



# HP ArcSight ESM

Software Version: 6.8c

## Cisco Monitoring Standard Content Guide

November 17, 2014

## Legal Notices

### Warranty

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.

The information contained herein is subject to change without notice.

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

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

This document is confidential.

### Restricted Rights Legend

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.

### Copyright Notice

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

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

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

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the HP ArcSight Technical Support Page: <a href="https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list">https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.hp.com">https://softwaresupport.hp.com</a>
<b>Protect 724 Community</b>	<a href="https://protect724.hp.com">https://protect724.hp.com</a>

# Contents

Chapter 1: Cisco Monitoring Overview .....	5
What is Standard Content? .....	5
Standard Content Packages .....	7
Cisco Monitoring Content .....	8
Chapter 2: Installation and Configuration .....	9
Installing the Cisco Monitoring Package .....	9
Modeling the Network .....	10
Categorizing Assets .....	11
Assigning User Permissions .....	11
Ensuring Filters Capture Relevant Events .....	12
Scheduling Reports .....	13
Configuring Trends .....	13
Viewing a Use Case Resource .....	14
Chapter 3: Cisco Monitoring Use Cases .....	15
Cisco Overview .....	17
Configuration .....	17
Cisco Overview Resources .....	17
Cisco Adaptive Security Appliance (ASA) .....	46
Configuration .....	46
Cisco Adaptive Security Appliance (ASA) Resources .....	46
Cisco Cross-Device .....	65
Devices .....	65
Configuration .....	65
Cisco Cross-Device Resources .....	66
Cisco Firewall Services Module (FWSM) .....	82
Configuration .....	82
Cisco Firewall Services Module (FWSM) Resources .....	82
Cisco Generic Firewall .....	99
Devices .....	99
Configuration .....	99

Cisco Generic Firewall Resources .....	100
Cisco Generic Intrusion Prevention System (IPS) .....	120
Devices .....	120
Configuration .....	120
Cisco Generic Intrusion Prevention System (IPS) Resources .....	121
Cisco Intrusion Prevention System (IPS) Sensor .....	132
Configuration .....	132
Cisco Intrusion Prevention System (IPS) Sensor Resources .....	132
Cisco IOS Intrusion Prevention System (IOS IPS) .....	141
Configuration .....	141
Cisco IOS Intrusion Prevention System (IOS IPS) Resources .....	141
Cisco Ironport Email Security Appliance (ESA) .....	149
Configuration .....	149
Cisco Ironport Email Security Appliance (ESA) Resources .....	149
Cisco Ironport Web Security Appliance (WSA) .....	158
Configuration .....	158
Cisco Ironport Web Security Appliance (WSA) Resources .....	158
Cisco Network .....	166
Configuration .....	166
Cisco Network Resources .....	166
Cisco Wireless .....	179
Configuration .....	179
Cisco Wireless Resources .....	179
Send Documentation Feedback .....	184

# Chapter 1: Cisco Monitoring Overview

This chapter discusses the following topics.

What is Standard Content? .....	5
Standard Content Packages .....	7
Cisco Monitoring Content .....	8

## 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 the CORR-Engine (Correlation Optimized Retention and Retrieval) and provides information on the health of the CORR-Engine.

**Note:** The ArcSight Admin DB CORR content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- ArcSight Content Management is an optional package that shows information about content package synchronization with the ArcSight Content Management feature. The information

includes a history of content packages synchronized from a primary source to multiple destinations, and any common issues or errors encountered. You can install this package during ArcSight Manager installation or from the ArcSight Console any time after installation.

- ArcSight ESM HA Monitoring is an optional package that lets you monitor systems that use the ESM High Availability Module. You can install this package during ArcSight Manager 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 Search Filters content package is installed automatically when you perform a new ArcSight Manager installation. However package installation is different during upgrade. If you are upgrading your system from a previous version, check to see if the package is installed after upgrade. If the package is not installed, install it from the ArcSight Console.

