

# **ArcSight™ ESM Standard Content Guide**

---

for System and Core Content

ESM v4.5 SP1

May 5, 2009



## ArcSight™ ESM Standard Content Guide for System and Core Content

Copyright © 2009 ArcSight, Inc. All rights reserved.

ArcSight, the ArcSight logo, ArcSight TRM, ArcSight NCM, ArcSight Enterprise Security Alliance, ArcSight Enterprise Security Alliance logo, ArcSight Interactive Discovery, ArcSight Pattern Discovery, ArcSight Logger, FlexConnector, SmartConnector, SmartStorage and CounterACT are trademarks of ArcSight, Inc. All other brands, products and company names used herein may be trademarks of their respective owners.

Follow this link to see a complete statement of ArcSight's copyrights, trademarks, and acknowledgements:  
<http://www.arcsight.com/company/copyright/>

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

This document is ArcSight Confidential.

### Revision History

Date	Product Version	Description
5/5/09	ESM v4.5 SP1	Updated topics for ESM v4.5 SP1. Repackaged as a separate topic from the other standard content components.

Document template version: 1.0.2.8

### ArcSight Customer Support

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
E-mail	<a href="mailto:support@arcsight.com">support@arcsight.com</a>
Support Web Site	<a href="https://support.arcsight.com">https://support.arcsight.com</a>
Customer Forum	<a href="https://forum.arcsight.com">https://forum.arcsight.com</a>

# Contents

---

<b>About the ArcSight™ ESM Standard Content Guide .....</b>	<b>vii</b>
Who Should Read this Guide .....	vii
Text Conventions .....	vii
Related Documentation .....	ix
Feedback .....	ix
 <b>Chapter 1: Standard Content Overview and Setup .....</b>	 <b>1</b>
What is Standard Content? .....	1
Standard Content Foundations .....	2
ArcSight System Content .....	3
Shared Resources .....	4
Anti-Virus .....	4
Conditional Variable Filters .....	4
Network Filters .....	4
Standard Content Packages .....	4
Navigating to Standard Content .....	5
Set Up Connectors and Model the Network .....	5
Standard Content-Related SmartConnectors .....	6
Network Modeling .....	7
Apply Standard Asset Categories to Assets .....	7
Categorize Internal Assets .....	7
How ESM Determines the Protected Network .....	7
Categorize Critical Assets .....	8
Configure Notification Destinations .....	8
Configure Active Lists .....	9
Configure Asset Auto-Creation Filters .....	9
Configure Connector Asset Auto-Creation Controller Filter .....	10
Configure Device Asset Auto Creation Controller Filter .....	12
Configure SNMP Trap Forwarding Filter .....	13
Configure Rules to Send Notifications and Open Cases .....	15
Configure Rules with Notifications to the Cert Team .....	16
Configure Rules with Notifications to the SOC Operators .....	17
Schedule Reports .....	17
Default Trends Schedule .....	17

---

ArcSight Administration Trends .....	18
Configuration Monitoring Trends .....	18
Intrusion Monitoring Trends .....	19
Network Monitoring Trends .....	19
Workflow Trends .....	20
How to Enable/Disable Trends .....	20
Getting Started Using Standard Content .....	21
Monitoring with Standard Content .....	21
Active Channels .....	21
Dashboards .....	22
Investigating with Standard Content .....	23
Reporting with Standard Content .....	23
<b>Chapter 2: System and Core Content Resource Reference .....</b>	<b>25</b>
System Content Overview .....	26
Internal ArcSight Function .....	26
Network Modeling Standard Resources .....	26
Asset Categories .....	27
Site Asset Categories .....	27
System Asset Categories .....	28
Vulnerabilities .....	29
Zones .....	30
Networks .....	32
Locations .....	33
Files .....	34
Correlation Evaluation .....	34
Priority Evaluation Infrastructure .....	34
Threat Escalation Active Lists .....	36
System Filters .....	38
Core Filters .....	38
Event Type Filters .....	39
SNMP Forwarding Filters .....	40
SOC Operations and Monitoring .....	41
System Active Channels .....	41
ArcSight System Active Channels .....	42
All Events Active Channels .....	42
Core Active Channels .....	42
System Field Sets .....	43
Active Channels .....	43
Inspect - Edit Field Sets .....	44
Sortable Field Sets .....	44
Benchmarking and Analysis .....	45
Pattern Discovery Profiles .....	45

---

Core Reports .....	46
Standard Report Templates .....	47
Customize Branding in Standard Templates .....	48
Making Custom Modifications to Standard Templates .....	48
<b>Appendix A: Upgrading ArcSight Standard Content .....</b>	<b>49</b>
Preparing Existing Content for Upgrade .....	49
Configurations that Persist .....	49
Configurations that Require Restoration After Upgrade .....	50
Backing Up Existing Resources Before Upgrade .....	50
About Running the Upgrade Installer .....	51
Verifying and Reapplying Configurations After Upgrade .....	51
Verify Proper Function of Customer-Created Content .....	51
Fixing Invalid Resources .....	52
<b>Index .....</b>	<b>53</b>

---

# About the ArcSight™ ESM Standard Content Guide

---

ArcSight™ Enterprise Security Management (ESM) comes with a series of coordinated resources that address common enterprise network security and ArcSight management tasks.

This guide addresses the system-level and core resources that are installed automatically with ESM to provide essential system health and status operations.

[“Who Should Read this Guide” on page vii](#)

[“Text Conventions” on page vii](#)

[“Related Documentation” on page ix](#)

[“Feedback” on page ix](#)

## Who Should Read this Guide

This guide is intended for ArcSight ESM users, administrators, and security managers with the responsibility to plan, implement, maintain, and use ArcSight ESM to monitor, investigate, and manage events in their network environments.

