

Standard Content Guide

Cisco Monitoring

ArcSight ESM 6.5c

October 11, 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
10/11/2013	Cisco Monitoring content for ArcSight ESM 6.5c	Final revision for release.

Contents

Chapter 1: Cisco Monitoring Overview	5
What is Standard Content?	5
Standard Content Packages	7
Cisco Monitoring Content	7
Chapter 2: Installation and Configuration	9
Installing the Cisco Monitoring Package	9
Configuring Cisco Monitoring Content	10
Modeling the Network	10
Categorizing Assets	11
Assigning User Permissions	12
Ensuring Filters Capture Relevant Events	12
Scheduling Reports	13
Configuring Trends	13
Chapter 3: Cisco Monitoring Use Cases	15
Cisco Overview	17
Configuration	17
Resources	17
Cisco Adaptive Security Appliance (ASA)	36
Configuration	36
Resources	36
Cisco Cross-Device	48
Devices	48
Configuration	48
Resources	48
Cisco Firewall Services Module (FWSM)	59
Configuration	59
Resources	59
Cisco Generic Firewall	70
Devices	70
Configuration	70
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)	103
Configuration	103
Resources	103
Cisco Ironport Web Security Appliance (WSA)	110
Configuration	110
Resources	110
Cisco Network	116
Configuration	116
Resources	116
Cisco Wireless	123
Configuration	123
Resources	123
Index	127

Chapter 1

Cisco Monitoring Overview

This chapter discusses the following topics.

["What is Standard Content?" on page 5](#)

["Standard Content Packages" on page 7](#)

["Cisco Monitoring Content" on page 7](#)

What is Standard Content?

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out-of-the box with minimal configuration. The content 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 installed using a series of packages, some of which are installed automatically with the ArcSight Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
 - ◆ ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
 - ◆ ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for ArcSight ESM with CORR- (Correlation Optimized Retention and Retrieval) Engine and provides information on the health of the CORR-Engine.
 - ◆ ArcSight Content Management is an optional package that shows information about content package synchronization with the ESM Content Management feature. The information includes a history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered. You can install this package during ArcSight ESM installation or from the ArcSight Console any time after installation.

- ◆ ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the ArcSight Command Center User's Guide.

**Note**

The ArcSight Admin DB CORR and ArcSight Search Filters content packages are installed automatically when you perform a new ArcSight ESM installation. However, when you upgrade your ArcSight ESM system, these content packages are not installed automatically. You can install these packages from the ArcSight Console any time after upgrade by right-clicking the package on the Packages tab in the Navigator and selecting Install Package.

Refer to the ArcSight ESM Upgrade Guide for information about upgrading ArcSight ESM.

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.
- **ArcSight Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks. You can install a Foundation during ArcSight ESM installation or from the ArcSight Console any time after installation.
- **Shared Libraries** - ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.
 - ◆ Anti Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
 - ◆ Conditional Variable Filters content is a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
 - ◆ Global Variables content is a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.
 - ◆ Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
 - ◆ Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

**Caution**

The resources in the ArcSight Core Security, ArcSight Administration, ArcSight DB CORR, Conditional Variable Filters, Global Variables, and Network Filters content packages are not locked even though they manage core functionality; HP recommends that you do not delete or modify these resources unless you are an advanced user who understands fully the resources and their dependencies.

Standard Content Packages

Standard content comes in packages (.arb files) that are either installed automatically or presented as an install-time option. The following graphic outlines the packages.

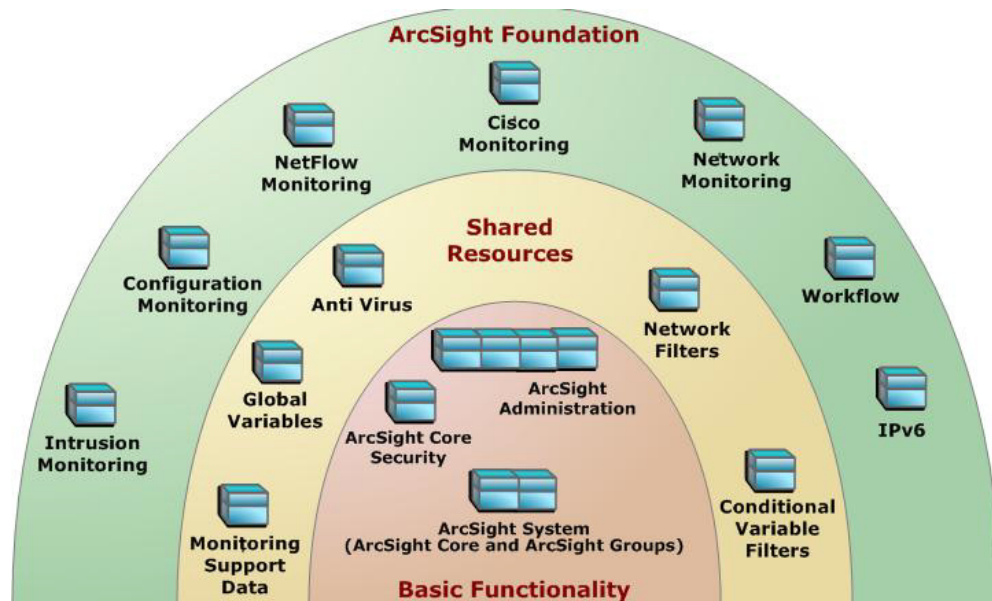


Figure 1-1 The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

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



Caution

When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources; for example, zones. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the ArcSight Console User's Guide.

Cisco Monitoring Content

Cisco Monitoring content provides both a broad overview of your Cisco infrastructure as well as 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.

This guide describes the Cisco Monitoring content. For information about ArcSight Core Security, ArcSight Administration, or ArcSight System content, refer to the ArcSight Core Security, ArcSight Administration, and ArcSight System Standard Content Guide. For information about an optional ArcSight Foundation, refer to the Standard Content Guide for

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

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

[“Installing the Cisco Monitoring Package” on page 9](#)

[“Configuring Cisco Monitoring Content” on page 10](#)

Installing the Cisco Monitoring Package

The Cisco Monitoring package is one of the standard content packages presented as install-time options. If you selected all of the standard content packages to be *installed* at installation time, the packages and their resources are installed in the ArcSight Database and available in the Navigator panel resource tree. The package icons in the Navigator panel package view appear blue.

If you opted to exclude a Foundation package during ESM installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears grey.

If you do not want the package to be available in any form, you can *delete* the package.

To install a package that is imported, but not installed:

- 1 On the Navigator panel Packages tab, navigate to the package you want to install.
- 2 Right-click the package and select **Install Package**.
- 3 In the Install Package dialog, click **OK**.
- 4 When the installation is complete, review the summary report and click **OK**.

The package resources are fully installed to the ArcSight Database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

To uninstall a package that is installed:

- 1 On the Navigator Panel Packages tab, navigate to the package you want to uninstall.
- 2 Right-click the package and select **Uninstall Package**.
- 3 In the Uninstall Package dialog, click **OK**.

The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog. If a message displays indicating that there is a conflict, select an option in the Resolution Options area and click **OK**.

- 4 When uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight Database and the Navigator panel resource tree, but remains available in the Navigator panel Packages tab, and can be re-installed at another time.

To delete a package and remove it from the ArcSight Console and the ArcSight Database:

- 1** On the Navigator Panel Packages tab, navigate to the package you want to delete.
- 2** Right-click the package and select **Delete Package**.
- 3** When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

Configuring Cisco Monitoring Content

The list below shows the general tasks you need to complete to configure Cisco Monitoring content with values specific to your environment.

- [“Modeling the Network” on page 10](#)
- [“Categorizing Assets” on page 11](#)
- [“Assigning User Permissions” on page 12](#)
- [“Ensuring Filters Capture Relevant Events” on page 12](#)
- [“Scheduling Reports” on page 13](#)
- [“Configuring Trends” on page 13](#)

Modeling the Network

Install and configure the appropriate SmartConnectors for the devices in your environment and model your 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 some of the standard content and makes it effective.

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

Categorizing Assets

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

Asset Category	Description
/Site Asset Categories/ Address Spaces/Protected	<p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>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 <i>Protected</i>.</p> <p>Note: Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p>
/System Asset Categories/ Criticality/High	<p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>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.</p>
/System Asset Categories/ Criticality/Very High	See /System Asset Categories/Criticality/High

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, refer to 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, refer to the ArcSight Console User's Guide or the ESM 101 guide.

Assigning User Permissions

By default, users in the `Default` user group can view Cisco Monitoring content, and users in the `ArcSight Administrators` and `Analyzer Administrators` user groups have read and write access to the content. Depending on how you have set up user access controls within your organization, you may need to adjust those controls to make sure the new content is accessible to the right users in your organization.

The following procedure assumes that you have user groups set up and users assigned to them. Follow the steps to assign user permissions to each of the following resource types:

- ◆ Active Channels
- ◆ Active Lists
- ◆ Dashboards
- ◆ Data Monitors
- ◆ Field Sets
- ◆ Filters
- ◆ Queries
- ◆ Query Viewers
- ◆ Reports
- ◆ Trends

To assign user permissions:

- 1 Log into the ArcSight Console with an account that has administrative privileges.
- 2 For all the resource types listed above, change the user permissions:
 - a In the Navigator panel, go to the resource type and navigate to `ArcSight Foundation/Cisco Monitoring`.
 - b Right-click the **Cisco Monitoring** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
 - c Select which user groups you want to have permissions to Cisco Monitoring resources and click **OK**.

Ensuring Filters Capture Relevant Events

Standard content relies on specific event field values to identify events of interest. Although this method applies to most of the events and devices, be sure to test key filters to verify that they actually capture the required events.

To ensure that a filter captures the relevant events:

- 1 Generate or identify the required events and verify that they are being processed by viewing them in an active channel or query viewer.
- 2 Navigate to the appropriate filter, right-click the filter and choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, the filter is functioning properly.

If you do not see the events of interest:

- a Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.

- b** Modify the filter condition to capture the events of interest. After applying the change, repeat [Step 2](#) to verify that the modified filter captures the required events.

Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. By default, Cisco Monitoring reports are not scheduled to run automatically.

Evaluate the reports that come with Cisco Monitoring, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the ArcSight Console User's Guide.

Configuring 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.

Cisco Monitoring content includes several trends, which are not enabled by default.