- **ArcSight System** content is installed automatically with the ArcSight Manager and consists of three packages: ArcSight Core, ArcSight Groups, and ArcSight Networks. ArcSight Core and ArcSight Groups contain 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. The ArcSight Networks package contains the zones that were in the ArcSight Core package in previous releases, in addition to local and global network resources.
- **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 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

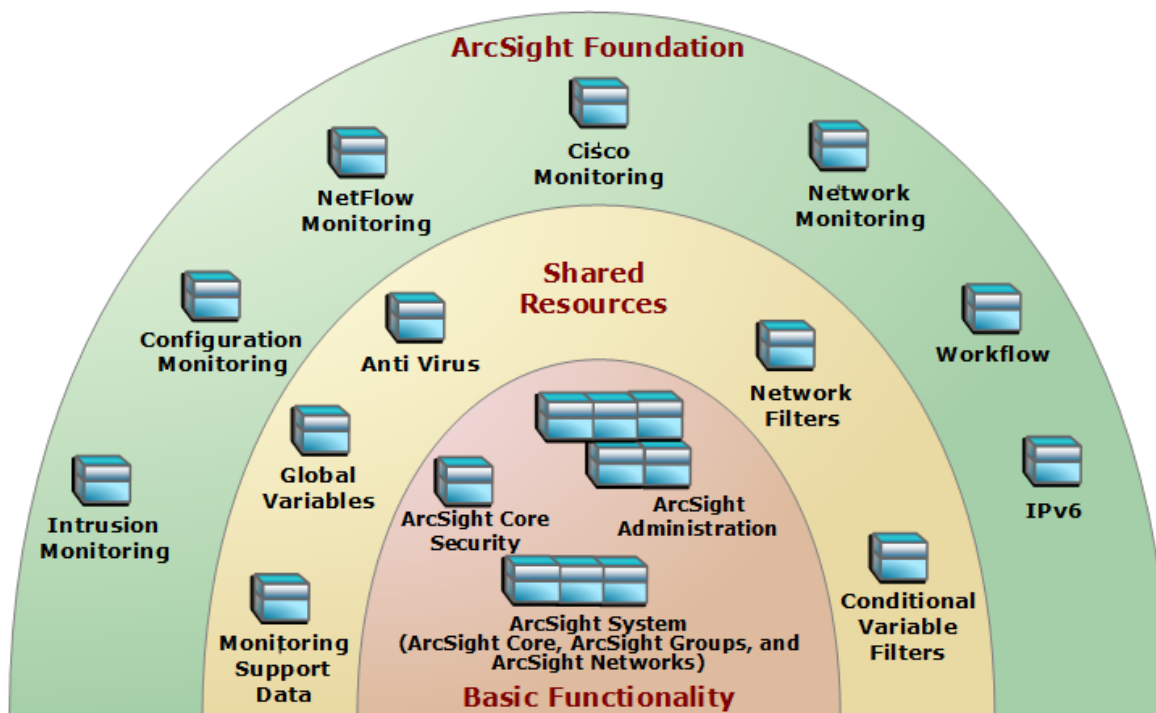
commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.

- 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 install-time options. The following graphic outlines the packages.



The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic 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. 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 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.

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.hp.com) (<https://protect724.hp.com>).



## Chapter 2: Installation and Configuration

This chapter discusses the following topics:

Installing the Cisco Monitoring Package .....	9
Modeling the Network .....	10
Categorizing Assets .....	11
Assigning User Permissions .....	11
Ensuring Filters Capture Relevant Events .....	12
Scheduling Reports .....	13
Configuring Trends .....	13
Viewing a Use Case Resource .....	14

### Installing the Cisco Monitoring Package

The Cisco Monitoring Foundation package is one of the standard content packages presented as install-time options. If you selected all 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 ArcSight Manager 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.

#### 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**.
4. 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**.
5. 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.

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

**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.

## Modeling the Network

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates 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 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 to activate standard content that uses these categories.

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><b>Note:</b> 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	Same as /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 and for all the resource types listed above, change the user permissions.
2. In the Navigator panel, go to the resource type and navigate to ArcSight Foundation/Cisco Monitoring.
3. Right-click the **Cisco Monitoring** group and select **Edit Access Control** to open the ACL editor in the Inspect/Edit panel.
4. 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 and apply the change.
- c. Right-click the filter and choose **Create Channel with Filter** 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, reports are not scheduled to run automatically.

Evaluate the reports that come with the content, 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**.

**Note:** 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 *ArcSight Console User's Guide*.

## Viewing a Use Case Resource

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

**To view the resources associated with a Cisco Monitoring use case resource:**

1. In the Navigator panel, select the **Use Cases** tab.
2. Open the ArcSight Foundation/Cisco Monitoring group.
3. Right-click a Cisco Monitoring use case resource and select the **Open Use Case** option, or double-click a use case resource.