Users should have knowledge of:

- Networks and network security
- Organizational policies and procedures regarding user access to resources stored on the protected network
- Using ArcSight tools to address specific network security scenarios

## Text Conventions

The following table lists the text conventions used in this guide.

Text	Description and Example
<b>Bold</b>	<p>Bold is used to indicate an on-screen element that a user should click. Always use this character format rather than manually bolding the item with the format   style menu or “bold” button.</p> <ul style="list-style-type: none"><li>• Enter a value and click <b>OK</b>.</li></ul>

Text	Description and Example
<code>Code</code>	<p>As described before, the code character tag is used for code elements discussed in-line in a paragraph.</p> <ul style="list-style-type: none"> <li>If the name of your active list entries text file is "<code>AdministrativeUsers.txt</code>," the script would look like this:</li> </ul>
<i>Emphasis or BookName</i>	<p><i>Italics</i> indicates emphasis or a book name:</p> <ul style="list-style-type: none"> <li><i>Do not</i> perform this procedure until you have backed up your data.</li> <li>For more information, see the <i>ArcSight Administrator's Guide</i>.</li> </ul>
<b>menu &gt; submenu</b>	<p>Right angle brackets are used to indicate steps in a command sequence and online Help topic sequences.</p> <ul style="list-style-type: none"> <li><b>menu &gt; submenu &gt; submenu</b></li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li><b>Authoring &gt; Rules &gt; Rule Actions &gt; Updating Session Lists</b></li> </ul>
tab   subtab	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none"> <li>tab   subtab   subtab</li> </ul>
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none"> <li>All Reports/System Reports/Asset/All Assets</li> </ul>
<variable>	<p>A text string enclosed in angular brackets is a variable for which you need to supply a value. (The bracketed text may also be in italics to emphasize that it is a variable.)</p> <p>Example:</p> <p>In <code>--nsp_password=&lt;password&gt;</code>, <code>&lt;password&gt;</code> is a variable for which you supply a value.</p>
{parameter1   parameter2   parameter3}	<p>Curly brackets enclose multiple parameters, at least one of which you must provide.</p> <p>Example:</p> <pre>--user_id_seq=&lt;user_id&gt;   -- user_login=&lt;user_login&gt;</pre> <p>In the above example, either supply the user ID of a user or his/her login name.</p>
[optional_parameter]	<p>Square brackets enclose parameters, variables, or values that are optional.</p> <p>Example:</p> <pre>[--cli_restrict=1]</pre>



## Related Documentation

In addition to this ArcSight™ ESM Standard Content Guide, ArcSight makes available the following product documentation. Many of these documents are available for download from the ESM Console by choosing the menu option **Help > Browse Documentation**. The latest and most complete set of documentation is always offered on the ArcSight Customer Support site (<https://support.arcsight.com>) through the Product Documentation link in the Knowledge Center section.

Document Title	Description
ArcSight ESM Administrator's Guide	Provides instructions for Administrators to configure ESM components and its network interfaces, and to maintain them for ongoing operations.
ArcSight ESM Installation and Configuration Guide	Provides ESM deployment architecture and component setup instructions, and instructions about how to install the components.
ArcSight ESM Upgrade Guide	Provides instructions about how to upgrade ArcSight ESM.
ArcSight ESM Release Notes	Describes what's new, and lists known issues.

## Feedback

To submit feedback regarding ArcSight ESM or documentation, go to the ArcSight Customer Support Web site at <https://support.arcsight.com>.



# Standard Content Overview and Setup

---

ArcSight Enterprise Security Management (ESM) comes with a series of coordinated resource systems that address common enterprise network security and ESM management tasks. These resource systems are referred to collectively as *standard content*.

With some basic configuration, standard content enables you to get started using ESM right away to effectively manage enterprise security operations without having to create additional resources. This topic describes the standard content and provides instructions for administrators about how to configure it using the ArcSight Console.

["What is Standard Content?" on page 1](#)  
["Standard Content Foundations" on page 2](#)  
["Standard Content Packages" on page 4](#)  
["Navigating to Standard Content" on page 5](#)  
["Set Up Connectors and Model the Network" on page 5](#)  
["Apply Standard Asset Categories to Assets" on page 7](#)  
["Configure Notification Destinations" on page 8](#)  
["Configure Asset Auto-Creation Filters" on page 9](#)  
["Configure Rules to Send Notifications and Open Cases" on page 15](#)  
["Schedule Reports" on page 17](#)  
["Default Trends Schedule" on page 17](#)  
["Getting Started Using Standard Content" on page 21](#)

## What is Standard Content?

Standard content is a series of coordinated Resources (filters, rules, dashboards, reports, and so on) that address common security and ESM management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration.

The content that comes with ArcSight ESM provides a full spectrum of security, network and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the ESM system.

The standard content is organized into functional groups called foundations. For more about the foundations, see the next topic, ["Standard Content Foundations" on page 2](#).

The standard content is installed using a series of packages, some of which are installed automatically with the ESM Manager to provide essential system health and status

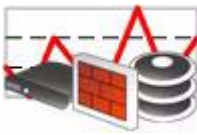


operations. The remaining packages are presented as install-time options organized by category.

## Standard Content Foundations

Each foundation is a coordinated system of resources that provides real-time monitoring capabilities for its area of focus, as well as after-the-fact analysis in the form of reports, trends, and trend reports.

With ESM, you can extend these foundations with additional resources specific to your needs, or you can use them as a template for building your own resources and tasks.

Several of the foundations rely on a series of common resources that provide core functions for common security scenarios. Resources that manage core ESM functions are **locked** to protect them from unintended change or deletion.

