

---

# Micro Focus Security ArcSight ESM

Software Version: 7.2 Service Pack 1

## ArcSight Administration and ArcSight System Standard Content Guide

Document Release Date: April 2020

Software Release Date: April 2020



## Legal Notices

### Copyright Notice

© Copyright 2001-2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

U.S. Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the U.S. Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 C.F.R. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Support

### Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
Support Web Site	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
ArcSight Product Documentation	<a href="https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

# Contents

Chapter 1: What is Standard Content? .....	7
Chapter 2: Installation and Configuration .....	13
Modeling the Network .....	13
Categorizing Assets .....	14
Configuring Active Lists .....	14
Configuring Filters .....	15
Enabling Rules .....	15
Configuring Notifications and Cases .....	16
Configuring Notification Destinations .....	16
Rules with Notifications to the CERT Team .....	17
Rules with Notifications to SOC Operators .....	17
Rules with Notifications to the Device Administrators Group .....	18
Scheduling Reports .....	18
Configuring Trends .....	18
Viewing Use Cases .....	19
Chapter 3: ArcSight Administration Content .....	22
Connector Overview .....	24
Configuring the Connector Overview Use Case .....	24
Using the Connector Overview Use Case .....	24
Viewing the Dashboards .....	24
ESM Overview .....	27
Using the ESM Overview Use Case .....	27
Viewing the Dashboard .....	27
Viewing the Active Channel .....	29
Logger Overview .....	30
Configuring the Logger Overview Use Case .....	30
Using the Logger Overview Use Case .....	31
Viewing the Dashboards .....	31
Connector Configuration Changes .....	33
Using the Connector Configuration Changes Use Case .....	33

Viewing the Active Channel .....	33
Running Reports .....	33
Connector Connection and Cache Status .....	35
Configuring the Connector Connection and Cache Status Use Case .....	35
Using the Connector Connection and Cache Status Use Case .....	36
Viewing the Dashboard .....	36
Viewing the Active Channels .....	36
Running Reports .....	37
ArcSight ESM Device Monitoring .....	38
Understanding Connector Device Status Events .....	38
Configuring the ArcSight ESM Device Monitoring Use Case .....	39
Using the ArcSight ESM Device Monitoring Use Case .....	40
Viewing the Active Channel .....	41
Viewing the Dashboards .....	41
Running Reports .....	44
ESM Licensing .....	46
Using the ESM Licensing Use Case .....	46
ESM User Sessions .....	48
Using the ESM User Sessions Use Case .....	48
Viewing the Dashboards .....	48
Running Reports .....	48
Actor Configuration Changes .....	50
Using the Actor Configuration Changes Use Case .....	50
Viewing the Dashboards .....	50
Viewing the Active Channel .....	50
Running Reports .....	50
ESM Resource Configuration Changes .....	52
Using the ESM Resource Configuration Changes Use Case .....	52
Viewing the Dashboard .....	52
Running Reports .....	52
Content Management .....	54
Configuring the Content Management Use Case .....	54
Using the Content Management Use Case .....	54
Viewing the Dashboard .....	55
Running Reports .....	55
Event Broker Monitoring .....	56
Event Broker Monitoring Audit Events .....	56
Using the Event Broker Monitoring Use Case .....	57

Viewing the Dashboard .....	58
Viewing the Active Channel .....	59
High Availability Monitoring .....	61
HA Monitoring Audit Events .....	61
Configuring the HA Monitoring Use Case .....	62
Using the HA Monitoring Use Case .....	62
Viewing the Active Channel .....	62
Viewing the Dashboard .....	63
Running the Report .....	66
ESM Events .....	67
Using the ESM Events Use Case .....	67
Viewing the Dashboards .....	67
Viewing the Active Channels .....	67
Running Reports .....	68
ESM Reporting Resource Monitoring .....	70
Using the ESM Reporting Resource Monitoring Use Case .....	70
Viewing the Dashboards .....	70
Viewing the Active Channels .....	70
Running Reports .....	71
ESM Resource Monitoring .....	72
Configuring the ESM Resource Monitoring Use Case .....	72
Using the ESM Resource Monitoring Use Case .....	72
Viewing the Dashboards .....	72
Running Reports .....	73
ESM Storage Monitoring (CORR-Engine) .....	75
Using the ESM Storage Monitoring (CORR-Engine) Use Case .....	75
Viewing the Dashboards .....	75
Running Reports .....	75
Logger Events .....	77
Using the Logger Events Use Case .....	77
Viewing the Active Channels .....	77
Logger System Health .....	78
Configuring the Logger System Health Use Case .....	78
Using the Logger System Health Use Case .....	79
Viewing the Dashboards .....	79
Viewing the Active Channel .....	80
Chapter 4: ArcSight Foundation Content .....	81

Security Threat Monitoring .....	82
Configuring the Security Threat Monitoring Use Case .....	83
Configuring the Child Use Cases .....	86
Using the Security Threat Monitoring Use Case .....	91
Viewing the Dashboard .....	92
Threat Intelligence Platform .....	93
Configuring the Threat Intelligence Platform Use Case .....	94
Using the Threat Intelligence Platform Use Case .....	97
Viewing the Dashboard .....	97
Chapter 5: ArcSight System Content .....	100
Actor Support Resources .....	101
Using the Actor Support Resources .....	101
Priority Formula Resources .....	102
Configuring the Priority Formula Resources Group .....	102
Priority Formula Rules .....	102
System Resources .....	104
Configuring System Resources .....	104
Using the System Resources .....	105
Viewing the Active Channels .....	105
Reports .....	106
Integration Commands .....	106
Send Documentation Feedback .....	108

# Chapter 1: What is Standard Content?

Standard content is a series of coordinated resources, such as dashboards, active channels, reports, filters, rules, and so on that is designed to give you pre-installed comprehensive correlation, monitoring, reporting, alerting, and case management with minimal configuration. The standard content provides a comprehensive set of tasks that monitor the health of the system.

Standard content is installed using a series of packages (.arb files), 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.

**ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products:

- The ArcSight Administration content package is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
- The ArcSight Admin DB CORR content package 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.

- The ArcSight Content Management content package 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.
- The ArcSight Event Broker Monitoring content package is an optional package that lets you monitor activities with ArcSight Event Broker. If ESM is configured to consume events from Event Broker, you can install and use this package during ArcSight Manager installation or from the ArcSight Console any time after installation.
- The ArcSight ESM HA Monitoring content package 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.

- The ArcSight Search Filters content package is installed automatically with the ArcSight Manager. It is used to filter searches performed in the ArcSight Command Center. Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in /All Packages/ArcSight Administration/ArcSight Search Filters are imported but require installation before you can use them.



**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 ready-to-use functionality. The ArcSight Networks package contains zones, and local and global network resources. Zones are provided for IPv4 and IPv6 addresses.

**Note:** ArcSight System resources manage core functionality. The resources are **locked** to protect them from unintended change or deletion.

**ArcSight Foundation** content contains the **Shared Libraries**, which are common resources that provide core functionality for common security scenarios:

- Conditional Variable Filters is a library of filters used by variables in standard content report queries, filters, and rule definitions.
- Global Variables contain 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.
- Network filters contain a set of filters required by ArcSight Administration.

The following resources are packages that you install with the Manager.

**Note:** The ArcSight Foundation 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.

- The ArcSight ClusterView is for ESM with distributed correlation. This resource group contains all the resources required to monitor the health of ESM distributed correlation cluster(s). The Cluster View dashboard is available on the ArcSight Command Center. This dashboard provides a visual map of your cluster configuration, EPS, available node services, connections, and cluster audit events. The ArcSight Console provides a ClusterView icon that changes color if something is wrong with connections. Users can click on the icon from the Console, which launches the Command Center dashboard. This ClusterView icon on the Console is disabled if you have ESM compact mode.

On the Console, the ClusterView package is located at /All Packages/ArcSight Foundation/ArcSight ClusterView. However, the resources will not be functional in compact mode.

- The ArcSight SocView resource group contains all the resources that provide updated information to the security analysts working for the enterprise's Security Operations Center. Various data monitors displaying information such as Top Attacks,

Malicious Activity, destination and source addresses, and so on, are assembled on the SOC Manager dashboard, which is available on the ArcSight Command Center.

On the Console, the package is located at /All Packages/ArcSight Foundation/ArcSight SocView.

- The Threat Intelligence Platform package contains resources that detect security attacks based on a threat intelligence data feed. This package uses Malware Information Sharing Platform (MISP) as a threat intelligence data feed. The threat intelligence data feed from MISP is directly imported to the ESM using the Model Import Connector (MIC). This package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases. The Threat Intelligence Platform package is an optional package. You have the option to select this optional package for installation while installing the ESM. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version to the current version, you do not have the option to install the Threat Intelligence Platform package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.

**Note:** This package, along with the Security Threat Monitoring package, feeds data to the MITRE Dashboard. You do not have to install both packages. The MITRE Dashboard works with either individual package (or both). You must install at least one of the packages, however, to use the MITRE Dashboard in the Command Center. Installing this package also installs the Security Monitoring - Base - Active Lists and Security Monitoring - Base packages.

On the Console, the package is located at /All Packages/ArcSight Foundation/Threat Intelligence Platform.

- The Security Threat Monitoring package monitors security threats based on security log events from the firewall, IDS/IPS, OS, Application, Scanner, Anti-Virus etc. This package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases. The Security Threat Monitoring package is an optional package. While installing the ESM, you have the option to select this package for installation. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version to the current version, you do not have the option to install the Security Threat Monitoring package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.

**Note:** This package, along with the Threat Intelligence Platform package, feeds data to the MITRE Dashboard. You do not have to install both packages. The MITRE Dashboard works with either individual package (or both). You must install at least one of the packages, however, to use the MITRE Dashboard in the

Command Center. Installing this package also installs the Security Monitoring - Base - Active Lists and Security Monitoring - Base packages.

On the Console, the package is located at /All Packages/ArcSight Foundation/Security Threat Monitoring.

- The Security Monitoring - Base package contains shared resources required by the Security Threat Monitoring and Threat Intelligence Platform packages. It also contains content to support the MITRE Dashboard. This base package acts as a supporting package for the Security Threat Monitoring and Threat Intelligence Platform packages. It is mandatory to install this package if you want to use the Security Threat Monitoring and Threat Intelligence Platform packages. This package is automatically installed when you install either both or any one of the Security Threat Monitoring and Threat Intelligence Platform packages.

On the Console, the package is located at /All Packages/ArcSight Foundation/Security Monitoring - Base.

- The Security Monitoring - Base - Active Lists package contains pre-defined active lists required by the Security Monitoring - Base package. This package is a base package which acts as a supporting package for the Security Monitoring - Base package. It is mandatory to install this package if you want to use the Security Threat Monitoring and Threat Intelligence Platform packages. This package is automatically installed when you install either both or any one of the Security Threat Monitoring and Threat Intelligence Platform packages.

**Downloads Groups** contains folders used by the security use cases, which are separate content packages that address specific security needs, such as VPN Monitoring, Suspicious Outbound Traffic Monitoring, Anomalous Traffic Detection, Brute Force Attack, and Reconnaissance, to name a few. These use cases are available from the ArcSight Marketplace portal.

Note that this applies to a fresh ESM installation. For upgrades from earlier versions, the package in /All Packages/Downloads are imported but require installation.

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

This document describes how to configure and use the standard content. For detailed information about using ArcSight ESM, see the ArcSight ESM documentation set, available as a unified help system from the ArcSight Console **Help** menu. PDF versions of the documentation set, as well as Security Use Case Guides, Release Notes, and individual SmartConnector Guides are available on the [ArcSight Documentation page](#).

For detailed information on the ArcSight ESM standard content resources, see the ArcSight ESM Standard Content Resources document, which is available on the [ArcSight Documentation page](#).

# Chapter 2: Installation and Configuration

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

**Note:** ArcSight Content Management, ESM HA Monitoring, and Event Broker Monitoring are *optional* packages provided in the ArcSight Administration package group. You can install either of these packages during ESM installation or from the ArcSight Console any time after installation.

To install after installation, go to the **Packages** tab in the Navigator, open the ArcSight Administration group, right-click the package you want to install and select **Install Package**. After you install the package, the ArcSight Administration group on the Use Cases tab lists the content use cases.

For detailed information about installing ESM, refer to the ArcSight *ESM Installation Guide*.

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

• <a href="#">Modeling the Network</a> .....	13
• <a href="#">Categorizing Assets</a> .....	14
• <a href="#">Configuring Active Lists</a> .....	14
• <a href="#">Configuring Filters</a> .....	15
• <a href="#">Enabling Rules</a> .....	15
• <a href="#">Configuring Notifications and Cases</a> .....	16
• <a href="#">Configuring Notification Destinations</a> .....	16
• <a href="#">Scheduling Reports</a> .....	18
• <a href="#">Configuring Trends</a> .....	18
• <a href="#">Viewing Use Cases</a> .....	19

## 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>
/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*.

## Configuring Active Lists

The standard content includes active lists. Certain active lists are populated automatically during run-time by rules. You do not have to add entries to these active

lists manually before you use them. Other active lists are designed to be populated *manually* with data specific to your environment. After the lists are populated with values, they are referenced by active channels, filters, rules, reports, and data monitors to provide more information about the assets in your environment.

You can add entries manually to active lists using the following methods. Both methods are described in the *ArcSight Console User's Guide*.

- One by one using the Active List editor in the ArcSight Console.
- In a batch by importing values from a CSV file.

For a list of the ArcSight Administration active lists you need to configure manually, refer to the configuration information for each use case presented in ["ArcSight Administration Content" on page 22](#).

For a list of the ArcSight System active lists you need to configure manually, refer to the configuration information for each resource group presented in ["ArcSight System Content" on page 100](#)

## Configuring Filters

For a list of the ArcSight Administration filters you need to configure, refer to the configuration information for each use case presented in ["ArcSight Administration Content" on page 22](#).

For a list of the ArcSight System filters you need to configure, refer to the configuration information for each resource group presented in ["ArcSight System Content" on page 100](#).

## Enabling Rules

Rules trigger only if they are deployed in the /All Rules/Real-time Rules group and are enabled.

- By default, all the **ArcSight System** rules are deployed in the /All Rules/Real-time Rules group and are also enabled.
- By default, all the **ArcSight Administration** rules are deployed in the /All Rules/Real-time rules group and all rules, are enabled except for all deployed rules under /Logger/System Health.

You can enable the Logger System Health rules if you have a Logger connected to your system. The Logger System Health rules are described in ["Logger Overview" on page 30](#).

- By default, the rules in the optional **Content Management** package under ArcSight Administration, are deployed in the *Real-time Rules* group but are disabled.
- By default, the rules in the optional **ArcSight ESM HA Monitoring** and **Event Broker Monitoring** packages under ArcSight Administration are deployed in the *Real-time Rules* group and are also enabled.

**To enable or disable a rule:**

1. In the Navigator panel, go to **Rules** and navigate to the *Real-time Rules* group.
2. Navigate to the rule you want to enable or disable.
3. Right-click the rule and select **Enable Rule** to enable the rule or **Disable Rule** to disable the rule.

## Configuring Notifications and Cases

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

By default, most notifications and create case actions are disabled in the standard content rules that send notifications about security-related events.

To enable rules to send notifications and open cases, first configure notification destinations (see ["Configuring Notification Destinations" below](#)), then enable the notification and case actions in the rules. For more information about working with Rule actions in the Rules Editor, refer to the *ArcSight Console User's Guide*.

## Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, most notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules.

The notification action is enabled by default in the following standard content rules:

- ArcSight Administration/Devices/**Alert - Critical Devices inactive for more than 1 hour**
- ArcSight Administration/ESM/HA Monitoring/**Alert - HA Status Change**
- ArcSight Administration/ESM/System Health/Resources/Domains/**Out of Domain Fields**
- ArcSight Administration/ESM/System Health/Storage/**ASM Database Free Space - Critical**



Make sure you configure notification destinations for the Device Administrators, SOC Operators, and the CERT team groups so that the notifications are received.

Refer to the *ArcSight Console User's Guide* for information on how to configure notification destinations.

## Rules with Notifications to the CERT Team

The following rule is configured to send notifications to the **CERT Team** notification destination group.

Rule Name	Rule URI
Out of Domain Fields	ArcSight Administration/ESM/System Health/Resources/Domains/

**Note:** The notification action for the **Out of Domain Fields** rule is enabled by default. Make sure you configure destinations for the CERT team to receive notifications when this rule triggers.

## Rules with Notifications to SOC Operators

The following rules are configured to send notifications to the **SOC Operators** notification destination group.

Rule Name	Rule URI
Connector Dropping Events	ArcSight Administration/Connectors/System Health/
Connector Still Down	ArcSight Administration/Connectors/System Health/
Connector Still Caching	ArcSight Administration/Connectors/System Health/
Excessive Rule Recursion	ArcSight Administration/ESM/System Health/Resources/Rules/
Rule Matching Too Many Events	ArcSight Administration/ESM/System Health/Resources/Rules/
ASM Database Free - Critical	ArcSight Administration/ESM/System Health/Storage/
Alert - HA Status Change	ArcSight Administration/ESM/HA Monitoring

**Note:** The notification action for the **ASM Database Free Space - Critical** and **Alert - HA Status Change** rules is enabled by default. Make sure you configure destinations for the SOC Operators group to receive notifications when these rules trigger.

## Rules with Notifications to the Device Administrators Group

The following rule is configured to send notifications to the **Device Administrators** notification destination group:

Rule Name	Rule URI
Alert - Critical Devices inactive for more than 1 hour	ArcSight Administration/Devices/

**Note:** The notification action in this rule is enabled by default. Make sure you configure destinations for the Device Administrators group to receive notifications when this rule triggers. See ["Configuring the ArcSight ESM Device Monitoring Use Case" on page 39](#).

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

ArcSight System content does not contain any trends. ArcSight Administration content includes trends, which are enabled by default. Majority of these enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually less busy than during peak daytime business hours. Exceptions are two /All Trends/Arcsight Administration/ESM trends:

- /Licensing/Storage Licensing Data is scheduled to run daily at 10:52.22 a.m.
- /System Health/Storage/ASM Database Free Space is scheduled to run daily at 2:34 p.m.

You can customize these schedules to suit your needs using the Trend scheduler in the ArcSight Console.

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

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

If the start date is not changed, the trend takes the default start date (derived from when the trend was first installed), and 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*.

ArcSight Administration contains resources that enable you to monitor the performance of your enabled trends. The **Trend Details** dashboard in the **ESM Reporting Resource Monitoring** use case (described on page 70) shows the runtime status for all enabled trends. The trend reports show statistics about trend performance for all enabled trends.

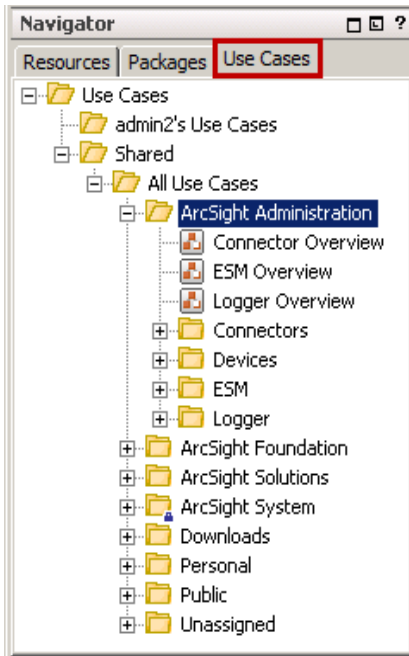
## Viewing Use Cases

ArcSight Administration resources are grouped together in the ArcSight Console in use cases. A use case groups a set of resources that help address a specific issue or business requirement.

**Note:** Currently, ArcSight System content does not contain any use cases. "[ArcSight System Content](#)" on page 100 documents System resources by grouping them by function.

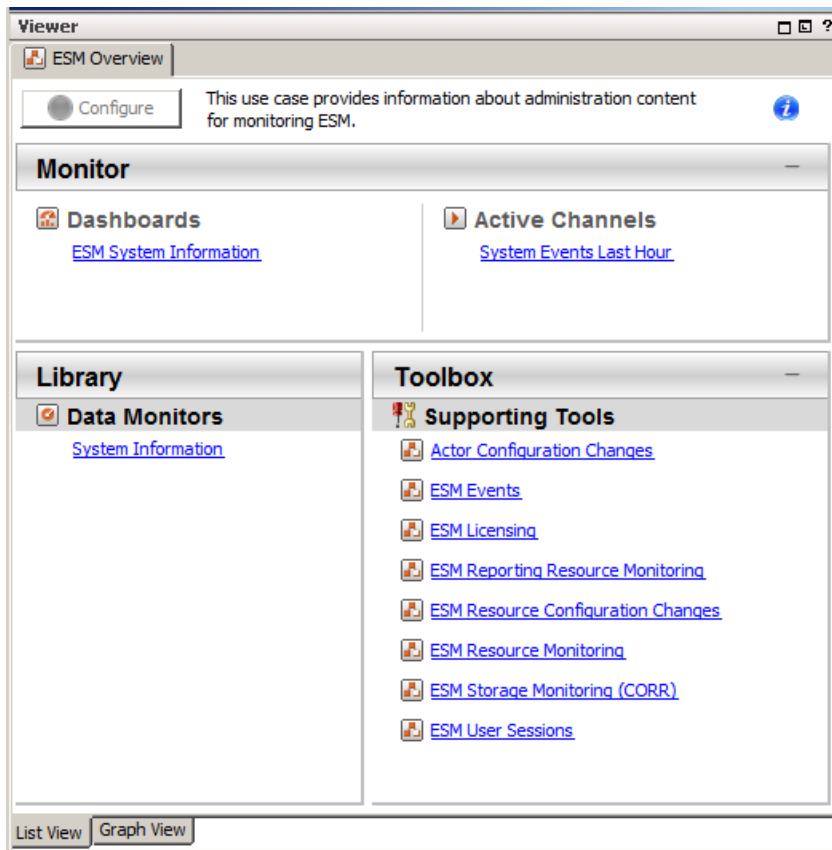
To view the resources in a use case:

1. In the Navigator panel, select the **Use Cases** tab.



2. Browse for a use case; for example, ArcSight Administration/ESM Overview.

3. Right-click the use case and select **Open Use Case**, or double-click the use case. The use case with its associated resources displays in the Viewer panel of the ArcSight Console.