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



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

Chapter 3

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 17	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 36	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 48	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 59	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 70	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 103	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 110	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 116	The Cisco Network use case identifies and provides information based on events reported by Cisco network equipment.
"Cisco Wireless" on page 123	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 70](#)
- [“Cisco Generic Intrusion Prevention System \(IPS\)” on page 83](#)

To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see [“Configuring Trends” on page 13](#).

These reports...	Require this trend...
Overview of Cisco Configuration Changes	Daily Configuration Changes
Overview of Logins Reported by Cisco Devices - Trend and Users	Daily Logins
Cisco Firewall Overview - Trend and Port	Daily Connection Setup Attempts
Cisco Intrusion Prevention System Overview	Daily Alerts

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 3-1 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 Foundation/Cisco Monitoring/Functionality/Cross-Device/
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/

Resource	Description	Type	URI
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)/
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)/

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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)/
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/

Resource	Description	Type	URI
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) /
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/

Resource	Description	Type	URI
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/
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 Foundation/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

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS) /
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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Top Categories	This data monitor shows the top categories recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /

Resource	Description	Type	URI
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 Foundation/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 Foundation/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	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
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/

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/
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) /
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/

Resource	Description	Type	URI
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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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/

Resource	Description	Type	URI
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/
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 Network Systems	This filter identifies events from all Cisco network devices (routers and switches). Modify this filter to include all Cisco network products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Events	This filter selects events from Cisco products.	Filter	ArcSight Foundation/Cisco Monitoring/

Resource	Description	Type	URI
Failed Logins by Destination Address	This query returns failed login attempts recorded by Cisco devices.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Recipients with Most Bandwidth	This query returns the top recipients with most bandwidth consumption.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/
Failed Logins by Source Address	This query returns failed authentication events recorded by Cisco devices, grouped by the source host.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/

Resource	Description	Type	URI
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 Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Alerts per Day	This query returns the count of alerts per day for the previous week.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Detail Successful Requests	This query returns all successful requests within the last two hours.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/

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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
Failed Logins by User	This query returns all failed login attempts and the involved users.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor)/

Resource	Description	Type	URI
Cisco Overall Denied Inbound Connections by Port	This query returns the count of denied inbound connections by destination port.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
Top Senders with Most Transactions	This query returns the top senders with most transactions.	Query	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
Successful Logins by User	This query returns all successful login attempts and the users involved.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Top Users with Successful Logins	This query returns the top users with successful login attempts.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
Top Recipients with Most Transactions	This query returns the top recipients with most transactions.	Query	ArcSight Foundation/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 Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Three Charts and Table Landscape	This template is designed to show three charts and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/3 Charts/With Table
Four Charts Landscape	This template is designed to show four charts. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/4 Charts/Without Table
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 Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/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/
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/
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/

Resource	Description	Type	URI
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/
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.

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Outbound Connection Setup Attempts per Day (Cisco ASA)	Daily Connection Setup Attempts
Inbound Connection Setup Attempts per Day (Cisco ASA)	

- 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 3-2 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 Foundation/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 Foundation/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 Foundation/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) /

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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)/
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)/

Resource	Description	Type	URI
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) /
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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) /
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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/

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/
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)/
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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	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/
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/

Resource	Description	Type	URI
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)/
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 where the Bytes In, Bytes Out, and Target Port or Application Protocol fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

Resource	Description	Type	URI
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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/

Resource	Description	Type	URI
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 Foundation/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 within the last 24 hours. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
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 Foundation/Cisco Monitoring/Functionality/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
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 70](#)
- ["Cisco Ironport Email Security Appliance \(ESA\)" on page 103](#)
- ["Cisco Ironport Web Security Appliance \(WSA\)" on page 110](#)
- ["Cisco Network" on page 116](#)

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 3-3 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 Foundation/Cisco Monitoring/Functionality/Cross-Device/
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 grouped by users. A chart shows the top ten users with most failed login attempts. A table shows the details of the failed login attempts grouped by user.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/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 all successful logins by destination address. A chart shows the top ten destination addresses. A table shows all successful events, grouped by destination.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/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 failed logins by source address. A chart shows the top ten sources with the most failed logins. A table lists all failed logins grouped by the source host.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/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/
Library Resources			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories

Resource	Description	Type	URI
Top Transport Protocols	This data monitor shows the top transport protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Top Categories	This data monitor shows the top categories recorded by Cisco devices within the last hour.	Data Monitor	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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	/All Field Sets/ArcSight System/Event Field Sets/Active Channels
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-Categorize d 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/I ntrusion 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/C ross-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/I ntrusion Prevention System/
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/
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/
Cisco Network Systems	This filter identifies events from all Cisco network devices (routers and switches). Modify this filter to include all Cisco network products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Failed Logins by Destination Address	This query returns failed login attempts recorded by Cisco devices.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Cisco Login Detail (Trend Based)	This query returns all logins recorded by Cisco devices within the last seven days.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
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 Foundation/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 where the Bytes In, Bytes Out, and Target Port or Application Protocol fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Event Count by Hour	This query counts the total number of Cisco events per hour within the last six hours.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Successful Login by Source Address	This query returns all successful authentication events, grouped by source host.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour within the last 24 hours. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Successful Logins by User	This query returns all successful login attempts and the users involved.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Top Users with Successful Logins	This query returns the top users with successful login attempts.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Failed Logins by User	This query returns all failed login attempts and the involved users.	Query	ArcSight Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Login Tracking/
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
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 Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

Resource	Description	Type	URI
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:

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Outbound Connection Setup Attempts per Day (Cisco FWSM)	Daily Connection Setup Attempts
Inbound Connection Setup Attempts per Day (Cisco FWSM)	

- 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 3-4 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 Foundation/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 Foundation/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) /

Resource	Description	Type	URI
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 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) /

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
Library Resources			
Cisco Firewall Message Types	This active list contains the mapping of Cisco firewall syslog message types.	Active List	ArcSight Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Cisco Top FWSM Sources	This data monitor shows the top 20 event-generating Cisco FWSM devices within the last hour.	Data Monitor	ArcSight Foundation/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 Foundation/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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	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/
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
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/
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/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
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 Foundation/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 where the Bytes In, Bytes Out, and Target Port or Application Protocol fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 within the last 24 hours. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM) /
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/Without Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
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.
- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Cisco Firewall Configuration Changes by Type	Daily Configuration Changes
Cisco Overall Denied Inbound Connections per Hour in the Previous Day	Daily Connection Setup Attempts
Cisco Overall Outbound Connection Setup Attempts per Day	
Cisco Overall Inbound Connection Setup Attempts per Day	
Cisco Overall Denied Outbound Connections per Hour in the Previous Day	

- 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 3-5 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 Foundation/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 Foundation/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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	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/
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/

Resource	Description	Type	URI
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/
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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 where the Bytes In, Bytes Out, and Target Port or Application Protocol fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
Cisco Overall Outbound Connections per Day	This query returns the count of outbound connections per day for the previous week.	Query	ArcSight Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
Bandwidth Usage per Hour	This query returns the count of TotalBytes (Bytes In + Bytes Out) per hour within the last 24 hours. The query looks for events where the Bytes In and Bytes Out fields are not empty.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Bandwidth Tracking/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Allowed Outbound Connections by Port	This query returns the count of allowed outbound connections by destination port.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Firewall/

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA) /
Three Charts Landscape	This template is designed to show three charts and a description field. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/3 Charts/Without Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/Without Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
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 Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

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](#)
- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Cisco IPS Configuration Changes per Day	Daily Configuration Changes
Top Cisco Alerts in a Month Cisco Alerts per Hour in the Previous Day Top Targets in Cisco Alerts over a Month Top Attackers in Cisco Alerts over a Month Cisco Alerts per Day	Daily Alerts

- 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 3-6 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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Daily Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/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 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 3-7 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	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /
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	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /
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	ArcSight Foundation/Cisco Monitoring/Products/Cisco Intrusion Prevention System Sensor (IPS Sensor) /

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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
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 3-8 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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table

Resource	Description	Type	URI
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:

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Cisco ESA Configuration Changes per Day	Daily Configuration Changes
Message Transaction per Hour in the Previous Day (Cisco ESA)	Daily Email Transactions
Message Transactions per Day (Cisco ESA)	

- 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 3-9 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 Foundation/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)/

Resource	Description	Type	URI
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)/
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)/

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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 Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
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 Foundation/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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	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/
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)/

Resource	Description	Type	URI
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 Recipients with Most Bandwidth	This query returns the top recipients with most bandwidth consumption.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

Resource	Description	Type	URI
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 Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Configuration Changes (Event Based)	This query returns all configuration changes recorded by Cisco devices within the last 24 hours.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Three Charts Landscape	This template is designed to show three charts and a description field. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/3 Charts/Without Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table

Resource	Description	Type	URI
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Daily Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
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:

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Cisco WSA Configuration Changes per Day	Daily Configuration Changes
Web Requests per Day in the Previous Week (Cisco WSA)	Daily Web Requests

- 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 3-10 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 Foundation/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)/

Resource	Description	Type	URI
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) /
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) /

Resource	Description	Type	URI
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)/
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 Foundation/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 Foundation/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)/

Resource	Description	Type	URI
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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Top Hosts with Most Web Traffic	This query returns information about the top hosts with most web traffic over the past day.	Query	ArcSight Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Detail Unsuccessful Requests	This query returns all unsuccessful requests.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/

Resource	Description	Type	URI
Top Denied Sites	This query returns the top 100 sites denied by Cisco WSA systems over the past day.	Query	ArcSight Foundation/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 Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Two Charts Landscape	This template is designed to show two charts and a description field. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/2 Charts/Without Table
Daily Web Requests	This trend stores web requests in a day.	Trend	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA) /
Daily Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/

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:

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Cisco Network Equipment Configuration Changes per Day	Daily Configuration Changes
Trend of Daily SNMP Access on Specific Cisco Target	Daily SNMP Access
Top Target Cisco SNMP Access in a Week	
Trend of Daily Cisco SNMP Access	

- Verify that the Cisco Network Systems filter captures events from Cisco network equipment in your environment. If necessary, the ArcSight Administrator can modify the filter to include any missing equipment.

