Transaction Details 25, 103
 - Modified Windows Privileged Accounts 209
 - Open Cases 253
 - Open Cases by Associated Impact 253
 - Open Cases by Consequence Severity 252
 - Open Cases by Operational Impact 253
 - Open Cases by Stage 251
 - Privileged Accounts Modified 209
 - Privileged Accounts Modified - Drilldown 209
 - Queued Stage Cases by Owner 251
 - Recently Closed Cases 252
 - Successful Logins by User in the Last 2 Hours 24, 53
 - Successful Requests 24, 108
 - Top Access Points with Most Distinct Associated Devices 119

- Top Access Points with Most Distinct Disassociated Devices 119
- Top Accessed Sites 25, 109
- Top Accessed Sites with Most Traffic 25, 108
- Top Attackers in Cisco Alerts over the Last 2 Hours 85
- Top Attackers in Cisco IOS IPS Alerts 98
- Top Bandwidth Usage by Destination 241
- Top Bandwidth Usage by Destination and Port 241
- Top Bandwidth Usage by Non-Well-Known Port 241
- Top Bandwidth Usage by Source 241
- Top Bandwidth Usage by Source and Port 241
- Top Bandwidth Usage by Source-Destination Pairs 241
- Top Bandwidth Usage by Source-Destination Pairs and Port 241
- Top Bandwidth Usage by Well-Known Port 241
- Top Cisco Alert Destinations Observed by IPS Sensor 92
- Top Cisco Alert Sources Observed by IPS Sensor 92
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours 72
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 63
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours 73
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) 42
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours 72
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 63
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours 73
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Hosts Accessed Most Sites 23, 109
- Top Hosts with Most Web Traffic 22, 108
- Top Ports across Allowed Inbound Connections in Last 2 Hours 72
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Ports across Allowed Outbound Connections in Last 2 Hours 72
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Ports across Denied Inbound Connections in Last 2 Hours 73
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco ASA) 42
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Ports across Denied Outbound Connections in Last 2 Hours 72
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 63
- Top Recipients in the Last 2 Hours 22, 102
- Top Recipients with Most Bandwidth in the Last 2 Hours 24, 103
- Top Senders in the Last 2 Hours 25, 103
- Top Senders with Most Bandwidth in the Last 2 Hours 24, 103
- Top Sites with Most Request Errors 23, 108
- Top Source Addresses with Most Failed Logins 25, 53
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours 73
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) 42
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 63
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours 73
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) 42
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours 73
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 63
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours 72
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) 41
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 62
- Top Systems with Most Delivery Connections 103
- Top Systems with Most Injection Connections 103
- Top Targets in Cisco Alerts over the Last 2 Hours 84
- Top Targets in Cisco IOS IPS Alerts 98
- Top Users with Most Failed Logins 24, 52
- Top Windows Devices by Event Count 204
- Unsuccessful Requests 109
- User Configuration Modifications - Today 260
- User Configuration Modifications - Yesterday 260
- Weekly Hosts With Multiple Failed Authentications 222

Weekly Users With Multiple Failed Authentications 223
 Weekly Users With Multiple Failed Authentications by Reason 223
 Weekly Users With Multiple Failed Authentications Detail 222
 Windows Account Lockouts 208
 Queued Stage Cases by Owner (Chart) query 258
 Queued Stage Cases by Owner query viewer 251

R

Recent Events data monitor 285
 Recently Closed Cases query 249, 257
 Recently Closed Cases query viewer 252
 Reconnaissance Activity active channel 15, 280
 Reconnaissance Events (Internal Targets) filter 289
 Reconnaissance Events by Attacker filter 289
 Reconnaissance Events by Target filter 291
 Reconnaissance Events by Target Zone filter 291
 Reconnaissance in Progress dashboard 280
 Rejected Injection Connection (Cisco ESA) filter 105
 report templates
 Security Intelligence Status Template 295
 reports
 Alert Counts by Device 166
 Alert Counts by Port 166
 Alert Counts by Severity 167
 Alert Counts by Type 167
 Alert Counts per Hour 166
 All Cases 254
 All Level 3 Notifications 271
 ArcSight Express, scheduling 13
 Associated Wireless Devices to Cisco APs 120
 Associations - Disassociations per Day (Cisco APs) 120
 Authentication Errors 193
 Average Time to Case Resolution - By Day 253
 Average Time to Case Resolution - By Severity 253
 Average Time to Case Resolution - By User 253
 Bandwidth Usage by Hour 126, 147, 174, 193
 Bandwidth Usage by Hour (Cisco ASA) 44
 Bandwidth Usage by Hour (Cisco Firewall) 75
 Bandwidth Usage by Hour (Cisco FWSM) 65
 Bandwidth Usage by Protocol 53, 125, 145, 173, 192
 Bandwidth Usage by Protocol (Cisco ASA) 44
 Bandwidth Usage by Protocol (Cisco Firewall) 74
 Bandwidth Usage by Protocol (Cisco FWSM) 65
 Bandwidth Usage per Hour 54
 Bandwidth Utilization - Last 24 Hours 274
 Bandwidth Utilization - Last Hour 273
 By User Account - Accounts Created 261
 Case Stages Overview 253
 Case Status Overview 248, 254
 Cases Created Today 254
 Cases per Target 254
 Cisco Access Points and Associated Wireless Devices 120
 Cisco Alerts per Day 86
 Cisco Alerts per Hour in the Previous Day 85
 Cisco Configuration Changes by Type 54
 Cisco Configuration Changes by Type (Cisco ASA) 43
 Cisco Configuration Changes by Type (Cisco FWSM) 64