# Chapter 3: ArcSight Administration Content

The ArcSight Administration resources provide statistics about the health and performance of the ArcSight system and its components. This content is essential for managing and tuning performance.

The ArcSight Administration use cases are listed in the table below.

**Note:** ArcSight Administration relies on a series of common resources that provide core functions for common security scenarios. These common resources are located under the Common group. You can identify these resources by the URI; for example, ArcSight Foundation/Common/Network Filters/.

Use Case	Purpose
<b>Overview</b>	
<a href="#">"Connector Overview" on page 24</a>	Provides administration content for monitoring connectors and devices.
<a href="#">"ESM Overview" on page 27</a>	Provides administration content for monitoring the system.
<a href="#">"Logger Overview" on page 30</a>	Provides Logger status and statistics.
<b>Connectors</b>	
<a href="#">"Connector Configuration Changes" on page 33</a>	Provides information about configuration changes (such as upgrades) and the versions of the connectors on the system.
<a href="#">"Connector Connection and Cache Status" on page 35</a>	Provides the connection status and caching status of connectors on the system.
<b>Devices</b>	
<a href="#">"ArcSight ESM Device Monitoring" on page 38</a>	Provides resources to help you monitor the status of devices that send events to connectors.
<b>ESM</b>	
<a href="#">"ESM Licensing" on page 46</a>	Provides information about licensing compliance.
<a href="#">"ESM User Sessions" on page 48</a>	Provides information about user access to the system.

Use Case	Purpose
<b>ESM - Configuration Changes</b>	
<a href="#">"Actor Configuration Changes" on page 50</a>	Provides information about changes to the actor resources.
<a href="#">"ESM Resource Configuration Changes" on page 52</a>	Provides information about changes to the various resources, such as rules, reports, and so on.
<b>ESM - Content Management</b>	
<a href="#">"Content Management" on page 54</a>	Provides information about content package synchronization with the Content Management feature, including the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.
<b>ESM - HA Monitoring</b>	
<a href="#">"High Availability Monitoring" on page 61</a>	Provides resources to help you monitor the status of ESM systems that are using the optional ESM High Availability Module (HA Module). The HA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.
<b>ESM - Event Broker Monitoring</b>	
<a href="#">"Event Broker Monitoring" on page 56</a>	Provides resources to help you monitor the status of connectivity and event consumption between an ArcSight Event Broker deployment and ESM.
<b>ESM - System Health</b>	
<a href="#">"ESM Events" on page 67</a>	Provides statistics on the flow of events through the system.
<a href="#">"ESM Reporting Resource Monitoring" on page 70</a>	Provides performance statistics for reports, trends, and query viewers.
<a href="#">"ESM Resource Monitoring" on page 72</a>	Provides processing statistics for various resources, such as trends, rules, and so on.
<a href="#">"ESM Storage Monitoring (CORR-Engine)" on page 75</a>	Provides information on the health of the CORR- (Correlation Optimized Retention and Retrieval) Engine. This does not apply if you are using ESM with the Oracle database.
<b>Logger</b>	
<a href="#">"Logger Events" on page 77</a>	Provides statistics for events sent through a Logger.
<a href="#">"Logger System Health" on page 78</a>	Provides performance statistics for any Logger connected to the system.

## Connector Overview

The Connector Overview use case provides resources to help you monitor connectors and devices.

## Configuring the Connector Overview Use Case

The Connector Overview use case uses the following active lists from the Connector Connection and Cache Status use case:

- **Connector Information**
- **Connectors - Caching**
- **Connectors - Down**
- **Connectors - Dropping Events**
- **Connectors - Still Caching**
- **Connectors - Still Down**
- **Black List - Connectors**

For information about configuring these active lists, refer to the configuration section in ["Connector Connection and Cache Status" on page 35](#).

## Using the Connector Overview Use Case

The **Connector Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor the status of your connectors and see the top devices that are contributing events. The Library section of the use case lists supporting resources.

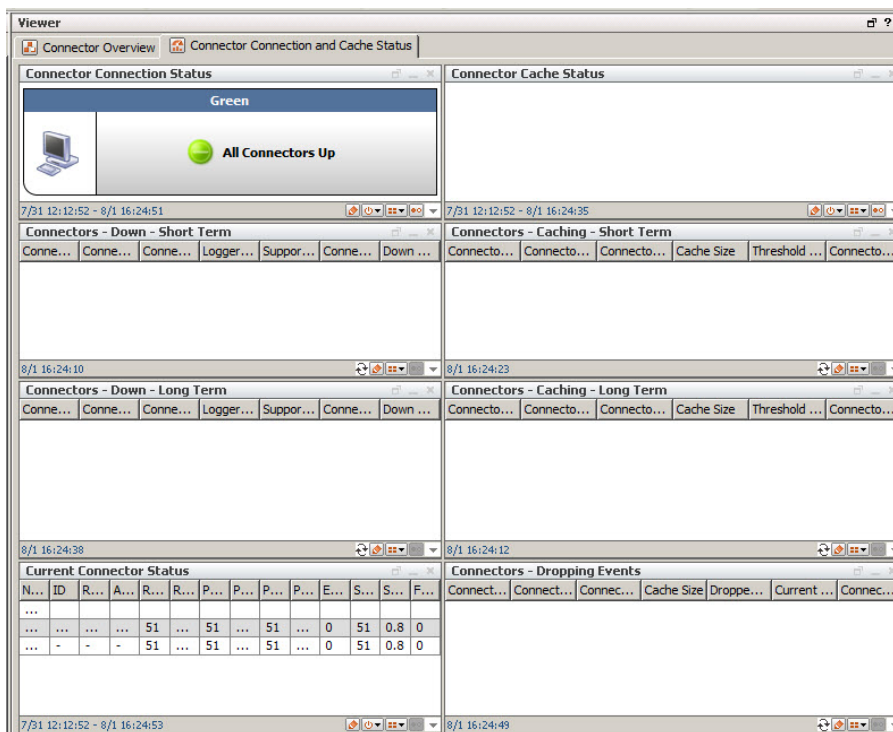
## Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- The **Current Event Sources** dashboard shows the top 20 devices that are contributing events. The device vendor and product type are listed.
- The **Connector Connection and Cache Status** dashboard displays the overall status of connectors and provides information about connectors that are down, caching, or



dropping events. An example dashboard is shown below.



Focus on any yellow or red icons, as they represent connectors that might require attention.

The **Connectors - Down - Short Term** and **Connectors - Down - Long Term** query viewers show connectors that have been down for less than 20 minutes (yellow icons) and for more than 20 minutes (red icons). Down time of less than 20 minutes might be acceptable; for example, scheduled maintenance of the host machine on which the connector is installed. However, more than 20 minutes might indicate an issue that requires investigation. Maybe the connector is configured improperly or needs to be restarted; or there is an underlying network, connection, or hardware problem.

You can find more information about each connector in the **Connector Connection Status** and **Connector Cache Status** data monitors. Check the **Failed Connection Attempts** column to see if the connector is repeatedly failing to connect to the ArcSight Manager. (You might need to undock the component to see this column on the far right side.)

The components on the right side of the dashboard show connectors that are caching events instead of sending them to the ArcSight Manager. Short term caching (for less than two hours) is expected behavior when the connector receives bursts of events or when the ArcSight Manager is down. However, investigate long term caching (more than two hours), as it can result in a full cache and the permanent loss of events. Check the **Cache Size** and **Threshold Size** columns to determine if the cache is nearing its maximum capacity. Check to see if events have been dropped. If so,

review the connector logs and ArcSight Manager logs for errors, and adjust the connector configuration properties as needed.

For answers to frequently asked questions about caching, see the *ArcSight SmartConnectors User's Guide*. For configuration information about a specific connector, see the configuration guide for that connector. For information about connector caching issues, check the [Protect 724](#) community.

## ESM Overview

The ESM Overview use case provides resources that help you monitor the ArcSight system. No configuration is required for this use case.

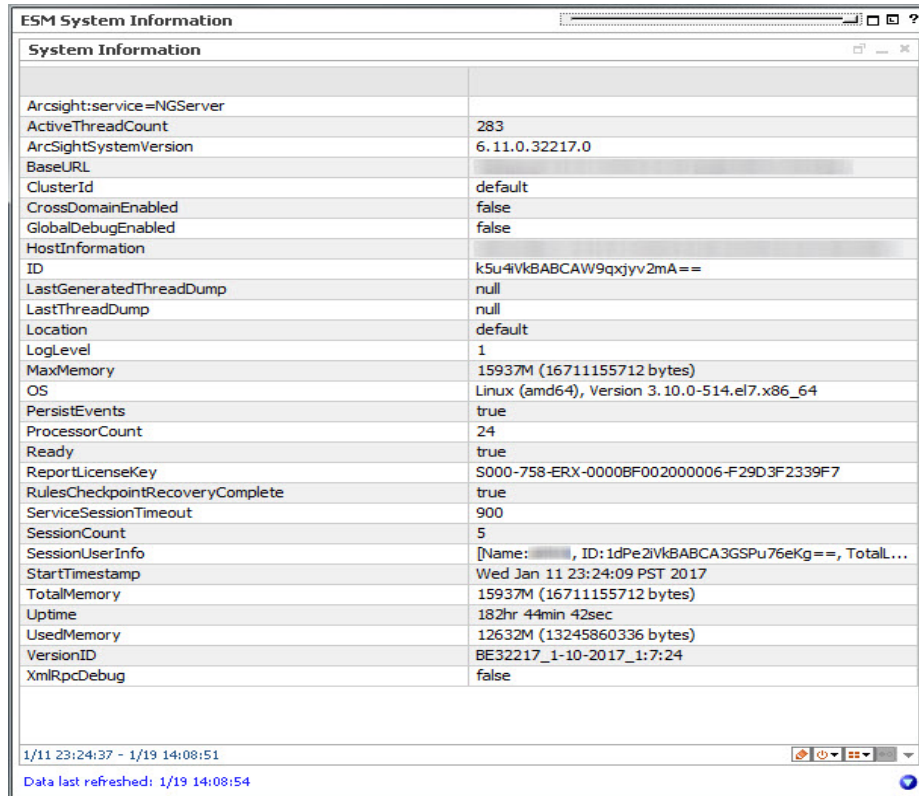
## Using the ESM Overview Use Case

The **ESM Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides the **ESM System Information** dashboard to help you monitor your ArcSight system and the **System Events Last Hour** active channel to help you investigate generated events. The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

## Viewing the Dashboard

To view the **ESM System Information** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays important information about the ArcSight system, such as the version, license, total amount of memory available to the system, and the amount of used memory. System resource availability and statistics, and other important settings are also shown. Following is an example dashboard:



ESM System Information	
System Information	
Arcsight:service=NGServer	
ActiveThreadCount	283
ArcSightSystemVersion	6.11.0.32217.0
BaseURL	
ClusterId	default
CrossDomainEnabled	false
GlobalDebugEnabled	false
HostInformation	
ID	k5u4VkBABCAW9qxjyv2mA==
LastGeneratedThreadDump	null
LastThreadDump	null
Location	default
LogLevel	1
MaxMemory	15937M (16711155712 bytes)
OS	Linux (amd64), Version 3.10.0-514.el7.x86_64
PersistEvents	true
ProcessorCount	24
Ready	true
ReportLicenseKey	S000-758-ERX-0000BF002000006-F29D3F2339F7
RulesCheckpointRecoveryComplete	true
ServiceSessionTimeout	900
SessionCount	5
SessionUserInfo	[Name: , ID: 1dPe2IVkBABCA3GSPu76eKg==, Total...
StartTimestamp	Wed Jan 11 23:24:09 PST 2017
TotalMemory	15937M (16711155712 bytes)
Uptime	182hr 44min 42sec
UsedMemory	12632M (13245860336 bytes)
VersionID	BE32217_1-10-2017_1:7:24
XmlRpcDebug	false

1/11 23:24:37 - 1/19 14:08:51  
Data last refreshed: 1/19 14:08:54

Some of the information on this dashboard is for internal system use.

### System Information Dashboard

System Information	Meaning
Arcsight:service=NGServer	Standard naming convention for the ESM server
ActiveThreadCount	(For internal system use)
ArcSight SystemVersion	ESM release version number, including build number
BaseURL	The URL to the ESM server
ClusterId	(For internal system use)
CrossDomainEnabled	Whether or not the server is enabled for cross-domain requests
GlobalDebugEnabled	(For internal system use)
Host Information	The ESM host name and IP address
ID	Resource ID for the ESM server system as shown in /All Assets/ArcSight System Administration/Managers/<ESM server>
LastGeneratedThreadDump	(For internal system use)
LastThreadDump	(For internal system use)
Location	The physical location of the Manager server, entered during setup (managersetup wizard). Shows default if nothing was entered.

## System Information Dashboard, continued

System Information	Meaning
LogLevel	(For internal system use)
MaxMemory	Returns the maximum amount of memory that the Java virtual machine will attempt to use. If there is no inherent limit then the value <code>java.lang.Long.MAX_VALUE</code> will be returned.
OS	Operating system platform on which the ESM server is installed
PersistEvents	Events are persisted on the database
Processor Count	Number of CPU cores on the system
Ready	System is ready
ReportLicenseKey	Unique license key for the ESM Report Template Designer (InetSoft)
RulesCheckpointRecoveryComplete	Denotes the completion of the rules checkpoint process. See the <i>ESM Administration Guide</i> for information on the rules checkpoint process.
ServiceSessionTimeout	(For internal system use)
SessionCount	Number of concurrent sessions to ESM using ArcSight Console, ArcSight Command Center, and ESM Web Services.
SessionUserInfo	Login name of the user viewing this dashboard, including the resource ID corresponding to that ESM user.
StartTimeStamp	Date and time when Manager was last started.
TotalMemory	Returns the total amount of memory in the Java virtual machine. The value returned may vary over time, depending on the host environment.
Uptime	Amount of time the system was up and running
UsedMemory	Current Java memory used by ESM
VersionID	ESM build number; concurs with <code>ArcSightSystemVersion</code>
XmlRpcDebug	(For internal system use)

## Viewing the Active Channel

To view the **System Events Last Hour** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all events generated by the ArcSight system during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events. Double-click an event to see details about the event in the Event Inspector.

## Logger Overview

The Logger Overview use case provides resources to help you monitor Logger status and statistics.

## Configuring the Logger Overview Use Case

If you have a Logger connected to your ArcSight system, follow the steps below to configure the Logger Overview use case:

### To configure the Logger Overview use case:

1. Enable the following rules in the /All Rules/Real-time Rules/ArcSight Administration/Logger/System Health folder:
  - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
  - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for the same sensor type for a Logger indicate OK.
  - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.

For information about enabling rules, refer to ["Enabling Rules" on page 15](#).
2. Edit the **My Logger** filter in the /All Filters/ArcSight Administration/Logger/System Health folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.
3. Enable the following data monitors:
  - a. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/ArcSight Appliances Overview folder:
    - **Logger Disk Usage**
    - **Logger Hardware Status**
  - b. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview folder:

- CPU Usage (Percent) - Last 10 Minutes
- Disk Read and Write (Kbytes per Second) - Last 10 Minutes
- Disk Usage
- EPS Usage (Events per Second) - Last 10 Minutes
- Memory Usage (Mbytes per Second) - Last 10 Minutes
- Network Usage (Bytes) - Last 10 Minutes
- Sensor Type Status

**Note:** These data monitors are disabled by default to avoid increasing the load on environments without a Logger.

For information about data monitors, refer to the *Enabling or Disabling a Data Monitor* section in the [ArcSight Console User's Guide](#).

## Using the Logger Overview Use Case

The **Logger Overview** use case is located in /All Use Cases/ArcSight Administration on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor all your ArcSight appliances and the hardware, storage, CPU, memory, network, and EPS usage for a specific Logger. The Library section of the use case lists supporting resources that help compile information in the dashboards.

## Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below:

- **ArcSight Appliances Overview** - Review the data monitors on this dashboard to check your ArcSight appliances. Focus on any red icons, as they represent appliances that might require attention. Examine the disk status for all appliances; a warning or critical status requires your attention.
- **My Logger Overview** - Review the data monitors on the dashboard to check the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the My Logger filter. The information is collected during the last ten minutes.

**Note:** The data monitors in the **My Logger Overview** and **ArcSight Appliances Overview** dashboards are disabled by default to avoid increasing the load on

environments without Logger. Enable these data monitors if you have a Logger in your environment as described in ["Configuring the Logger Overview Use Case" on page 30](#).



## Connector Configuration Changes

The Connector Configuration Changes use case provides information about configuration changes (such as upgrades) and the versions of the connectors on the system. No configuration is required for this use case.

### Using the Connector Configuration Changes Use Case

The **Connector Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/Connectors on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides an active channel to help you monitor connector upgrades, and several reports that show the status and historical information about connector upgrades. The Library section of the use case lists supporting resources that help compile information in the active channel and the reports.

### Viewing the Active Channel

To view the **Connector Upgrades** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events related to connector upgrades received within the last two hours. The active channel uses the Connector Upgrades field set. Use this active channel as a baseline for your monitoring.

### Running Reports

The **Connector Configuration Changes** use case provides several reports that show connector upgrade history. You can provide these historical reports to the stakeholders in your company, when needed.

By default, the reports use data for the last week from the time you run the report. You can change the start and end time of the report for longer- or shorter-term analysis when you run the report.

#### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- The **Connector Upgrades Count** report shows the total count of successful and failed connector upgrades in a pie chart and the counts per day in a table.
- The **Connector Versions** report lists all the connectors with their latest versions, grouped by connector type, connector zone, and connector address.
- The **Connector Versions by Type** report lists all the connectors by connector type, grouped by connector version, connector zone, and connector address.
- The **Failed Connector Upgrades** report lists the connectors with failed upgrades, grouped by connector zone, connector address, connector name, and connector ID. The report also shows the reason for the failure.
- The **Successful Connector Upgrades** report lists the connectors with successful upgrades, sorted chronologically.
- The **Upgrade History by Connector** report shows the upgrade history by connector sorted chronologically. When running this report, use the connector ID located in the connector resource and copy-paste the ID into the ConnectorID field in the Custom Parameters for the report.
- The **Upgrade History by Connector Type** report shows the upgrade history by connector type, grouped by connector zone, connector address, connector name, and connector ID.
- The **Version History by Connector** report shows the version history by connector, sorted chronologically. When running this report, use the connector ID (located in the connector resource) and copy-paste it in to the ConnectorID field in the Custom Parameters for the report.
- The **Version History by Connector Type** report shows the version history by connector type, grouped by connector zone, connector address, connector name, and connector ID.

## Connector Connection and Cache Status

The Connector Connection and Cache Status use case provides the connection status and caching status of connectors on the system. Connectors can be connected directly to the ArcSight system or through Loggers.

### Configuring the Connector Connection and Cache Status Use Case

The Connector Configuration and Cache Status use case requires the following configuration for your environment:

Customize the following active lists:

- In the **Connectors - Down** active list, adjust the Time to Live (TTL) attribute, if needed. By default, the TTL is set to 20 minutes. A connector down for fewer than 20 minutes is considered to be down for a short term. After 20 minutes, the entry for this active list expires and the connector information is moved to the **Connectors - Still Down** active list, unless the connector comes back up before 20 minutes.
- In the **Connectors - Caching** active list, adjust the Time to Live (TTL) attribute, if needed. By default, the TTL is set to two hours. A connector that has been caching for fewer than two hours is considered to be caching for a short term. Connectors caching for up to two hours are not considered to be a problem. After two hours, the entry for this active list expires and the connector information is moved to the **Connectors - Still Caching** active list, unless the connector cache is emptied in fewer than two hours, and it is removed by the Connector Cache Empty rule.
- Populate the **Black List - Connectors** active list with the URI and IP address of each connector you want to exclude from being evaluated by the Connector UP and Connector Down rules. These rules detect connectors that are started and are reporting events, and those that are shut down. These rules can send a notification (if notifications are enabled) when the connectors have been down for a certain period of time. You might want to exclude connectors that you start and stop manually, connectors that are scheduled to run once every week (such as vulnerability scanners), or connectors that you are testing (starting and stopping frequently during the setup process).
- *Optional:* Populate the **Connector Information** active list with the contact information for each connector, if needed. For example, you can add contact information for connectors maintained by other individuals or organizations. Add the contact information in the Support Information field in the format provided (poc= | email= | phone= | dept= | action=).