Foundation	Description
<b>Configuration Monitoring Foundation</b>	 <p>The Configuration Monitoring foundation identifies, analyzes, and remediates undesired modifications to systems, devices, and applications. Configuration monitoring is concerned mainly with monitoring hosts and user accounts for configuration-related activity, such as installing new applications, adding new systems to the network, anti-virus/network scanner/IDS engine and signature updates, and asset vulnerability postures.</p> <p>The configuration monitoring foundation helps you monitor how your networks change over time, measure daily statistics, understand the changes made, and know who's making them. Trends help you know what is normal and spot anomalies that should be investigated.</p>
<b>Intrusion Monitoring Foundation</b>	 <p>The focus of the Intrusion Monitoring foundation is to identify hostile activity and take appropriate action. This foundation provides statistics about intrusion-related activity, which can be used for incident investigation as well as routine monitoring and reporting. As with previous releases, the essential security monitoring functions of the Intrusion Monitoring foundation make up the bulk of the ESM standard content.</p> <p>The Intrusion Monitoring foundation targets generic intrusion types as well as specific types of attacks, such as worms, viruses, denial-of-service (DoS) attacks, and so on.</p>
<b>Network Monitoring Foundation</b>	 <p>The Network Monitoring foundation monitors the status of network throughput and network infrastructure.</p> <p>This foundation provides statistics about traffic and bandwidth usage that helps you identify anomalies and areas of the network that need attention.</p>

Foundation	Description
<b>ArcSight Workflow Foundation</b>	 <p>The ArcSight Workflow foundation is a system of active channels and reports that support incident response tracking using the ESM incident response system.</p> <p>Qualifying events in the other ESM foundation packages trigger notifications and cases that get escalated through the ESM incident response stages.</p>
<b>ArcSight Administration Foundation</b>	 <p>The ArcSight Administration foundation provides statistics about the health and performance of ArcSight products. This foundation is installed automatically, and is essential for managing and tuning the performance of ESM content and components.</p>

## ArcSight System Content



The ArcSight System content consists of resources that ESM requires for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.

System Function	Description
Internal ESM function	The system content contains sets of resources that manage ESM network modeling, vulnerability handling, and other internal ESM functions. These resources are leveraged by many basic systems and correlation tasks.
Correlation evaluation	System content rules, active lists, and filters help drive parts of the ESM correlation engine, such as priority formula calculations and basic out-of-the-box event processing.
Security center operations and monitoring	The system content provides standard field sets and active channels to provide basic operations and monitoring functions as soon as ESM is installed.
Benchmarking and analysis	ESM provides several benchmarking and analysis tools as add-on modules. As part of the system content, ESM includes two basic Pattern Discovery profiles. These profiles will be active only if you have Pattern Discovery installed.

This content is installed automatically with ArcSight ESM so that these functions and the infrastructure that supports them are immediately available. To safeguard against accidental damage or deletion, these resources are locked (read and write protected).

The core content infrastructure also serves the systems and solutions you deploy, and ESM content you create yourself.

For details about the resources that make up the system content, see [Chapter 2, System and Core Content Resource Reference](#), on page 25.

## Shared Resources



ESM contains common resources that support the five foundations. These resources are delivered in their own packages. Dependencies between these resources and the foundation packages they support are managed by the Package resource.

### Anti-Virus

The Anti-Virus content is a set of filters, reports, and report queries used by other foundations, such as Configuration Monitoring and Intrusion Monitoring.

### Conditional Variable Filters

The Conditional Variable Filters are a library of filters used by variables in standard content report queries, filters, and rule definitions. They express conditions that can also be used by any content in any package.

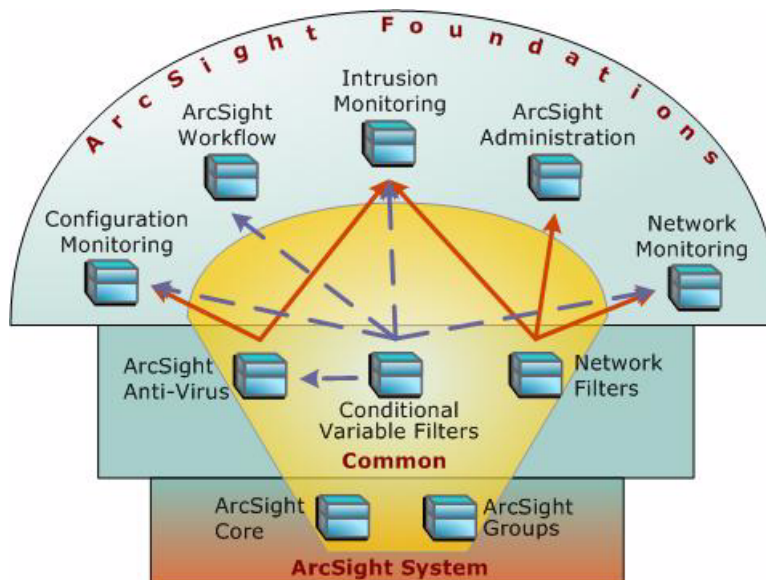
The Conditional Variable Filters are used by other standard content foundations, such as Anti Virus, Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow foundations.

### Network Filters

Network filters are a set of filters required by other standard content foundations, such as Intrusion Monitoring and Network Monitoring. The Network Filters package is installed automatically with ESM.

## Standard Content Packages

ESM standard content comes in a series of packages that are either installed automatically with ESM or presented as an install-time option. The following graphic outlines the packages available with ESM, and demonstrates their interoperability.