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 3-11 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 Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Events	This active channel shows all network events reported by Cisco network equipment (routers, switches).	Active Channel	ArcSight Foundation/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 Foundation/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/

Resource	Description	Type	URI
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/
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/

Resource	Description	Type	URI
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/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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/

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 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/
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 selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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/

Resource	Description	Type	URI
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 Network Systems	This filter identifies events from all Cisco network devices (routers and switches). Modify this filter to include all Cisco network products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
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 Foundation/Cisco Monitoring/Functionality/Network/Device SNMP Authentication Failures/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Network/

Resource	Description	Type	URI
Daily SNMP Access - Base	This query returns all SNMP access to Cisco devices. This serves as a base query for a trend.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Network/
Cisco SNMP Access (Trend Based)	This query returns all SNMP Access recorded Cisco devices within the last seven days.	Query	ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Cross-Device/Configuration Changes/
Simple Table Portrait	This template is designed to show a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Table
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Simple Table Landscape	This template is designed to show a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Table

Resource	Description	Type	URI
Simple Chart Landscape	This template is designed to show one chart. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/Without Table
Two Charts One Table Landscape	This template is designed to show two charts and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/2 Charts/With Table
Daily Configuration Changes	This trend keeps track of all attempts to change a configuration recorded by a Cisco device.	Trend	ArcSight Foundation/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:

- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

These reports...	Require this trend...
Associations - Disassociations per Day (Cisco APs)	Daily Associations - Disassociations

- 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 3-12 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 Foundation/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/

Resource	Description	Type	URI
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/
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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Wireless/

Resource	Description	Type	URI
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 Foundation/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/
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 Foundation/Cisco Monitoring/Functionality/Wireless/
Disassociated Devices per AP	This query returns the count of wireless devices that disassociated with an Access Point.	Query	ArcSight Foundation/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 Foundation/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 Foundation/Cisco Monitoring/Functionality/Wireless/
Disassociated Devices	This query returns all devices that leave (disassociate with) an Aironet Access Point.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Association - Disassociation Details	This query returns all association or disassociation events grouped by hour within the last day.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/

Resource	Description	Type	URI
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 Foundation/Cisco Monitoring/Functionality/Wireless/
Associated APs per Device	This query returns all associated Access Points per wireless device.	Query	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Chart and Table Landscape	This template is designed to show one chart and a table. The orientation is landscape.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Chart and Table Portrait	This template is designed to show one chart and a table. The orientation is portrait.	Report Template	/All Report Templates/ArcSight System/1 Chart/With Table
Daily Associations - Disassociations	This trend tracks all disassociation/association events related to Cisco Aironet Access Points.	Trend	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/

Index

A

Access Points dashboard 123

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 36
- Alert, Critical and Error Events from Cisco Firewall Systems 71
- Alert, Critical and Error Events from Cisco FWSM Systems 59
- Cisco ASA Events 36
- Cisco FWSM Events 59
- Cisco IOS IPS Events 97
- Cisco IPS Sensor Events 91
- Cisco Ironport ESA Events 103
- Cisco Ironport WSA Events 110
- Cisco Network Events 116
- Device Interface Notifications 116
- 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 116
- Events from Cisco Wireless Systems 123
- IPS Syslog Events from Cisco ASA Systems 36
- Status Events from Cisco IOS IPS Systems 97
- Status Events from Cisco IPS Sensor Systems 91
- Status Events from Cisco IPS Systems 84

active lists

- Cisco Firewall Message Types 22, 41, 64
- HTTP Status Code Classes 112

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 36

Alert, Critical and Error Events from Cisco Firewall Systems active channel 71

Alert, Critical and Error Events from Cisco FWSM Systems active channel 59

Allowed Inbound Connections by Destination Address (Cisco ASA) query 44

Allowed Inbound Connections by Destination Address (Cisco FWSM) query 67

Allowed Inbound Connections by Port (Cisco ASA) query 44

Allowed Inbound Connections by Port (Cisco FWSM) query 68

Allowed Inbound Connections by Source Address (Cisco ASA) query 44

Allowed Inbound Connections by Source Address (Cisco FWSM) query 66

Allowed Outbound Connections by Destination Address (Cisco ASA) query 44

Allowed Outbound Connections by Destination Address (Cisco FWSM) query 68

Allowed Outbound Connections by Port (Cisco ASA) query 47

Allowed Outbound Connections by Port (Cisco FWSM) query 67

Allowed Outbound Connections by Source Address (Cisco ASA) query 45

Allowed Outbound Connections by Source Address (Cisco FWSM) query 68

Application Protocol is NULL filter 42, 53, 64, 77

ArcSight Administration overview 5

ArcSight Core Security overview 5

ArcSight Foundations overview 6

ArcSight System overview 6

asset categories

Business Impact Analysis 22, 41, 51, 64, 76, 86, 93, 99

Protected 22, 41, 64, 76

Associated APs per Device query 126

Associated Devices in a Day - Event Based query 125

Associated Devices in a Day (Event Based) query viewer 123

Associated Devices per AP query 125

Associated Wireless Devices to Cisco APs report 124

Association - Disassociation Details query 125

Association - Disassociation per Day query 125

Associations - Disassociations (Trend Based) query viewer 124

Associations - Disassociations per Day (Cisco APs) report 124

Attacker and Target Address Present filter 27, 42, 64, 77

Attacker Host or Address Present filter 25, 41, 52, 64, 77, 88, 94, 100, 106

Attacker or Target User Present filter 26, 42, 53, 65, 78, 88, 95, 101, 107, 113, 120

Attacker User Present filter 27, 54

Authentication Errors (Cisco ASA) query 44

B

Bandwidth Usage by Hour (Cisco ASA) report 40

Bandwidth Usage by Hour (Cisco Firewall) report 75

Bandwidth Usage by Hour (Cisco FWSM) report 63

Bandwidth Usage by Protocol (Cisco ASA) report 40
Bandwidth Usage by Protocol (Cisco Firewall) report 74
Bandwidth Usage by Protocol (Cisco FWSM) report 63
Bandwidth Usage by Protocol query 43, 55, 66, 79
Bandwidth Usage by Protocol report 50
Bandwidth Usage per Hour query 45, 55, 66, 80
Bandwidth Usage per Hour report 51
Business Impact Analysis asset category 22, 41, 51, 64, 76, 86, 93, 99

C

Categories field set 25, 52
Chart and Table Landscape report template 47, 57, 69, 82, 90, 108, 115, 121, 126
Chart and Table Portrait report template 47, 57, 69, 82, 90, 109, 115, 126
Cisco Access Points and Associated Wireless Devices report 124
Cisco Adaptive Security Appliance (ASA) use case 35
Cisco Aironet filter 125
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 30, 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 79
Cisco Application Protocol Present filter 26, 53
Cisco ASA Allowed Connections Overview dashboard 37
Cisco ASA Denied Connections Overview dashboard 36
Cisco ASA Event Counts by Hour in Last 6 Hours query 32, 45
Cisco ASA Event Counts by Hour per Device query 34, 47, 82
Cisco ASA Event Flow Statistics by Device data monitor 23, 41
Cisco ASA Event Overview dashboard 18, 37
Cisco ASA Events active channel 36
Cisco ASA Hourly Event Count query viewer 19, 38
Cisco ASA Hourly Event per Device query viewer 21, 38, 73
Cisco ASA Inbound Connections per Day query 46
Cisco ASA IPS Alert Events filter 43
Cisco ASA Outbound Connections per Day query 45
Cisco ASA Successful Configuration Changes filter 43
Cisco ASA Systems filter 28, 43, 54, 65, 78
Cisco Configuration Change Detail (Trend Based) query 33, 57
Cisco Configuration Change Detail (Trend Based) query

viewer 19, 49
Cisco Configuration Changes (Event Based) query 31, 43, 55, 66, 79, 89, 96, 101, 108, 114
Cisco Configuration Changes by Type (Cisco ASA) report 39
Cisco Configuration Changes by Type (Cisco FWSM) report 63
Cisco Configuration Changes by Type report 51
Cisco Configuration Changes by User (Cisco ASA) report 39
Cisco Configuration Changes by User (Cisco FWSM) report 63
Cisco Configuration Changes by User (Event Based) query 30, 46, 56, 67, 80, 89, 95, 101, 107, 114, 121
Cisco Configuration Changes by User report 51
Cisco Configuration Changes Overview dashboard 18, 49
Cisco Configuration Changes per Day report 51
Cisco Configuration Changes per Hour in the Previous Day report 50
Cisco Critical Network Events filter 119
Cisco Cross-Device use case 35
Cisco Current Event Sources dashboard 17, 48
Cisco Denied Connections by Destination Host - Template query 78
Cisco Denied Connections by Port - Template query 79
Cisco Denied Connections by Source Host - Template query 81
Cisco Device Critical Events query 120
Cisco Device Critical Events report 117
Cisco Device Errors query 121
Cisco Device Errors report 118
Cisco Device Interface Notifications field set 25, 52, 118
Cisco Device Interface Status Messages query 120
Cisco Device Interface Status Messages report 118
Cisco Device SNMP Authentication Failures by User query 120
Cisco Device SNMP Authentication Failures query 120
Cisco ESA Configuration Changes by Type report 105
Cisco ESA Configuration Changes by User report 105
Cisco ESA Configuration Changes in the Last 6 Hours query 30, 56
Cisco ESA Configuration Changes in the Last 6 Hours query viewer 21, 49
Cisco ESA Configuration Changes per Day in the Last 7 Days query 108
Cisco ESA Configuration Changes per Day report 105
Cisco ESA Delivery Connection Count by Hour query 108
Cisco ESA Injection Connection Count by Hour query 108
Cisco Event Count by Hour query 29, 55
Cisco Event Count by Hour query viewer 20, 49
Cisco Event Statistics dashboard 17, 48
Cisco Events filter 28, 43, 54, 65, 78, 88, 95, 101, 107, 113, 120, 125
Cisco Events with Protocols field set 25, 52
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 75
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 19, 49
Cisco Firewall Configuration Changes in the Last 6 Hours query 31, 55