The Connector Information active list collects information about connectors that have reported into the system, as well as information from the ArcSight Manager when the connector is first registered. Do not add information to this active list for connectors that are not already reported into the system and registered.

For information about how to configure an active list, refer to the *ArcSight Console User's Guide*.

## Using the Connector Connection and Cache Status Use Case

The **Connector Connection and Cache Status** use case is located in /All Use Cases/ArcSight Administration/Connectors on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard, two active channels and two reports to help you monitor connector connection and status. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channels, and reports.

### Viewing the Dashboard

To view the **Connector Connection and Cache Status** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the status of your connectors in real time. You can see which connectors have been down for a short time or a long time, and which connectors are dropping or caching events. Use this dashboard as a baseline for your monitoring. Investigate any connectors that have been down for a long period of time and any connectors that are dropping or caching events.

### Viewing the Active Channels

The **Connector Connection and Cache Status** use case provides two active channels. To open an active channel in the Viewer panel, click the link for the active channel in the use case.

- The **Connector Caching Events** active channel shows information about connector *cache* status audit events and correlation events from the related connector monitoring rules.
- The **Connector Connection Status Events** active channel shows information about connector *connection* status audit events and correlation events from the related connector monitoring rules.

## Running Reports

The **Connector Connection and Cache Status** use case provides two reports that show connector cache history and connector status. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Cache History by Connectors** shows the cache history by connector, sorted chronologically. By default, the report shows all of the connectors known by the system. You can specify the connector URI (located in the Connector Information active list) in the ConnectorURI field in the custom parameters for the report to narrow down the connector cache histories reported, from groups (such as /All Connectors/Site Connectors/) to a specific connector (such as /All Connectors/Site Connectors/DMZ/WUC-1). The default time range of this report is the past three to four months.
- **Current Cache Status** lists the connectors that are currently caching and dropping events.

## ArcSight ESM Device Monitoring

The ArcSight ESM Device Monitoring use case enables you to monitor the status of ArcSight ESM devices that send events to SmartConnectors (connectors). You can monitor all devices continuously and detect inactive devices promptly with minimum impact on the ArcSight ESM system. For example, you can see which firewall is inactive, which web server is new, and if a critical device is inactive for more than one hour.

A connector can use the Device Status Monitoring (DSM) feature to generate Connector Device Status events periodically reporting the status of each device communicating with it. A device is a unique combination of these five fields: `deviceHostName`, `deviceVendor`, `deviceProduct`, `deviceZone`, and `customer`.

When a device is sending base events to the connector and the connector is receiving them, the status of a device is *active*. When a connector receives no events from a device for a set period of time, the status of a device is *inactive*. The inactive status does not provide details about the network status, hardware or software issues on the device or connector.

**Note:** The ArcSight ESM Device Monitoring content monitors devices that send events to SmartConnectors (connectors that work on security events). The content does not support Model Import connectors.

## Understanding Connector Device Status Events

When DSM is enabled, the connector generates a `Connector Device Status` internal event for each device it is tracking. The event contains the information in the following table.

To enable DSM, see ["Configuring the ArcSight ESM Device Monitoring Use Case" on the next page](#).

Connector Device Status Event Fields	Field Value
Event Name	Connector Device Status
Device Event Class ID	agent:043
Device Custom String1	device vendor (from the base events received from the device)
Device Custom String2	device product (from the base event received from the device)

Connector Device Status Event Fields	Field Value
Device Custom Number1	total event count (total number of events for this device since the SmartConnector started)
Device Custom Number2	event count SLC (since last check) (number of events for this device since the last internal event was sent)
Source Address	device address (source device sending base events to the connector)
Source Hostname	device hostname (source device sending base events to connector)
Device Custom Date1	Last Event Received (connector time when the last event was received from the device)
deviceEventCategory	/Agent/Connection/Device/Status
agentSeverity	low
deviceVendor	ArcSight
deviceProduct	ArcSight

When a new device sends the first event to the connector, the connector starts generating the Connector Device Status events for this device. The **All Monitored Devices** rule is configured to trigger when the Connector Device Status events have a non-zero Device Custom Number2 (indicating that the device is active and sending base events to the connector since the last check).

## Configuring the ArcSight ESM Device Monitoring Use Case

The ArcSight ESM Device Monitoring use case requires the following configuration for your environment:

1. Enable Device Status Monitoring (DSM) on your connector. When DSM is enabled, a Connector Device Status internal event is sent for each device tracked by the connector with the following information: the last time the connector received an event from the device, the total number of events from this device since the connector started, and the number of events sent by this device since the last check.
  - a. On the **Resources** tab of the ArcSight Console Navigator panel, go to **Connectors**, right click the connector on which you want to enable DSM, then select **Configure**.  
  
The **Inspect/Edit** panel for the Connector Editor opens. On the **Connector** tab, the **Name** field is populated automatically with the name assigned during connector installation.
  - b. On the **Default** tab, set the **Enable Device Status Monitoring (in millisec)** option.

By default, DSM is disabled on a connector; the **Enable Device Status Monitoring (in millisec)** option is set to -1. The minimum positive value you can assign is one minute (60000 milliseconds).

**Caution:** Enabling DSM can create a heavy load on busy connectors. Micro Focus recommends that you set DSM to ten minutes or more; for example, 600000.

- c. Restart the connector.
2. Populate the **Critical Monitored Devices** active list with the devices that are critical in your environment. This active list is then updated automatically when the Critical Monitored Devices rule triggers. The **Critical Monitored Devices** dashboard shows only the devices included in this active list.  
  
To add devices that are critical to your environment, you can export the specific devices from the **All Monitored Devices** active list and import them to the **Critical Monitored Devices** active list. If you have a predefined list of critical devices, you can import a csv file containing all your critical devices to the **Critical Devices** active list. When the Critical Monitored Devices rule triggers, the entries from the **Critical Devices** active list are added to the **Critical Monitored Devices** active list.
3. Populate the **Whitelisted Monitored Devices** active list with the devices that you do not want to monitor. For example, include in this active list non-critical devices or devices that only respond once a day. The **Whitelisted Monitored Devices** active list is used in the **All Monitored Devices** rule condition.
4. Configure notification destinations for the Device Administrators group so that the correct administrators are notified when the **Alert - Critical Devices inactive for more than 1 hour** rule triggers. The send notification action in the **Alert - Critical Devices inactive for more than 1 hour** rule is enabled by default. For details on how to configure notification destinations, refer to the *ArcSight Console User's Guide*.

## Using the ArcSight ESM Device Monitoring Use Case

The **ArcSight Device Monitoring** use case is located in /All Use Cases/ArcSight Administration/Devices on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor your ESM devices, including critical assets, and investigate device status events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.



## Viewing the Active Channel

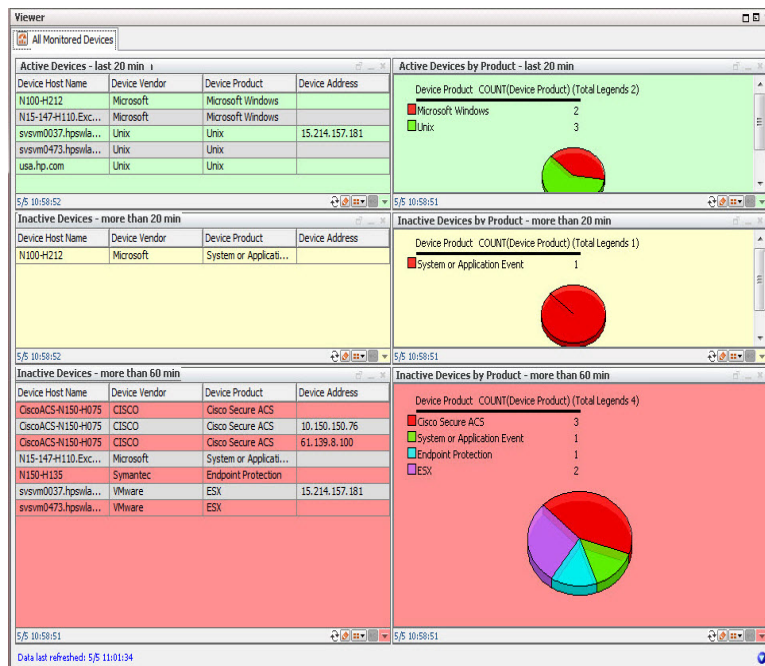
To view the **ArcSight ESM Device Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and shows all Device Status events received within the last two hours. Double-click an event to see details about the event in the Event Inspector.

## Viewing the Dashboards

The **ArcSight Device Monitoring** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

**Tip:** View the dashboards for short-term activity and inactivity monitoring (for example, 20 minutes to one hour). For longer term activity, run the ArcSight ESM Device Monitoring reports. See ["Running Reports" on page 44](#).

### All Monitored Devices Dashboard



This dashboard provides query viewers that show information about all known devices (all the devices in the **All Monitored Devices** active list). The query viewers are color coded so you can identify problems quickly.


- The **Active Devices - last 20 min** query viewer displays information about devices that have reported events within the last 20 minutes. The **Active Devices by Product - last 20 min** query viewer displays the number of devices that have reported events

within the last 20 minutes, in a pie chart by device product type.

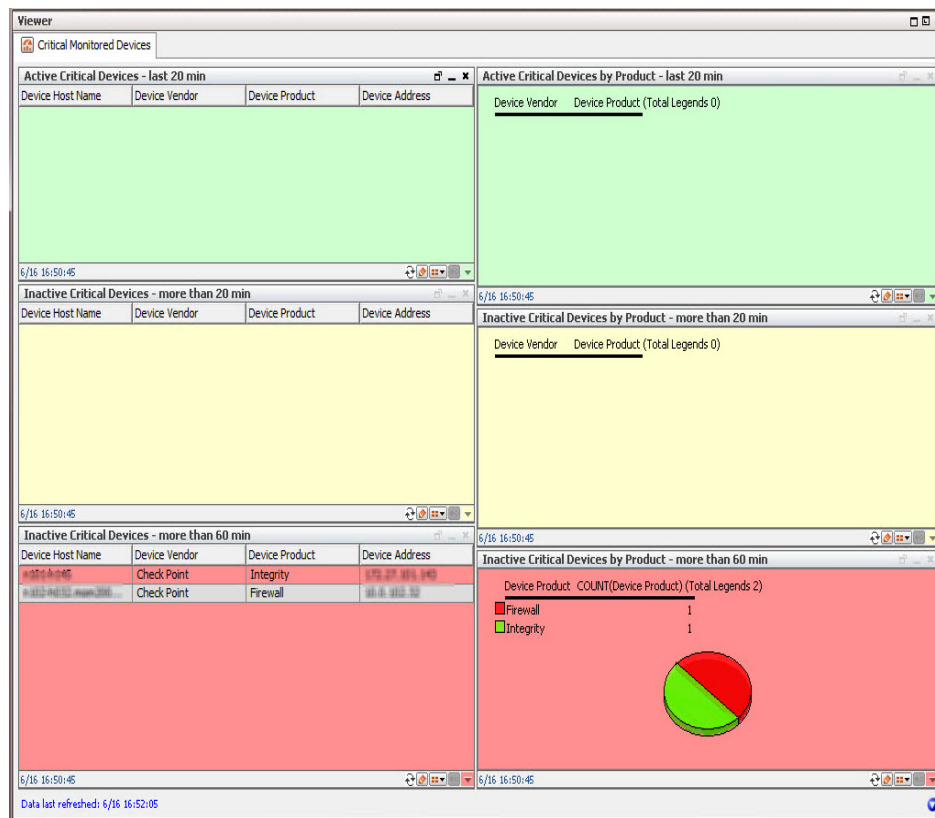
- The **Inactive Devices - more than 20 min** query viewer displays information about devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.
- The **Inactive Devices - more than 60 min** query viewer displays information about devices that have not reported events within the last 60 minutes. The **Inactive Devices by Product - more than 60 min** query viewer displays the number of devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

Focus on the devices in the **Inactive Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

Drill down to see details about an event on the dashboard, such as the Agent Name, Event Count SLC, Creation Time, and so on:

- If the view in the query viewer is a pie chart, change the view to a table (click the **View as** button  on the bottom right of the query viewer).
- Right click an event in the query viewer and select **Drilldown > Show device details for selected Device Product**.

## Critical Monitored Devices Dashboard



This dashboard provides several query viewers that show an overview of your critical devices (the devices in the **Critical Monitored Devices** active list).

- The **Active Critical Devices - last 20 min** query viewer displays information about critical devices that have reported events within the last 20 minutes. The **Active Critical Devices by Product - last 20 min** query viewer displays the number of critical devices that have reported events within the last 20 minutes, in a pie chart by device product type.
- The **Inactive Critical Devices - more than 20 min** query viewer displays information about critical devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 20 min** query viewer displays the number of critical devices that have not reported events within the last 20 minutes but have reported events within the last 60 minutes, in a pie chart by device product type.
- The **Inactive Critical Devices - more than 60 min** query viewer displays information about critical devices that have not reported events within the last 60 minutes. The **Inactive Critical Devices by Product - more than 60 min** query viewer displays the number of critical devices that have not reported events within the last 60 minutes, in a pie chart by device product type.

Focus on the devices in the **Inactive Critical Devices - more than 60 min** query viewers, as these devices might require attention. Not reporting events for more than 60 minutes might be acceptable; for example, scheduled maintenance of a device. However, this might indicate an issue that requires investigation. Maybe the device is improperly configured or needs to be restarted; or there is an underlying network, connection, or hardware problem.

## Running Reports

The **ArcSight Device Monitoring** use case provides several reports that show historical information about your ESM devices. You can provide these historical reports to the stakeholders in your company, when needed. You can run the following reports for longer-term activity and inactivity monitoring.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- The **All Devices Detected Inactive - Last 24 Hours** report displays information about all devices that are *inactive* within the last 24 hours.
- The **All Devices Detected Inactive - Last 7 Days** report displays information about all devices that are *inactive* within the last seven days.
- The **All Monitored Devices** report displays information about all known devices (devices listed in the **All Monitored Devices** active list).
- The **Critical Devices Detected Inactive - Last 24 Hours** report displays information about critical devices that are *inactive* within the last 24 hours (critical devices are listed in the **Critical Monitored Devices** active list).
- The **Critical Devices Detected Inactive - Last 7 Days** report displays information about critical devices that are *inactive* within the last seven days.
- The **Critical Monitored Devices** report displays information about all critical devices being monitored.
- The **New Devices Detected - Last 24 Hours** report displays information about the new devices detected within the last 24 hours.

- The **New Devices Detected - Last 7 Days** report displays information about new devices detected within the last seven days.

## ESM Licensing

The ESM Licensing use case provides information about licensing compliance. No configuration is required for this use case.

### Using the ESM Licensing Use Case

The **ESM Licensing** use case is located in /All Use Cases/ArcSight Administration/ESM on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several reports that provide a historical view of ESM license compliance. You can provide these reports to the stakeholders in your company, when needed. The Library section of the use case lists supporting resources that help compile information in the reports.

#### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actors Licensing Report** shows the licensing history for actors within the last seven days. A chart shows the current count and the count limit.
- **Assets Licensing Report** shows the licensing history for assets within the last seven days. A chart shows the current count and the count limit.
- **Console Users Licensing Report** shows the licensing history for console users within the last seven days. A chart shows the current count and the count limit.
- **Devices Licensing Report** shows the licensing history for devices within the last seven days. A chart shows the current count and the count limit.
- **Web Users Licensing Report** shows the licensing history for web users (using the ArcSight ESM Command Center) within the last seven days. A chart shows the current count and the count limit.

- **Licensing Report** shows the licensing history for each of the license types within the last seven days. The chart shows the current count and the count limit in a chart.
- **Licensing Report (All)** shows the licensing history for all the license types within the last seven days. A chart shows the current count and the count limit for each of the license types.
- **Storage Licensing Report** shows an overview of the storage used by the system for each day, with a breakdown of the raw event data size sent by each connector and by connector type.

## ESM User Sessions

The ESM User Sessions use case provides information about user access to the ArcSight system. No configuration is required for this use case.

### Using the ESM User Sessions Use Case

The **ESM User Sessions** use case is located in /All Use Cases/ArcSight Administration/ESM on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards to help you monitor user access to ArcSight ESM (user login and logout activity, including login session and notification information) and several reports that provide a historical view of ArcSight user login and logout activity. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

### Viewing the Dashboards

To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel.

- **ArcSight User Status** displays information about ArcSight Manager user sessions, including the username, the IP address and zone for the system from which the user is connecting, and the status of the connection (Logged In, Logged Out, or Login Timed Out).
- **ArcSight User Activity** displays information about the users currently logged into the ArcSight ESM system, such as the username, IP address of the system from which the user is connecting, the client type and version, and the last access time. Recent user session information and notification activity generated by ArcSight ESM rules are also provided.

### Running Reports

The **ESM User Sessions** use case provides several reports that show information about ESM user sessions. You can provide these historical reports to the stakeholders in your company, when needed.

#### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.



2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ArcSight User Login Trends** shows a summary of the number of ArcSight user logins for the previous day. A bar chart shows the total number of logins by user and a table shows the number of logins by user per hour.
- **ArcSight User Logins - Last Hour** shows details for all the ArcSight user logins within the past hour. The report contains a table showing the source host, the username, and the login time.
- **User Login Logout Report** shows successful and failed user login events, and logout events.

## Actor Configuration Changes

The Actor Configuration Changes use case provides information about changes to the actor resources. No configuration is required for this use case.

### Using the Actor Configuration Changes Use Case

The **Actor Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/ESM/Configuration Changes on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two dashboards, an active channel, and several reports to help you monitor changes made to the actor resources. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channel, and reports.

### Viewing the Dashboards

The **Actor Configuration Changes** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Actor Administration** displays a list of all the authenticators for actors.
- **Actor Change Log** displays an overview of the actor resource changes (the total number of changes by type within the last hour) and the most recent events related to changes in actors (including creation, deletion, and modification of single-value and multi-value parameters of actor resources).

### Viewing the Active Channel

To view the **Actor Audit Events** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all events where there are data changes to the actor resources.

### Running Reports

The **Actor Configuration Changes** use case provides several reports that give you a historical view of the changes made to the actor resources. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Actor Full Name and Email Changes** shows information from actor audit events that result from changes to the Full Name or Email attribute of an actor. The report shows the old and new information.
- **Actor Manager and Department Changes** shows information from actor audit events that result from changes to the Department or Manager attribute of an actor. This report shows the old and the new information.
- **Actor Title and Status Changes** shows information from actor audit events that result from changes to the Title or Status attribute of an actor. The report shows the old and new information.
- **Configuration Changes by Type** shows recent actor configuration changes. A table lists all the changes grouped by type and user, and sorts them chronologically.
- **Configuration Changes by User** shows recent actor configuration changes. A table lists all the changes grouped by user and type, and sorts them chronologically.
- **Created** shows a list of all the actors created the previous day.
- **Deleted** displays audit event information for actors that have been deleted.
- **IDM Deletions of Actors** shows the list of all the actors that have been marked as deleted by the IDM. This is not the same as deleting the actor resource from the ArcSight ESM system.
- **Updated** shows a list of all the actors updated the previous day.

## ESM Resource Configuration Changes

The ESM Resource Configuration Changes use case provides information about changes to the ESM resources, such as rules, reports, and so on. No configuration is required for this use case.

### Using the ESM Resource Configuration Changes Use Case

The **ESM Resource Configuration Changes** use case is located in /All Use Cases/ArcSight Administration/ESM/Configuration Changes on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor all changes to content resources and several reports that provide information about recently deleted, created, or updated ESM resources. The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

### Viewing the Dashboard

To view the **Resource Change Log** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays the total number of ESM resource changes by type within the last hour in a pie chart. Detailed information about logs associated with these changes is also provided.

### Running Reports

The **ESM Resource Configuration Changes** use case provides several reports that provide historical information about recently deleted, created, or updated ESM resources. You can provide these historical reports to the stakeholders in your company, when needed.

#### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **ESM Configuration Changes by Type** shows recent ESM configuration changes. A table lists all the changes grouped by type, sorted chronologically. Use this report to find all the configuration changes of a certain type.
- **ESM Configuration Changes by User** shows recent ESM configuration changes. A table lists all the changes grouped by user, sorted chronologically. Use this report to find all the configuration changes made by a specific user.
- **Resource Created Report** shows a list of all the resources created by ESM users the previous day.
- **Resource Deleted Report** shows a list of all the resources deleted by ESM users the previous day.
- **Resource History Report** shows a list of all the resources that have been created, updated, or deleted by ESM users the previous day.
- **Resource Updated Report** shows a list of all the resources updated by ESM users the previous day.