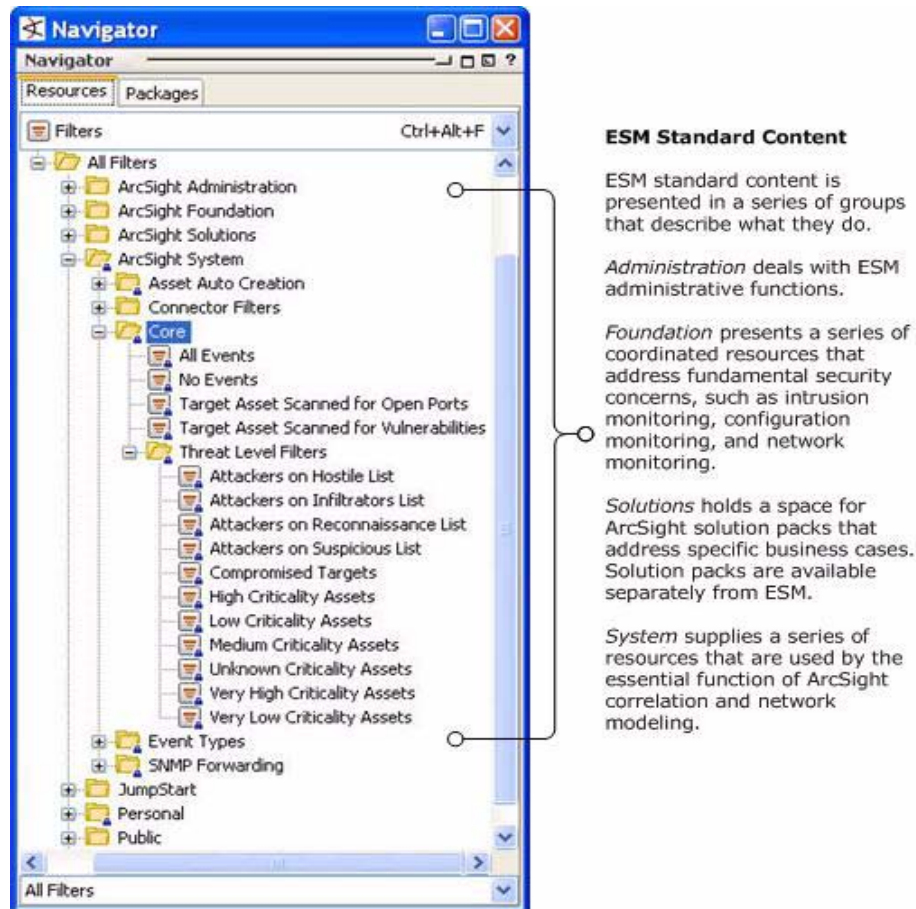


**Figure 1-1** The ArcSight System packages at the base provide core content required for ArcSight operation. The Common packages in the center contain shared resources that support the foundation packages. The packages shown on top are ArcSight Foundations that address common network security and ESM management scenarios.

Depending on the options selected when ESM was installed, you will see the ArcSight System resources and some or all of the other package content.

## Navigating to Standard Content

Standard content consists of just about every kind of resource available in ESM. If you look in any resource menu after installing ESM, you will find standard content. The example below shows the Core filters in the ArcSight system tree, and describes the standard content groups that are present when all the standard content is installed.



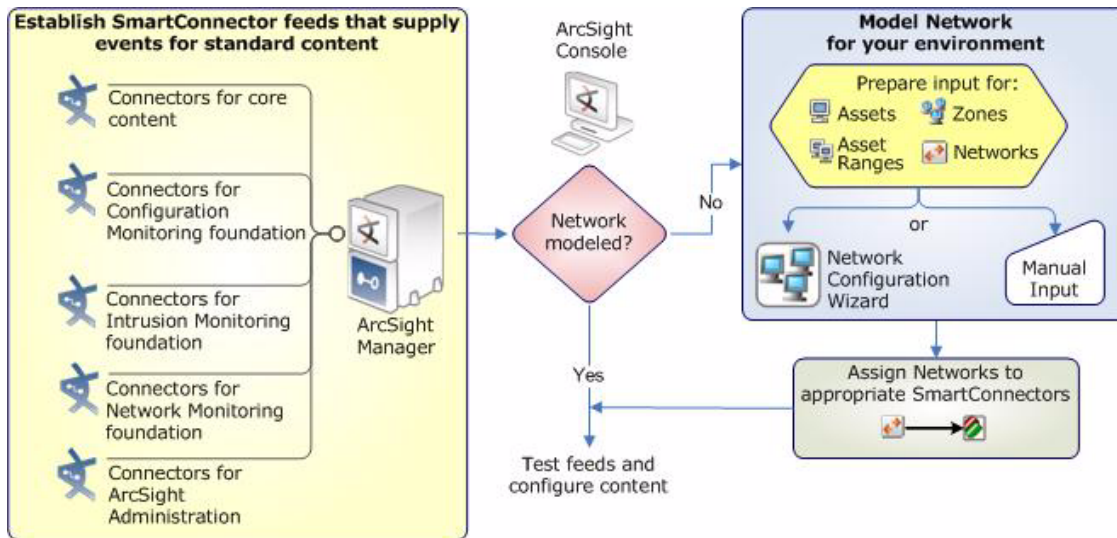
**Figure 1-2** Every resource in the ESM resource menu contains standard content, a coordinated set of resources that address common security scenarios and facilitate basic ESM functions. This sample shows the Core filters in the ArcSight System group in the Filters branch.

## Set Up Connectors and Model the Network

The graphic below outlines the process for establishing the feeds necessary to drive the standard content:

- 1 Establish relevant SmartConnector feeds
- 2 Model the network
- 3 Assign networks to the appropriate SmartConnectors

## 4 Test feeds and configure content



**Figure 1-3** Configuring ESM standard content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM.

## Standard Content-Related SmartConnectors

The standard content is designed to address event throughput, network health, and basic security-related scenarios. Depending on which packages you installed, verify that you have the minimum types of SmartConnectors reporting into ESM.