- Cisco Firewall Configuration Changes per Day in the Last 7 Days query 78
- Cisco Firewall Configuration Changes per Day report 76
- Cisco Firewall Denied Connections in Last 2 Hours dashboard 71
- 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 22, 41, 64
- Cisco Firewall Overview - Top Allowed Systems report 22
- Cisco Firewall Overview - Top Denied Systems report 22
- Cisco Firewall Overview - Trend and Port report 22
- Cisco Firewall Services Module (FWSM) use case 35
- Cisco Firewall Successful Configuration Changes filter 78
- Cisco Firewall Systems filter 28, 43, 54, 65, 78
- Cisco Firewall-Categorized Events filter 26, 42, 65, 78
- Cisco FWSM Allowed Connections Overview dashboard 59
- Cisco FWSM Denied Connections Overview dashboard 59
- Cisco FWSM Event Counts by Hour per Device query 34, 69, 82
- Cisco FWSM Event Counts by Hour query 31, 66
- Cisco FWSM Event Flow Statistics by Device data monitor 23, 64
- Cisco FWSM Event Overview dashboard 18, 60
- Cisco FWSM Events active channel 59
- Cisco FWSM Hourly Event Count query viewer 20, 60
- Cisco FWSM Hourly Event per Device query viewer 21, 61, 73
- Cisco FWSM Inbound Connections per Day query 67
- Cisco FWSM Outbound Connections per Day query 66
- Cisco FWSM Successful Configuration Changes filter 28, 65
- Cisco FWSM Systems filter 26, 42, 53, 65, 78
- Cisco Generic Firewall Event Overview dashboard 71
- Cisco Generic Firewall use case 35
- Cisco Generic Intrusion Prevention System (IPS) use case 35
- Cisco Generic IPS Alert Overview dashboard 84
- Cisco Generic IPS Event Overview dashboard 84
- Cisco Intrusion Prevention System (IPS) Sensor use case 35
- Cisco Intrusion Prevention System Overview report 22
- Cisco IOS Intrusion Prevention System (IOS IPS) use case 34
- 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 24, 99
- Cisco IOS IPS Event Overview dashboard 18, 98
- Cisco IOS IPS Events active channel 97
- Cisco IOS IPS Hourly Event Count per Device query viewer 21, 98
- Cisco IOS IPS Hourly Event Count query viewer 20, 98
- Cisco IOS IPS Successful Configuration Changes filter 25, 99
- Cisco IOS IPS Systems filter 25, 52, 87, 94, 100
- Cisco IPS Alert Events filter 27, 53, 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 29, 55
- Cisco IPS Configuration Changes in the Last 6 Hours query viewer 19, 49
- 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 24, 93
- Cisco IPS Sensor Event Overview dashboard 18, 92
- Cisco IPS Sensor Event Types data monitor 24, 87, 93
- Cisco IPS Sensor Events active channel 91
- Cisco IPS Sensor Successful Configuration Changes filter 26, 95
- Cisco IPS Sensor Systems filter 28, 54, 88, 95, 101
- Cisco IPS Status Events filter 88, 94, 100
- Cisco IPS Successful Configuration Changes filter 87
- Cisco IPS Systems filter 27, 54, 88, 94, 100
- Cisco IPS-Categorized Events filter 26, 53, 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 34
- Cisco Ironport ESA Events active channel 103
- Cisco Ironport ESA Systems filter 27, 53, 106
- Cisco Ironport Web Security Appliance (WSA) use case 35
- Cisco Ironport WSA Events active channel 110
- Cisco Ironport WSA Systems filter 26, 53, 113
- Cisco Login Detail (Trend Based) query 31, 55
- Cisco Login Details in the Last 7 Days (Trend Based) query viewer 20, 49
- Cisco Network Configuration Changes per Day in the Last 7 Days query 120
- Cisco Network Device Inbound Interface Status Events filter 119
- Cisco Network Device Interface Down Messages filter 119
- Cisco Network Device Interface Status Events filter 119
- Cisco Network Device Outbound Interface Status Events filter 119
- Cisco Network Equipment Configuration Change By Event query 121
- Cisco Network Equipment Configuration Changes by Device report 117
- Cisco Network Equipment Configuration Changes by Type report 118
- Cisco Network Equipment Configuration Changes by User report 117
- Cisco Network Equipment Configuration Changes in the Last 6 Hours query 30, 56
- Cisco Network Equipment Configuration Changes in the Last 6 Hours query viewer 19, 49
- Cisco Network Equipment Configuration Changes per Day report 117
- Cisco Network Error Events filter 119
- Cisco Network Event Count by Hour query 121
- Cisco Network Event Count by Hour query viewer 117
- Cisco Network Event Flow Statistics by Device data

- monitor 118
- Cisco Network Event Overview dashboard 117
- Cisco Network Events active channel 116
- Cisco Network Events filter 119
- Cisco Network SNMP Authentication Failures report 117
- Cisco Network Systems filter 28, 54, 120
- Cisco Network use case 35
- 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 33, 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 31, 79
- Cisco Overall Allowed Inbound Connections by Source Host report 76
- Cisco Overall Allowed Outbound Connections by Destination Host query 32, 80
- Cisco Overall Allowed Outbound Connections by Destination Host report 73
- Cisco Overall Allowed Outbound Connections by Port query 80
- Cisco Overall Allowed Outbound Connections by Source Host query 32, 80
- Cisco Overall Allowed Outbound Connections by Source Host report 73
- Cisco Overall Denied Inbound Connections by Destination Host query 30, 81
- Cisco Overall Denied Inbound Connections by Destination Host report 75
- Cisco Overall Denied Inbound Connections by Destination Port report 74
- Cisco Overall Denied Inbound Connections by Port query 32, 44, 66, 79
- Cisco Overall Denied Inbound Connections by Source Host query 30, 46, 67, 80
- Cisco Overall Denied Inbound Connections by Source Host report 75
- Cisco Overall Denied Inbound Connections per Hour - Event Based query 68
- 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 74
- Cisco Overall Denied Outbound Connections by Destination Host query 33, 81
- 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 31, 46, 68, 81
- Cisco Overall Denied Outbound Connections by Source Host query 30, 45, 67, 80
- Cisco Overall Denied Outbound Connections by Source Host report 74
- Cisco Overall Denied Outbound Connections per Hour - Event Based query 68
- Cisco Overall Denied Outbound Connections per Hour in the Previous Day report 75
- Cisco Overall Inbound Connection Setup Attempts per Day report 73
- Cisco Overall Inbound Connections per Day query 32, 79
- Cisco Overall Outbound Connection Setup Attempts per Day report 75
- Cisco Overall Outbound Connections per Day query 29, 79
- Cisco Overall Outbound Connections per Hour in the Previous Day query 79
- Cisco Select Category Present filter 28, 54
- Cisco SNMP Access (Trend Based) query 121
- Cisco SNMP Access On Certain Target (Trend Based) query 121
- Cisco SNMP Authentication Failures by Device query 120
- Cisco Successful Network Configuration Changes filter 120
- Cisco Target Port Present filter 28, 54
- Cisco Top ASA Event Sources by Message Types data monitor 23, 41
- Cisco Top ASA Sources data monitor 24, 41
- Cisco Top Event Sources by Device data monitor 24, 52
- Cisco Top Event Sources by Device Group data monitor 23, 52
- Cisco Top Event Sources by Product data monitor 23, 52
- Cisco Top Firewall Product Sources data monitor 77
- Cisco Top FWSM Event Sources by Message Types data monitor 23, 64
- Cisco Top FWSM Sources data monitor 24, 64
- 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 23, 99
- Cisco Top IOS IPS Event Types data monitor 23, 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 23, 93
- Cisco Top Network Devices data monitor 118
- Cisco Transportation Protocol Present filter 28, 54
- Cisco Wireless AP Device Association filter 125
- Cisco Wireless AP Device Disassociation filter 125
- Cisco Wireless Event Flow Statistics by AP data monitor 125
- Cisco Wireless Events field set 125
- Cisco Wireless Systems filter 125
- Cisco Wireless use case 35
- Cisco WSA Configuration Changes by Type report 111
- Cisco WSA Configuration Changes by User report 112
- Cisco WSA Configuration Changes in the Last 6 Hours query 30, 56
- Cisco WSA Configuration Changes in the Last 6 Hours query viewer 20, 50
- Cisco WSA Configuration Changes per Day in the Last 7 Days query 113
- Cisco WSA Configuration Changes per Day report 111
- Common IPS Event Types filter 27, 88, 100
- Configuration Changes per Day in the Last 7 Days query 33, 56
- Configuration Changes per Hour in the Previous Day query 29, 55
- Connection Overview (Cisco ESA) report 105
- Connections Accepted by Address (Cisco ASA) query 44

Connections Denied by Address (Cisco ASA) query 44
content packages 7

D

Daily Alerts - Base query 33, 57, 90, 95, 101
Daily Alerts trend 34, 58, 90, 96, 102
Daily Associations - Disassociations (Base) query 126
Daily Associations - Disassociations trend 126
Daily Configuration Changes - Base query 31, 57, 81, 90, 108, 114, 121
Daily Configuration Changes trend 34, 57, 82, 90, 109, 115, 122
Daily Connection Setup Attempts - Base query 33, 46, 56, 68, 81
Daily Connection Setup Attempts trend 34, 47, 57, 69, 82
Daily Email Transactions trend 34, 109
Daily Logins - Base query 34, 57
Daily Logins per Product query 32
Daily Logins trend 34, 58
Daily Message Transactions - Base query 29, 107
Daily SNMP Access - Base query 121
Daily SNMP Access trend 122
Daily Web Requests - Base query 114
Daily Web Requests trend 115
dashboards
 Access Points 123
 Cisco ASA Allowed Connections Overview 37
 Cisco ASA Denied Connections Overview 36
 Cisco ASA Event Overview 18, 37
 Cisco Configuration Changes Overview 18, 49
 Cisco Current Event Sources 17, 48
 Cisco Event Statistics 17, 48
 Cisco Firewall Allowed Connections in Last 2 Hours 71
 Cisco Firewall Denied Connections in Last 2 Hours 71
 Cisco FWSM Allowed Connections Overview 59
 Cisco FWSM Denied Connections Overview 59
 Cisco FWSM Event Overview 18, 60
 Cisco Generic Firewall Event Overview 71
 Cisco Generic IPS Alert Overview 84
 Cisco Generic IPS Event Overview 84
 Cisco IOS IPS Alert Overview 98
 Cisco IOS IPS Event Overview 18, 98
 Cisco IPS Sensor Alert Overview 92
 Cisco IPS Sensor Event Overview 18, 92
 Cisco Network Event Overview 117
 Device Interface Status 116
 Login Overview 17, 49
 Sender and Recipient Overview 18, 103
 Transaction Connections Overview 103
 Web Transactions 18, 110
data monitors
 Cisco ASA Event Flow Statistics by Device 23, 41
 Cisco FWSM Event Flow Statistics by Device 23, 64
 Cisco IOS IPS Event Flow Statistics by Device 24, 99
 Cisco IPS Event Flow Statistics by Device Product 87
 Cisco IPS Event Types 87
 Cisco IPS Sensor Event Flow Statistics by Device 24, 93
 Cisco IPS Sensor Event Types 24, 87, 93