## Content Management

The Content Management use case provides resources that show information about content package synchronization with the ESM Content Management feature. The information includes the history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered during synchronization.

**Note:** The Content Management use case is available only if you install the optional ArcSight Content Management package located in the ArcSight Administration package group.

For information about the ESM Content Management feature, refer to the *ArcSight Command Center User's Guide*.

## Configuring the Content Management Use Case

Enable the **Content Management Data** rule. This rule maintains the **Content Management History** active list. To enable the rule, right-click the rule in the Rules section of the Content Management use case and select **Enable Rule**.

Enable the **Content Management Data Failure** rule. This rule sends a notification to the **Content Management** notification group each time a failure event occurs. Also, this rule maintains the **Content Management History Failure** active list. To enable the rule, right-click the rule in the Rules section of the Content Management use case and select **Enable Rule**.

To create a notification group for Content Management see the [ArcSight Console User's Guide](#).

## Using the Content Management Use Case

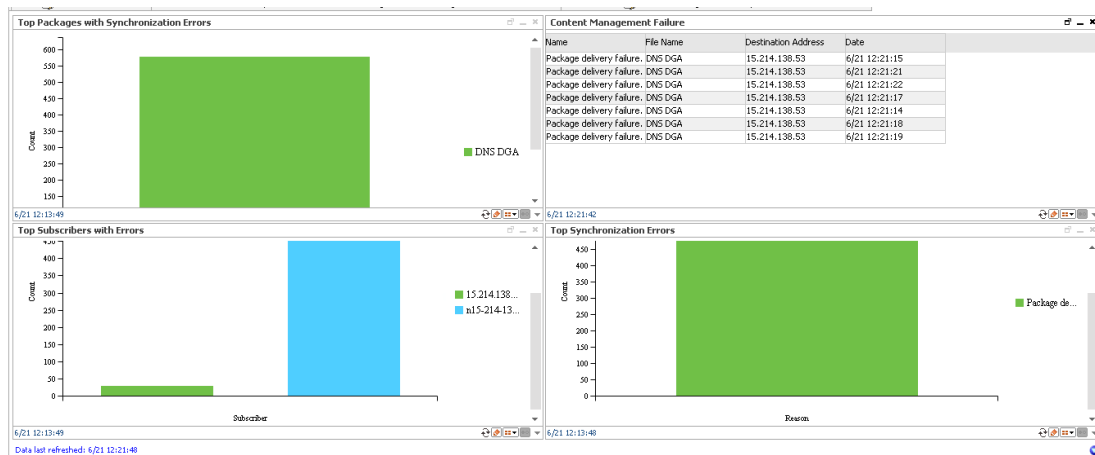
The **Content Management** use case is located in /All Use Cases/ArcSight Administration/ESM/Content Management on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard to help you monitor the history of content packages synchronized across peered ArcSight Manager or subscribers. Several reports provide a history of content package synchronization and information about content packages with synchronization errors or subscription errors.

The Library section of the use case lists supporting resources that help compile information in the dashboard and reports.

## Viewing the Dashboard

To view the **Synchronization Status History** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel as shown below:



The **Synchronization Status History** dashboard shows the following:

- The content packages with the most issues related to either package update delivery or installation after the package has been delivered.
- The most common issues with delivery or installation of managed packages.
- The subscribers experiencing the most issues with managed package delivery or installation.
- The Content Management failure events that have occurred recently.

## Running Reports

The **Content Management** use case provides several reports that provide a historical view of the content package synchronization history and information about content packages with synchronization errors or subscription errors. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Top Packages with Synchronization Errors** shows information about the content packages with the most update delivery issues or installation issues after the package has been delivered.
- **Synchronization Status History** shows information about the history of content packages synchronized across peered ArcSight Managers or subscribers.
- **Top Synchronization Errors** shows information about the most common issues experienced by subscribers with managed package delivery or installation.
- **Top Subscribers with Errors** shows information about the subscribers experiencing the most issues with managed package delivery or installation.

## Event Broker Monitoring

The Event Broker Monitoring optional package provides resources to help you monitor the status of connectivity and event consumption by ESM from an ArcSight Event Broker deployment.

After Event Broker and connectors are properly configured for connectivity and topic identification, ESM can consume topics from Event Broker.

### Prerequisites:

Using the resources from the Event Broker Monitoring package assumes that your environment has a deployment of the ArcSight Event Broker, and Event Broker is set up with one topic specifically for ESM consumption.

See the *Micro Focus Security ArcSight Data Platform Event Broker Administrator's Guide* and the accompanying *Release Notes*.

## Event Broker Monitoring Audit Events

The Event Broker Monitoring content uses information from the Event Broker audit events generated by the ArcSight Manager.

The Device Event Class ID and Name fields, with more fields in the audit event are displayed in the Event Broker Audit Events active channel. See ["Viewing the Active Channel" on page 59](#).

The following table lists the Event Broker audit events.



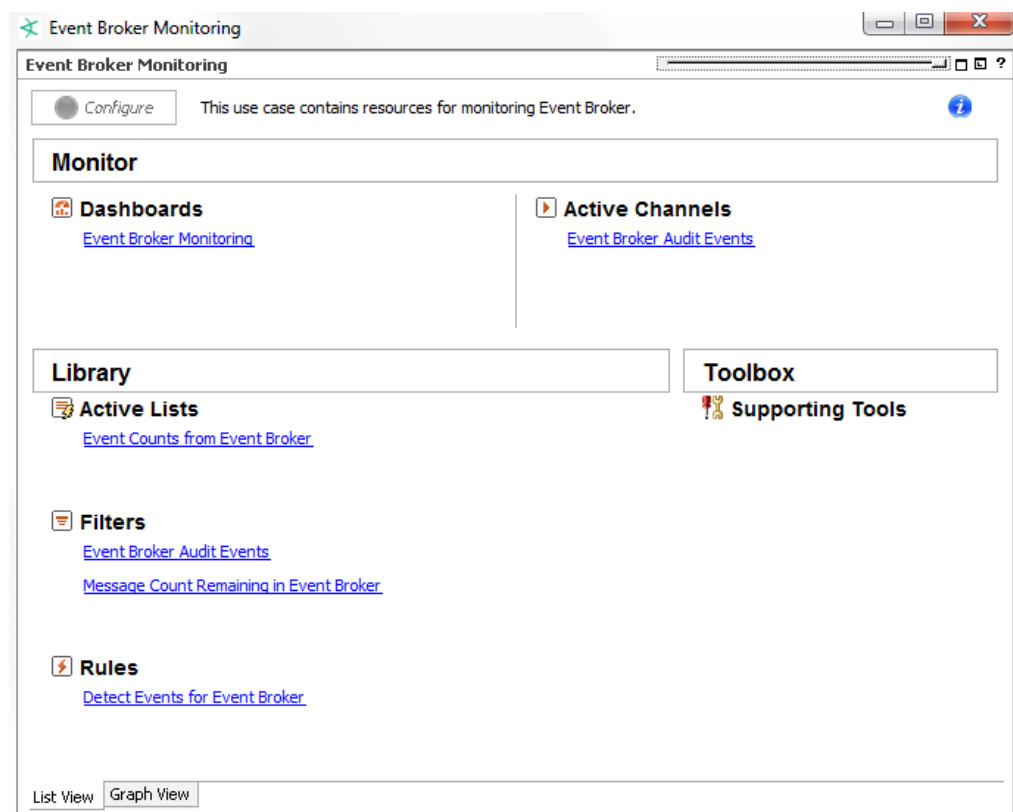
## Event Broker Audit Events

Device Event Class ID	Audit Event Description
eventbroker:100	Connection to Event Broker is up
eventbroker:101	Connection to Event Broker is down
eventbroker:102	Number of messages remaining in Event Broker
eventbroker:103	Number of events forwarded from Event Broker to ESM

## Using the Event Broker Monitoring Use Case

The **Event Broker Monitoring** use case is an optional module installed in /All Use Cases/ArcSight Administration/ESM/Event Broker Monitoring on the **Use Cases** tab of the Navigator.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.



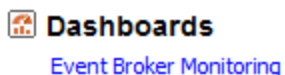
The Monitor section of the use case provides a dashboard and an active channel to help you monitor the status of Event Broker activity in terms of events received by ESM, and status of connectivity between ESM and Event Broker.

The Library section of the use case lists supporting resources that help compile information in the dashboard and active channel.

## Viewing the Dashboard

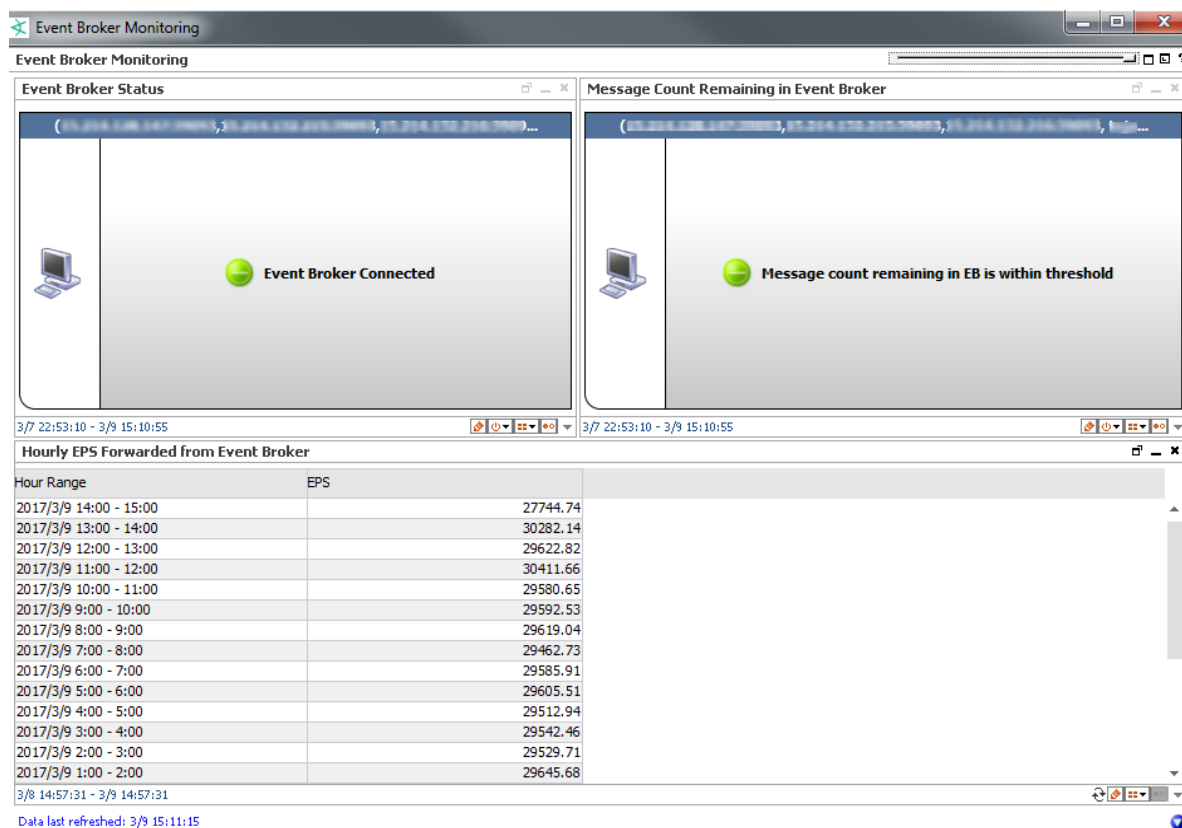
Launch the Event Broker Monitoring dashboard either from the use case, or from the Console's Resources Navigator:

- On the Event Broker Monitoring use case, click the Dashboards link, **Event Broker Monitoring**:



- On the Navigator Resources panel, expand /All Dashboards/ArcSight Administration/ESM/Event Broker Monitoring.
  - Right-click **Event Broker Monitoring** and select **Show Dashboard**, or
  - Double-click **Event Broker Monitoring**.

Following is an example of the Event Broker Monitoring dashboard:



**Note:** If you change the Event Broker host information in the Manager, it will take 24 hours before the host information is completely updated on the data monitors. Query viewer information on hourly EPS rate is up to date because it is refreshed every 15

minutes.


The dashboard includes:

Data Monitors	<ul style="list-style-type: none"><li>• Event Broker Status This is a Last State data monitor. A green circle indicates that ESM is connected to the Event Broker host. If the connection is broken, you should investigate if the Event Broker host itself is up.</li><li>• Message Count Remaining in Event Broker This is a Last State data monitor. It indicates that there are messages in Event Broker that are yet to be consumed by ESM. If the circle is green, the message count is within acceptable thresholds.</li></ul>
Query Viewer	<p>Hourly EPS Forwarded from Event Broker</p> <p>The query viewer displays the total events per second consumed from Event Broker, every hour. It is refreshed every 15 minutes. If you want to update the data manually, click the <b>Refresh</b> button ↺.</p>

## Viewing the Active Channel

Launch the Event Broker Audit Events active channel either from the Event Broker Monitoring use case, or from the Console's Resources Navigator:

- On the Event Broker Monitoring use case, click the Active Channels link, **Event Broker Audit Events**:

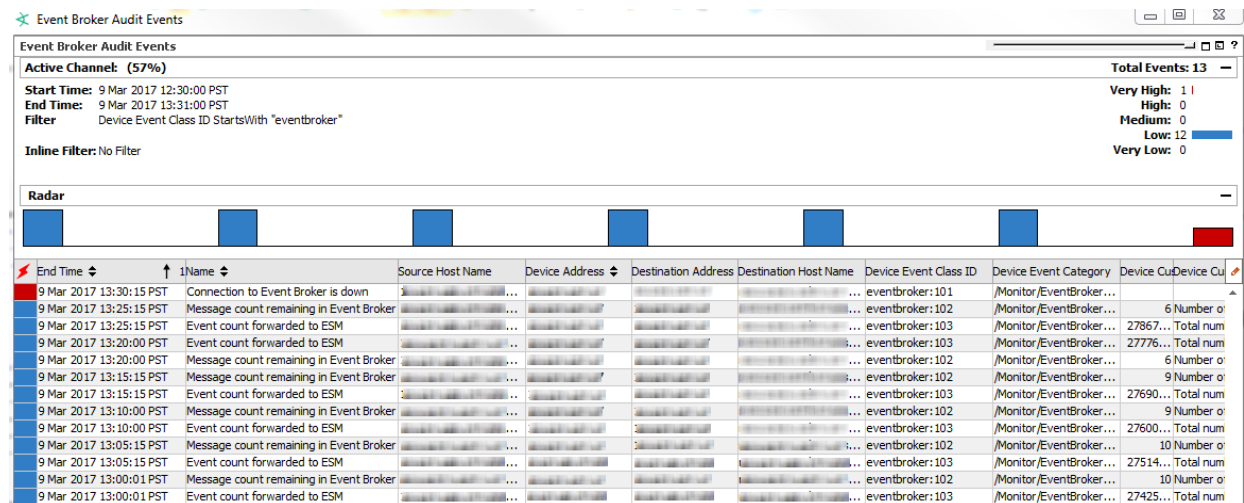
 **Active Channels**  
[Event Broker Audit Events](#)

- On the Navigator Resources panel, expand /All Active Channels/ArcSight Administration/ESM/Event Broker Audit Monitoring.
  - Right-click **Event Broker Audit Events** and select **Show Active Channel**, or
  - Double-click **Event Broker Audit Events**.

Following is an example (a partial view) of the active channel:

# ArcSight Administration and ArcSight System Standard Content Guide

## Chapter 3: ArcSight Administration Content



The Device Event Class ID and Name are among the columns of information displayed on this channel. The Source columns (address and hostname) correspond to the Event Broker host, while the Destination columns correspond to the ESM consumer.

**Tip:** Under Device Event Class ID, look for eventbroker:101, which corresponds to the event name Connection to Event Broker is down. If not followed by eventbroker:100, which corresponds to Connection to Event Broker is started, contact your Event Broker administrator to investigate and fix the connection problem.

## High Availability Monitoring

The High Availability (HA) Monitoring use case lets you monitor the status of ESM systems that are using the optional ESM High Availability Module (HA Module). The HA Module provides for a backup ESM machine with automatic failover capability should the primary ESM machine experience any communications or operational problems.

The HA Monitoring use case is part of the optional ArcSight ESM HA Monitoring content package. This content package is not installed by default on the ArcSight Manager. If you are using the HA Module, you can opt to install the content package during ArcSight Manager installation or from the ArcSight Console any time after installation (right click the **ArcSight ESM HA Monitoring** package in the ArcSight Administration folder on the **Packages** tab in the Navigator and select **Install Package**).

The HA Monitoring use case provides several resources that help you monitor HA events. You can see the current HA status, the current Primary System, all ESM System status changes within the last 24 hours, and the last ten HA status changes.

The HA Monitoring content shows you general HA status information and alerts you to problems. For more detailed diagnostics and troubleshooting, refer to the *ESM High Availability Module User's Guide*.

**Note:** The HA Monitoring content displays data only if you have installed the HA Module and you have set up HA according to the *ESM High Availability Module User's Guide*.

**Important:** The HA Monitoring active channel shows historical data (events generated since ArcSight Manager installation). The HA Monitoring dashboard displays the current status (events arriving in real time). If you install the ArcSight ESM HA Monitoring content package after ArcSight Manager installation when the HA link is established and fully in sync, the HA Monitoring dashboard does not display the current OK status if no new HA events are being generated.

## HA Monitoring Audit Events

The HA Monitoring content uses information from the HA audit events generated by the ArcSight Manager. The Device Event Class ID, Event Name, and Event Message fields in the audit event are displayed in the **HA Monitoring** active channel and the **ESM HA Status** dashboard. The **ESM HA Status** dashboard provides the current HA status, which is derived from the audit event fields. In most cases, the current HA status and the Event Name field of the HA audit event are identical.

The **HA Monitoring** active channel and the **ESM HA Status** dashboard are described in ["Using the HA Monitoring Use Case" below](#)

The following table lists the HA audit events.

Device Event Class ID	Event Name	Event Message
highavailability:100	Primary Manager Started	Manager started up due to HA failover or restart
highavailability:200	HA Status Failed	HA system failure
highavailability:300	DRBD Sync in Progress	Secondary system data syncing in progress <b>Note:</b> DRBD is the Distributed Replicated Block Device.
highavailability:400	iPDU status Failed	iPDU failover control function failed: iPDU agent stopped or cannot communicate with iPDU <b>Note:</b> iPDU is the Intelligent Power Distribution Unit.
highavailability:500	HA Status OK	HA system restored

## Configuring the HA Monitoring Use Case

The HA Monitoring use case includes the **Alert - HA Status Change** rule. This rule triggers when an HA status change event (HA audit event) is generated. After the rule triggers, a notification is sent to the SOC Operators team. Make sure that you have configured notification destinations so that the correct SOC operators are notified when an HA status event is generated. For details on how to configure notification destinations, refer to the *ArcSight Console User's Guide*.

## Using the HA Monitoring Use Case

The **HA Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/HA Monitoring on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides a dashboard, an active channel and a report to help you monitor the status of ESM systems using the optional ESM HA Module. The Library section of the use case lists supporting resources that help compile information in the dashboard, active channel, and report.

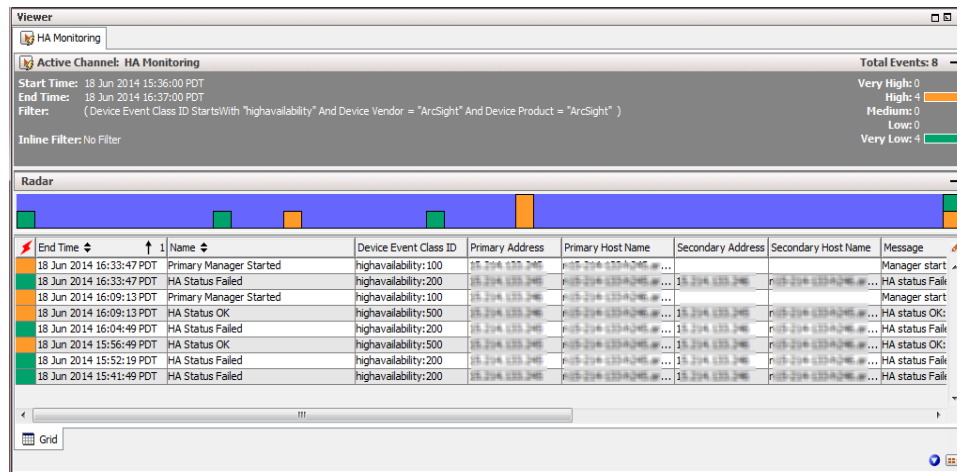
## Viewing the Active Channel

To view the **HA Monitoring** active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel and displays all HA status events

received within the last hour, including information such as when the Primary Manager started, when HA failed, and when HA returned to an OK state.

The active channel shows detailed information about the HA audit events generated by the ArcSight Manager, such as the Device Event Class ID, the Event Name, the Event Message, and other information. The IP address and hostname of both the Primary System and Secondary System are also shown. See ["HA Monitoring Audit Events" on page 61](#) for a list of the audit events generated by the ArcSight Manager.