Cisco Configuration Changes by User 54
 Cisco Configuration Changes by User (Cisco ASA) 43
 Cisco Configuration Changes by User (Cisco FWSM) 65
 Cisco Configuration Changes per Day 54
 Cisco Configuration Changes per Hour in the Previous Day 53
 Cisco Device Critical Events 114
 Cisco Device Errors 114
 Cisco Device Interface Status Messages 114
 Cisco ESA Configuration Changes by Type 104
 Cisco ESA Configuration Changes by User 104
 Cisco ESA Configuration Changes per Day 104
 Cisco Firewall Configuration Changes by Device 76
 Cisco Firewall Configuration Changes by Type 75
 Cisco Firewall Configuration Changes by User 75
 Cisco Firewall Configuration Changes per Day 76
 Cisco Firewall Overview - Top Allowed Systems 25
 Cisco Firewall Overview - Top Denied Systems 25
 Cisco Firewall Overview - Trend and Port 26
 Cisco Intrusion Prevention System Overview 26
 Cisco IOS IPS Configuration Changes by Type 99
 Cisco IOS IPS Configuration Changes by User 98
 Cisco IPS Configuration Changes by Device 86
 Cisco IPS Configuration Changes by Type 85
 Cisco IPS Configuration Changes by User 85
 Cisco IPS Configuration Changes per Day 86
 Cisco IPS Sensor Configuration Changes by Type 93
 Cisco IPS Sensor Configuration Changes by User 93
 Cisco Network Equipment Configuration Changes by Device 114
 Cisco Network Equipment Configuration Changes by Type 115
 Cisco Network Equipment Configuration Changes by User 114
 Cisco Network Equipment Configuration Changes per Day 114
 Cisco Network SNMP Authentication Failures 114
 Cisco Overall Alert Count by Device 86
 Cisco Overall Alert Count by Port 86
 Cisco Overall Alert Count by Severity 86
 Cisco Overall Alert Count by Type 85
 Cisco Overall Allowed Inbound Connections by Destination Host 74
 Cisco Overall Allowed Inbound Connections by Source Host 76
 Cisco Overall Allowed Outbound Connections by Destination Host 74
 Cisco Overall Allowed Outbound Connections by Source Host 74
 Cisco Overall Denied Inbound Connections by Destination Host 76
 Cisco Overall Denied Inbound Connections by Destination Port 74
 Cisco Overall Denied Inbound Connections by Source Host 75
 Cisco Overall Denied Inbound Connections per Hour in the Previous Day 75
 Cisco Overall Denied Outbound Connections by Destination Host 76
 Cisco Overall Denied Outbound Connections by Destination Port 76
 Cisco Overall Denied Outbound Connections by

- Source Host 75
- Cisco Overall Denied Outbound Connections per Hour in the Previous Day 76
- Cisco Overall Inbound Connection Setup Attempts per Day 73
- Cisco Overall Outbound Connection Setup Attempts per Day 75
- Cisco WSA Configuration Changes by Type 109
- Cisco WSA Configuration Changes by User 110
- Cisco WSA Configuration Changes per Day 109
- Computer Accounts Created Weekly 210
- Computer Accounts Deleted Weekly 209
- Computer Accounts Modified Weekly 210
- Configuration Changes by Type 125, 133, 140, 147, 157, 174, 184, 193, 261
- Configuration Changes by User 125, 132, 140, 146, 156, 173, 184, 193, 261
- Connection Counts by User 156, 192
- Connection Durations by User 157
- Connection Overview (Cisco ESA) 104
- Connections Accepted by Address 193
- Connections Denied by Address 192
- Connections Denied by Hour 192
- Daily Accounts Locked Out 209
- Database Errors and Warnings 140
- Denied Inbound Connections by Address 146
- Denied Inbound Connections by Address (Cisco ASA) 42
- Denied Inbound Connections by Address (Cisco FWSM) 65
- Denied Inbound Connections by Port 147
- Denied Inbound Connections by Port (Cisco ASA) 44
- Denied Inbound Connections by Port (Cisco FWSM) 64
- Denied Inbound Connections per Hour 145
- Denied Inbound Connections per Hour (Cisco FWSM) 64
- Denied Outbound Connections by Address 145
- Denied Outbound Connections by Address (Cisco ASA) 44
- Denied Outbound Connections by Address (Cisco FWSM) 63
- Denied Outbound Connections by Port 145
- Denied Outbound Connections by Port (Cisco ASA) 43
- Denied Outbound Connections by Port (Cisco FWSM) 63
- Denied Outbound Connections per Hour 145
- Denied Outbound Connections per Hour (Cisco FWSM) 65
- Device Critical Events 174
- Device Errors 174
- Device Events 174
- Device Interface Down Notifications 173
- Device Interface Status Messages 173
- Device SNMP Authentication Failures 172
- Errors Detected in Anti-Virus Deployment 132
- Exposed Vulnerabilities by Asset 296
- Exposed Vulnerability Count by Asset 296
- Failed Anti-Virus Updates 133
- Failed Login Attempts 157, 183, 266
- Failed Logins by Destination Address 54, 145, 157, 173, 183, 192, 266
- Failed Logins by Source Address 54, 146, 157, 174, 184, 193, 267
- Failed Logins by User 53, 146, 156, 173, 184, 193, 266
- Host Configuration Modifications by OS 261
- Inbound Connection Setup Attempts per Day (Cisco ASA) 43
- Inbound Connection Setup Attempts per Day (Cisco FWSM) 64
- Inbound Traffic - Top Protocols 273
- Inbound Traffic - Top Source Hosts 273
- Login Errors by User 184, 267
- Login Event Audit 140, 145, 172, 183, 191, 266
- Logins per Day 53
- Logins per Hour in the Previous Day 53
- Max Time to Case Resolution - By User 254
- Message Transaction per Hour in the Previous Day (Cisco ESA) 104
- Message Transactions per Day (Cisco ESA) 104
- Modified Windows Privileged Accounts 210
- Modified Windows Privileged Group Members 209
- Notification Overview 270
- Notification Statistics Summary 270
- Notification Status Report 271
- Notifications By Acknowledgement Status 270
- Open Cases 254
- Outbound Connection Setup Attempts per Day (Cisco ASA) 43
- Outbound Connection Setup Attempts per Day (Cisco FWSM) 64
- Outbound Traffic - Top Protocols 274
- Outbound Traffic - Top Source Hosts 273
- Overview of Cisco Configuration Changes 25
- Overview of Logins Reported by Cisco Devices - Systems 25
- Overview of Logins Reported by Cisco Devices - Trend and Users 26
- Password Changes 140, 157, 183, 192, 261
- Request Error Statistics (Cisco WSA) 110
- Security Intelligence Status Report 17, 281
- Successful Logins by Destination Address 54, 146, 158, 173, 184, 192, 267
- Successful Logins by Source Address 54, 146, 157, 174, 184, 193, 267
- Successful Logins by User 53, 145, 156, 172, 183, 191, 266
- Summary of Allowed Traffic by Specific Cisco Firewall 75
- Summary of Denied Traffic by Specific Cisco Firewall 74
- Top Accessed Sites (Cisco WSA) 109
- Top Accessed Sites with Most Traffic (Cisco WSA) 109
- Top Alert Destinations 167
- Top Alert Sources 166
- Top Alerts from IDS and IPS 166
- Top Attackers 166
- Top Attackers in Cisco Alerts 86
- Top Attackers in Cisco Alerts over a Month 86
- Top Bandwidth Destination Hosts 54
- Top Bandwidth Destination Hosts (Cisco Firewall) 77
- Top Bandwidth Destination Hosts (Cisco FWSM) 64
- Top Bandwidth Hosts 125, 146, 173, 192
- Top Bandwidth Source Hosts 53
- Top Bandwidth Source Hosts (Cisco ASA) 45