Cisco Network Event Flow Statistics by Device 118
Cisco Top ASA Event Sources by Message Types 23, 41
Cisco Top ASA Sources 24, 41
Cisco Top Event Sources by Device 24, 52
Cisco Top Event Sources by Device Group 23, 52
Cisco Top Event Sources by Product 23, 52
Cisco Top Firewall Product Sources 77
Cisco Top FWSM Event Sources by Message Types 23, 64
Cisco Top FWSM Sources 24, 64
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 23, 99
Cisco Top IOS IPS Event Types 23, 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 23, 93
Cisco Top Network Devices 118
Cisco Wireless Event Flow Statistics by AP 125
Device Inbound Interface Status 118
Device Outbound Interface Status 118
Event Flow by Cisco Firewall Products in the Last 2 Hours 77
Event Flow Statistics by Device in Last 2 Hours (Cisco ESA) 106
Event Flow Statistics by Device in Last 2 Hours (Cisco WSA) 25, 112
Last 10 Cisco FWSM Successful Configuration Changes 25, 64
Last 10 Cisco IOS IPS Successful Configuration Changes 24, 99
Last 10 Cisco IPS Sensor Successful Configuration Changes 24, 93
Most Frequent Ports 24, 52
Top Access Points with Most Association Events 124
Top Access Points with Most Disassociation Events 124
Top Activities across Cisco Firewall Devices 76
Top Application Protocols 23, 52
Top Categories 24, 52
Top Systems with Most Rejected Injection Connections 106
Top Transport Protocols 23, 52
Delivery Connection (Cisco ESA) filter 106
Delivery Connections by Hour query viewer 104
Delivery Connections query 107
Delivery Connections query viewer 104
Denied Inbound Connections by Address (Cisco ASA) report 39
Denied Inbound Connections by Address (Cisco FWSM) report 63
Denied Inbound Connections by Destination Address (Cisco ASA) query 46
Denied Inbound Connections by Destination Address (Cisco FWSM) query 66
Denied Inbound Connections by Port (Cisco ASA) query 44
Denied Inbound Connections by Port (Cisco ASA) report 40

Denied Inbound Connections by Port (Cisco FWSM) query 66

Denied Inbound Connections by Port (Cisco FWSM) report 62

Denied Inbound Connections by Source Address (Cisco ASA) query 46

Denied Inbound Connections by Source Address (Cisco FWSM) query 66

Denied Inbound Connections per Hour (Cisco FWSM) report 62

Denied Outbound Connections by Address (Cisco ASA) report 41

Denied Outbound Connections by Address (Cisco FWSM) report 62

Denied Outbound Connections by Destination Address (Cisco ASA) query 45

Denied Outbound Connections by Destination Address (Cisco FWSM) query 67

Denied Outbound Connections by Port (Cisco ASA) query 45

Denied Outbound Connections by Port (Cisco ASA) report 39

Denied Outbound Connections by Port (Cisco FWSM) query 67

Denied Outbound Connections by Port (Cisco FWSM) report 62

Denied Outbound Connections by Source Address (Cisco ASA) query 46

Denied Outbound Connections by Source Address (Cisco FWSM) query 68

Denied Outbound Connections per Hour (Cisco FWSM) report 63

Denied Web Server Requests filter 113

Detail Successful Requests query 30, 114

Detail Unsuccessful Requests query 114

Device Inbound Interface Status data monitor 118

Device Interface Notifications active channel 116

Device Interface Status dashboard 116

Device Outbound Interface Status data monitor 118

Disassociated Devices in a Day (Event Based) query viewer 124

Disassociated Devices per AP query 125

Disassociated Devices query 125

E

Email Message Transaction (Cisco ESA) filter 26, 106

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

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 106

Event Flow Statistics by Device in Last 2 Hours (Cisco WSA) data monitor 25, 112

Events from Cisco Firewall Systems active channel 71

Events from Cisco IPS Systems active channel 84

Events from Cisco Network Systems active channel 116

Events from Cisco Wireless Systems active channel 123

F

Failed Logins by Destination Address query 29, 54

Failed Logins by Destination Address report 51

Failed Logins by Source Address query 29, 55

Failed Logins by Source Address report 51

Failed Logins by User in the Last 2 Hours query viewer 20, 49

Failed Logins by User query 31, 57

Failed Logins by User report 50

Failed VPN Connection Events (Cisco ASA) filter 42

field sets

- Categories 25, 52
- Cisco Device Interface Notifications 25, 52, 118
- Cisco Events with Protocols 25, 52
- Cisco Firewall Events 77
- Cisco Wireless Events 125

filters

- Application Protocol is NULL 42, 53, 64, 77
- Attacker and Target Address Present 27, 42, 64, 77
- Attacker Host or Address Present 25, 41, 52, 64, 77, 88, 94, 100, 106
- Attacker or Target User Present 26, 42, 53, 65, 78, 88, 95, 101, 107, 113, 120
- Attacker User Present 27, 54
- Cisco Aironet 125
- Cisco Application Protocol Present 26, 53
- Cisco ASA IPS Alert Events 43
- Cisco ASA Successful Configuration Changes 43
- Cisco ASA Systems 28, 43, 54, 65, 78
- Cisco Critical Network Events 119
- Cisco Events 28, 43, 54, 65, 78, 88, 95, 101, 107, 113, 120, 125
- Cisco Firewall Category Device Group Present 78
- Cisco Firewall Successful Configuration Changes 78
- Cisco Firewall Systems 28, 43, 54, 65, 78
- Cisco Firewall-Categorized Events 26, 42, 65, 78
- Cisco FWSM Successful Configuration Changes 28, 65
- Cisco FWSM Systems 26, 42, 53, 65, 78
- Cisco IOS IPS Alert Events 100
- Cisco IOS IPS Successful Configuration Changes 25, 99
- Cisco IOS IPS Systems 25, 52, 87, 94, 100
- Cisco IPS Alert Events 27, 53, 87, 94, 100
- Cisco IPS Error Events 87, 94, 99
- Cisco IPS Sensor Alert Events 94
- Cisco IPS Sensor Successful Configuration Changes 26, 95
- Cisco IPS Sensor Systems 28, 54, 88, 95, 101
- Cisco IPS Status Events 88, 94, 100
- Cisco IPS Successful Configuration Changes 87
- Cisco IPS Systems 27, 54, 88, 94, 100
- Cisco IPS-Categorized Events 26, 53, 88, 94, 100
- Cisco IPS-Categorized IOS IPS Events 100
- Cisco IPS-Categorized IPS Sensor Events 94
- Cisco Ironport ESA Systems 27, 53, 106
- Cisco Ironport WSA Systems 26, 53, 113
- Cisco Network Device Inbound Interface Status Events 119
- Cisco Network Device Interface Down Messages 119
- Cisco Network Device Interface Status Events 119
- Cisco Network Device Outbound Interface Status Events 119

- Cisco Network Error Events 119
 - Cisco Network Events 119
 - Cisco Network Systems 28, 54, 120
 - Cisco Select Category Present 28, 54
 - Cisco Successful Network Configuration Changes 120
 - Cisco Target Port Present 28, 54
 - Cisco Transportation Protocol Present 28, 54
 - Cisco Wireless AP Device Association 125
 - Cisco Wireless AP Device Disassociation 125
 - Cisco Wireless Systems 125
 - Common IPS Event Types 27, 88, 100
 - Delivery Connection (Cisco ESA) 106
 - Denied Web Server Requests 113
 - Email Message Transaction (Cisco ESA) 26, 106
 - Failed VPN Connection Events (Cisco ASA) 42
 - Firewall Accepts 28, 43, 65, 78
 - Firewall Access Events 27, 42, 54, 65, 77
 - Firewall Deny 27, 42, 65, 77
 - Inbound Events 26, 42, 65, 77
 - Injection Connection (Cisco ESA) 106
 - Internal Attackers 28, 43, 65, 78
 - Internal Targets 28, 43, 65, 77
 - Login Attempts 26, 53
 - Outbound Events 26, 42, 65, 78
 - Rejected Injection Connection (Cisco ESA) 106
 - SNMP Authentication Failed 119
 - SNMP Events 119
 - Successful Configuration Changes 27, 42, 64, 77, 88, 94, 100, 106, 113, 119
 - Successful Configuration Changes (Cisco ESA) 106
 - Successful Logins 25, 52
 - Successful VPN Connection Events (Cisco ASA) 43
 - Successful Web Transactions 27, 112
 - Successful WSA Configuration Changes 113
 - Target Host or Address Present 25, 41, 52, 64, 77, 87, 94, 100, 106, 119
 - Target User Present 26, 42, 53, 119
 - Unsuccessful Logins 27, 53
 - Unsuccessful Web Server Requests 28, 113
 - VPN Authentication Errors (Cisco ASA) 43
 - VPN Events 42
 - Web Requests 25, 113
 - Windows Events with a Non-Machine User 27, 53
 - Firewall Accepts filter 28, 43, 65, 78
 - Firewall Access Events filter 27, 42, 54, 65, 77
 - Firewall Deny filter 27, 42, 65, 77
 - Four Charts Landscape report template 34
- ## H
- HTTP Status Code Classes active list 112
- ## I
- Inbound Connection Setup Attempts per Day (Cisco ASA) report 40
 - Inbound Connection Setup Attempts per Day (Cisco FWSM) report 62
 - Inbound Events filter 26, 42, 65, 77
 - Injection Connection (Cisco ESA) filter 106
 - Injection Connections by Hour query viewer 104
 - Injection Connections query 107
 - Injection Connections query viewer 104
 - Internal Attackers filter 28, 43, 65, 78
 - Internal Targets filter 28, 43, 65, 77
 - IOS IPS Event Counts by Hour per Device query 29, 101
 - IOS IPS Event Counts by Hour query 33, 101
 - IPS Configuration Changes per Day in the Last 7 Days query 90
 - IPS Sensor Event Counts by Hour per Device query 29, 95
 - IPS Sensor Event Counts by Hour query 31, 95
 - IPS Sensor Hourly Event Count per Device query viewer 19, 92
 - IPS Sensor Hourly Event Count query viewer 19, 92
 - IPS Syslog Events from Cisco ASA Systems active channel 36
- ## L
- Last 10 Cisco FWSM Successful Configuration Changes data monitor 25, 64
 - Last 10 Cisco IOS IPS Successful Configuration Changes data monitor 24, 99
 - Last 10 Cisco IPS Sensor Successful Configuration Changes data monitor 24, 93
 - Login Attempts filter 26, 53
 - Login Overview dashboard 17, 49
 - Logins per Day in the Last 7 Days query 30, 56
 - Logins per Day report 50
 - Logins per Hour in the Previous Day query 55
 - Logins per Hour in the Previous Day report 50
- ## M
- Message Transaction Details query 32, 108
 - Message Transaction Details query viewer 21, 104
 - Message Transaction per Hour in the Previous Day (Cisco ESA) report 105
 - Message Transactions per Day (Cisco ESA) report 105
 - Message Transactions per Day in the Previous Week query 108
 - Message Transactions per Hour in the Previous Day query 108
 - Most Frequent Ports data monitor 24, 52
- ## O
- Outbound Connection Setup Attempts per Day (Cisco ASA) report 39
 - Outbound Connection Setup Attempts per Day (Cisco FWSM) report 63
 - Outbound Events filter 26, 42, 65, 78
 - Overview of Cisco Configuration Changes report 21
 - Overview of Logins Reported by Cisco Devices - Systems report 22
 - Overview of Logins Reported by Cisco Devices - Trend and Users report 22
- ## P
- packages
 - deleting 10
 - installing 9
 - uninstalling 9
 - Protected asset category 22, 41, 64, 76
- ## Q
- queries