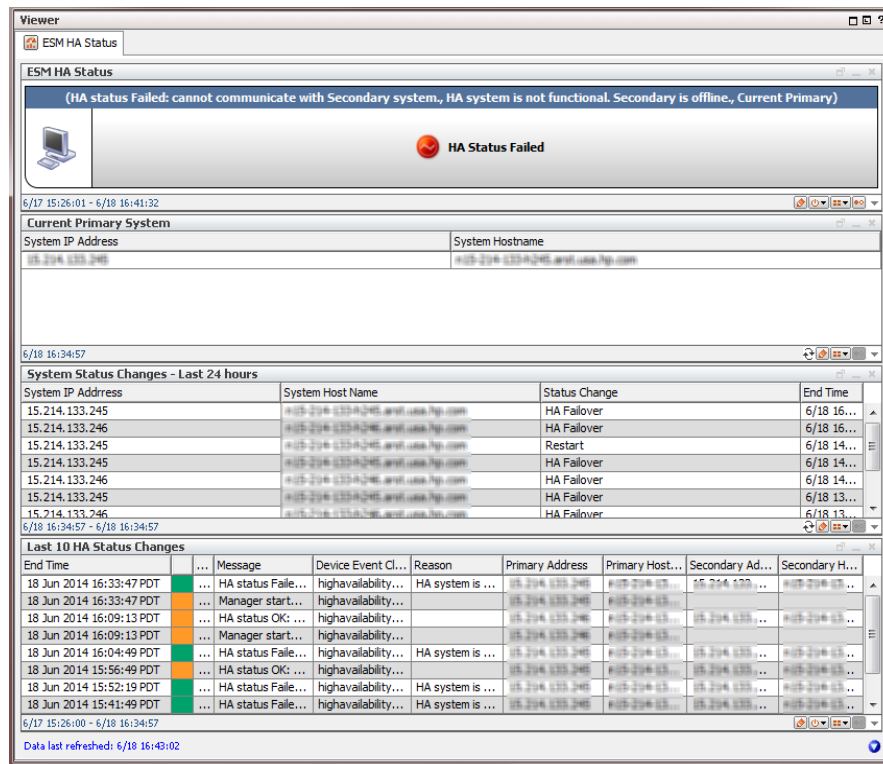
An example of the **HA Monitoring** active channel is shown below.



**Tip:** Double-click an event in the active channel to see details about the event in the Event Inspector.

## Viewing the Dashboard

To view the **ESM HA Status** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel and displays an overview of the ArcSight ESM High Availability (HA) state.



The dashboard data monitors and query viewers are described below.

- The **ESM HA Status** data monitor shows the current HA status (such as HA Status Failed or HA Status OK). The Event Message and event reason from the latest audit event generated by the ArcSight Manager provide additional details and are also displayed at the top of the data monitor.

**Tip:** To find out details about the current Primary System, such as the system hostname, IP address, and start time, click the data monitor heading. When the data monitor heading changes color, right click anywhere in the data monitor and select **Drilldown > Current Primary System**.

To generate a report showing all HA status updates within the last seven days, right click anywhere in the data monitor and select **Drilldown > ESM HA Status - last 7 days**.

The following table describes each HA status alert shown in the middle of the **ESM HA Status** data monitor and provides a description for each, including general troubleshooting tips. "[HA Monitoring Audit Events](#)" on page 61 provides a list of the HA Monitoring audit events and includes the Device Event Class ID, Event Name, and Event Message fields for each event. The current HA status is generated from the audit event fields.



ESM HA Status	Description
<b>HA Status Failed</b>	<p>The Secondary System has become unavailable and cannot assume the role of the Primary System. The audit event is generated every five minutes until the Secondary System is restored.</p> <p>Investigate the failure. Possible causes are:</p> <ul style="list-style-type: none"> <li>• Failure of either network interface card (NIC)</li> <li>• Cross-over cable failure or disconnect</li> <li>• Secondary System failure or shutdown</li> <li>• Secondary System hard drive failure</li> <li>• Secondary System reboot</li> <li>• ArcSight ESM license expired</li> </ul>
<b>HA Status OK</b>	<p>The Secondary System has changed from HA Status Failed to HA Status OK. It might take 30 seconds for the audit event to generate after the Secondary System and high-availability service is restored.</p>
<b>HA Status Unknown</b>	<p>There is a failover and the Secondary System has taken over to become the Primary System, or the Primary System has restarted. This status indicates two situations:</p> <ul style="list-style-type: none"> <li>• The Primary System was restarted but no HA failover occurred.</li> <li>• HA failover occurred and the former Secondary System started up as the Primary System.</li> </ul> <p>This status turns into either "HA Status OK" or "HA Status Failed" a few minutes after the Primary System starts up.</p>
<b>DRBD Sync in Progress</b>	<p>The Distributed Replicated Block Device (DRBD) storage system began the process of synchronizing the Primary and Secondary System hard drives, and continues every five minutes until synchronization is complete. Each audit event includes the amount of data between the two systems that has been synchronized as a percentage until it reaches 100 percent.</p> <p><b>Note:</b> This status is typically short. The system detects the HA status as soon as the Primary System starts up.</p>
<b>iPDU status Failed</b>	<p>The Intelligent Power Distribution Unit (iPDU) agent cannot communicate with the iPDU on either the Primary or Secondary System. The audit events are sent once every five minutes until communication is re-established. After the iPDU status returns to UP, you see the status HA Status OK.</p>

- The **Current Primary System** query viewer shows the IP address and hostname of the current Primary System. Right click on the entry in the table and select **Drilldown > System Status Changes** to see all status changes for the System.
- The **System Status changes - Last 24 Hours** query viewer shows System changes, such as restarts and failovers, within the last 24 hours.
- The **Last 10 HA Status Changes** data monitor shows the last ten HA status changes. Right-click on an entry in the table and select **Drilldown > System Status Changes** to see all status changes for the selected System.

## Running the Report

The HA Monitoring use case provides the **ESM HA Status Updates - last 7 days** report. Run this report to see all HA status updates within the last seven days. You can provide this historical report to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

**Tip:** You can also run the report from the **ESM HA Status** data monitor of the **ESM HA Status** dashboard by right-clicking the data monitor heading and selecting **Drilldown > ESM HA Status - last 7 days**.

## ESM Events

The ESM Events use case provides statistics on the flow of events through the ArcSight system. No configuration is required for this use case.

### Using the ESM Events Use Case

The **ESM Events** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides several dashboards to help you monitor your ArcSight ESM and non-ArcSight ESM events (including event throughput), active channels that show system monitoring events generated by the local ArcSight ESM system and all events generated by ArcSight, and reports that provide historical information about ArcSight events. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

### Viewing the Dashboards

The **ESM Events** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Event Count History** displays the total number of non-ArcSight ESM events within the last seven days and within the last 30 days.
- **Event Overview** displays an overview of non-ArcSightESM events focusing on event counts, events by connector, by vendor and product, and by device IP address.
- **Event Throughput** displays event throughput information in addition to an overview of the system activity related to connectors.
- **Latest Events By Priority** displays event count distribution by priority. Additional detailed event count distribution for low, high, elevated, and severe priority ratings are also shown.

### Viewing the Active Channels

The **ESM Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.

- **ASM Events** shows ArcSight System Monitoring events generated by the local ArcSightESM system.
- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.

## Running Reports

The **ESM Events** use case provides several reports that show information about ArcSight events. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Destination Counts** shows destination details and the sum of event counts for each destination.
- **Event Count by Agent Severity** shows events by agent severity with event counts.
- **Event Count by Source Destination Pairs** shows event counts by source-destination pairs.
- **Event Name Counts** shows event names and their event counts.
- **Events by ArcSight Priority (Summary)** displays a table of all events, grouped by ArcSight priority, showing the count of each event occurrence within that priority. Note: This report shows all ArcSight events; use the `FilterBy` parameter to limit the output to the areas of most interest.
- **Hourly Distribution Chart for Event** shows the hourly distribution of specific events.
- **Hourly Distribution Chart for a Destination Port** shows the hourly distribution of events for destinations with a specific port.
- **Hourly Distribution Chart for a Source Port** shows the hourly distribution of events for sources with a specific port.
- **Hourly Event Counts (Area Chart)** shows the hourly distribution of event counts.

- **Hourly Stacked Chart by ArcSight Priority (3D Stacked Bar Chart)** shows the hourly distribution of events by priority rating.
- **Source Counts by Event Name** shows event names by source address in addition to event counts.
- **Top 10 Events** shows the top events by count.
- **Top 10 Inbound Events** shows the top inbound events by count.
- **Top 10 Outbound Events** shows the top outbound events by count.

## ESM Reporting Resource Monitoring

The ESM Reporting Resource Monitoring use case provides performance statistics for reports, trends, and query viewers. No configuration is required for this use case.

### Using the ESM Reporting Resource Monitoring Use Case

The **ESM Reporting Resource Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards, active channels, and reports to help you monitor, investigate and report on performance statistics for reports, trends, and query viewers. The Library section of the use case lists supporting resources that help compile information in the dashboards, active channels, and reports.

### Viewing the Dashboards

The **ESM Reporting Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Query Running Time Overview** shows the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by query type.
- **Query Viewer Details** shows query details for query viewers.
- **Report Details** shows query details for reports.
- **Reporting Subsystem Statistics** shows an overview of the resources and processing time devoted to reports.
- **Trend Details** shows query details for trends.

### Viewing the Active Channels

The **ESM Reporting Resource Monitoring** use case provides three active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Query Viewer Status** shows all the query viewer-related events received within the last two hours.
- **Reports Status** shows all the report-related events received within the last two hours.

- **Trends Status** shows all the trend-related events within the last two hours. The Trend Name field shows the name of the Trend and the URI. The Trend Infos field shows information on the Trend event.

## Running Reports

The **ESM Reporting Resource Monitoring** use case provides several reports that show information about queries. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Failed Queries** shows the failed queries for trends, reports, and query viewers made within the past week.
- **Longest QueryViewer Queries** shows query duration information for query viewers made during the past week. A chart shows the top ten longest queries for a query viewer and a table shows the duration details for query viewers.
- **Longest Report Queries** shows query duration information for reports made during the past week. The chart shows the ten longest report queries and the table shows the duration details for the report queries.
- **Longest Trend Query** shows query duration information for trends made during the past week. A chart shows the ten longest trend queries and a table shows the duration details for trend queries.
- **Query Counts by Type** shows the number of queries made within the past week, grouped by type.

## ESM Resource Monitoring

The ESM Resource Monitoring use case provides processing statistics for various resources, such as trends, reporting, rules, and data monitors.

## Configuring the ESM Resource Monitoring Use Case

Enable the notification action for the following rules, if appropriate for your organization:

- **Excessive Rule Recursion**
- **Rule Matching Too Many Events**

For information about how to enable notification actions, see the *ArcSight Console User's Guide*.

## Using the ESM Resource Monitoring Use Case

The **ESM Resource Monitoring** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards that show statistics about the rules engine, reporting, queries used for reports and trends, and data monitors.

Also, reports are provided to show information about the resources being used by your ESM system. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

## Viewing the Dashboards

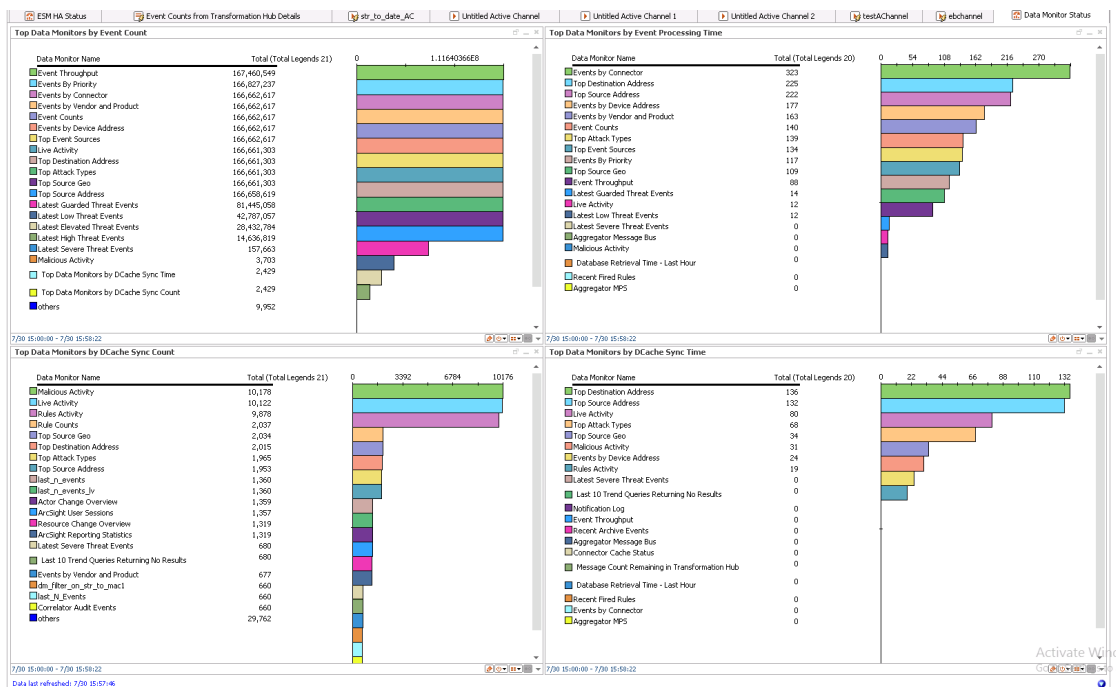
The **ESM Resource Monitoring** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Query Running Time Overview** displays the top ten longest queries for reports, trends, and query viewers. The dashboard also shows query counts by type and query failures during the last 24 hours.
- **Reporting Subsystems Statistics** displays an overview of the resources and processing time devoted to reports.
- **Rules Status** displays information about the rules engine. Detailed information and event count distribution about partial rule matches, top firing rules, recently fired rules, and error logs are shown.



**Note:** The Sortable Rules Stats data monitor on the Rules Status dashboard does not include pre-persistence rules.

- **Data Monitor Status** displays information about the load and performance of data monitors. The dashboard provides information about the top data monitors based on event count, event processing time, distributed cache synchronization count, and distributed cache synchronization time. Data Monitors that cause unusual load on the system and reduce event throughput are likely to be displayed on this dashboard. The Data Monitor Status Dashboard is shown below:



**Note:** Data monitors based on distributed cache synchronization data are visible only when ESM is used in distributed mode.

## Running Reports

The **ESM Resource Monitoring** use case provides several reports that show information about the resources being used by your ESM system. You can provide these historical reports to the stakeholders in your company, when needed.

### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-

term analysis.

3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below:

- **Active List Access** shows active list access statistics. A chart shows the number of added, deleted, and updated active list entries the previous day, grouping the counts by ten-minute intervals. A table shows details of the active list access, grouping the number by time interval and active list name.
- **Correlation Events Statistics** shows information about correlation events. A chart shows the number of correlation events within the last hour, grouping them by ten-minute intervals. A table shows details of the number of correlation events, grouping them by rule name and time interval.
- **Data Monitor Evaluations Statistics** shows a chart with the average number of data monitor evaluations per second.
- **Fired Rule Events** shows all events that were triggered by a rule (correlation events) and includes the number of times the rule triggered and the ESM priority of the event.
- **Invalid Resources** shows a list of resources that are invalid. A chart shows the count of invalid resources by resource type. A table lists all the invalid resources grouped by type and sorted by URI.
- **Number of Events Matching Rules** shows the total number of events matching rules within the last hour, grouping them by ten-minute intervals. A chart shows the number of events matching filter rules, join rules, and the total of both rule types.
- **Rules Engine Warning Messages** shows warning messages received from the rules engine during the past 24 hours.
- **Session List Access** shows session list access statistics. A chart shows the number of added, deleted, and updated session list entries in the last hour, grouping the counts by ten-minute intervals. A table shows the details of the session list access, grouping the number by time interval and active list name.
- **Top Accessed Active Lists** shows the top ten accessed active lists. A chart shows the top ten accessed active lists the previous day, grouping the counts by ten-minute intervals. A table shows the details of the active list access, grouping the number by active list name and time interval.
- **Top Accessed Session Lists** shows the top ten accessed session lists. A chart shows the top ten accessed session lists within the last hour, grouping the counts by ten-minute intervals. A table shows details of the session list access, grouping the number by active list name and time interval.

## ESM Storage Monitoring (CORR-Engine)

The ESM Storage Monitoring (CORR-Engine) use case provides information on the health of the CORR (Correlation Optimized Retention and Retrieval)- Engine. This does not apply if you are using ESM with the Oracle database.

No configuration is required for this use case.

### Using the ESM Storage Monitoring (CORR-Engine) Use Case

The **ESM Storage Monitoring (CORR-Engine)** use case is located in /All Use Cases/ArcSight Administration/ESM/System Health on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and reports to help you monitor and report on database performance and the status of the database archive, including critical archive failures and archive task failures. The Library section of the use case lists supporting resources that help compile information in the dashboards and reports.

### Viewing the Dashboards

The **ESM Storage Monitoring (CORR-Engine)** use case provides two dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **Active Status** displays database archive information.
- **Database Performance Statistics** displays an overview of database related statistics, such as available space, insert, and retrieval times.

### Running Reports

The **ESM Storage Monitoring (CORR-Engine)** use case provides several reports that show information about the ESM Storage Monitoring (CORR) engine. You can provide these historical reports to the stakeholders in your company, when needed.

#### To run a report:

1. Click the link for the report listed in the **Reports** section of the use case.

2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

The reports are described below.

- **Event Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC\_EVENT\_DATA database table space for the last 30 days.
- **System Data Free Space - Last 30 Days** shows the free space percentages by day for the ARC\_SYSTEM\_DATA database table space for the last 30 days.
- **ASM Database Free Space** shows the current free space percentages for the ASM database table spaces. The report shows the percentages for the ARC\_EVENT\_DATA and ARC\_SYSTEM\_DATA table spaces.
- **ASM Database Free Space - by Day** shows the free space percentages by day for each of the ASM database table spaces. The report has one chart and one table, and has a custom parameter that can be used to choose one of the table spaces (ARC\_EVENT\_DATA or ARC\_SYSTEM\_DATA, if this is an Oracle installation, ARC\_EVENT\_INDEX and ARC\_SYSTEM\_INDEX are also available).
- **ASM Database Free Space - by Hour** shows the free space percentages by hour for the ASM database table spaces. The report shows the percentages by hour for the ARC\_EVENT\_DATA and ARC\_SYSTEM\_DATA table spaces.
- **Archive Processing** shows the archives that take the longest to process and the time it takes to archive information.
- **Archive Status Report** shows the current status of archive and disk space used.

## Logger Events

The Logger Events use case provides statistics for events sent through a Logger. No configuration is required for this use case.

### Using the Logger Events Use Case

The **Logger Events** use case is located in /All Use Cases/ArcSight Administration/Logger on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides two active channels to help you investigate Logger application and platform events. The Library section of the use case lists supporting resources that help compile information in the active channels.

### Viewing the Active Channels

The **Logger Events** use case provides two active channels. To view an active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel. The active channels are described below.

- **Logger Application Events** shows all the Logger application events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.
- **Logger Platform Events** shows all the Logger platform events received within the last hour. The active channel displays the Logger user and IP address, and the client address (web browser) for each event.

## Logger System Health

The Logger System Health use case provides performance statistics for any Logger connected to the ArcSight system.

## Configuring the Logger System Health Use Case

If you have a Logger connected to the ArcSight system, configure the Logger System Health use case for your environment as follows:

1. Enable the following rules in the /All Rules/Real-time Rules/ArcSight Administration/Logger/System Health folder:
  - **Logger Sensor Status**—This rule detects Logger system health events related to hardware sensor status. The rule updates the Logger Status and Logger Sensor Type Status active lists with the Logger address, sensor type, sensor name, and sensor status.
  - **Logger Sensor Type Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensors statuses for the same sensor type for a Logger indicate OK.
  - **Logger Status**—This rule detects Logger Sensor Status correlation events and triggers only if all the sensor statuses for a Logger indicate OK.  
For information about enabling rules, refer to the *ArcSight Console User's Guide*.
2. Edit the **My Logger** filter in the /All Filters/ArcSight Administration/Logger/System Health folder. On the **Filter** tab, change the **Device Address** in the condition from the default 127.0.0.1. to the IP address of your Logger.
3. Enable the following data monitors:
  - a. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/CPU and Memory folder:
    - **CPU Usage (Percent) - Last 10 Minutes**
    - **CPU Usage (Percent) - Last Hour**
    - **Memory Usage (Mbytes per Second) - Last 10 Minutes**
    - **Memory Usage (Mbytes per Second) - Last Hour**
  - b. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Hardware folder:
    - **CPU Sensors**
    - **FAN Sensors**

- **System Sensors**

- c. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/My Logger Overview folder:

- **Sensor Type Status**

- d. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Network folder:

- **EPS Usage (Events per Second) - Last 10 Minutes**

- **EPS Usage (Events per Second) - Last Hour**

- **Network Usage (Bytes) - Last 10 Minutes**

- **Network Usage (Bytes) - Last Hour**

- e. Enable the following data monitors in the //Data Monitors/Shared/All Data Monitors/ArcSight Administration/Logger/My Logger/Storage folder:

- **Disk Read and Write (Kbytes per Second) - Last 10 Minutes**

- **Disk Read and Write (Kbytes per Second) - Last Hour**

- **Disk Usage (Percent)**

For information about data monitors, refer to the *Enabling or Disabling a Data Monitor* section in the [ArcSight Console User's Guide](#).