- Top Bandwidth Source Hosts (Cisco Firewall) 74
- Top Bandwidth Source Hosts (Cisco FWSM) 64
- Top Bandwidth Target Hosts (Cisco ASA) 44
- Top Bandwidth Usage by Destination 242
- Top Bandwidth Usage by Destination Port 242
- Top Bandwidth Usage by Source 242
- Top Bandwidth Usage Daily Report 242
- Top Bandwidth Usage Weekly Report 242
- Top Cisco Alerts 85
- Top Cisco Alerts in a Month 86
- Top Denied Sites (Cisco WSA) 109
- Top Hosts Accessed Most (Distinct) Sites (Cisco WSA) 109
- Top Hosts by Number of Connections 147, 174, 194
- Top Hosts with Most Web Traffic (Cisco WSA) 109
- Top Infected Systems 132, 281
- Top Recipients with Most Bandwidth Consumption (Cisco ESA) 104
- Top Recipients with Most Transactions (Cisco ESA) 104
- Top Senders with Most Bandwidth Consumption (Cisco ESA) 103
- Top Senders with Most Transactions (Cisco ESA) 104
- Top Sites with Most Request Errors (Cisco WSA) 110
- Top Sources with Most Denied Requests (Cisco WSA) 110
- Top Sources with Most Request Errors (Cisco WSA) 109
- Top Target Cisco SNMP Access in a Week 114
- Top Targets 167
- Top Targets in Cisco Alerts 86
- Top Targets in Cisco Alerts over a Month 85
- Top Users by Average Session Length 191
- Top Windows Devices by Event Count 204
- Traffic Snapshot 273
- Traffic Statistics 248, 273
- Trend of Daily Cisco SNMP Access 114
- Trend of Daily SNMP Access on Specific Cisco Target 115
- Unacknowledged Level 3 Notifications 270
- Update Summary 133
- User Accounts Created Weekly 210
- User Accounts Deleted Weekly 209
- User Accounts Disabled Weekly 210
- User Accounts Enabled Weekly 209
- User Administration 184, 248
- Virus Activity by Time 133, 281
- VPN Authentication Errors (Cisco ASA) 43
- VPN Connection Counts by User (Cisco ASA) 43
- VPN Connections Accepted by Address (Cisco ASA) 43
- VPN Connections Denied by Address (Cisco ASA) 44
- Web Requests per Day in the Previous Week (Cisco WSA) 109
- Web Requests per Hour in the Previous Day (Cisco WSA) 110
- Weekly Accounts Locked Out 210
- Weekly Hosts With Multiple Failed Authentications 223
- Weekly Policy Changes by Type 227
- Weekly Users With Multiple Failed Authentications 223
- Windows Critical Services Started Or Stopped 231
- Windows Security Audit Logs Cleared 231
- Windows System Time Changes 231
- Worm Infected Systems 166
- Request Error Statistics (Cisco WSA) report 110
- Request Errors query 112
- Resource URIs 14
- resources
 - Authentication 222
 - Microsoft Windows Monitoring (Overview) 204
 - Policy Changes 227
 - System Services and Auditing 231
- Root-Admin Failed Logins data monitor 267, 287
- Root-Admin Failed Logins filter 268, 289
- Root-Admin Logins data monitor 267, 285
- Root-Admin Logins filter 268, 290
- rules
 - Account Added to Privileged Group 212
 - Account Locked Out 213
 - Account Locked Out Multiple Times in 24 Hours 214
 - Account Removed from Privileged Group 211
 - Authentication Attempted to Disabled Account 224
 - Authentication Attempted to Non-Existing Account 223
 - Blaster DDOS From Infected Host 282
 - Blaster Infected Host 283
 - Case Deleted 254
 - Case Escalation 255
 - Case Investigation Started 255
 - Computer Account Changed 211
 - Computer Account Created 213
 - Computer Account Deleted 213
 - CrashOnAuditFail Modified 233
 - Critical Service Request Start 232
 - Critical Service Request Stop 234
 - Critical Service Started 234
 - Critical Service Stopped 233
 - Failed Authentication - Windows Domain Account 223
 - Failed Authentication - Windows Workstation 224
 - High Number of Connections 126, 147, 274
 - High Number of Denied Connections for A Source Host 126, 147, 274
 - High Number of Denied Inbound Connections 126, 147, 274
 - High Number of IDS Alerts for Backdoor 168, 284
 - High Number of IDS Alerts for DoS 167, 282
 - Install Service Attempt 233
 - Locked Account Re-enabled 211
 - Lockout Attempt Failed 211
 - Lockout Policy Changed 228
 - Monitor New Case 255
 - Notify on Successful Attack 283
 - Password Policy Changed 228
 - Possible Internal Network Sweep 283
 - Possible Outbound Network Sweep 284
 - Privileged Account Deleted 213
 - Privileged Account Disabled 212
 - Privileged Account Enabled 212
 - Privileged Account Locked Out 214
 - Privileged Account Modified 212
 - Privileged Account Password Changed 214
 - SYN Flood Detected by IDS or Firewall 147, 167, 283
 - System Audit Policy Changed 228