- Allowed Inbound Connections by Destination Address (Cisco ASA) 44
- Allowed Inbound Connections by Destination Address (Cisco FWSM) 67
- Allowed Inbound Connections by Port (Cisco ASA) 44
- Allowed Inbound Connections by Port (Cisco FWSM) 68
- Allowed Inbound Connections by Source Address (Cisco ASA) 44
- Allowed Inbound Connections by Source Address (Cisco FWSM) 66
- Allowed Outbound Connections by Destination Address (Cisco ASA) 44
- Allowed Outbound Connections by Destination Address (Cisco FWSM) 68
- Allowed Outbound Connections by Port (Cisco ASA) 47
- Allowed Outbound Connections by Port (Cisco FWSM) 67
- Allowed Outbound Connections by Source Address (Cisco ASA) 45
- Allowed Outbound Connections by Source Address (Cisco FWSM) 68
- Associated APs per Device 126
- Associated Devices in a Day - Event Based 125
- Associated Devices per AP 125
- Association - Disassociation Details 125
- Association - Disassociation per Day 125
- Authentication Errors (Cisco ASA) 44
- Bandwidth Usage by Protocol 43, 55, 66, 79
- Bandwidth Usage per Hour 45, 55, 66, 80
- 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 30, 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 79
- Cisco ASA Event Counts by Hour in Last 6 Hours 32, 45
- Cisco ASA Event Counts by Hour per Device 34, 47, 82
- Cisco ASA Inbound Connections per Day 46
- Cisco ASA Outbound Connections per Day 45
- Cisco Configuration Change Detail (Trend Based) 33, 57
- Cisco Configuration Changes (Event Based) 31, 43, 55, 66, 79, 89, 96, 101, 108, 114
- Cisco Configuration Changes by User (Event Based) 30, 46, 56, 67, 80, 89, 95, 101, 107, 114, 121
- Cisco Denied Connections by Destination Host - Template 78
- Cisco Denied Connections by Port - Template 79
- Cisco Denied Connections by Source Host - Template 81
- Cisco Device Critical Events 120
- Cisco Device Errors 121
- Cisco Device Interface Status Messages 120
- Cisco Device SNMP Authentication Failures 120
- Cisco Device SNMP Authentication Failures by User 120
- Cisco ESA Configuration Changes in the Last 6 Hours 30, 56
- Cisco ESA Configuration Changes per Day in the Last 7 Days 108
- Cisco ESA Delivery Connection Count by Hour 108
- Cisco ESA Injection Connection Count by Hour 108
- Cisco Event Count by Hour 29, 55
- Cisco Firewall Configuration Changes in the Last 6 Hours 31, 55
- Cisco Firewall Configuration Changes per Day in the Last 7 Days 78
- Cisco Firewall Event Counts by Hour 79
- Cisco FWSM Event Counts by Hour 31, 66
- Cisco FWSM Event Counts by Hour per Device 34, 69, 82
- Cisco FWSM Inbound Connections per Day 67
- Cisco FWSM Outbound Connections per Day 66
- Cisco IPS Configuration Changes in the Last 6 Hours 29, 55
- Cisco Login Detail (Trend Based) 31, 55
- Cisco Network Configuration Changes per Day in the Last 7 Days 120
- Cisco Network Equipment Configuration Change By Event 121
- Cisco Network Equipment Configuration Changes in the Last 6 Hours 30, 56
- Cisco Network Event Count by Hour 121
- Cisco Overall Allowed Inbound Connections by Destination Host 33, 81
- Cisco Overall Allowed Inbound Connections by Port 79
- Cisco Overall Allowed Inbound Connections by Source Host 31, 79
- Cisco Overall Allowed Outbound Connections by Destination Host 32, 80
- Cisco Overall Allowed Outbound Connections by Port 80
- Cisco Overall Allowed Outbound Connections by Source Host 32, 80
- Cisco Overall Denied Inbound Connections by Destination Host 30, 81
- Cisco Overall Denied Inbound Connections by Port 32, 44, 66, 79
- Cisco Overall Denied Inbound Connections by Source Host 30, 46, 67, 80
- Cisco Overall Denied Inbound Connections per Hour - Event Based 68
- Cisco Overall Denied Inbound Connections per Hour in the Previous Day 81
- Cisco Overall Denied Outbound Connections by Destination Host 33, 81
- Cisco Overall Denied Outbound Connections by Port 31, 46, 68, 81
- Cisco Overall Denied Outbound Connections by Source Host 30, 45, 67, 80
- Cisco Overall Denied Outbound Connections per Hour - Event Based 68
- Cisco Overall Inbound Connections per Day 32, 79
- Cisco Overall Outbound Connections per Day 29, 79
- Cisco Overall Outbound Connections per Hour in the

- Previous Day 79
- Cisco SNMP Access (Trend Based) 121
- Cisco SNMP Access On Certain Target (Trend Based) 121
- Cisco SNMP Authentication Failures by Device 120
- Cisco WSA Configuration Changes in the Last 6 Hours 30, 56
- Cisco WSA Configuration Changes per Day in the Last 7 Days 113
- Configuration Changes per Day in the Last 7 Days 33, 56
- Configuration Changes per Hour in the Previous Day 29, 55
- Connections Accepted by Address (Cisco ASA) 44
- Connections Denied by Address (Cisco ASA) 44
- Daily Alerts - Base 33, 57, 90, 95, 101
- Daily Associations - Disassociations (Base) 126
- Daily Configuration Changes - Base 31, 57, 81, 90, 108, 114, 121
- Daily Connection Setup Attempts - Base 33, 46, 56, 68, 81
- Daily Logins - Base 34, 57
- Daily Logins per Product 32
- Daily Message Transactions - Base 29, 107
- Daily SNMP Access - Base 121
- Daily Web Requests - Base 114
- Delivery Connections 107
- Denied Inbound Connections by Destination Address (Cisco ASA) 46
- Denied Inbound Connections by Destination Address (Cisco FWSM) 66
- Denied Inbound Connections by Port (Cisco ASA) 44
- Denied Inbound Connections by Port (Cisco FWSM) 66
- Denied Inbound Connections by Source Address (Cisco ASA) 46
- Denied Inbound Connections by Source Address (Cisco FWSM) 66
- Denied Outbound Connections by Destination Address (Cisco ASA) 45
- Denied Outbound Connections by Destination Address (Cisco FWSM) 67
- Denied Outbound Connections by Port (Cisco ASA) 45
- Denied Outbound Connections by Port (Cisco FWSM) 67
- Denied Outbound Connections by Source Address (Cisco ASA) 46
- Denied Outbound Connections by Source Address (Cisco FWSM) 68
- Detail Successful Requests 30, 114
- Detail Unsuccessful Requests 114
- Disassociated Devices 125
- Disassociated Devices per AP 125
- Failed Logins by Destination Address 29, 54
- Failed Logins by Source Address 29, 55
- Failed Logins by User 31, 57
- Injection Connections 107
- IOS IPS Event Counts by Hour 33, 101
- IOS IPS Event Counts by Hour per Device 29, 101
- IPS Configuration Changes per Day in the Last 7 Days 90
- IPS Sensor Event Counts by Hour 31, 95
- IPS Sensor Event Counts by Hour per Device 29, 95
- Logins per Day in the Last 7 Days 30, 56
- Logins per Hour in the Previous Day 55
- Message Transaction Details 32, 108
- Message Transactions per Day in the Previous Week 108
- Message Transactions per Hour in the Previous Day 108
- Request Errors 114
- Successful Login by Source Address 31, 55
- Successful Logins by Destination Address 29, 55
- Successful Logins by User 32, 56
- Top Accessed Sites 32, 113
- Top Accessed Sites with Most Traffic 32, 114
- Top Attackers and Reporting Devices in Cisco Alerts 89
- Top Attackers in Cisco Alerts 31, 89
- Top Attackers in Cisco Alerts (Trend Based) 89
- Top Attackers in Cisco IOS IPS Alerts 101
- Top Bandwidth Destination Hosts 46, 57, 68, 81
- Top Bandwidth Source Hosts 45, 56, 67, 80
- Top Cisco Alert Destinations Observed by IPS Sensor 95
- Top Cisco Alert Sources Observed by IPS Sensor 95
- Top Cisco Alerts 33, 90
- Top Cisco Alerts (Trend Based) 89
- Top Denied Sites 115
- Top Hosts with Most Web Traffic 30, 114
- Top Recipients with Most Bandwidth 29, 107
- Top Recipients with Most Transactions 33, 108
- Top Senders with Most Bandwidth 29, 107
- Top Senders with Most Transactions 32, 107
- Top Sites with Most Request Errors 32, 113
- Top Source Hosts Accessed Most Sites 31, 115
- Top Source Hosts with Most Denied Requests 114
- Top Source Hosts with Most Request Errors 113
- Top Systems Receiving Most Delivery Connections 107
- Top Systems Sending Most Injection Connections 107
- Top Systems Sending Most Rejected Injection Connections 107
- Top Target Weekly Cisco SNMP Access on Device 121
- Top Targets and Reporting Devices in Cisco Alerts 89
- Top Targets in Cisco Alerts 33, 89
- Top Targets in Cisco Alerts (Trend Based) 90
- Top Targets in Cisco IOS IPS Alerts 101
- Top Users with Most Failed Logins 33, 56
- Top Users with Successful Logins 33, 56
- Users by Connection Count (Cisco ASA) 45
- Web Requests per Day in the Previous Week 114
- Web Requests per Hour in the Previous Day 114
- query viewers
 - Associated Devices in a Day (Event Based) 123
 - Associations - Disassociations (Trend Based) 124
 - 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 19, 38
 - Cisco ASA Hourly Event per Device 21, 38, 73
 - Cisco Configuration Change Detail (Trend Based) 19, 49
 - Cisco ESA Configuration Changes in the Last 6