Package	Device Types
Anti-Virus (required by Configuration and Intrusion Monitoring foundations)	Anti-virus software, such as: <ul style="list-style-type: none"> <li>• Symantec EndPoint Protection</li> <li>• TrendMicro</li> <li>• McAfee AV</li> </ul>
Configuration Monitoring	<ul style="list-style-type: none"> <li>• Operating systems</li> <li>• Security applications (Network and host-based IDS, anti-virus)</li> <li>• User management services (authentication, authorization, and accounting services)</li> <li>• Basic network devices (firewalls, routers, switches, VPN)</li> </ul>
Intrusion Monitoring	<ul style="list-style-type: none"> <li>• Network and host-based IDS</li> <li>• Intrusion Prevention Systems (IPS)</li> <li>• Anti-virus</li> <li>• Firewalls</li> </ul>
Network Monitoring	<ul style="list-style-type: none"> <li>• Routers</li> <li>• Firewalls</li> <li>• Switches</li> <li>• Real-time flow monitor</li> </ul>



## Network Modeling

ArcSight ESM uses a model of the network to keep track of the network nodes participating in the event traffic. Having your network modeled and critical assets categorized using the ESM standard asset categories is what activates much of the standard content and makes it effective.

There are several ways to model your network, including the ESM Network Modeling Wizard. If you are modeling the network using the Network Modeling wizard, review the next topic [“Apply Standard Asset Categories to Assets” on page 7](#) before creating the comma-separated values lists to load into the ESM network model.

For more about the network model and how to populate it, see “Modeling Your Network and Managing Assets” in the *ESM User’s Guide* or the Console Help.

For more about the Network Modeling wizard, see “Populating the Network Model Using the Wizard” in the *ESM User’s Guide* or the Console Help.

To learn more about the architecture of the ESM network modeling tools, see Chapter 4, “ArcSight Network Model” in *ArcSight 101*.

## Apply Standard Asset Categories to Assets

Once your network model is populated with assets, apply the standard asset categories to them to activate standard content that uses these categories to apply criticality and business context to events. Asset categories can be assigned individually using the Asset editor, or in a batch using the Network Modeling wizard.

The asset categories most essential for engaging ESM standard content are discussed in this topic.

For more about asset categories and instructions about how to apply them using the Console tools, see “Asset Categories” in the *ESM User’s Guide* or the Console Help.

For more about the Network Modeling wizard, see “Populating the Network Model Using the Wizard” in the *ESM User’s Guide* or the Console Help.

## Categorize Internal Assets

Internal Assets are considered to be assets inside the company network. Assets that are not categorized as specifically internal to the network are considered by ESM to be external. This includes assets with different asset categories, and those that are not categorized at all (such as external web sites, unknown external hosts, and so on).

For all assets that are internal to the network, classify them in the following asset category:

```
/All Asset Categories/Site Asset Categories/  
Address Spaces/Protected/
```

## How ESM Determines the Protected Network

There is a set of filters in [All Filters/ArcSight Foundation/Common/Network Filters/Boundary Filters](#) that are used to determine whether a system is internal or external by checking to see if an asset or its zone is categorized with [/All Asset Categories/Site Asset Categories/Address Spaces/Protected](#).

In general, assets do not inherit the categories applied to the zone it belongs to. However, any address contained in the Private Address Space Zones is categorized as *Protected*. For

example, an asset with an IP address of **192.168.0.1** is not automatically categorized as *Protected*, however, because it belongs to one of the Private Address Spaces zones, it is considered *Internal* because it belongs to a zone that is categorized as *Protected*. This system provides a minimal structure to help discern between internal and external traffic if you do not have all your assets categorized.

## Categorize Critical Assets

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

Assets that are considered critical to protect, such as those that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations, should be classified as critical assets using the following criticality asset category:

[/All Asset Categories/System Asset Categories/Criticality/High](#)

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, see "Priority Calculations and Ratings" in the *ESM User's Guide* or the Console Help.

## Configure Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, the notifications are disabled in the standard content rules, so the admin user will need to configure the destinations AND enable the notification in the rules. For details about enabling the notifications in standard content rules, see "[Configure Rules to Send Notifications and Open Cases](#)" on page 15.

The standard content rules reference two notification groups: CERT Team and SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center.

- 1** In the Navigator panel, go to **Notifications > Destinations > Shared > All Destinations > CERT Team**
- 2** Right-click Level 1 and select New Destination.
- 3** In the Destination Editor, enter the following values in the Attributes tab and click **OK**:

Field	Value
Name	Enter a name for the destination, such as the user name of the contact, or the role, such as Investigator or Manager.
Start/End Time	If applicable, enter the start and end times of the period this person is available, for example, Start: 08:00:00 AM; End: 04:59:59 PM.

Field	Value
Destination Type	<p>From the drop-down menu, select the method by which the notification will be delivered:</p> <ul style="list-style-type: none"> <li>• <b>Console</b> — Notification popup in this user's ArcSight account</li> <li>• <b>E-Mail</b> — User's e-mail account</li> <li>• <b>Pager</b> — User's pager. Enter the pager's PIN number and service provider.</li> <li>• <b>Cell Phone</b> — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.</li> </ul>
User/Group	<p>From the drop-down menu, select the individual user or user group who will receive the notification. This field is required if you selected Console as the destination type, or if you want to use the contacts specified in the User's profile.</p>

- 4 Repeat steps 1, 2, and 3 for each escalation level you want to add. Add more escalation levels as needed.
- 5 Repeat steps 1, 2, 3, and 4 for the SOC Operators destination (**Notifications > Destinations > Shared > All Destinations > SOC Operators**).

## Configure Active Lists

The ArcSight System content includes active lists that are designed to be populated manually with data specific to your environment. Once populated with values, these lists are cross-referenced by active channels, filters, rules, reports, and data monitors to give ESM more information about the assets in your environment. For details about active lists and how they work, see *ESM 101* and the topic *Active Lists* in the Console Help.

The active lists that should be configured are:

- **Trusted/Untrusted** active lists in ArcSight System (Lists | Active Lists | [All Active Lists/Arcsight System/Attackers](#)). For more about the Trusted and Untrusted lists, see ["Attackers Active Lists" on page 36](#).