- Track Closed Case 255
- Track Deleted Case 254
- Track New Case 255
- Track Updated Case 255
- Unable to Log Events 233
- User Account Created 214
- User Account Deleted 212
- User Account Disabled 213
- User Account Enabled 213
- User Session (Accounting User) Started 158
- User Session (Accounting User) Stopped 158
- User Session (Administrative User) Started 159
- User Session (Administrative User) Stopped 158
- User Session (Normal User) Started 159
- User Session (Normal User) Stopped 158
- User VPN Session Started 126, 194
- User VPN Session Stopped 126, 194
- Warning - Insecure Configuration 296
- Warning - Vulnerable Software 296
- Windows Audit Events Discarded 231
- Windows Security Audit Log Cleared 234
- Windows System Starting 232
- Windows System Time Changed 232
- Worm Outbreak Detected 167, 282

S

- Security Activity dashboard 16, 281
- Security Activity Statistics dashboard 16, 280
- Security and Threat use case 17
- Security field set 288
- Security Highlights field set 288
- Security Intelligence Status Report report 17, 281
- Security Intelligence Status Template report template 295
- Sender and Recipient Overview dashboard 22, 102
- Service Started Action Count is NULL filter 237
- Service Stopped Action Count is NULL filter 236
- session lists
 - Accounts Locked Out Multiple Times in 24 Hours 220
 - Case Tracking 250, 259
 - Created Computer Accounts 219
 - Created User Accounts 220
 - Deleted Computer Accounts 220
 - Deleted User Accounts 219
 - Disabled User Accounts 220
 - Enabled User Accounts 219
 - Failed Authentications 226
 - Locked Out Accounts 220
 - Modified Computer Accounts 219
 - Policy Changes 229
 - User Sessions 164
 - User VPN Sessions 130, 202
- Single-digit Day filter 257
- Single-digit Hour filter 257
- Single-digit Minute filter 256
- Single-digit Month filter 257
- SIS-Assets Compromised Table Query query 294
- SIS-Cases Added Table Query query 294
- SIS-Event Count by Agent Severity Chart Query query 294
- SIS-Notifications Sent Table Query query 294
- SIS-Top Attackers Chart Query query 294
- SIS-Top Attacks Table Query query 293
- SIS-Top Events Table Query query 294
- SIS-Top Firing Rules Table Query query 293
- SIS-Top Target Ports Chart Query query 295
- SIS-Top Targets Chart Query query 294
- SmartConnector
 - Microsoft Windows Event Log- Unified 203
- SNMP Authentication Failed filter 116
- SNMP Authentication Failures by Device query 181
- SNMP Events filter 116
- Standard field set 127, 141, 149, 159, 169, 175, 185, 195, 263, 288
- Status Events from Cisco IOS IPS Systems active channel 97
- Status Events from Cisco IPS Sensor Systems active channel 91
- Status Events from Cisco IPS Systems active channel 84
- Successful Attacks filter 293
- Successful Configuration Changes (Cisco ESA) filter 105
- Successful Configuration Changes filter 30, 46, 66, 77, 88, 94, 100, 105, 110, 116, 129, 141, 150, 196, 264
- Successful Firewall Login Events filter 151
- Successful Login by Source Address query 35, 58
- Successful Login by User (Chart) query 154, 163, 182, 189, 202, 269
- Successful Login by User query 154, 163, 180, 189, 200, 269
- Successful Login Events filter 149, 176, 185, 196
- Successful Logins by Destination Address (Chart) query 155, 164, 181, 190, 201, 269
- Successful Logins by Destination Address focused report 152, 161, 179, 188, 198
- Successful Logins by Destination Address query 33, 58
- Successful Logins by Destination Address report 54, 146, 158, 173, 184, 192, 267
- Successful Logins by Source Address (Chart) query 153, 162, 179, 188, 199, 268
- Successful Logins by Source Address focused report 152, 161, 177, 187, 197
- Successful Logins by Source Address report 54, 146, 157, 174, 184, 193, 267
- Successful Logins by Source-Destination Pair query 154, 163, 182, 189, 202, 269
- Successful Logins by User focused report 152, 161, 178, 187, 198
- Successful Logins by User in the Last 2 Hours query viewer 24, 53
- Successful Logins by User query 36, 59
- Successful Logins by User report 53, 145, 156, 172, 183, 191, 266
- Successful Logins filter 29, 55
- Successful Network Login Events filter 177
- Successful Operating System Login Events filter 186
- Successful Password Changes filter 141, 160, 186, 196, 263
- Successful Requests query viewer 24, 108
- Successful VPN Connection Events (Cisco ASA) filter 47
- Successful VPN Connection Events filter 197
- Successful VPN Login Events filter 196
- Successful Web Transactions filter 30, 110
- Successful WSA Configuration Changes filter 110
- Summary of Allowed Traffic by Specific Cisco Firewall report 75
- Summary of Denied Traffic by Specific Cisco Firewall report 74