- Hours 21, 49
- Cisco Event Count by Hour 20, 49
- Cisco Firewall Configuration Changes in Last 6 Hours 19, 49
- Cisco Firewall Hourly Event Count 72
- Cisco FWSM Hourly Event Count 20, 60
- Cisco FWSM Hourly Event per Device 21, 61, 73
- Cisco IOS IPS Hourly Event Count 20, 98
- Cisco IOS IPS Hourly Event Count per Device 21, 98
- Cisco IPS Configuration Changes in the Last 6 Hours 19, 49
- Cisco Login Details in the Last 7 Days (Trend Based) 20, 49
- Cisco Network Equipment Configuration Changes in the Last 6 Hours 19, 49
- Cisco Network Event Count by Hour 117
- Cisco WSA Configuration Changes in the Last 6 Hours 20, 50
- Delivery Connections 104
- Delivery Connections by Hour 104
- Disassociated Devices in a Day (Event Based) 124
- Failed Logins by User in the Last 2 Hours 20, 49
- Injection Connections 104
- Injection Connections by Hour 104
- IPS Sensor Hourly Event Count 19, 92
- IPS Sensor Hourly Event Count per Device 19, 92
- Message Transaction Details 21, 104
- Successful Logins by User in the Last 2 Hours 20, 50
- Successful Requests 21, 111
- Top Access Points with Most Distinct Associated Devices 124
- Top Access Points with Most Distinct Disassociated Devices 124
- Top Accessed Sites 21, 111
- Top Accessed Sites with Most Traffic 21, 111
- Top Attackers in Cisco Alerts over the Last 2 Hours 85
- Top Attackers in Cisco IOS IPS Alerts 98
- 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) 37
- Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 61
- 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) 38
- Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 60
- 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) 38
- Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 61
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours 72
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) 37
- Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 60
- Top Hosts Accessed Most Sites 19, 111
- Top Hosts with Most Web Traffic 19, 111
- Top Ports across Allowed Inbound Connections in Last 2 Hours 71
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) 37
- Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 60
- Top Ports across Allowed Outbound Connections in Last 2 Hours 71
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) 37
- Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 60
- Top Ports across Denied Inbound Connections in Last 2 Hours 72
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco ASA) 38
- Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 60
- Top Ports across Denied Outbound Connections in Last 2 Hours 72
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco ASA) 38
- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 61
- Top Recipients in the Last 2 Hours 18, 104
- Top Recipients with Most Bandwidth in the Last 2 Hours 20, 104
- Top Senders in the Last 2 Hours 21, 105
- Top Senders with Most Bandwidth in the Last 2 Hours 20, 104
- Top Sites with Most Request Errors 20, 110
- Top Source Addresses with Most Failed Logins 21, 50
- 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) 38
- Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) 61
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours 72
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) 38
- Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) 60
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours 72
- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) 37

- Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) 61
 - 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) 37
 - Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) 61
 - Top Systems with Most Delivery Connections 104
 - Top Systems with Most Injection Connections 104
 - 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 20, 49
 - Unsuccessful Requests 111
- R**
- Rejected Injection Connection (Cisco ESA) filter 106
 - report templates
 - Chart and Table Landscape 47, 57, 69, 82, 90, 108, 115, 121, 126
 - Chart and Table Portrait 47, 57, 69, 82, 90, 109, 115, 126
 - Four Charts Landscape 34
 - Simple Chart Landscape 47, 57, 69, 82, 122
 - Simple Table Landscape 47, 57, 69, 82, 90, 96, 101, 108, 115, 121
 - Simple Table Portrait 121
 - Three Charts and Table Landscape 34
 - Three Charts Landscape 82, 108
 - Two Charts Landscape 115
 - Two Charts One Table Landscape 122
 - reports
 - Associated Wireless Devices to Cisco APs 124
 - Associations - Disassociations per Day (Cisco APs) 124
 - Bandwidth Usage by Hour (Cisco ASA) 40
 - Bandwidth Usage by Hour (Cisco Firewall) 75
 - Bandwidth Usage by Hour (Cisco FWSM) 63
 - Bandwidth Usage by Protocol 50
 - Bandwidth Usage by Protocol (Cisco ASA) 40
 - Bandwidth Usage by Protocol (Cisco Firewall) 74
 - Bandwidth Usage by Protocol (Cisco FWSM) 63
 - Bandwidth Usage per Hour 51
 - Cisco Access Points and Associated Wireless Devices 124
 - Cisco Alerts per Day 86
 - Cisco Alerts per Hour in the Previous Day 85
 - Cisco Configuration Changes by Type 51
 - Cisco Configuration Changes by Type (Cisco ASA) 39
 - Cisco Configuration Changes by Type (Cisco FWSM) 63
 - Cisco Configuration Changes by User 51
 - Cisco Configuration Changes by User (Cisco ASA) 39
 - Cisco Configuration Changes by User (Cisco FWSM) 63
 - Cisco Configuration Changes per Day 51
 - Cisco Configuration Changes per Hour in the Previous Day 50
 - Cisco Device Critical Events 117
 - Cisco Device Errors 118
 - Cisco Device Interface Status Messages 118
 - Cisco ESA Configuration Changes by Type 105
 - Cisco ESA Configuration Changes by User 105
 - Cisco ESA Configuration Changes per Day 105
 - Cisco Firewall Configuration Changes by Device 75
 - 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 22
 - Cisco Firewall Overview - Top Denied Systems 22
 - Cisco Firewall Overview - Trend and Port 22
 - Cisco Intrusion Prevention System Overview 22
 - 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 117
 - Cisco Network Equipment Configuration Changes by Type 118
 - Cisco Network Equipment Configuration Changes by User 117
 - Cisco Network Equipment Configuration Changes per Day 117
 - Cisco Network SNMP Authentication Failures 117
 - 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 73
 - Cisco Overall Allowed Outbound Connections by Source Host 73
 - Cisco Overall Denied Inbound Connections by Destination Host 75
 - 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 74
 - 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 74
 - Cisco Overall Denied Outbound Connections per Hour in the Previous Day 75
 - Cisco Overall Inbound Connection Setup Attempts per Day 73
 - Cisco Overall Outbound Connection Setup Attempts per Day 75
 - Cisco WSA Configuration Changes by Type 111
 - Cisco WSA Configuration Changes by User 112
 - Cisco WSA Configuration Changes per Day 111

- Connection Overview (Cisco ESA) 105
 - Denied Inbound Connections by Address (Cisco ASA) 39
 - Denied Inbound Connections by Address (Cisco FWSM) 63
 - Denied Inbound Connections by Port (Cisco ASA) 40
 - Denied Inbound Connections by Port (Cisco FWSM) 62
 - Denied Inbound Connections per Hour (Cisco FWSM) 62
 - Denied Outbound Connections by Address (Cisco ASA) 41
 - Denied Outbound Connections by Address (Cisco FWSM) 62
 - Denied Outbound Connections by Port (Cisco ASA) 39
 - Denied Outbound Connections by Port (Cisco FWSM) 62
 - Denied Outbound Connections per Hour (Cisco FWSM) 63
 - Failed Logins by Destination Address 51
 - Failed Logins by Source Address 51
 - Failed Logins by User 50
 - Inbound Connection Setup Attempts per Day (Cisco ASA) 40
 - Inbound Connection Setup Attempts per Day (Cisco FWSM) 62
 - Logins per Day 50
 - Logins per Hour in the Previous Day
 - Message Transaction per Hour in the Previous Day (Cisco ESA) 105
 - Message Transactions per Day (Cisco ESA) 105
 - Outbound Connection Setup Attempts per Day (Cisco ASA) 39
 - Outbound Connection Setup Attempts per Day (Cisco FWSM) 63
 - Overview of Cisco Configuration Changes 21
 - Overview of Logins Reported by Cisco Devices - Systems 22
 - Overview of Logins Reported by Cisco Devices - Trend and Users 22
 - Request Error Statistics (Cisco WSA) 112
 - Successful Logins by Destination Address 51
 - Successful Logins by Source Address 51
 - Successful Logins by User 50
 - Summary of Allowed Traffic by Specific Cisco Firewall 74
 - Summary of Denied Traffic by Specific Cisco Firewall 74
 - Top Accessed Sites (Cisco WSA) 111
 - Top Accessed Sites with Most Traffic (Cisco WSA) 111
 - Top Attackers in Cisco Alerts 86
 - Top Attackers in Cisco Alerts over a Month 86
 - Top Bandwidth Destination Hosts 51
 - Top Bandwidth Destination Hosts (Cisco Firewall) 76
 - Top Bandwidth Destination Hosts (Cisco FWSM) 62
 - Top Bandwidth Source Hosts 50
 - Top Bandwidth Source Hosts (Cisco ASA) 41
 - Top Bandwidth Source Hosts (Cisco Firewall) 73
 - Top Bandwidth Source Hosts (Cisco FWSM) 62
 - Top Bandwidth Target Hosts (Cisco ASA) 40
 - Top Cisco Alerts 85
 - Top Cisco Alerts in a Month 86
 - Top Denied Sites (Cisco WSA) 112
 - Top Hosts Accessed Most (Distinct) Sites (Cisco WSA) 112
 - Top Hosts with Most Web Traffic (Cisco WSA) 111
 - Top Recipients with Most Bandwidth Consumption (Cisco ESA) 105
 - Top Recipients with Most Transactions (Cisco ESA) 105
 - Top Senders with Most Bandwidth Consumption (Cisco ESA) 105
 - Top Senders with Most Transactions (Cisco ESA) 105
 - Top Sites with Most Request Errors (Cisco WSA) 112
 - Top Sources with Most Denied Requests (Cisco WSA) 112
 - Top Sources with Most Request Errors (Cisco WSA) 111
 - Top Target Cisco SNMP Access in a Week 118
 - Top Targets in Cisco Alerts 86
 - Top Targets in Cisco Alerts over a Month 85
 - Trend of Daily Cisco SNMP Access 117
 - Trend of Daily SNMP Access on Specific Cisco Target 118
 - VPN Authentication Errors (Cisco ASA) 40
 - VPN Connection Counts by User (Cisco ASA) 39
 - VPN Connections Accepted by Address (Cisco ASA) 39
 - VPN Connections Denied by Address (Cisco ASA) 40
 - Web Requests per Day in the Previous Week (Cisco WSA) 112
 - Web Requests per Hour in the Previous Day (Cisco WSA) 112
 - Request Error Statistics (Cisco WSA) report 112
 - Request Errors query 114
- ## S
- Sender and Recipient Overview dashboard 18, 103
 - shared libraries 6
 - Simple Chart Landscape report template 47, 57, 69, 82, 122
 - Simple Table Landscape report template 47, 57, 69, 82, 90, 96, 101, 108, 115, 121
 - Simple Table Portrait report template 121
 - SNMP Authentication Failed filter 119
 - SNMP Events filter 119
 - 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 Configuration Changes (Cisco ESA) filter 106
 - Successful Configuration Changes filter 27, 42, 64, 77, 88, 94, 100, 106, 113, 119
 - Successful Login by Source Address query 31, 55
 - Successful Logins by Destination Address query 29, 55
 - Successful Logins by Destination Address report 51
 - Successful Logins by Source Address report 51
 - Successful Logins by User in the Last 2 Hours query viewer 20, 50
 - Successful Logins by User query 32, 56
 - Successful Logins by User report 50
 - Successful Logins filter 25, 52