The resources that make up a use case resource are displayed in the Viewer. The Cisco Monitoring use cases are listed in ["Cisco Monitoring Use Cases" on page 15](#).

## 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.

### Cisco Use Cases

Use Case	Description
<a href="#">"Cisco Overview" on page 17</a>	"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. "
<a href="#">"Cisco Adaptive Security Appliance (ASA)" on page 46</a>	"The Cisco Adaptive Security Appliance (ASA) use case provides firewall information based on events reported by Cisco Adaptive Security Appliances."
<a href="#">"Cisco Cross-Device" on page 65</a>	"The Cisco Cross-Device use case provides information about logins, configuration changes, and bandwidth consumption across all Cisco devices in your environment."
<a href="#">"Cisco Firewall Services Module (FWSM)" on page 82</a>	"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."
<a href="#">"Cisco Generic Firewall" on page 99</a>	"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."
<a href="#">"Cisco Generic Intrusion Prevention System (IPS)" on page 120</a>	"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. " on page 120

### Cisco Use Cases, continued

Use Case	Description
"Cisco Intrusion Prevention System (IPS) Sensor" on page 132	"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)." on page 132
"Cisco IOS Intrusion Prevention System (IOS IPS)" on page 141	"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 149	"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 158	"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 166	"The Cisco Network use case identifies and provides information based on events reported by Cisco network equipment."
"Cisco Wireless" on page 179	"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"](#)
- ["Cisco Generic Intrusion Prevention System \(IPS\)"](#)

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

Report	Required 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 Connections Setup Attempts
Cisco Intrusion Prevention System Overview	Daily Alerts

## Cisco Overview Resources

The following table lists all the resources in the Cisco Overview use case.

### Resources that Support the Cisco Overview Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/

**Resources that Support the Cisco Overview Use Case, continued**

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

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Overview Use Case, continued**

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)/

**Resources that Support the Cisco Overview Use Case, continued**

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

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Cisco WSA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport WSA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco Event Count by Hour	This query viewer shows the total number of Cisco events per hour within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Cisco ESA Configuration Changes in the Last 6 Hours	This query viewer shows all configuration changes recorded by Cisco Ironport ESA devices within the last six hours. It also provides drilldowns to all changes in a particular hour.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Successful Requests	This query viewer shows all successful requests within the last two hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco IOS IPS Hourly Event Count per Device	This query viewer shows the count of IOS IPS events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Cisco FWSM Hourly Event per Device	This query viewer shows the count of FWSM events per device within the last six hours.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
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)/

**Resources that Support the Cisco Overview Use Case, continued**

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



**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/
<b>Library Resources</b>			

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Cisco Top IOS IPS Devices	This data monitor shows the top 20 event-generating Cisco IPS Sensor devices within the last hour.	Data Monitor	ArcSight 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)/

**Resources that Support the Cisco Overview Use Case, continued**

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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Overview Use Case, continued**

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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Email Message Transaction (Cisco ESA)	This filter selects events from Cisco Ironport Email Security Appliance (ESA) systems, where an (successful or dropped) email transaction is recorded.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco Ironport WSA Systems	This filter selects events from Cisco Ironport Web Security Appliance (WSA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Application Protocol Present	This filter selects all Cisco events where the application protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Ironport ESA Systems	This filter identifies events from Cisco Ironport Email Security Appliance (ESA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Successful Web Transactions	This filter selects successful web server requests.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Attacker and Target Address Present	This filter identifies events in which both the attacker and target address fields are populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/



**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Windows Events with a Non-Machine User	This filter identifies Microsoft Windows events that have a non-machine/system user in either the attacker or the target fields.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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/

**Resources that Support the Cisco Overview Use Case, continued**

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

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco ASA Systems	This filter selects all events from Cisco Adaptive Security Appliance (ASA) products.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco FWSM Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco FWSM device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Cisco 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/
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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
Top Hosts with Most Web Traffic	This query returns information about the top hosts with most web traffic over the past day.	Query	ArcSight 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)/
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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)/
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/



**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Overview Use Case, continued**

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)/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Overview Use Case, continued**

Resource	Description	Type	URI
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 **Outbound Connection Setup Attempts per Day (Cisco ASA)** and the **Inbound Connection Setup Attempts per Day (Cisco ASA)** reports require the **Daily Connection Setup Attempts** trend to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).
- Verify that the **Cisco ASA Systems** filter includes all the Cisco ASA systems present in your network. If necessary, the ArcSightAdministrator can update the filter to include missing devices.