SYN Flood Detected by IDS or Firewall rule 147, 167, 283
 SYN Traffic filter 275
 System Audit Policy Changed rule 228
 System Notifications and Escalation use case 250
 System Services and Auditing dashboard 231
 System Services and Auditing use case 206, 230
 System Services and Auditing Violations filter 236
 System Time Changes - Chart query 237
 System Time Changes - Table query 237
 System Time Changes active list 234

T

Target Address is NULL filter 134, 263, 289
 Target Host Name is NULL filter 134, 263, 291
 Target Host or Address Present filter 29, 45, 55, 66, 77, 87, 94, 100, 105, 115
 Target Information is NULL filter 264
 Target Port Activity by Attacker data monitor 168, 287
 Target Port Activity By Attacker filter 169, 291
 Target Port is NULL filter 264, 276
 Target User ID is NULL filter 160, 195
 Target User Present filter 30, 46, 56, 116
 Target User with Domain Information filter 205, 216, 225, 229, 237
 Target Zone AND Host are NULL but Address is NOT NULL filter 263
 Target Zone AND Host are NULL filter 264
 Target Zone is NULL filter 135, 264, 292
 Target Zone OR Host is NULL filter 265
 Target_HostName global variable 205, 215, 224, 229, 235
 Target_NTDomain global variable 205, 215, 224, 229, 236
 Target_User global variable 205, 215, 224, 228, 236
 TargetHost global variable 262
 TCP Traffic filter 275
 Threat View dashboard 16, 281
 Top 10 Accepted Ports (Inbound) data monitor 148
 Top 10 Accepted Ports (Outbound) data monitor 148
 Top 10 Alert Destinations data monitor 168
 Top 10 Alert Sources data monitor 168
 Top 10 Alert Types data monitor 168
 Top 10 Alerts data monitor 169
 Top 10 Alerts focused report 169
 Top 10 Anti-Virus Errors data monitor 133
 Top 10 Assets by Exposed Vulnerability Counts query 297
 Top 10 Attackers focused report 169
 Top 10 Attackers query 170
 Top 10 Database Errors data monitor 141
 Top 10 Denied Ports (Inbound) data monitor 148
 Top 10 Denied Ports (Outbound) data monitor 148
 Top 10 Event Types last Hour data monitor 204
 Top 10 Hosts With Denied Inbound Connections data monitor 148
 Top 10 Hosts With Denied Outbound Connections data monitor 148
 Top 10 Infected Systems data monitor 133
 Top 10 Infections data monitor 134
 Top 10 Targets focused report 169
 Top 10 Targets query 170
 Top 10 Users With Failed Logins data monitor 148, 175, 185, 195
 Top 10 Users with Failed Logins data monitor 286
 Top 10 Windows Users Last Hour data monitor 204
 Top 10 Zones Scanned data monitor 287
 Top Access Points with Most Association Events data monitor 120
 Top Access Points with Most Disassociation Events data monitor 120
 Top Access Points with Most Distinct Associated Devices query viewer 119
 Top Access Points with Most Distinct Disassociated Devices query viewer 119
 Top Accessed Sites (Cisco WSA) report 109
 Top Accessed Sites query 36, 111
 Top Accessed Sites query viewer 25, 109
 Top Accessed Sites with Most Traffic (Cisco WSA) report 109
 Top Accessed Sites with Most Traffic query 35, 112
 Top Accessed Sites with Most Traffic query viewer 25, 108
 Top Actions data monitor 139
 Top Activities across Cisco Firewall Devices data monitor 77
 Top Alert Destinations query 170
 Top Alert Destinations report 167
 Top Alert Sources query 169
 Top Alert Sources report 166
 Top Alerts from IDS and IPS report 166
 Top Anti-Virus Errors query 137
 Top Application Protocols data monitor 27, 55
 Top Attacker IPs data monitor 285
 Top Attackers and Reporting Devices in Cisco Alerts query 89
 Top Attackers in Cisco Alerts (Trend Based) query 89
 Top Attackers in Cisco Alerts over a Month report 86
 Top Attackers in Cisco Alerts over the Last 2 Hours query viewer 85
 Top Attackers in Cisco Alerts query 34, 89
 Top Attackers in Cisco Alerts report 86
 Top Attackers in Cisco IOS IPS Alerts query 101
 Top Attackers in Cisco IOS IPS Alerts query viewer 98
 Top Attackers query 277
 Top Attackers report 166
 Top Bandwidth Destination Hosts (Cisco Firewall) report 77
 Top Bandwidth Destination Hosts (Cisco FWSM) report 64
 Top Bandwidth Destination Hosts query 50, 60, 70, 82
 Top Bandwidth Destination Hosts report 54
 Top Bandwidth Hosts focused report 152, 178, 198
 Top Bandwidth Hosts query 129, 154, 180, 200, 278
 Top Bandwidth Hosts report 125, 146, 173, 192
 Top Bandwidth Source Hosts (Cisco ASA) report 45
 Top Bandwidth Source Hosts (Cisco Firewall) report 74
 Top Bandwidth Source Hosts (Cisco FWSM) report 64
 Top Bandwidth Source Hosts query 49, 59, 69, 81
 Top Bandwidth Source Hosts report 53
 Top Bandwidth Target Hosts (Cisco ASA) report 44
 Top Bandwidth Usage by Day - Trend on Trend query 244
 Top Bandwidth Usage by Destination - Trend on Trend query 244
 Top Bandwidth Usage by Destination - Trend query 245
 Top Bandwidth Usage by Destination and Port query 245
 Top Bandwidth Usage by Destination and Port query viewer 241