The ArcSight System content also includes Active lists that are populated automatically during run-time by rules. These active lists do need not to have entries made to them manually before being used. You can, however, add manual entries to these lists.

You can manually add entries to active lists two ways:

- One by one using the Active List editor in the ArcSight Console. For instructions, see the topic *Editing Active List Entries* in the Console Help.
- In a batch by importing values from a CSV file. For instructions, see the topic *Importing an Active List* in the Console Help.

## Configure Asset Auto-Creation Filters

A standard feature of ESM is that it automatically creates assets in the ArcSight asset model 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, however, 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.

Likewise, if an ArcSight Connector reports from a DHCP subnet, every time a system is assigned a DHCP address, ESM would model a new Connector, which falsely adds Connector nodes to the network model.

To limit how ESM automatically models assets in these cases, ArcSight provides two filters in the ArcSight System group that you can configure with the names of devices and Connectors that you need to include or exclude from the auto-creation feature.



The Auto Asset Creation filters are part of the locked system content. The filters cannot be moved or renamed, but they can be configured by users who have write privileges to them, in this case, ArcSight Administrators and Analyzer Administrators.

---

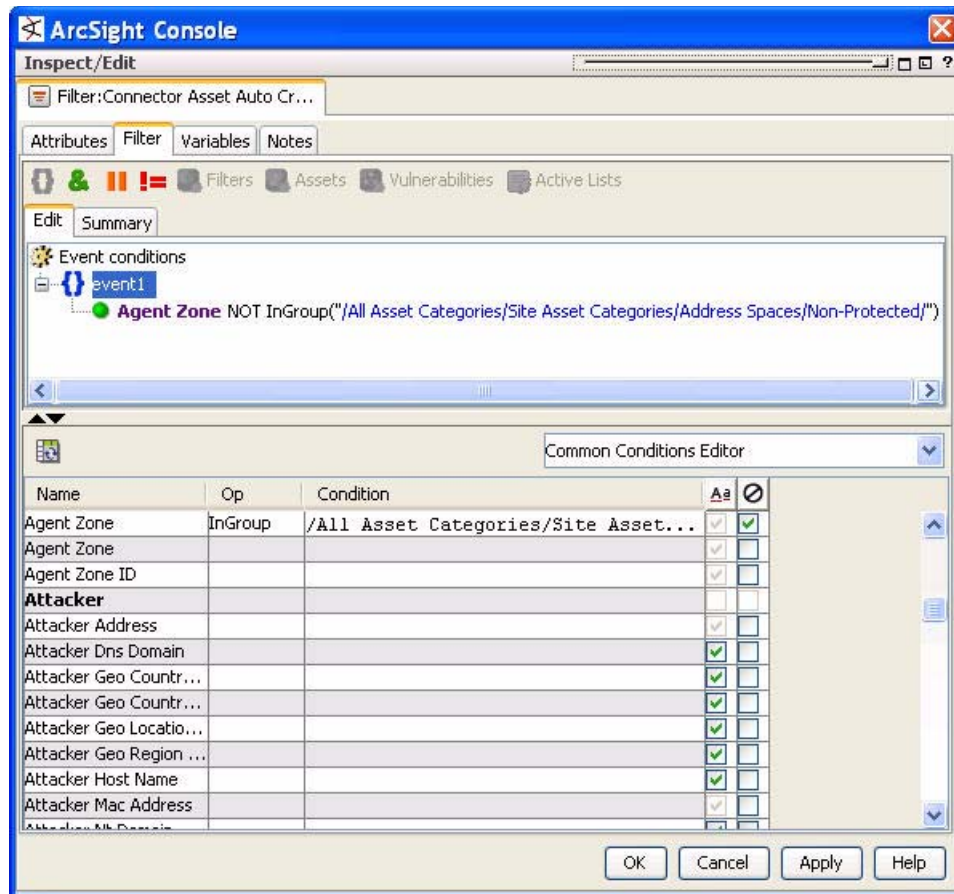
## Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs ESM to create an asset for network nodes represented in the events received from the SmartConnectors present in your environment.

By default, the *Connector Asset Auto Creation Controller* filter is configured with the generic condition [True](#), which matches all events. As necessary, you can configure this filter to specify assets to exclude from the asset auto creation feature.

One way to configure the filter is to 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.

The example below shows the *Connector Asset Auto Creation Controller* filter configured to exclude Connector traffic coming from devices categorized as being in non-protected address spaces.