## Using the Logger System Health Use Case

The **Logger System Health** use case is located in /All Use Cases/ArcSight Administration/Logger on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

The Monitor section of the use case provides dashboards and an active channel to help you monitor and investigate the health of the Logger system defined in the **My Logger** filter. The Library section of the use case lists supporting resources that help compile information in the dashboards and active channel.

## Viewing the Dashboards

The **Logger System Health** use case provides several dashboards. To view a dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel. The dashboards are described below.

- **CPU and Memory** shows the CPU and memory usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.
- **Hardware** shows the status for all the hardware sensors on the Logger defined in the My Logger filter. The dashboard includes the CPU Sensors, FAN Sensors, and System Sensors data monitors.
- **My Logger Overview** shows an overview of the hardware, storage, CPU, memory, network, and EPS usage for the Logger defined in the **My Logger** filter.
- **Network** shows the network and EPS usage within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.
- **Storage** shows the disk usage and the disk read/write speed within the last ten minutes and the last hour for the Logger defined in the **My Logger** filter.

## Viewing the Active Channel

The **Logger System Health** use case provides the **Logger System Health Events** active channel, which shows all Logger system health events received within the last hour. To view the active channel, click the link for the active channel in the use case. The active channel opens in the Viewer panel.



## Chapter 4: ArcSight Foundation Content

The ArcSight Foundation content contains Shared Libraries, which are common resources that provide core functionality for common security scenarios. It also contains the resources that you can install with the Manager.

The ArcSight Foundation use cases are listed in the table below.

**Note:** When you perform a new ArcSight Manager installation, not all of the ArcSight Foundation content packages are installed automatically. Some of the packages should be selected manually by you, during 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.

Use Case	Purpose
<b>Security Threat Monitoring</b>	
<a href="#">"Security Threat Monitoring" on the next page</a>	This use case contains the default security threat monitoring content.
<b>Threat Intelligence Platform</b>	
<a href="#">"Threat Intelligence Platform" on page 93</a>	This use case contains resources that detect security attacks based on a threat intelligence feed.

# Security Threat Monitoring

The Security Threat Monitoring package monitors security threats based on security log events from the firewall, IDS/IPS, OS, Application, Scanner, Anti-Virus etc.

**Note:** The Security Threat Monitoring is an optional package. While installing the ESM, you have the option to select this package for installation. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version, you do not have the option to install the Security Threat Monitoring package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.

The Security Threat Monitoring package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases.

This package supports the following use cases:

- Application Monitoring
- Entity Monitoring
- Host Monitoring
- Malware Monitoring
- Network Monitoring
- Perimeter Monitoring
- Vulnerability Monitoring

This package supports the following MITRE ATT&CK tactics:

- TA0001 Initial Access
- TA0002 Execution
- TA0003 Persistence
- TA0004 Privilege Escalation
- TA0005 Defense Evasion
- TA0006 Credential Access
- TA0007 Discovery
- TA0008 Lateral Movement
- TA0010 Exfiltration

- TA0011 Command and Control
- TA0040 Impact

The following MITRE ATT&CK techniques were added to Security Threat Monitoring 2.0:

T1002, T1003, T1028, T1031, T1035, T1038, T1039, T1041, T1047, T1050, T1052, T1053, T1055, T1059, T1061, T1064, T1072, T1078, T1085, T1086, T1087, T1089, T1090, T1091, T1107, T1113, T1114, T1115, T1117, T1118, T1121, T1127, T1129, T1140, T1151, T1168, T1170, T1173, T1175, T1179, T1183, T1191, T1196, T1200, T1203, T1204, T1215, T1216, T1218, T1220, T1223

**Note:** To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

For more information on the supported use cases, tactics, and techniques see [ESM Default Content on the ArcSight Marketplace](#) and [MITRE ATT&CK Navigator](#).

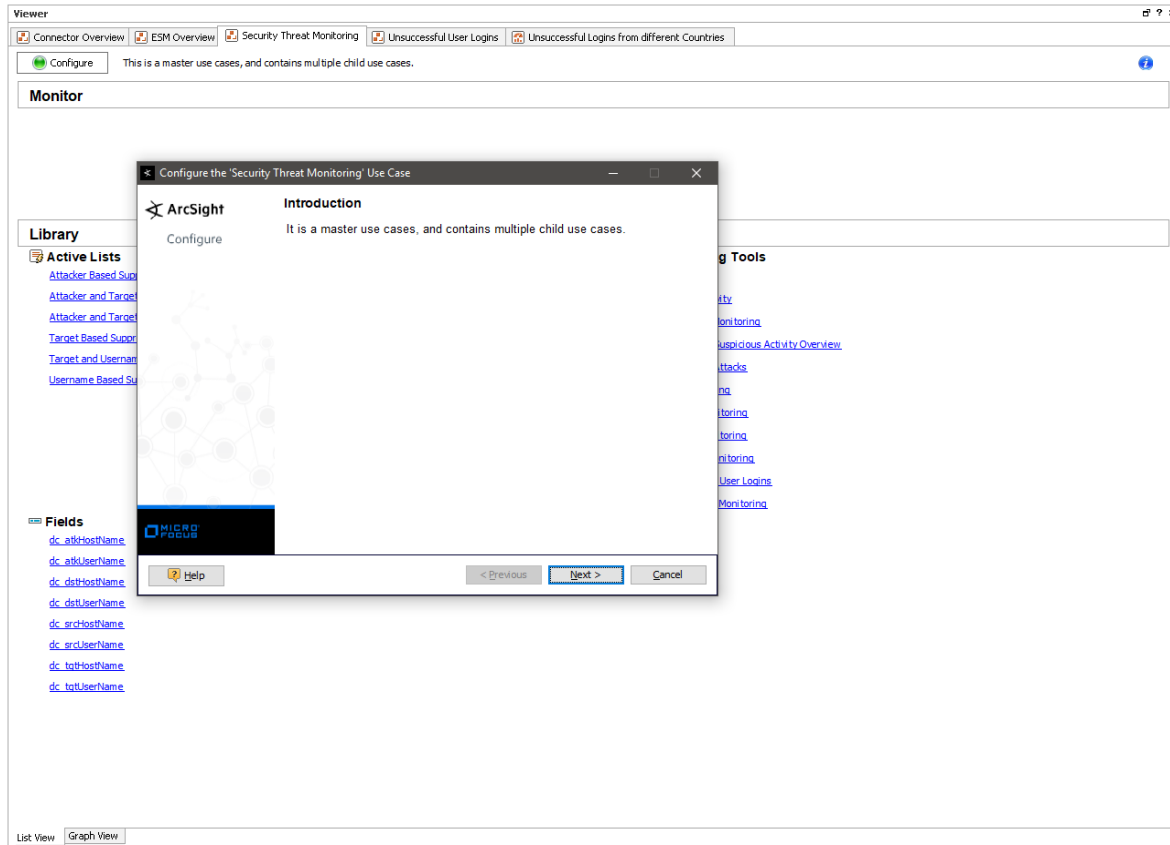
## Configuring the Security Threat Monitoring Use Case

**To configure the Security Threat Monitoring master use case:**

1. Navigate to the **Security Threat Monitoring** use case present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.
2. Double click on the **Security Threat Monitoring** use case. The **Security Threat Monitoring** use case opens in the Viewer panel.
3. On the **Security Threat Monitoring** use case Viewer panel, under the Library section, you can see the active lists and fields. Under the Toolbox section, you can see the child use cases.
4. Click Configure, present just above the Monitor section, to configure the **Security Threat Monitoring** use case. A configuration wizard to guide you through configuration tasks appears on your screen.

# ArcSight Administration and ArcSight System Standard Content Guide

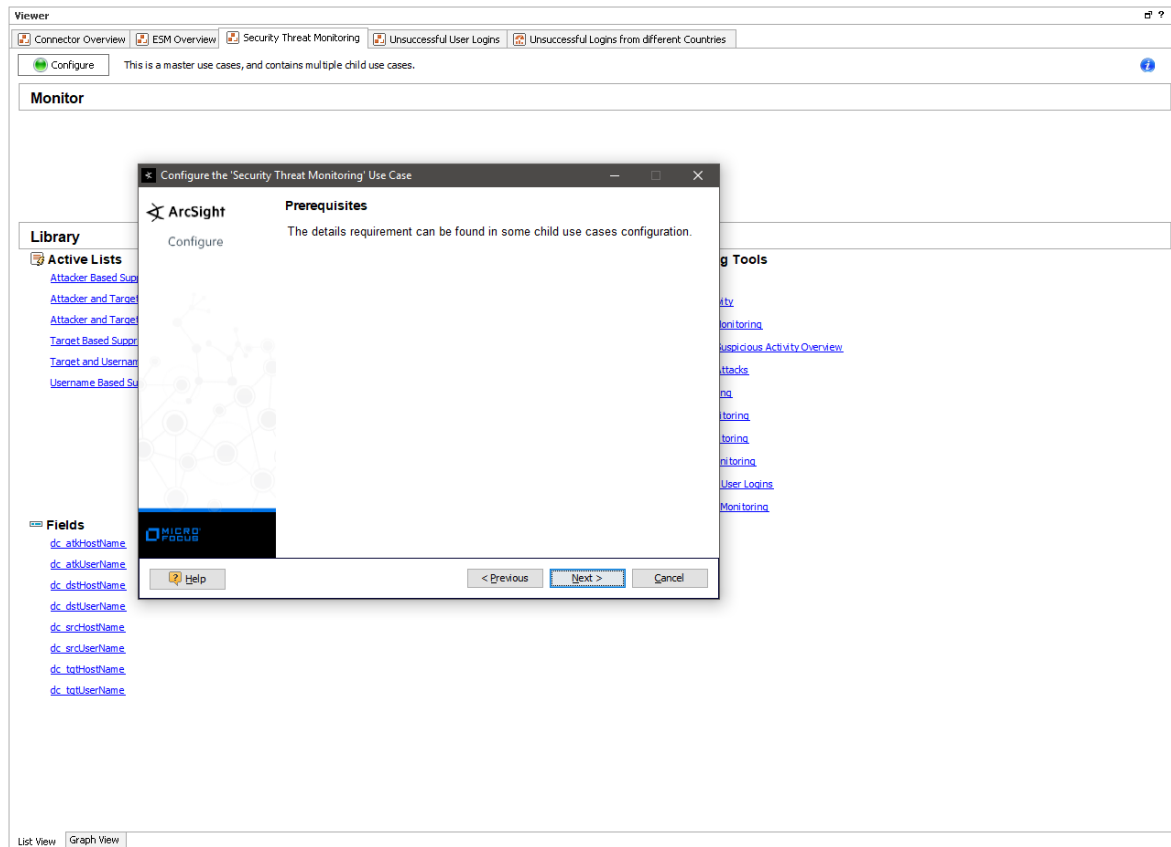
## Chapter 4: ArcSight Foundation Content



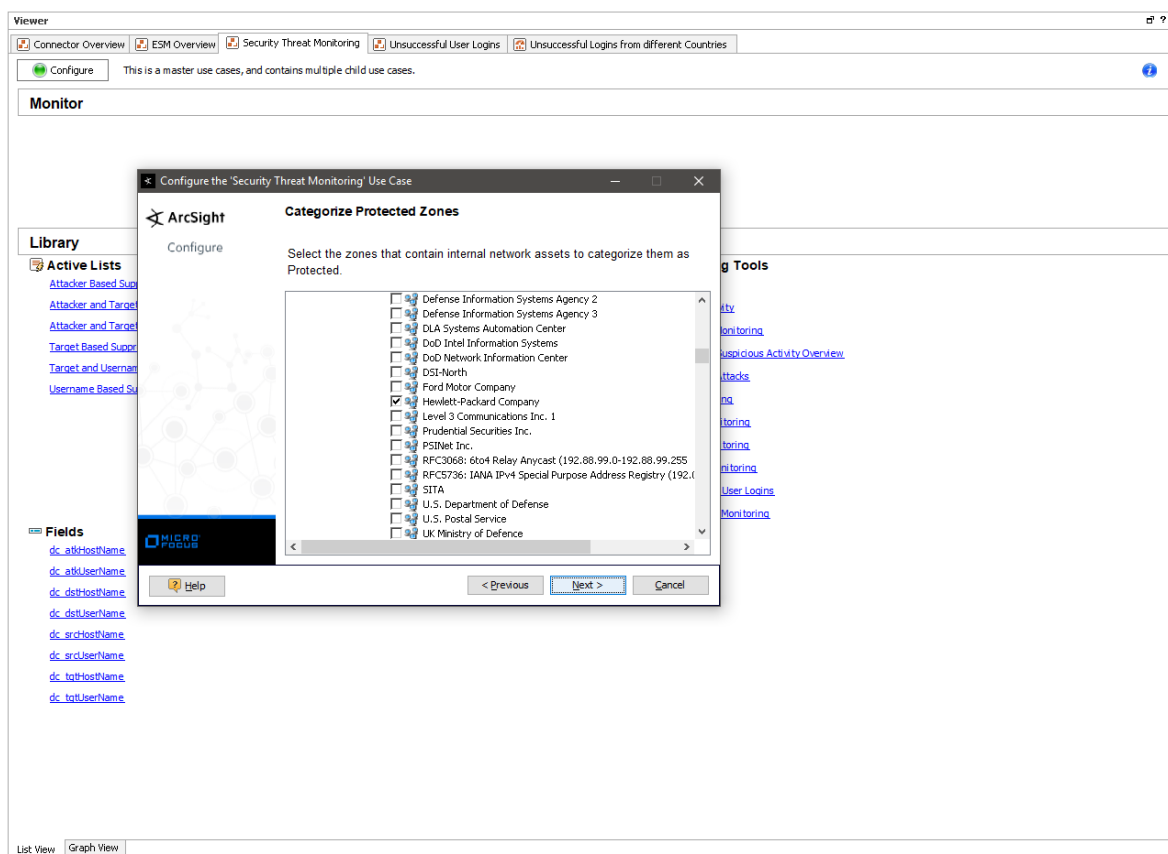
5. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.

# ArcSight Administration and ArcSight System Standard Content Guide

## Chapter 4: ArcSight Foundation Content



6. Click Next. The wizard takes you to the Categorize Protected Zones screen. Select the zones that contain internal network assets to categorize them as Protected.



7. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
8. Click Next to save the configuration settings to the use case resources. The wizard takes you to the Configuration Complete screen.
9. Click Finish.

## Configuring the Child Use Cases

The Security Threat Monitoring package has multiple child use cases. The child use cases for Security Threat Monitoring are given below:

Child Use Cases
<b>Application Monitoring</b>
<ul style="list-style-type: none"><li>• Application Monitoring</li></ul>
<b>Entity Monitoring</b>
<ul style="list-style-type: none"><li>• Account Activity</li><li>• Brute Force Attacks</li><li>• Unsuccessful User Logins</li></ul>
<b>Host Monitoring</b>

<b>Child Use Cases</b>
<ul style="list-style-type: none"><li>• Host Monitoring</li></ul>
<b>Malware Monitoring</b>
<ul style="list-style-type: none"><li>• Malware Monitoring</li></ul>
<b>Network Monitoring</b>
<ul style="list-style-type: none"><li>• Attacks and Suspicious Activity Overview</li><li>• Network Monitoring</li></ul>
<b>Perimeter Monitoring</b>
<ul style="list-style-type: none"><li>• Perimeter Monitoring</li></ul>
<b>Vulnerability Monitoring</b>
<ul style="list-style-type: none"><li>• Vulnerability Monitoring</li></ul>

For your reference, an example to configure the **Unsuccessful User Login** use case is given below.

The **Unsuccessful User Login** use case includes different resources to monitor the below unsuccessful login activities:

- Consecutive Unsuccessful Logins to Administrative Account.
- Consecutive Unsuccessful Logins to Same Account from different Countries.
- Consecutive Unsuccessful Logins to Same Account from different IPs.
- Multiple Failed Login to Different Accounts from Single Source.
- General Unsuccessful Logins.
- Failed Login count by user accounts, source and destination systems.

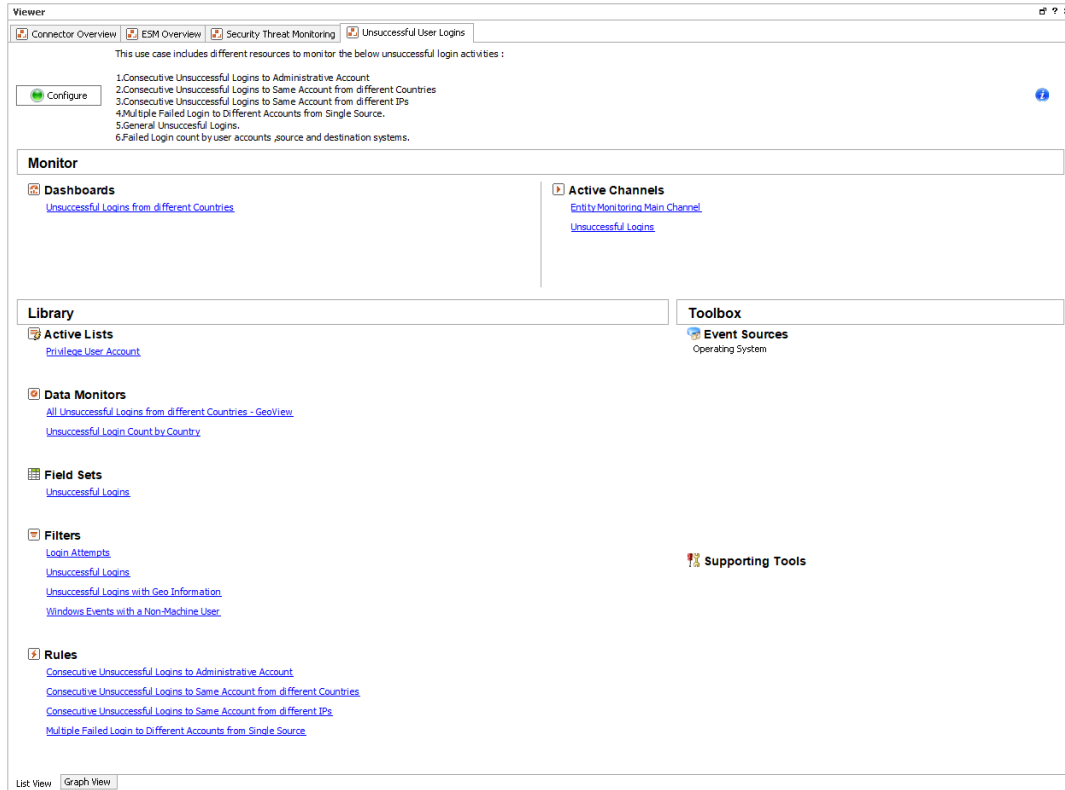
**Note:** If a rule is based on Windows Event ID 4688, ensure that the Audit Process Creation policy is enabled on the Microsoft system you want to monitor. For more information, see Microsoft's documentation.

### To configure the Unsuccessful User Login use case:

1. Navigate to the following location in the ESM Console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/Unsuccessful User Login/.
2. Double click on the **Unsuccessful User Login** use case. The **Unsuccessful User Login** use case opens in the Viewer panel as shown below.