- Top Bandwidth Usage by Destination Port report 242
- Top Bandwidth Usage by Destination query 244
- Top Bandwidth Usage by Destination query viewer 241
- Top Bandwidth Usage by Destination report 242
- Top Bandwidth Usage by Destination trend 246
- Top Bandwidth Usage by Hour - Trend on Trend query 244
- Top Bandwidth Usage by Hour - Trend query 245
- Top Bandwidth Usage by Hour trend 246
- Top Bandwidth Usage by Non-Well-Known Port query 245
- Top Bandwidth Usage by Non-Well-Known Port query viewer 241
- Top Bandwidth Usage by Port - Trend on Trend query 245
- Top Bandwidth Usage by Port - Trend query 244
- Top Bandwidth Usage by Port trend 246
- Top Bandwidth Usage by Source - Trend on Trend query 245
- Top Bandwidth Usage by Source - Trend query 245
- Top Bandwidth Usage by Source and Port query 244
- Top Bandwidth Usage by Source and Port query viewer 241
- Top Bandwidth Usage by Source query 244
- Top Bandwidth Usage by Source query viewer 241
- Top Bandwidth Usage by Source report 242
- Top Bandwidth Usage by Source trend 246
- Top Bandwidth Usage by Source-Destination Pairs and Port query 245
- Top Bandwidth Usage by Source-Destination Pairs and Port query viewer 241
- Top Bandwidth Usage by Source-Destination Pairs query 244
- Top Bandwidth Usage by Source-Destination Pairs query viewer 241
- Top Bandwidth Usage by Well-Known Port query 245
- Top Bandwidth Usage by Well-Known Port query viewer 241
- Top Bandwidth Usage Daily Report report 242
- Top Bandwidth Usage Events query 244
- Top Bandwidth Usage Events trend 246
- Top Bandwidth Usage Weekly Report report 242
- Top Browsers data monitor 139
- Top Categories data monitor 28, 55, 139, 288
- Top Cisco Alert Destinations Observed by IPS Sensor query 95
- Top Cisco Alert Destinations Observed by IPS Sensor query viewer 92
- Top Cisco Alert Sources Observed by IPS Sensor query 95
- Top Cisco Alert Sources Observed by IPS Sensor query viewer 92
- Top Cisco Alerts (Trend Based) query 89
- Top Cisco Alerts in a Month report 86
- Top Cisco Alerts query 36, 90
- Top Cisco Alerts report 85
- Top Connection Durations query 163
- Top Connections Accepted by Address query 200
- Top Connections Denied by Address query 201
- Top Connectors data monitor 286
- Top Denied Sites (Cisco WSA) report 109
- Top Denied Sites query 112
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 63
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours query viewer 72
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 42
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours query viewer 73
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 63
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours query viewer 72
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours query viewer 73
- Top Device System Authentication Events query 179
- Top Event Sources data monitor 127
- Top Firewall Blocked Machines data monitor 287
- Top Hosts Accessed Most (Distinct) Sites (Cisco WSA) report 109
- Top Hosts Accessed Most Sites query viewer 23, 109
- Top Hosts by Number of Connections focused report 151, 178, 198
- Top Hosts by Number of Connections query 153, 181, 201
- Top Hosts by Number of Connections report 147, 174, 194
- Top Hosts with Most Web Traffic (Cisco WSA) report 109
- Top Hosts with Most Web Traffic query 33, 112
- Top Hosts with Most Web Traffic query viewer 22, 108
- Top IDS and IPS Alerts query 170
- Top Infected Systems query 137, 294
- Top Infected Systems report 132, 281
- Top NetFlow Bandwidth Usage Monitoring dashboard 240
- Top Non-US Destinations - Graph data monitor 275
- Top Non-US Destinations data monitor 275
- Top Non-US Destinations filter 275, 290
- Top Non-US Sources - Graph data monitor 274
- Top Non-US Sources data monitor 274
- Top Non-US Sources filter 276, 290
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Ports across Allowed Inbound Connections in Last 2 Hours query viewer 72
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62