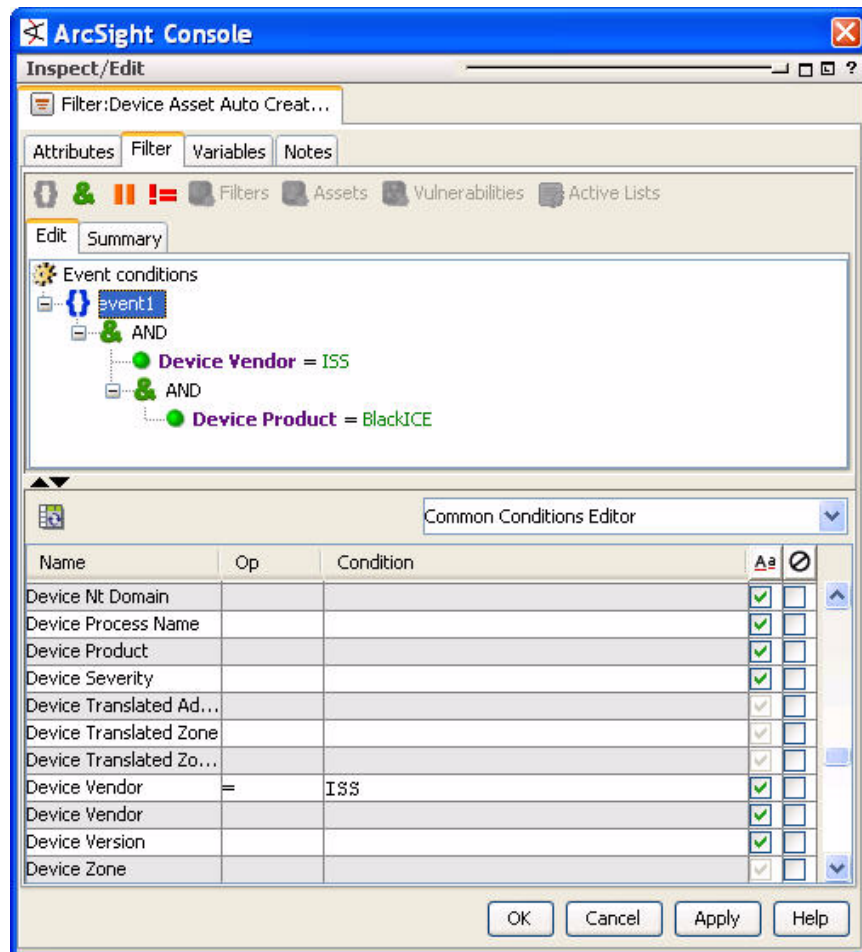


- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 In the event fields grid at the bottom of the pane, select **Agent Zone**.
- 4 In the Op column, select the **InGroup** operator.
- 5 In the Condition column, select the non-protected asset category from the drop-down menu.
- 6 Select the NOT checkbox (⊗).
- 7 Repeat steps 3 through 5 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 8 Click **OK** to apply changes and close the Filter editor.

## Configure Device Asset Auto Creation Controller Filter

By default, the *Device Asset Auto Creation Controller* filter is configured with the generic condition **True**, which matches all events. As necessary, you can 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.

The example below shows the *Device Asset Auto Creation Controller* filter configured to only create assets for traffic coming from the ISS intrusion detection scanner BlackICE.



- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the Filter tab. Delete the default condition **True** (select the condition and press **Delete**).
- 3 Select **event1** and add an AND operator (click the AND icon **&**).
- 4 Select **event1** and use the event fields grid to build the condition, or right-click event1 and select **New Condition**. Navigate to **Device > Device Vendor**. In the Condition field, enter the vendor name, in this case **ISS**.
- 5 Add the device vendor and product you wish to include.

- a If you are adding only one device vendor and product pair, select the Device Vendor condition and add another **AND** operator. Navigate to Device > Device Product. In the Condition field, enter the device name, in this case **BlackICE**.
- b If you are adding more than one device vendor and product pair, select the Device Vendor condition and add an **OR** operator. Navigate to Device > Device Product. In the Condition field, enter the device name.

For example, the condition would look like this:

OR

```

AND
    Device Vendor A
    Device Product 1
AND
    Device Vendor B
    Device Product 2
AND
    Device Vendor C
    Device Product 3

```

- 6 Repeat steps 3 through 6 for every device and device vendor whose events you want to exclude from the auto asset creation feature.
- 7 Click **OK** to apply changes and close the Filter editor.

## Configure SNMP Trap Forwarding Filter

If you do not have SNMP traps enabled, you can skip this section and move on to [“Configure Rules to Send Notifications and Open Cases” on page 15](#).

The System filters group contains an SNMP Trap Sender filter ([All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#)). The SNMP Trap Sender filter only needs to be configured if you have the SNMP Trap Sender enabled to forward events via SNMP to a network management system, such as HP Openview.

By default, this filter is configured with the filter [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#). If you leave this default setting and you have SNMP forwarding enabled, all ArcSight correlation events will be trapped and forwarded to the network management system.

To configure this filter to forward certain events as an SNMP trap, you can do either of the following:

- Change the default condition in the SNMP Trap Sender filter so it expresses which events should be 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.
- Change the server configuration (via [server.properties](#)) to point the SNMP trap sender to another filter, and set that filter up as per your convenience.

### Change Default Condition in SNMP Trap Forwarding Filter

- 1 In the Navigator panel, navigate to [All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender](#). Double-click the filter or right-click and select **Edit** to open it in the Filter editor in the Inspect/Edit panel.
- 2 At the Filter tab, change the default condition [/All Filters/ArcSight System/Event Types/ArcSight Correlation Events](#) to list the type(s) of

events you want forwarded, or to point to another filter that expresses these parameters.

For example, you can create a filter that specifies all events with a priority greater than 8, or events from all Top Secret systems.

### Change SNMP Trap Sender in `server.properties`

If you wish to use a filter other than the default `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender`, you must point the SNMP trap sender to the new filter in the ESM Manager `server.properties` file.



These instructions apply **only** if you have SNMP forwarding already enabled at the Manager, *and* if you are using a filter other than the default SNMP Trap Sender filter to forward events.

If the SNMP forwarding feature is not already enabled at the Manager, the `server.properties` file will not contain the string that needs to be modified.

- 1 On the ArcSight ESM Manager machine at a command line, stop the Manager service.
  - ◆ Unix: `/etc/init.d/arcsight_manager stop`
  - ◆ Windows: Stop the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu
- 2 Make a backup copy of the file `$ARCSIGHT_HOME/config/server.properties`.
- 3 In a text editor, open the file `$ARCSIGHT_HOME/config/server.properties` and look for the following lines:

```
# -----
# SNMP Trap Sender configuration.
# -----
# Configuration for the SNMP trapsender. Copy these properties into
# your server.properties file and remove the '#'s (comments). By
# default, the SNMP trap sender is disabled.
#
# set the following property to true to enable trap sending
snmp.trapsender.enabled=false

# Filter that determines what arcsight events will be sent out as
# traps
snmp.trapsender.uri=/All Filters/ArcSight System/SNMP
Forwarding/SNMP Trap Sender
```

- 4 Change the `snmp.trapsender.uri` from `/All Filters/ArcSight System/SNMP Forwarding/SNMP Trap Sender` to the URI for the filter you want to use.
- 5 Save and close the `server.properties` file.
- 6 Restart the Manager service.
  - ◆ Unix: `/etc/init.d/arcsight_manager start`
  - ◆ Windows: Start the ArcSight Manager service from the **Control Panel > Administrative Tools > Services** menu

To enable the SNMP trap sender, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.