## Cisco Adaptive Security Appliance (ASA) Resources

The following table lists all the resources in the Cisco Adaptive Security Appliance (ASA) use case.

### Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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



**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Denied Outbound Connections by Port (Cisco ASA)	This report shows a summary of the denied outbound traffic blocked by Cisco ASA devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
VPN Connections Accepted by Address (Cisco ASA)	This report shows successful VPN connection data to a Cisco ASA system. A chart summarizes the top VPN device addresses with successful connections. A table shows details of the successful connections.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Outbound Connection Setup Attempts per Day (Cisco ASA)	This report shows a summary of the outbound connection setup attempts reported by Cisco ASA devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco Configuration Changes by Type (Cisco ASA)	This report displays all successful configuration changes to Cisco ASA devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Top Bandwidth Target Hosts (Cisco ASA)	This report shows a summary of the bandwidth usage, recorded by a Cisco ASA device, grouped by the top target hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Denied Inbound Connections by Port (Cisco ASA)	This report shows a summary of the denied inbound traffic blocked by Cisco ASA devices, grouped by destination port. A chart shows the top ten ports with the highest denied connections count. A report lists all the ports sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Bandwidth Usage by Protocol (Cisco ASA)	This report shows a summary of the bandwidth usage recorded by a Cisco ASA device, grouped by application protocol. A chart shows the top ten protocols with the highest bandwidth usage. A table lists all the protocols sorted by bandwidth usage. This report shows you the applications that are consuming the most bandwidth.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Bandwidth Usage by Hour (Cisco ASA)	This report shows a summary of the bandwidth usage per hour, recorded by a Cisco ASA device. A chart shows the average bandwidth usage per hour for the past 24 hours (by default). Use this report to find high bandwidth usage hours during the day.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
VPN Connections Denied by Address (Cisco ASA)	This report shows denied VPN connection data from a Cisco ASA system. A chart summarizes the top VPN device addresses with denied connections. A table shows details of the denied connections.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/VPN/
Denied Outbound Connections by Address (Cisco ASA)	This report shows a summary of the denied outbound traffic, blocked by Cisco ASA devices, grouped by local address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
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)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
<b>Library Resources</b>			
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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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/



**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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/
Application Protocol is NULL	This filter is used by a dependent variable to check whether the event target has an application protocol associated with it.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Firewall Access Events	This filter selects events where a firewall has detected traffic attempting to pass through it. This filter does not look for the outcome of the attempt.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Firewall Deny	This filter selects events where a firewall denied passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Internal Targets	This filter looks for events targeting systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco ASA Successful Configuration Changes	This filter selects successful configuration changes recorded by a Cisco ASA device or module.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Cisco ASA IPS Alert Events	This filter selects IPS alert events from Cisco ASA Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Adaptive Security Appliance (ASA)/
Firewall Accepts	This filter selects all events where a firewall granted passage to traffic.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Cisco Firewall Systems	This filter selects events from all Cisco firewall devices/modules in the network. Modify this filter to include all firewall products in the network.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Internal Attackers	This filter looks for events coming from systems inside the company network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events 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/
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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
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/
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)/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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 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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

Resource	Description	Type	URI
Denied Inbound Connections by Source Address (Cisco ASA)	This query returns the count of denied inbound connections by Cisco ASA devices, grouped by source address (attacker zone, address, and hostname).	Query	ArcSight 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/

**Resources that Support the Cisco Adaptive Security Appliance (ASA) Use Case, continued**

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)"
- "Cisco Generic Firewall"
- "Cisco Ironport Email Security Appliance (ESA)"
- "Cisco Ironport Web Security Appliance (WSA)"
- "Cisco Network"

## Cisco Cross-Device Resources

The following table lists all the resources in the Cisco Cross-Device use case.