- Top Ports across Allowed Outbound Connections in Last 2 Hours query viewer 72
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 42
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Ports across Denied Inbound Connections in Last 2 Hours query viewer 73
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 63
- Top Ports across Denied Outbound Connections in Last 2 Hours query viewer 72
- Top Protocols query 276
- Top Recipients in the Last 2 Hours query viewer 22, 102
- Top Recipients with Most Bandwidth Consumption (Cisco ESA) report 104
- Top Recipients with Most Bandwidth in the Last 2 Hours query viewer 24, 103
- Top Recipients with Most Bandwidth query 32, 106
- Top Recipients with Most Transactions (Cisco ESA) report 104
- Top Recipients with Most Transactions query 36, 107
- Top Senders in the Last 2 Hours query viewer 25, 103
- Top Senders with Most Bandwidth Consumption (Cisco ESA) report 103
- Top Senders with Most Bandwidth in the Last 2 Hours query viewer 24, 103
- Top Senders with Most Bandwidth query 32, 106
- Top Senders with Most Transactions (Cisco ESA) report 104
- Top Senders with Most Transactions query 35, 106
- Top Sites with Most Request Errors (Cisco WSA) report 110
- Top Sites with Most Request Errors query 36, 111
- Top Sites with Most Request Errors query viewer 23, 108
- Top Source Addresses with Most Failed Logins query viewer 25, 53
- Top Source Hosts Accessed Most Sites query 34, 112
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 42
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 63
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours query viewer 73
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 42
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours query viewer 73
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 63
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours query viewer 73
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 41
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 62
- Top Source Hosts across Denied Outbound Connections in Last 2 Hours query viewer 72
- Top Source Hosts with Most Denied Requests query 112
- Top Source Hosts with Most Request Errors query 111
- Top Sources with Most Denied Requests (Cisco WSA) report 110
- Top Sources with Most Request Errors (Cisco WSA) report 109
- Top Successful Attacks data monitor 287
- Top Systems Receiving Most Delivery Connections query 106
- Top Systems Sending Most Injection Connections query 106
- Top Systems Sending Most Rejected Injection Connections query 106
- Top Systems with Most Delivery Connections query viewer 103
- Top Systems with Most Injection Connections query viewer 103
- Top Systems with Most Rejected Injection Connections data monitor 104
- Top Target Cisco SNMP Access in a Week report 114
- Top Target IPs data monitor 287
- Top Target Weekly Cisco SNMP Access on Device query 117
- Top Targets and Reporting Devices in Cisco Alerts query 89
- Top Targets in Cisco Alerts (Trend Based) query 90
- Top Targets in Cisco Alerts over a Month report 85
- Top Targets in Cisco Alerts over the Last 2 Hours query viewer 84
- Top Targets in Cisco Alerts query 36, 89
- Top Targets in Cisco Alerts report 86
- Top Targets in Cisco IOS IPS Alerts query 101
- Top Targets in Cisco IOS IPS Alerts query viewer 98
- Top Targets query 277
- Top Targets report 167
- Top Transport Protocols data monitor 26, 55, 286
- Top Users by Average Session Length report 191
- Top Users by Connection Count data monitor 159
- Top Users by Connection Count query 163, 202
- Top Users by Login Activity data monitor 175, 185, 194
- Top Users with Most Failed Logins query 36, 59
- Top Users with Most Failed Logins query viewer 24, 52
- Top Users with Successful Logins query 36, 59
- Top VPN Connection Durations query 201
- Top VPN Servers with Authentication Errors data monitor 195
- Top VPN Servers with Denied Connections data monitor 195
- Top VPN Servers with Successful Connections data monitor 195
- Top VPN Users with Authentication Errors data monitor 194
- Top Web Sites data monitor 139
- Top Windows Devices by Event Count - Trend query 206
- Top Windows Devices by Event Count query viewer 204
- Top Windows Devices by Event Count report 204
- Top Zones with Anti-Virus Errors query 137
- TotalBytes global variable 242
- Track Closed Case rule 255
- Track Deleted Case rule 254
- Track New Case rule 255
- Track Updated Case rule 255
- Traffic Monitoring dashboard 16, 273
- Traffic Monitoring use case 250
- Traffic Moving Average (ICMP) data monitor 275
- Traffic Moving Average (SYN) data monitor 275

- Traffic Moving Average (TCP) data monitor 274
- Traffic Moving Average (UDP) data monitor 275
- Traffic Moving Average dashboard 273
- Traffic Snapshot report 273
- Traffic Statistics report 248, 273
- Transaction Connections Overview dashboard 102
- Trend of Daily Cisco SNMP Access report 114
- Trend of Daily SNMP Access on Specific Cisco Target report 115
- Trend on Case Audit Events query 259
- trends
 - Case History Data 259
 - Daily Alerts 37, 60, 90, 96, 101
 - Daily Associations - Disassociations 122
 - Daily Connection Setup Attempts 37, 50, 60, 70, 82
 - Daily Email Transactions 37, 107
 - Daily Logins 37, 60
 - Daily SNMP Access 118
 - Daily Web Requests 112
 - Top Bandwidth Usage by Destination 246
 - Top Bandwidth Usage by Hour 246
 - Top Bandwidth Usage by Port 246
 - Top Bandwidth Usage by Source 246
 - Top Bandwidth Usage Events 246
 - Windows Events by Event and Device 206
- Trojaned Machines data monitor 285
- Trusted List active list 284, 296

U

- UDP Traffic filter 275
- Unable to Log Events rule 233
- Unacknowledged Level 3 Notifications query 272
- Unacknowledged Level 3 Notifications report 270
- Unsuccessful Logins filter 30, 56
- Unsuccessful Requests query viewer 109
- Unsuccessful Web Server Requests filter 31, 111
- Untrusted List active list 284
- Update Events filter 134
- Update Summary Chart query 137
- Update Summary query 138
- Update Summary report 133
- URIs, linked 14
- use cases
 - Account Management 206
 - Anti-Virus 130
 - Authentication 206, 221
 - BlueCoat 130
 - Case Tracking and Escalation 250
 - Cisco Adaptive Security Appliance (ASA) 39
 - Cisco Cross-Device 38
 - Cisco Firewall Services Module (FWSM) 38
 - Cisco Generic Firewall 38
 - Cisco Generic Intrusion Prevention System (IPS) 38
 - Cisco Intrusion Prevention System (IPS) Sensor 38
 - Cisco IOS Intrusion Prevention System (IOS IPS) 37
 - Cisco Ironport Email Security Appliance (ESA) 38
 - Cisco Ironport Web Security Appliance (WSA) 38
 - Cisco Network 38
 - Cisco Overview 18
 - Cisco Wireless 38
 - Configuration Changes 250
 - Database 130
 - Devices 18