# ArcSight Administration and ArcSight System Standard Content Guide

## Chapter 4: ArcSight Foundation Content

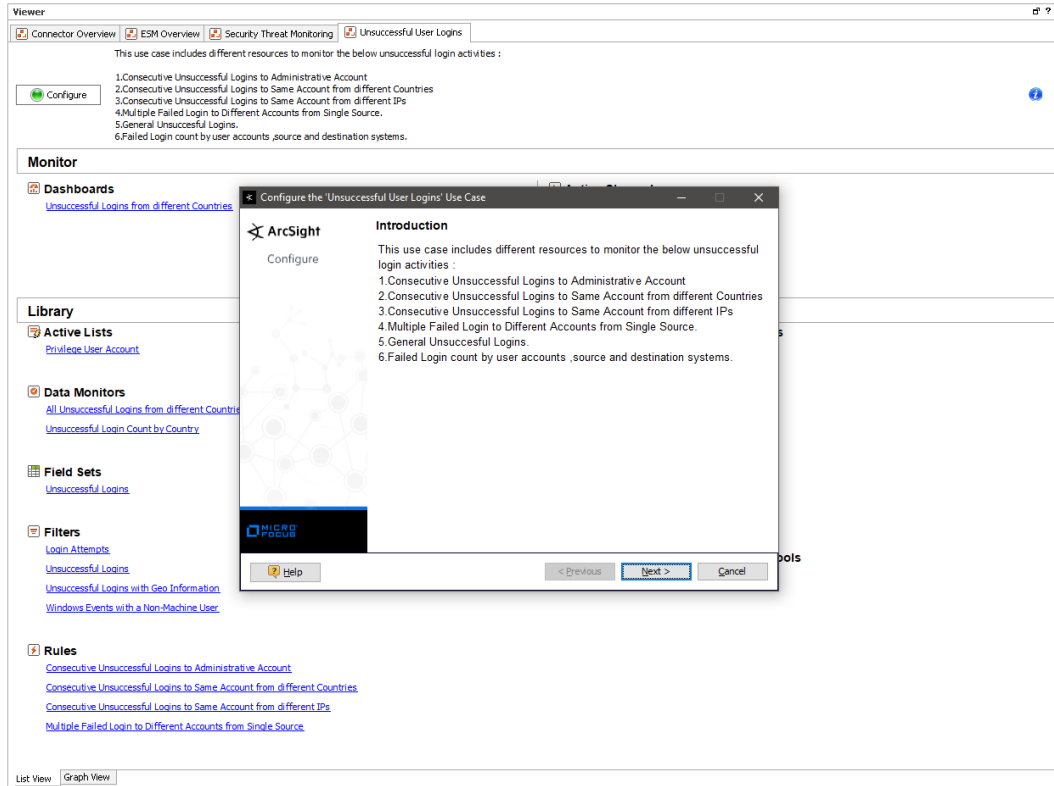


3. On the **Unsuccessful User Login** use case Viewer panel, under the Library section, you can see the associated active lists, data monitors, field sets, filters, and rules. Under the Monitor section, you can see the dashboards and active channels.
4. Click **Configure**, present just above the Monitor section, to configure the **Unsuccessful User Login** use case. A configuration wizard to guide you through configuration tasks appears on your screen.

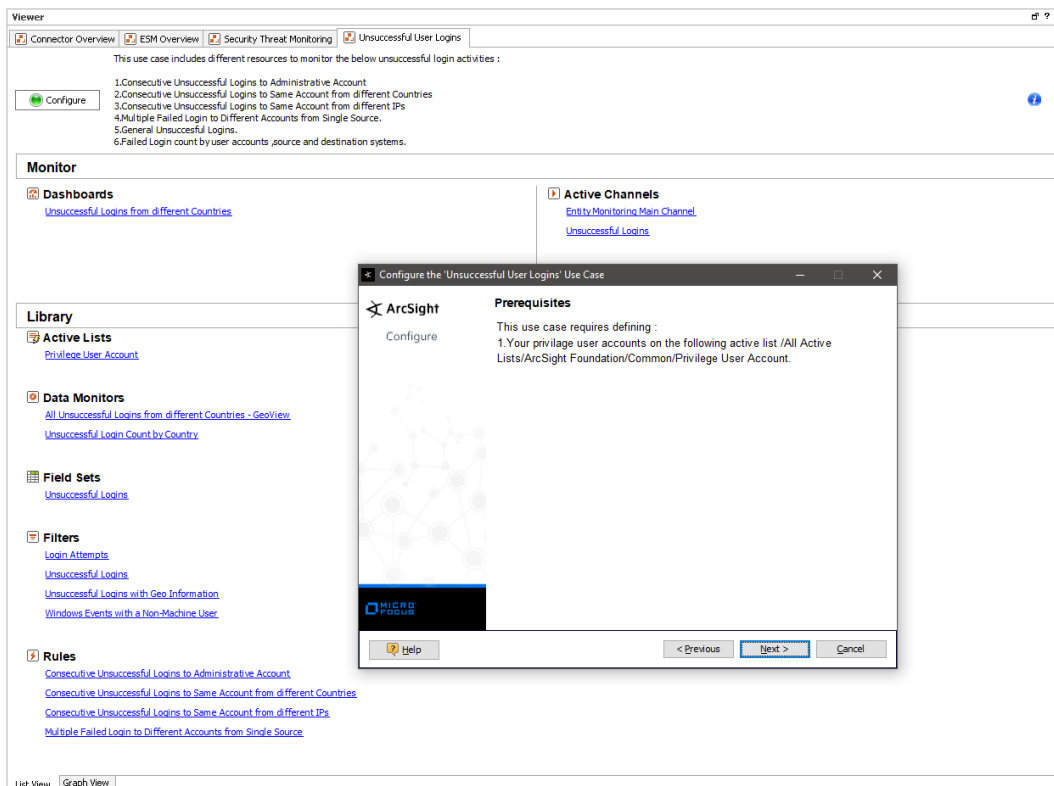


# ArcSight Administration and ArcSight System Standard Content Guide

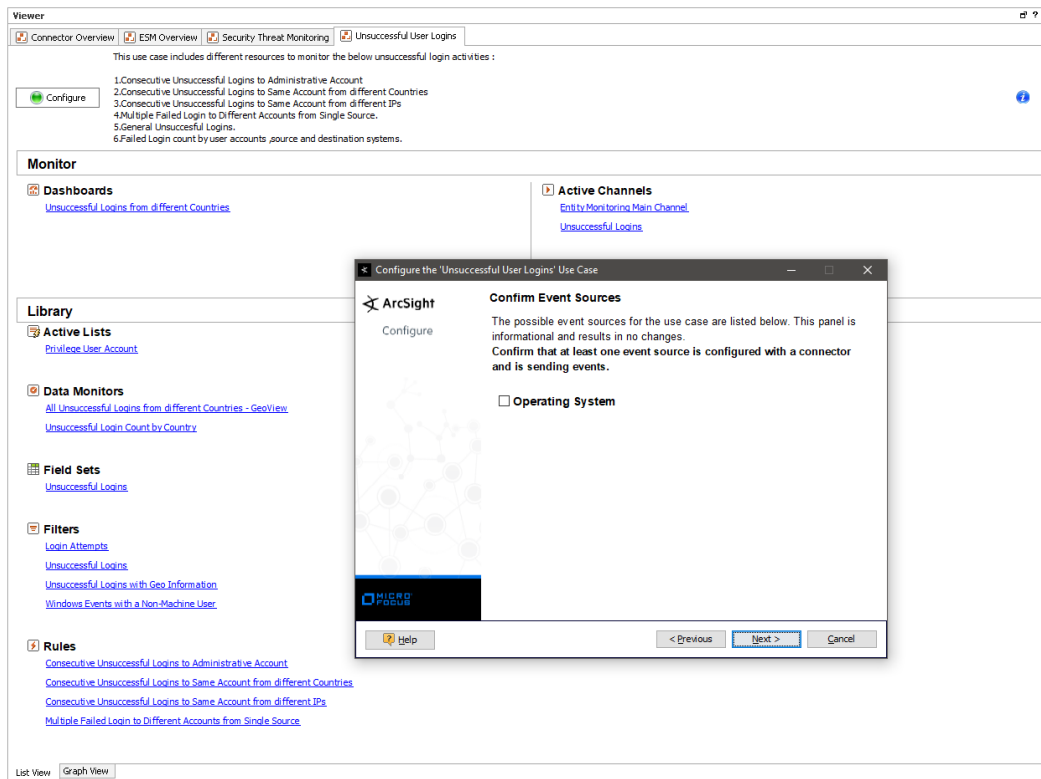
## Chapter 4: ArcSight Foundation Content



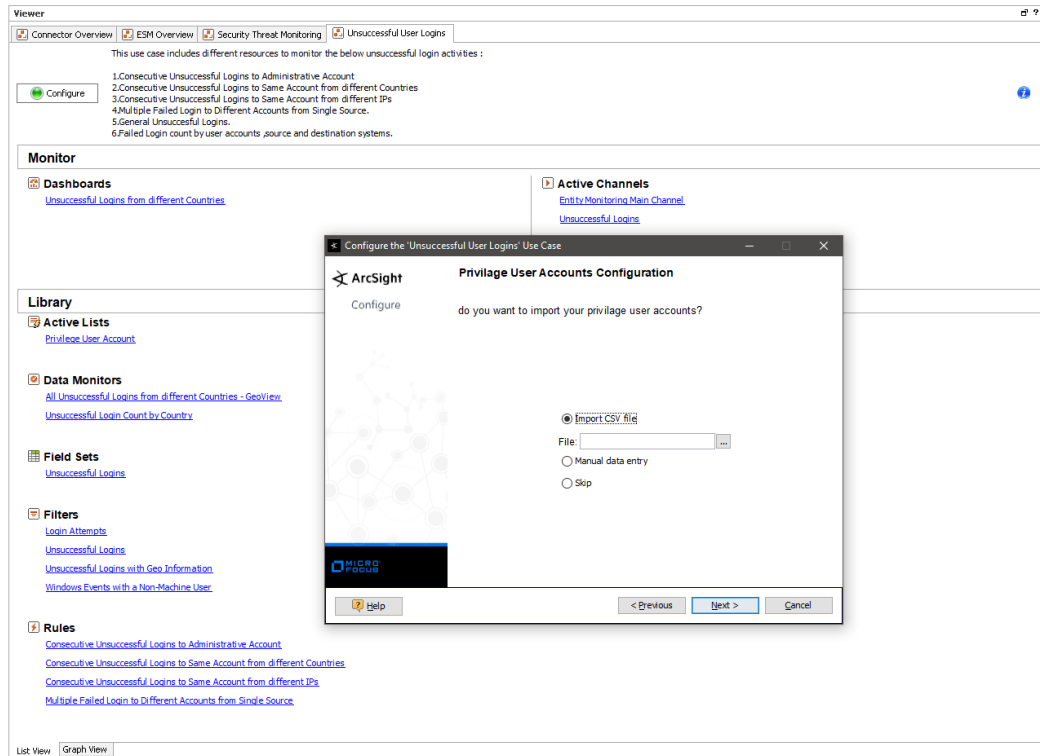
5. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.



6. Click Next. The wizard takes you to the Confirm Event Sources screen. The possible event sources of this use case are listed on this screen. Ensure that at least one event source is configured with a connector and is sending events.



7. Click Next. The wizard takes you to the Privilege User Accounts Configuration screen. You can either import your privilege user accounts or enter the information manually.



8. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
9. Click Next to save the configuration settings to the use case resources. The wizard takes you to the Configuration Complete screen.
10. Click Finish.

## Using the Security Threat Monitoring Use Case

The **Security Threat Monitoring** use case consists of a master use case and multiple child use cases.

The master use case is known as **Security Threat Monitoring** and is present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.

The child use cases for Security Threat Monitoring are present at the following location in the ESM Console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

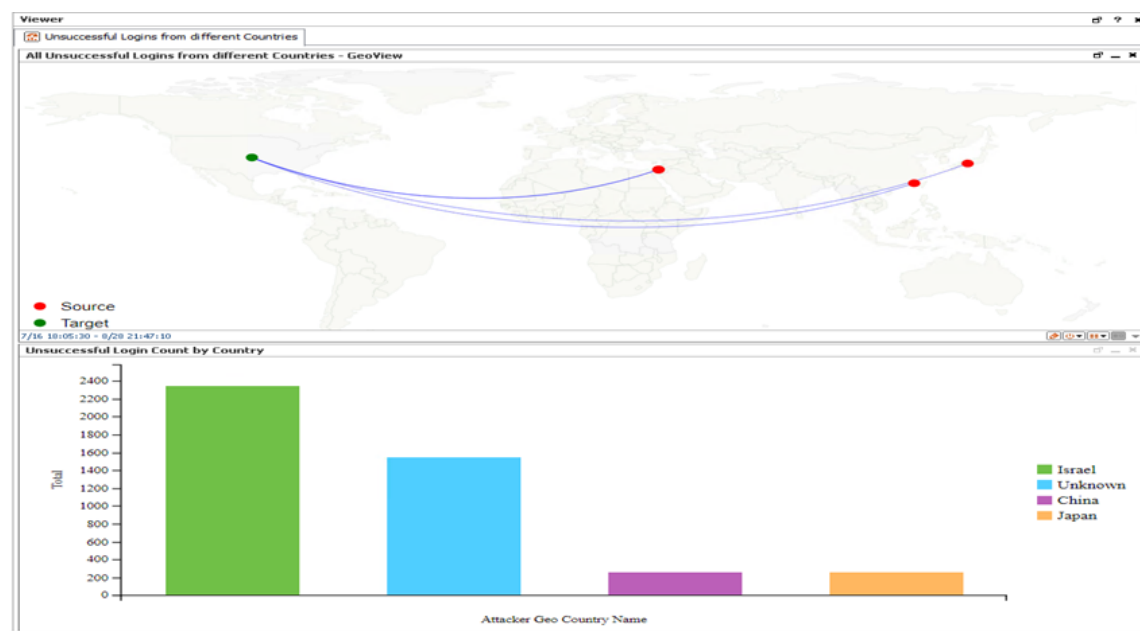
For your reference, an example to use the **Unsuccessful User Login** child use case is given below.

The **Unsuccessful User Login** use case is present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Security Threat Monitoring/Entity Monitoring/.

To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

## Viewing the Dashboard

To view the **Unsuccessful Logins from different Countries** dashboard, click the link for the dashboard in the **Unsuccessful User Login** use case. The dashboard opens in the Viewer panel as shown below:



The **Unsuccessful Logins from different Countries** dashboard shows the following:

- All Unsuccessful Logins from different Countries.
- Unsuccessful Login Count by Country.

# Threat Intelligence Platform

The Threat Intelligence Platform package contains resources that detect security attacks based on a threat intelligence data feed. This package uses Malware Information Sharing Platform (MISP) as a threat intelligence data feed. The threat intelligence data feed from MISP is directly imported to the ESM using the Model Import Connector (MIC). This package requires installation of MIC for MISP. For more information on MIC, see [Model Import Connector for MISP](#).

**Note:** The Threat Intelligence Platform package is an optional package. You have the option to select this optional package for installation while installing the ESM. If you do not select this package while installing the ESM, the package is imported (not installed), and it appears inactive (greyed out) in the ESM. If you are upgrading your ESM from a previous version to the current version, you do not have the option to install the Threat Intelligence Platform package. However, this package is imported during upgrade, and then you can right click on the package to install it after upgrade.

The Threat Intelligence Platform package follows the MITRE ATT&CK framework, which supports many MITRE ATT&CK tactics, techniques, and use cases.

This package supports the following use cases:

- Botnet Activity
- Dangerous Browsing
- Internal Asset Found in Reputation List
- Phishing
- Ransomware
- Suspicious Activity
- Suspicious DNS Query
- Suspicious Email
- Suspicious File Hash

This package supports the following MITRE ATT&CK tactics:

- TA0001 Initial Access
- TA0011 Command and Control
- TA0040 Impact

The following MITRE ATT&CK techniques were added to Threat Intelligence Platform 2.0:

T1043, T1065, T1092, T1193

**Note:** To customize a rule so that it works with the ArcSight MITRE ATT&CK content, see [Customizing Rules to Work with ArcSight MITRE Package](#).

For more information on the supported use cases, tactics, and techniques see [ESM Default Content on the ArcSight Marketplace](#) and [MITRE ATT&CK Navigator](#).

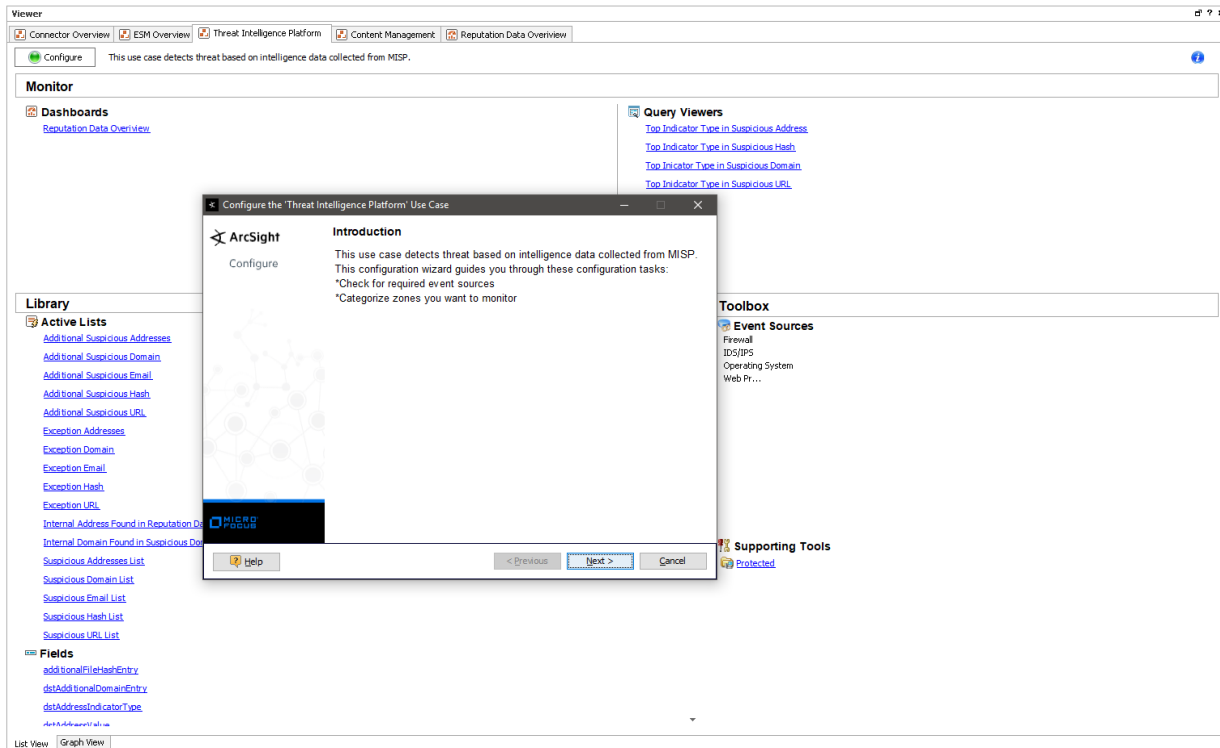
## Configuring the Threat Intelligence Platform Use Case

To configure the Threat Intelligence Platform use case:

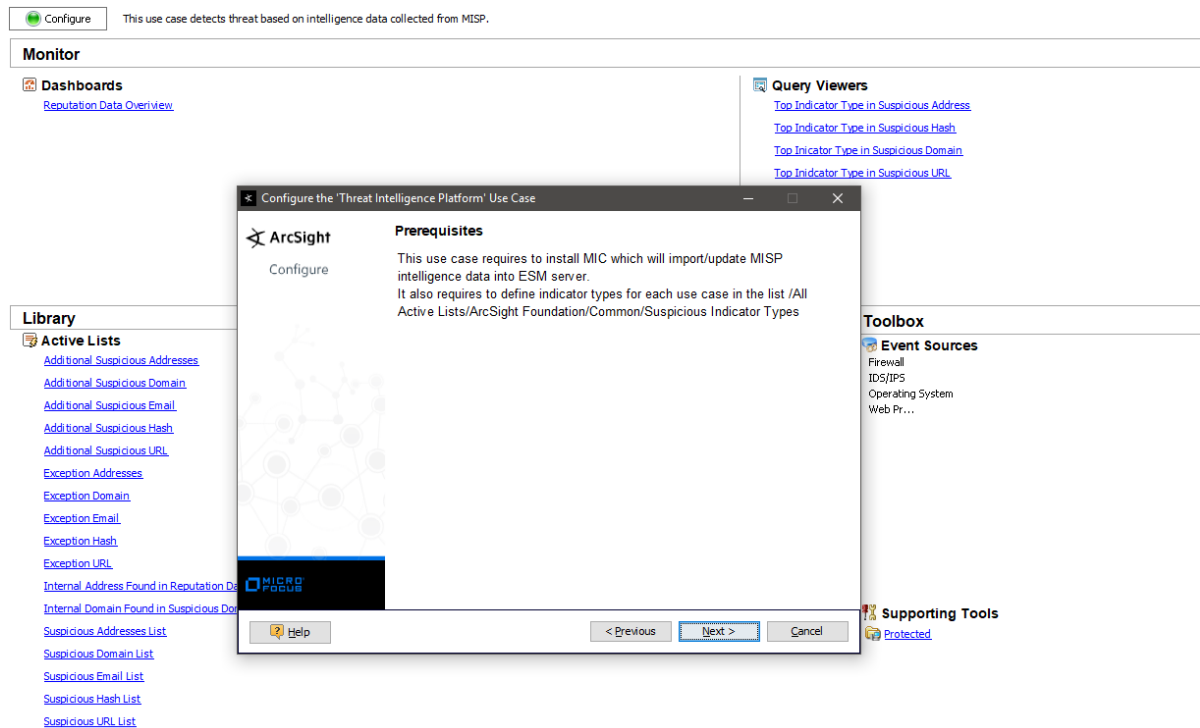
1. Navigate to the **Threat Intelligence Platform** use case present at the following location in the ESM console: /All Use Cases/ArcSight Foundation/Threat Intelligence Platform/.
2. Double click on the **Threat Intelligence Platform** use case. The **Threat Intelligence Platform** use case opens in the Viewer panel.
3. On the **Threat Intelligence Platform** use case Viewer panel, under the Library section, you can see the active lists, fields, filters, and rules. Under the Toolbox section, you can see the event sources and supporting tools. Under the Monitor section, you can see the dashboards and query viewers.
4. Click Configure, present just above the Monitor section, to configure the **Threat Intelligence Platform** use case. A configuration wizard to guide you through configuration tasks appears on your screen.