### Resources that Support the Cisco Cross-Device Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

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)/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/
<b>Library Resources</b>			
Business Impact Analysis	This is a site asset category.	Asset Category	Site Asset Categories
Top Transport Protocols	This data monitor shows the top transport protocols recorded by Cisco devices within the last hour.	Data Monitor	ArcSight 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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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



**Resources that Support the Cisco Cross-Device Use Case, continued**

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 IOS IPS Systems	This filter selects events from Cisco IOS IPS systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IOS Intrusion Prevention System (IOS IPS)/
Successful Logins	This filter identifies successful logins by both administrative and non-administrative users.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Attacker Host or Address Present	This filter identifies events that have either the Attacker Host Name or Attacker Address event fields populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco IPS-Categorized Events	This filter passes all Cisco Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)-related events. Note that not all events from an IPS device or module are related to IPS functionality or categorized as such.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
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)/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
Cisco Ironport WSA Systems	This filter selects events from Cisco Ironport Web Security Appliance (WSA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Target User Present	This filter checks whether the Target User Name field is populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Application Protocol Present	This filter selects all Cisco events where the application protocol is present.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Cross-Device/
Attacker or Target User Present	This filter identifies events that have either the Attacker User Name or Target User Name event field populated.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco Ironport ESA Systems	This filter identifies events from Cisco Ironport Email Security Appliance (ESA) systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco Ironport Email Security Appliance (ESA)/
Cisco IPS Alert Events	This filter selects alert events from Cisco Intrusion Detection/Prevention Systems.	Filter	ArcSight Foundation/Cisco Monitoring/Functionality/Intrusion Prevention System/
Windows Events with a Non-Machine User	This 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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

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 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/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This query returns the count of TotalBytes (Bytes In + Bytes Out) by protocol. The query looks for events 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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Cross-Device Use Case, continued**

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



**Resources that Support the Cisco Cross-Device Use Case, continued**

Resource	Description	Type	URI
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/
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 **Outbound Connection Setup Attempts per Day (Cisco FWSM)** and the **Inbound Connection Setup Attempts per Day (Cisco FWSM)** reports require the **Daily Connection Setup Attempts** trend to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).
- 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.

### Cisco Firewall Services Module (FWSM) Resources

The following table lists all the resources in the Cisco Firewall Services Module (FWSM) use case.

#### Resources that Support the Cisco Firewall Services Module (FWSM) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
Cisco FWSM Denied Connections Overview	This dashboard shows an overview of all the denied connection events originating from Cisco FWSM modules.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Cisco FWSM Event Overview	This dashboard shows an overview of all the events originating from Cisco FWSM devices. The dashboard displays the top FWSM devices with the most events, the event moving average per device, and the recent configuration modification events.	Dashboard	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
Top Bandwidth Destination Hosts (Cisco FWSM)	This report shows a summary of the bandwidth usage, recorded by a Cisco FWSM module, grouped by the top target (destination) hosts. A chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Outbound Connection Setup Attempts per Day (Cisco FWSM)	This report shows a summary of the outbound connection setup attempts reported by Cisco FWSM devices per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
Cisco Configuration Changes by Type (Cisco FWSM)	This report displays all successful configuration changes to Cisco FWSM modules. Events are grouped by type and then user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco Firewall Services Module (FWSM)/
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)/



**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
<b>Library Resources</b>			
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/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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/
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/
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

Resource	Description	Type	URI
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)/
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/



**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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/
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/
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)/

**Resources that Support the Cisco Firewall Services Module (FWSM) Use Case, continued**

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
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.

Report	Required 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	Daily Connection Setup Attempts
Cisco Overall Inbound Connection Setup Attempts per Day	Daily Connection Setup Attempts
Cisco Overall Denied Outbound Connections per Hour in the Previous Day	Daily Connection Setup Attempts

- 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.

## Cisco Generic Firewall Resources

The following table lists all the resources in the Cisco Generic Firewall use case.

### Resources that Support the Cisco Generic Firewall Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/



#### Resources that Support the Cisco Generic Firewall Use Case, continued

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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
Cisco Overall Denied Inbound Connections by Destination Host	This report shows a summary of the denied inbound traffic, blocked by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes by Device	This report displays all successful configuration changes to Cisco firewall devices. Events are grouped by reporting device, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Firewall Configuration Changes per Day	This report shows a summary of the Cisco firewall configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/
Cisco Overall Denied Outbound Connections by Destination Host	This report shows a summary of the denied outbound traffic, blocked by Cisco firewall devices, grouped by destination address. A chart shows the top ten addresses with the highest denied connections count. A report lists all the addresses sorted by connection count.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Firewall/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/
<b>Library Resources</b>			
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/

#### Resources that Support the Cisco Generic Firewall Use Case, continued

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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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