Successful Requests query viewer 21, 111
 Successful VPN Connection Events (Cisco ASA) filter 43
 Successful Web Transactions filter 27, 112
 Successful WSA Configuration Changes filter 113
 Summary of Allowed Traffic by Specific Cisco Firewall report 74
 Summary of Denied Traffic by Specific Cisco Firewall report 74

T

Target Host or Address Present filter 25, 41, 52, 64, 77, 87, 94, 100, 106, 119
 Target User Present filter 26, 42, 53, 119
 Three Charts and Table Landscape report template 34
 Three Charts Landscape report template 82, 108
 Top Access Points with Most Association Events data monitor 124
 Top Access Points with Most Disassociation Events data monitor 124
 Top Access Points with Most Distinct Associated Devices query viewer 124
 Top Access Points with Most Distinct Disassociated Devices query viewer 124
 Top Accessed Sites (Cisco WSA) report 111
 Top Accessed Sites query 32, 113
 Top Accessed Sites query viewer 21, 111
 Top Accessed Sites with Most Traffic (Cisco WSA) report 111
 Top Accessed Sites with Most Traffic query 32, 114
 Top Accessed Sites with Most Traffic query viewer 21, 111
 Top Activities across Cisco Firewall Devices data monitor 76
 Top Application Protocols data monitor 23, 52
 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 31, 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 Bandwidth Destination Hosts (Cisco Firewall) report 76
 Top Bandwidth Destination Hosts (Cisco FWSM) report 62
 Top Bandwidth Destination Hosts query 46, 57, 68, 81
 Top Bandwidth Destination Hosts report 51
 Top Bandwidth Source Hosts (Cisco ASA) report 41
 Top Bandwidth Source Hosts (Cisco Firewall) report 73
 Top Bandwidth Source Hosts (Cisco FWSM) report 62
 Top Bandwidth Source Hosts query 45, 56, 67, 80
 Top Bandwidth Source Hosts report 50
 Top Bandwidth Target Hosts (Cisco ASA) report 40
 Top Categories data monitor 24, 52
 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 33, 90
 Top Cisco Alerts report 85
 Top Denied Sites (Cisco WSA) report 112
 Top Denied Sites query 115
 Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 37
 Top Destination Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 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 38
 Top Destination Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 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 38
 Top Destination Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 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 37
 Top Destination Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 Top Destination Hosts across Denied Outbound Connections in Last 2 Hours query viewer 72
 Top Hosts Accessed Most (Distinct) Sites (Cisco WSA) report 112
 Top Hosts Accessed Most Sites query viewer 19, 111
 Top Hosts with Most Web Traffic (Cisco WSA) report 111
 Top Hosts with Most Web Traffic query 30, 114
 Top Hosts with Most Web Traffic query viewer 19, 111
 Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 37
 Top Ports across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 Top Ports across Allowed Inbound Connections in Last 2 Hours query viewer 71
 Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 37
 Top Ports across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 Top Ports across Allowed Outbound Connections in Last 2 Hours query viewer 71
 Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 38
 Top Ports across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 Top Ports across Denied Inbound Connections in Last 2 Hours query viewer 72
 Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 38

- Top Ports across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 - Top Ports across Denied Outbound Connections in Last 2 Hours query viewer 72
 - Top Recipients in the Last 2 Hours query viewer 18, 104
 - Top Recipients with Most Bandwidth Consumption (Cisco ESA) report 105
 - Top Recipients with Most Bandwidth in the Last 2 Hours query viewer 20, 104
 - Top Recipients with Most Bandwidth query 29, 107
 - Top Recipients with Most Transactions (Cisco ESA) report 105
 - Top Recipients with Most Transactions query 33, 108
 - Top Senders in the Last 2 Hours query viewer 21, 105
 - Top Senders with Most Bandwidth Consumption (Cisco ESA) report 105
 - Top Senders with Most Bandwidth in the Last 2 Hours query viewer 20, 104
 - Top Senders with Most Bandwidth query 29, 107
 - Top Senders with Most Transactions (Cisco ESA) report 105
 - Top Senders with Most Transactions query 32, 107
 - Top Sites with Most Request Errors (Cisco WSA) report 112
 - Top Sites with Most Request Errors query 32, 113
 - Top Sites with Most Request Errors query viewer 20, 110
 - Top Source Addresses with Most Failed Logins query viewer 21, 50
 - Top Source Hosts Accessed Most Sites query 31, 115
 - Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 38
 - Top Source Hosts across Allowed Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 - 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 38
 - Top Source Hosts across Allowed Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 60
 - Top Source Hosts across Allowed Outbound Connections in Last 2 Hours query viewer 72
 - Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco ASA) query viewer 37
 - Top Source Hosts across Denied Inbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 - Top Source Hosts across Denied Inbound Connections in Last 2 Hours query viewer 72
 - Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco ASA) query viewer 37
 - Top Source Hosts across Denied Outbound Connections in Last 2 Hours (Cisco FWSM) query viewer 61
 - Top Source Hosts across Denied Outbound Connections in Last 2 Hours query viewer 72
 - Top Source Hosts with Most Denied Requests query 114
 - Top Source Hosts with Most Request Errors query 113
 - Top Sources with Most Denied Requests (Cisco WSA) report 112
 - Top Sources with Most Request Errors (Cisco WSA) report 111
 - Top Systems Receiving Most Delivery Connections query 107
 - Top Systems Sending Most Injection Connections query 107
 - Top Systems Sending Most Rejected Injection Connections query 107
 - Top Systems with Most Delivery Connections query viewer 104
 - Top Systems with Most Injection Connections query viewer 104
 - Top Systems with Most Rejected Injection Connections data monitor 106
 - Top Target Cisco SNMP Access in a Week report 118
 - Top Target Weekly Cisco SNMP Access on Device query 121
 - 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 33, 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 Transport Protocols data monitor 23, 52
 - Top Users with Most Failed Logins query 33, 56
 - Top Users with Most Failed Logins query viewer 20, 49
 - Top Users with Successful Logins query 33, 56
 - Transaction Connections Overview dashboard 103
 - Trend of Daily Cisco SNMP Access report 117
 - Trend of Daily SNMP Access on Specific Cisco Target report 118
 - trends
 - Daily Alerts 34, 58, 90, 96, 102
 - Daily Associations - Disassociations 126
 - Daily Configuration Changes 34, 57, 82, 90, 109, 115, 122
 - Daily Connection Setup Attempts 34, 47, 57, 69, 82
 - Daily Email Transactions 34, 109
 - Daily Logins 34, 58
 - Daily SNMP Access 122
 - Daily Web Requests 115
 - Two Charts Landscape report template 115
 - Two Charts One Table Landscape report template 122
- ## U
- Unsuccessful Logins filter 27, 53
 - Unsuccessful Requests query viewer 111
 - Unsuccessful Web Server Requests filter 28, 113
 - use cases
 - Cisco Adaptive Security Appliance (ASA) 35
 - Cisco Cross-Device 35
 - Cisco Firewall Services Module (FWSM) 35
 - Cisco Generic Firewall 35
 - Cisco Generic Intrusion Prevention System (IPS) 35
 - Cisco Intrusion Prevention System (IPS) Sensor 35
 - Cisco IOS Intrusion Prevention System (IOS IPS) 34
 - Cisco Ironport Email Security Appliance (ESA) 34
 - Cisco Ironport Web Security Appliance (WSA) 35
 - Cisco Network 35
 - Cisco Wireless 35
 - Users by Connection Count (Cisco ASA) query 45
- ## V
- VPN Authentication Errors (Cisco ASA) filter 43
 - VPN Authentication Errors (Cisco ASA) report 40
 - VPN Connection Counts by User (Cisco ASA) report 39

VPN Connections Accepted by Address (Cisco ASA) report 39

VPN Connections Denied by Address (Cisco ASA) report 40

VPN Events filter 42

W

Web Requests filter 25, 113

Web Requests per Day in the Previous Week (Cisco WSA) report 112

Web Requests per Day in the Previous Week query 114

Web Requests per Hour in the Previous Day (Cisco WSA) report 112

Web Requests per Hour in the Previous Day query 114

Web Transactions dashboard 18, 110

Windows Events with a Non-Machine User filter 27, 53