# ArcSight Administration and ArcSight System Standard Content Guide

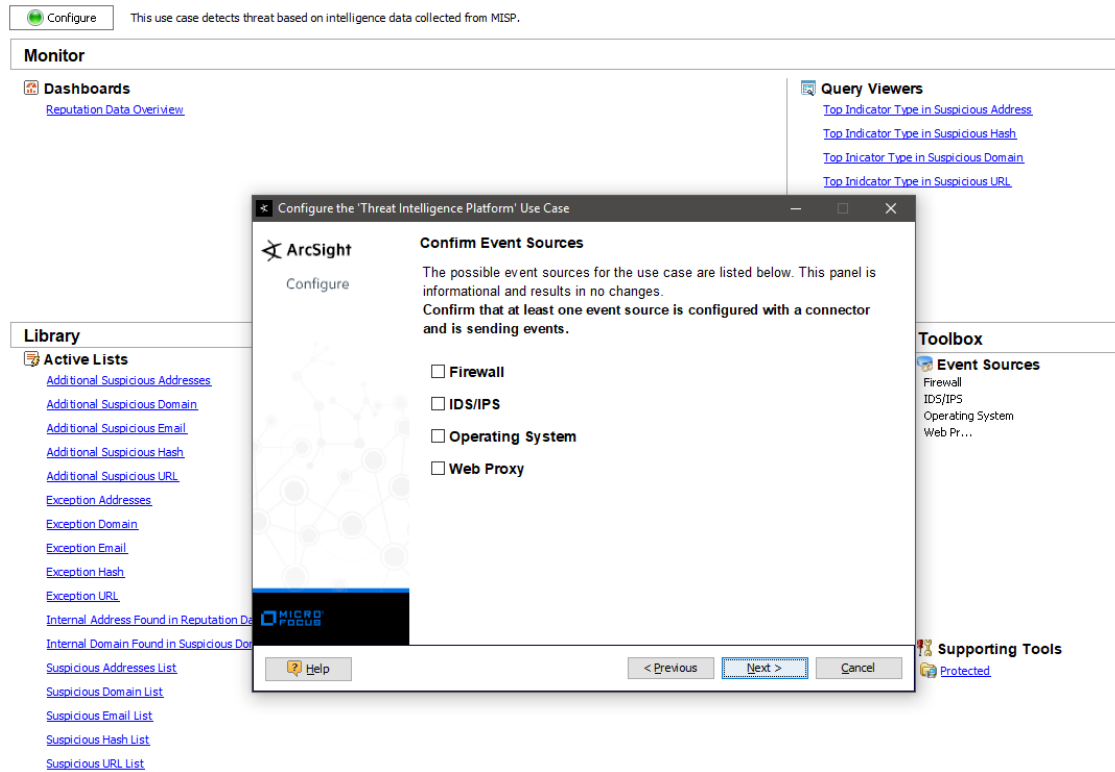
## Chapter 4: ArcSight Foundation Content



5. This configuration wizard guides you through the following configuration tasks:  
**Check for required event sources** and **Categorize zones you want to monitor**.
6. Click Next. The wizard takes you to the Prerequisites screen. Ensure you have all the prerequisites to go ahead with the configuration of this use case.

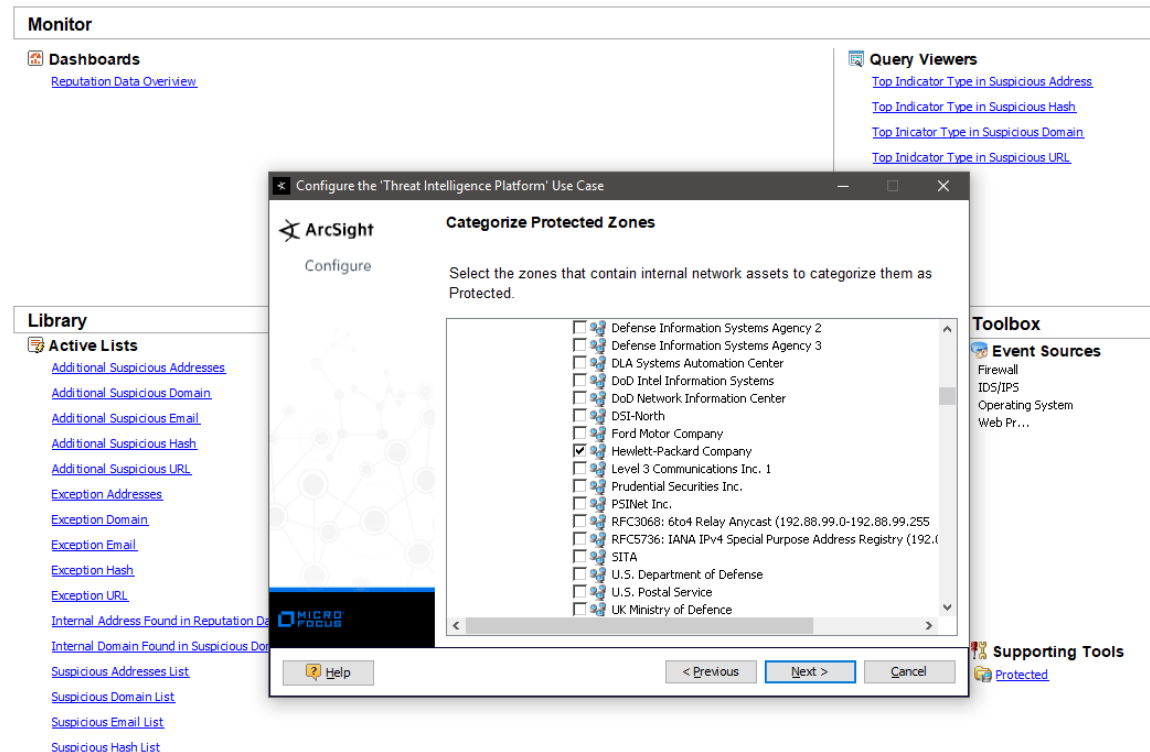


- Click Next. The wizard takes you to the Confirm Event Sources screen. The possible event sources of this use case are listed on this screen. Ensure that at least one event source is configured with a connector and is sending events.



- Click Next. The wizard takes you to the Categorize Protected Zones screen. Select the zones that contain internal network assets to categorize them as Protected.





9. Click Next. The wizard takes you to the Summary of Settings to Apply screen.
10. Click Next to save the configuration settings to the use case resources. The wizard takes you to the **Configuration Complete** screen.
11. Click Finish.

## Using the Threat Intelligence Platform Use Case

The **Threat Intelligence Platform** use case is located at /All Packages/ArcSight Foundation/Threat Intelligence Platform on the **Use Cases** tab of the Navigator. To open the use case, either double-click the use case or right-click the use case and select **Open Use Case**. The use case displays in the Viewer panel.

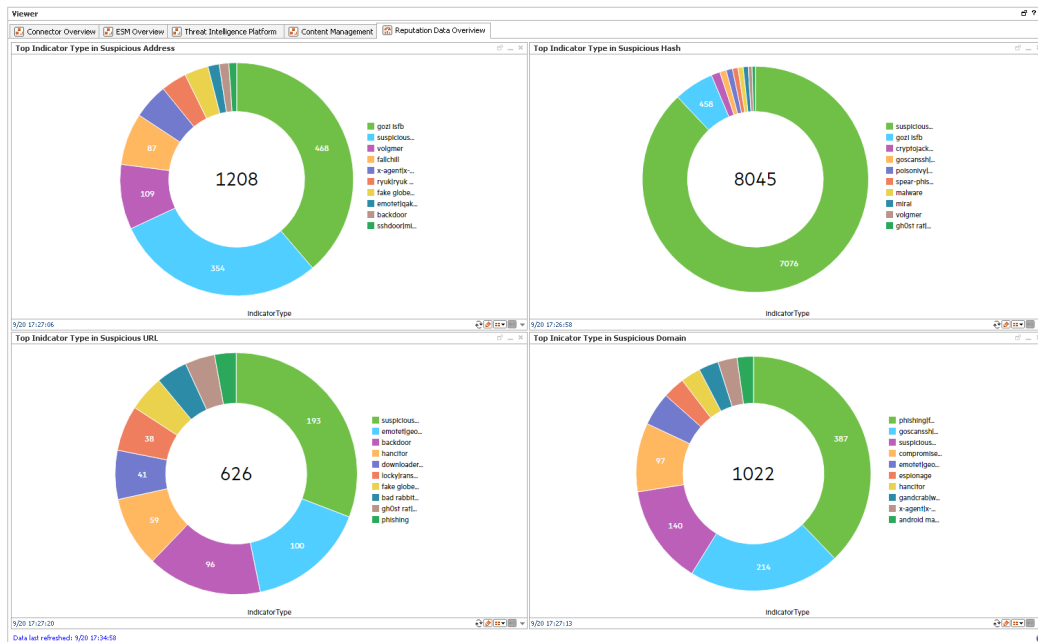
**Note:** For this use case, install MIC, which imports/updates MISP intelligence data into the ESM server. Also, define indicator types for each use case in the list /All Active Lists/ArcSight Foundation/Common/Suspicious Indicator Types.

## Viewing the Dashboard

You can view the following dashboards in the Threat Intelligence Platform package:

- Reputation Data Overview
- Threat Intelligence Overview

To view the **Reputation Data Overview** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel as shown below:



The **Reputation Data Overview** dashboard shows the following:

- The top Indicator Type in Suspicious Address.
- The top Indicator Type in Suspicious Hash.
- The top Indicator Type in Suspicious URL.
- The top Indicator Type in Suspicious Domain.

To view the **Threat Intelligence Overview** dashboard, click the link for the dashboard in the use case. The dashboard opens in the Viewer panel as shown below:

The **Threat Intelligence Overview** dashboard shows the following:

- Threat Intelligence Alerts by Type
- Last 20 Threat Intelligence Alerts
- Top Threat Intelligence Alerts by Target
- Top Threat Intelligence Alerts by Attacker

**Note:** To view detailed information about each graphic view in the **Threat Intelligence Overview** dashboard, use the drill-down feature present in each of the graphic views. To use the drill-down feature, right-click on the graphic view for which

you want to view the detailed information.

# Chapter 5: ArcSight System Content

The ArcSight System content consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for default functionality. Resources that manage core functionality are **locked** to protect them from unintended change or deletion.

In this section, the ArcSight System resources are grouped together based on the functionality they provide. The ArcSight System resource groups are listed in the table below.

Resource Group	Purpose
<a href="#">"Actor Support Resources" on the next page</a>	Includes resources that support the actors feature.
<a href="#">"Priority Formula Resources" on page 102</a>	Includes resources that directly or indirectly affect the Priority Formula.
<a href="#">"System Resources" on page 104</a>	Includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

# Actor Support Resources

The actors feature maps people and their activity to events from applications and network assets by leveraging user attributes defined within identity management systems, and correlating them with user account information from the user authentication systems in your network. Correlating user identifiers from the event traffic that reflects their activity throughout the day makes it possible to ensure that users are doing role-appropriate activity across the assets in your organization, and to detect and track inappropriate access and suspicious activity. For more information on Actors, see the *ArcSight Console User's Guide*.

**Note:** Actors are a licensed feature; they do not apply to every environment.

## Using the Actor Support Resources

The actor support resources consist of several reports located in the /All Reports/ArcSight System/Core/ folder on the **Resource** tab of the Navigator:

- **Actor Context Report by Target Username** shows activity related to an actor based on the ActorByTargetUserName global variable.
- **Actor Context Report by Account ID** shows activity related to an actor based on the ActorByAccountID global variable.
- **Actor Context Report by Attacker Username** shows activity related to an actor based on the ActorByAttackerUserName global variable.
- **Actor Context Report by Custom Fields** shows activity related to an actor based on the ActorByCustomFields global variable.

### To run a report:

1. Right-click the report in the Navigator tree on the **Resource** tab and select **Run**.
2. In the Report Parameters dialog, set the parameters, then click **OK**. For example, you can change the report format from HTML (the default) to pdf, csv, xls, or rtf, change the page size, and update the report start and end time for longer- or shorter-term analysis.
3. The HTML report opens automatically in your browser. For formats other than HTML, either open the report or save the report to your computer when prompted.

# Priority Formula Resources

The Priority Formula Resources group includes resources that directly or indirectly affect the Priority Formula. The Priority Formula is a series of five criteria against which each event is evaluated to determine its relative importance, or urgency, to your network. The Priority Formula is also referred to as the Threat Level Formula. For more information about the Priority Formula, refer to the *ArcSight Console User's Guide* or the *ESM 101* guide.

There are no monitoring resources for the priority formula. However, there are several rules that detect successful hostile attempts and identify correlation events that originate from other reconnaissance rules. See ["Priority Formula Rules" below](#).

## Configuring the Priority Formula Resources Group

Configure the following active lists:

- Populate the **Trusted List** active list with the IP sources on your network that are known to be safe.
- Populate the **Untrusted List** active list with the IP sources on your network that are known to be unsafe.

For more information about working with active lists, see ["Configuring Active Lists" on page 14](#).

**Note:** You can set up rules to add and remove entries from the **Trusted List** and **Untrusted List** active lists dynamically. The information in these active lists is then used in the Priority Formula.

## Priority Formula Rules

The Priority Formula resources consist of several rules located in the /All Rules/ArcSight System/ folder on the **Resource** tab of the Navigator.

- **Reconnaissance - Attackers** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events from an attacker. The rule adds the attacker to the Reconnaissance List active list.
- **Reconnaissance - Targets** identifies correlation events that originate from other reconnaissance rules. The events signify successful reconnaissance events targeted by an external attacker to an internal asset. The rule adds the target information into the Scanned List active list.
- **Compromise - Success** detects any successful attempt to compromise a device from

a source that is not listed in the Trusted List active list, with either the attacker information (zone and address) or the target information present. The rule triggers whenever an event is categorized as Success and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List and Infiltrators List active lists, and the target address is added to the Compromised List and Hit List active lists.

- **Hostile - Attempt** detects any hostile attempt on a device that is not already compromised from a source that is not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Attempt and Hostile, and the target does not belong to a compromised active list.
- **Hostile - Success** detects any successful hostile attempts on a device that is not already compromised from a source not listed in the Trusted List active list. The rule triggers whenever an event is categorized as Success and Hostile, and the target does not belong to a compromised active list. On the first event, the severity is set to medium, the attacker address is added to the Infiltrators List active list, the target address is added to the Compromised List active list, and the target information is removed from Hit List active list.
- **Compromise - Attempt** detects any attempt to compromise a device from a source that is not listed in a trusted active list. The rule triggers whenever an event is categorized as Attempt and Compromise. On the first event, agent severity is set to high, the attacker address is added to the Hostile List active list, and the target address is added to the Hit List active list.
- **Incident Resolved - Remove From List** detects a Resolved message in an ArcSight Data Monitor Value Change event from the Attacked or Compromised Systems data monitor (in the Executive View dashboard), which is sent when a user marks an asset within the data monitor as resolved. This rule only triggers if you have the Intrusion Monitoring package installed from a previous ESM release.

## System Resources

The System Resources group includes resources that are either required by the system to operate or are customizable so you can adjust the behavior of the system.

## Configuring System Resources

Configure the following filters:

- Modify the **Connector Asset Auto-Creation Controller** filter to specify which assets to exclude from the asset auto creation feature.  
The **Connector Asset Auto Creation Controller** filter directs the creation of an asset for network nodes represented in events received from the connectors present in your environment. By default, the **Connector Asset Auto Creation Controller** filter is configured with the generic condition `True`, which matches all events. You can exclude connectors from a specific zone, such as a VPN zone, (where the asset already exists, but traffic is coming into the network from an alternate VPN interface). You can also exclude traffic from different types of connectors, such as from a particular device and vendor. For more information about asset auto creation, refer to the *ArcSight Console User's Guide*.
- Modify the **Device Asset Auto-Creation Controller** filter.  
ArcSight creates assets in the asset model automatically for events whose devices are not already modeled either manually or using an asset scanner. Depending on what devices you have reporting to ArcSight and what devices report in to your network, this can cause more individual assets to be added to your asset model than necessary. For example, every time a laptop logs onto the network via a VPN or wireless network, a new asset ID is generated for that device. By default, the **Device Asset Auto Creation Controller** filter is configured with the generic condition `True`, which matches all events. Configure this filter to specify traffic from specific devices and device vendors, or event categories, such as `Hostile`. When you specify an event category, the filter directs the system to only create assets for events with this severity.
- Modify the **SNMP Trap Sender** filter if you have the SNMP Trap Sender enabled to forward events through SNMP to a network management system.  
By default, this filter is configured with the `/ArcSight System/Event Types/ArcSight Correlation Events` filter. If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events are trapped and forwarded to the network management system.  
To configure this filter to forward certain events as an SNMP trap, change the default condition in the **SNMP Trap Sender** filter to specify which events are forwarded as traps. You can express this condition directly in the **SNMP Trap Forwarding** filter, or you can create another filter that expresses these parameters and point to it in the



SNMP Trap Sender filter. To enable the SNMP trap sender, refer to the *ArcSight ESM Administrator's Guide*.

## Using the System Resources

The System Resources group consists of several active channels that show events received by ArcSight ESM over different periods of time, two reports that are used by the ArcSight console for internal processing, and several integration commands that you can use in ArcSight ESM active channels and dashboards.

### Viewing the Active Channels

The System Resources group provides several active channels located in the /All Active Channels/ArcSight System/ folder on the **Resource** tab of the Navigator. To open an active channel, right-click the active channel in the resource tree and select **Show Active Channel**. The active channels are described below:

- **System Events Last Hour** shows all events generated by ArcSight during the last hour. A filter prevents the active channel from showing events that contributed to a rule triggering, commonly referred to as correlation events.
- **Today** shows all events received today since midnight. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events.
- **Last 5 Minutes** in /All Active Channels/ArcSight System/All Events shows events received during the last five minutes. The active channel includes a sliding window that always displays the last five minutes of event data.
- **Last Hour** in /All Active Channels/ArcSight System/All Events shows events received during the last hour. The active channel includes a sliding window that always displays an hour of event data.
- **Live** in /All Active Channels/ArcSight System/Core shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlated events.
- **Personal Live** in /All Active Channels/ArcSight System/Core shows events received during the last two hours. The active channel includes a sliding window that always displays the last two hours of event data. A filter prevents the active channel from showing events that contributed to the triggering of a rule, commonly referred to as correlation events. This active channel also hides all the events that have been assigned to the current user.

## Reports

The System Resources group consists of two reports located in the /All Reports/ArcSight System/Core/ folder on the **Resource** tab of the Navigator:

- **Assets having Vulnerabilities** is used by the ArcSight Console for internal processing; do not run this locked report.
- **Selected Case Report** is a basic report template for case management. Refer to the *ArcSight Console User's Guide* topic on "Creating a Report on a Case."
- **Vulnerabilities of an Asset** is used by the ArcSight Console for internal processing; do not run this locked report.

## Integration Commands

ArcSight ESM provides several integration commands; a set of tools that make it possible to invoke scripts and utilities directly from the ArcSight Console. You can use these commands directly from dashboards and active channels. You can edit these commands from the /All Integration Commands/ArcSight System/Tools folder in the Resource tree of the Navigator panel.

- **Nslookup (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find details about an IPv4 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.
- **Nslookup-IPV6 (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find details about an IPv6 hostname in the Domain Name System (DNS). Use this command from an ArcSight Console running Linux.
- **Nslookup (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to find details about a Domain Name System (DNS). Use this command from an ArcSight Console running Windows.
- **Ping (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to test whether a particular host is reachable across an IPv4 network. Use this command from an ArcSight Console running Linux.
- **Ping6 (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to test whether a particular host is reachable across an IPv6 network. Use this command from an ArcSight Console running Linux.
- **Ping (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to test whether a particular host is reachable across an IPv4 or IPv6 network. Use this command from an ArcSight Console running Windows.

- **Portinfo (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to find information about the selected port. Use this command from an ArcSight Console running Linux.
- **Portinfo (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to find information about the selected port. Use this command from an ArcSight Console running Windows.
- **Traceroute (Linux)** in /All Integration Commands/ArcSight System/Tools/Linux enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Linux.
- **Traceroute (Windows)** in /All Integration Commands/ArcSight System/Tools/Windows enables you to determine the route taken by packets across an IP network. Use this command from an ArcSight Console running Windows.
- **Web Search** enables you to run a search with the selected item, device vendor, and device product in the selected event.
- **Whois (Linux)** /All Integration Commands/ArcSight System/Tools/Linux enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Linux.
- **Whois (Windows)** /All Integration Commands/ArcSight System/Tools/Windows enables you to determine the owner of a domain name or an IP address on the Internet. Use this command from an ArcSight Console running Windows.

# 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 computer, click the link above and an email window opens with the following information in the subject line:

**Feedback on ArcSight Administration and ArcSight System Standard Content Guide (ESM 7.2 Service Pack 1)**

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 [arcsight\\_doc@microfocus.com](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!