### Resources that Support the Cisco Generic Firewall Use Case, continued

Resource	Description	Type	URI
Outbound Events	This filter looks for events coming from inside the company network targeting the public network.	Filter	ArcSight Foundation/Cisco Monitoring/General Filters/
Cisco 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/



**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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/
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/
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Firewall Use Case, continued**

Resource	Description	Type	URI
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/
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

**Resources that Support the Cisco Generic Firewall Use Case, continued**

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 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 132](#)
- ["Cisco IOS Intrusion Prevention System \(IOS IPS\)" on page 141](#)

## 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 ["Cisco Intrusion Prevention System \(IPS\) Sensor"](#) and ["Cisco IOS Intrusion Prevention System \(IOS IPS\)"](#) use cases.
- To generate meaningful data, the following reports require trends to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).

Report	Required Trend
Cisco IPS Configuration Changes per Day	Daily Configuration Changes
Top Cisco Alerts in a Month	Daily Alerts
Cisco Alerts per Hour in the Previous Day	Daily Alerts



Report	Required Trend
Top Targets in Cisco Alerts over a Month	Daily Alerts
Top Attackers in Cisco Alerts over a Month	Daily Alerts
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**

## Cisco Generic Intrusion Prevention System (IPS) Resources

The following table lists all the resources in the Cisco Generic Intrusion Prevention System (IPS) use case.

### Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/
<b>Library Resources</b>			
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/
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

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/
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/
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/



**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

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/
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/

**Resources that Support the Cisco Generic Intrusion Prevention System (IPS) Use Case, continued**

Resource	Description	Type	URI
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 120](#).

## 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**

## Cisco Intrusion Prevention System (IPS) Sensor Resources

The following table lists all the resources in the Cisco Intrusion Prevention System (IPS) Sensor use case.

### Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

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)/
<b>Library Resources</b>			
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)/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

Resource	Description	Type	URI
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)/
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/



**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

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/
Cisco IPS Sensor Alert Events	This filter selects alert events from Cisco IPS Sensor systems.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IPS Sensor/
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)/

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

Resource	Description	Type	URI
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)/
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

**Resources that Support the Cisco Intrusion Prevention System (IPS) Sensor Use Case, continued**

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 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 120](#).

## Configuration

Verify that the **Cisco IOS IPS Systems** filter includes all Cisco IOS IPS devices present in your network. If necessary, the ArcSightAdministrator 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**

## Cisco IOS Intrusion Prevention System (IOS IPS) Resources

The following table lists all the resources in the Cisco IOS Intrusion Prevention System (IOS IPS) use case.

### Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

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)/
<b>Library Resources</b>			
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)/



**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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/
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco IOS Intrusion Prevention System (IOS IPS) Use Case, continued**

Resource	Description	Type	URI
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
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](#).

Report	Required 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)	Daily Email Transactions

- Verify that the **Cisco Ironport ESA Systems** filter includes all the Cisco Ironport Email Security Appliances present in your network. If necessary, the ArcSightAdministrator can modify the filter to include any missing devices.

## Cisco Ironport Email Security Appliance (ESA) Resources

The following table lists all the resources in the Cisco Ironport Email Security Appliance (ESA) use case.

### Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

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

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

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

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

Resource	Description	Type	URI
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)/



**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

Resource	Description	Type	URI
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)/
<b>Library Resources</b>			
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/

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

Resource	Description	Type	URI
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)/

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

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/
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)/

**Resources that Support the Cisco Ironport Email Security Appliance (ESA) Use Case, continued**

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/
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
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](#).

Report	Required 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 ArcSightAdministrator can modify the filter to include any missing devices.

### Cisco Ironport Web Security Appliance (WSA) Resources

The following table lists all the resources in the Cisco Ironport Web Security Appliance (WSA) use case.

#### Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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)/

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

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

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

Resource	Description	Type	URI
Top Accessed Sites (Cisco WSA)	This report shows a summary of the top accessed sites.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco WSA Configuration Changes by Type	This report displays all successful configuration changes to Cisco WSA devices. Events are grouped by type and user, and sorted chronologically.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Accessed Sites with Most Traffic (Cisco WSA)	This report shows a summary of the top accessed sites with most traffic.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Sources with Most Request Errors (Cisco WSA)	This report shows a summary of the top source hosts with most web request errors.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Cisco WSA Configuration Changes per Day	This report shows a summary of the Cisco WSA configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Hosts with Most Web Traffic (Cisco WSA)	This report shows a summary of the top source hosts with the most web bandwidth consumption.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Denied Sites (Cisco WSA)	This report shows a summary of the top sites denied by Cisco WSA systems.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Top Hosts Accessed Most (Distinct) Sites (Cisco WSA)	This report shows a summary of the top hosts that accessed most sites.	Report	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/



**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

Resource	Description	Type	URI
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)/
<b>Library Resources</b>			
HTTP Status Code Classes	This active list stores the HTTP return status code classes.	Active List	ArcSight Foundation/Cisco Monitoring

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

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)/
Successful Web Transactions	This filter selects successful web server requests.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Successful WSA Configuration Changes	This filter selects successful Cisco WSA configuration changes.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Web Requests	This filter selects all web requests to Cisco WSAs.	Filter	ArcSight Foundation/Cisco Monitoring/Products/Cisco IronPort Web Security Appliance (WSA)/
Successful Configuration Changes	This filter 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)/

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

Resource	Description	Type	URI
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)/
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)/

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

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/
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)/

**Resources that Support the Cisco Ironport Web Security Appliance (WSA) Use Case, continued**

Resource	Description	Type	URI
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)/
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](#).

Report	Required 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	Daily SNMP Access
Trend of Daily Cisco SNMP Access	Daily SNMP Access

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

## Cisco Network Resources

The following table lists all the resources in the Cisco Network use case.

### Resources that Support the Cisco Network Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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/
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/

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
Cisco Device Critical Events	This report shows information about critical events on Cisco network devices. These critical events might be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Cisco Network Equipment Configuration Changes per Day	This report shows a summary of all Cisco network equipment configuration changes per day within the last seven days.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/
Trend of Daily Cisco SNMP Access	This report shows daily SNMP access among all the Cisco traffic.	Report	ArcSight Foundation/Cisco Monitoring/Functionality/Network/



**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Network Use Case, continued**

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/
<b>Library Resources</b>			

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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/

#### Resources that Support the Cisco Network Use Case, continued

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/

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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/

**Resources that Support the Cisco Network Use Case, continued**

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/

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
Cisco Device Critical Events	This query returns critical base events from Cisco network devices where the device group is /Network Equipment or /Operating System, and the object starts with /Network.	Query	ArcSight 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/

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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/
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/



**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
Cisco SNMP Access (Trend Based)	This query returns all SNMP Access recorded Cisco devices within the last seven days.	Query	ArcSight 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

**Resources that Support the Cisco Network Use Case, continued**

Resource	Description	Type	URI
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
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 **Associations - Disassociations per Day (Cisco APs)** report requires the **Daily Associations - Disassociations** trend to be enabled. For more information about enabling trends, see ["Configuring Trends" on page 13](#).
- Verify that the **Cisco Aironet** filter captures all events from Aironet access points in your network.
- If necessary, the ArcSightAdministrator can modify the **Cisco Aironet** 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.

## Cisco Wireless Resources

The following table lists all the resources in the Cisco Wireless use case.

### Resources that Support the Cisco Wireless Use Case

Resource	Description	Type	URI
<b>Monitor Resources</b>			
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/

#### Resources that Support the Cisco Wireless Use Case, continued

Resource	Description	Type	URI
Associated Devices in a Day (Event Based)	This query viewer shows all devices that accessed the Wireless network through an Aironet AP within the last two hours. It provides various drilldowns from the wireless devices and APs listed.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Top Access Points with Most Distinct Associated Devices	This query viewer shows the top access points with the most distinct associated wireless devices within the last two hours, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
Top Access Points with Most Distinct Disassociated Devices	This query viewer shows the count of wireless devices that disassociated with an AP, and provides drilldowns.	Query Viewer	ArcSight Foundation/Cisco Monitoring/Functionality/Wireless/
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/

### Resources that Support the Cisco Wireless Use Case, continued

Resource	Description	Type	URI
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/
<b>Library Resources</b>			
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/
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/

### Resources that Support the Cisco Wireless Use Case, continued

Resource	Description	Type	URI
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/

### Resources that Support the Cisco Wireless Use Case, continued

Resource	Description	Type	URI
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/
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/

## Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

### **Feedback on Cisco Monitoring Standard Content Guide (ESM 6.8c)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arc-doc@hp.com](mailto:arc-doc@hp.com).

We appreciate your feedback!