- Firewall 130
- Identity Management 131
- IDS - IPS 130
- Logins 250
- Microsoft Windows Monitoring 18
- NetFlow Monitoring 17
- Network 130
- Operating System 130
- Operations 18
- Policy Changes 206, 227
- Security and Threat 17
- System Notifications and Escalation 250
- System Services and Auditing 206, 230
- Traffic Monitoring 250
 - viewing 14
- VPN 130
- Vulnerabilities 17
- User Account Created rule 214
- User Account Deleted rule 212
- User Account Disabled rule 213
- User Account Enabled rule 213
- User Accounts Created Weekly - Chart query 217
- User Accounts Created Weekly - Table query 217
- User Accounts Created Weekly report 210
- User Accounts Created, Deleted, Disabled, or Enabled data monitor 215
- User Accounts Created, Deleted, Disabled, or Enabled filter 216
- User Accounts Deleted Weekly - Chart query 217
- User Accounts Deleted Weekly - Table query 216
- User Accounts Deleted Weekly report 209
- User Accounts Disabled Weekly - Chart query 218
- User Accounts Disabled Weekly - Table query 218
- User Accounts Disabled Weekly report 210
- User Accounts Enabled Weekly - Chart query 217
- User Accounts Enabled Weekly - Table query 218
- User Accounts Enabled Weekly report 209
- User Administration (Chart) query 188, 249
- User Administration query 189, 250
- User Administration report 184, 248
- User Configuration Modifications - Today query viewer 260
- User Configuration Modifications - Yesterday query viewer 260
- User Configuration Modifications query 265
- User Session (Accounting User) Started rule 158
- User Session (Accounting User) Stopped rule 158
- User Session (Administrative User) Started rule 159
- User Session (Administrative User) Stopped rule 158
- User Session (Normal User) Started rule 159
- User Session (Normal User) Stopped rule 158
- User Sessions session list 164
- User VPN Session Started rule 126, 194
- User VPN Session Stopped rule 126, 194
- User VPN Sessions session list 130, 202
- Users by Connection Count (Cisco ASA) query 49
- Users by Connection Count query 162, 201
- Users with Open Connections query 162
- Users with Open VPN Connections query 202

V

- Very High Events data monitor 287
- Very High Events filter 290
- Virus Activity by Host data monitor 134

Virus Activity by Hour query 136, 293
 Virus Activity by Time report 133, 281
 Virus Activity by Zone data monitor 134
 Virus Activity filter 135
 Virus Activity Statistics dashboard 132
 Virus Information field set 127, 134, 288
 VPN Authentication Errors (Cisco ASA) filter 47
 VPN Authentication Errors (Cisco ASA) report 43
 VPN Authentication Errors filter 197
 VPN Configuration Changes filter 128, 196, 265
 VPN Connection Counts by User (Cisco ASA) report 43
 VPN Connection Statistics dashboard 191
 VPN Connections Accepted by Address (Cisco ASA) report 43
 VPN Connections Denied by Address (Cisco ASA) report 44
 VPN Events active channel 124, 191
 VPN Events filter 46, 127, 195, 263
 VPN Login Events filter 196
 VPN Login Overview dashboard 191
 VPN use case 130
 Vulnerabilities use case 17
 Vulnerability Events active channel 280
 Vulnerability field set 288

W

Warning - Insecure Configuration rule 296
 Warning - Vulnerable Software rule 296
 Web Requests filter 29, 110
 Web Requests per Day in the Previous Week (Cisco WSA) report 109
 Web Requests per Day in the Previous Week query 112
 Web Requests per Hour in the Previous Day (Cisco WSA) report 110
 Web Requests per Hour in the Previous Day query 112
 Web Transactions dashboard 22, 108
 Weekly Account Lockouts - Chart query 217
 Weekly Account Lockouts - Table query 219
 Weekly Accounts Locked Out report 210
 Weekly Hosts With Multiple Failed Authentications - Chart query 226
 Weekly Hosts With Multiple Failed Authentications query viewer 222
 Weekly Hosts With Multiple Failed Authentications report 223
 Weekly Hosts With Multiple Failed Authentications-Table query 226
 Weekly Policy Changes by Type report 227
 Weekly Policy Changes query 229
 Weekly Users With Multiple Failed Authentications - Chart query 225
 Weekly Users With Multiple Failed Authentications by Reason - Chart query 225
 Weekly Users With Multiple Failed Authentications by Reason query viewer 223
 Weekly Users With Multiple Failed Authentications Detail query viewer 222
 Weekly Users With Multiple Failed Authentications query viewer 223
 Weekly Users With Multiple Failed Authentications report 223
 Weekly Users With Multiple Failed Authentications-Table query 226
 Well-Known Ports filter 244
 Windows - Systems Starting Up active list 228, 235
 Windows Account Lockouts query viewer 208
 Windows Audit Events Discarded rule 231
 Windows Critical Services Started Or Stopped report 231
 Windows Events by Device Trend query 206
 Windows Events by Event and Device trend 206
 Windows Events filter 205, 216, 225, 229, 236
 Windows Events with a Non-Machine User filter 30, 56
 Windows Failed Authentications - All active channel 222
 Windows Failed Authentications - Domain Accounts active channel 222
 Windows Failed Authentications - Workstations active channel 222
 Windows Monitoring Correlation Events active channel 204
 Windows Monitoring Correlation field set 205
 Windows Monitoring dashboard 16, 204
 Windows Monitoring Events active channel 204
 Windows Monitoring field set 205
 Windows Security Audit Log Cleared rule 234
 Windows Security Audit Logs Cleared report 231
 Windows System Services and Auditing Violations data monitor 235
 Windows System Starting rule 232
 Windows System Time Changed rule 232
 Windows System Time Changes report 231
 WindowsLogonTypes.csv file 225
 Worm Activity filter 169, 289
 Worm Activity Status data monitor 168, 287
 Worm Infected Machines data monitor 286
 Worm Infected Systems active list 168, 284
 Worm Infected Systems data monitor 168, 286
 Worm Infected Systems query 170
 Worm Infected Systems report 166
 Worm Outbreak Detected rule 167, 282
 Worm Outbreak filter 169, 291
 Worm Outbreak Overview dashboard 165, 281
 Worm Traffic filter 169, 293

X

X-OS-Traffic active channel 124

Y

Year global variable 256