## Configure Rules to Send Notifications and Open Cases

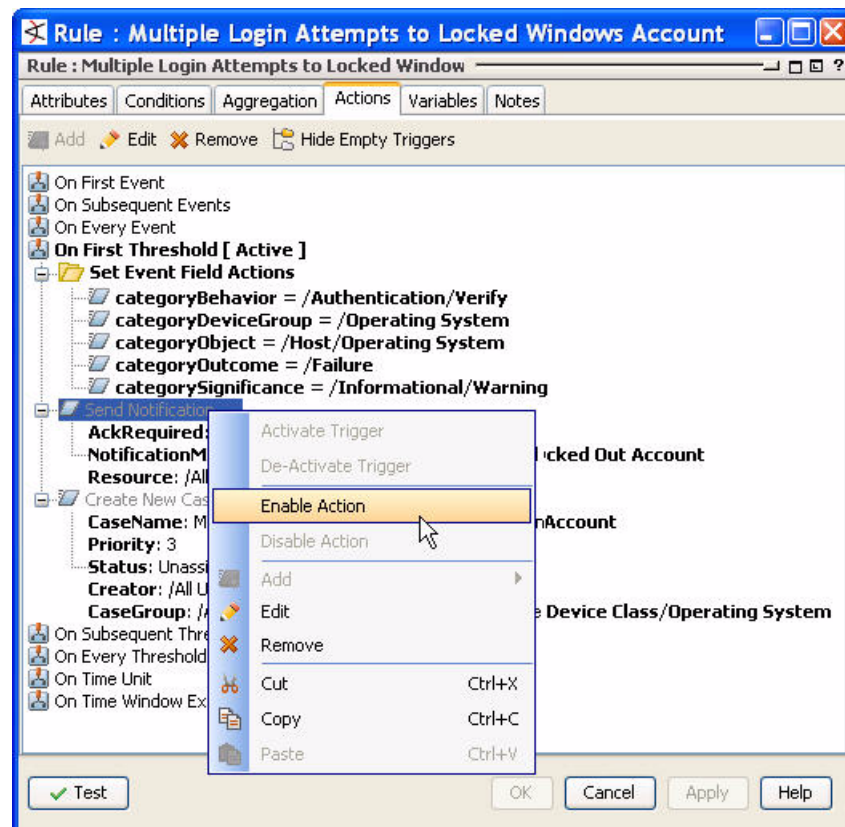
Standard content depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that the standard content is designed to find.

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group. For ESM administration scenarios, notifications are enabled, but case creation is disabled.

To enable standard content rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 8](#), then enable the notification and case actions in the rules.

- 1 In the Navigator panel, navigate to each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 16](#) and [“Configure Rules with Notifications to the SOC Operators” on page 17](#).
- 2 Open the rule for editing in the Inspect/Edit panel (double-click the rule or right-click it and select **Edit**).
- 3 In the Rule Editor in the Inspect/Edit panel, click the **Action** tab.
- 4 Find the *Send Notification* action. The disabled action will appear in grey text. To enable it, select the **Send Notification** action name, right-click it, and select **Enable**.

The example below shows the Action tab for the rule *Multiple Login Attempts to Locked Windows Account*.



- 5 To also create a case when the rule conditions are met, edit the action to give it an owner and enable the action.
  - a Select the *Create New Case* action and click **Edit** in the toolbar at the top of the Actions tab.
  - b In the *Edit Action* dialog box in the Owner drop-down menu, navigate to and select an appropriate ESM user. Click **OK**.
  - c Select, then right-click the *Create New Case* action and select **Enable**. Click **OK**.
- 6 Repeat steps 1 through 6 for each rule listed in [“Configure Rules with Notifications to the Cert Team” on page 16](#) and [“Configure Rules with Notifications to the SOC Operators” on page 17](#).

For more about working with Rule actions in the Rules Editor, see “Creating Rule Actions” and “Applying Rule Actions” in the *ESM User's Guide* or the Console Help.

## Configure Rules with Notifications to the Cert Team

The following security-related rules send notifications to the **CERT Team** notification group. In these rules, both the notification and case creation actions are disabled by default.

Cases created by these rules should be assigned to the appropriate user or user group in your organization.

Rule URI (File Path)	Rule Name
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Traffic Anomalies/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Suspicious/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/Attempts/	Windows Account Locked Out Multiple Times
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Insecure Configuration
/All Rules/ArcSight Foundation/Configuration Monitoring/Detail/Vulnerabilities/	Warning - Vulnerable Software
/All Rules/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Attackers/	Notify on Successful Attack

## Configure Rules with Notifications to the SOC Operators

The following ArcSight Administration rules send notifications to the **SOC Operators** notification group. For these rules, the notification is enabled, and the case creation is disabled by default. Cases created by these rules are assigned to the ESM Admin user.

Rule URI	Rule Name
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Dropping Events
/All Rules/ArcSight Administration/Connectors/System Health/	Connector Still Down
/All Rules/ArcSight Administration/Connectors/System Health/Custom/	Critical Device Not Reporting
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Excessive Rule Recursion
/All Rules/ArcSight Administration/ESM/System Health/Resources/Rules/	Rule Matching Too Many Events
/All Rules/ArcSight Administration/ESM/System Health/Storage/	ASM Database Free Space - Critical

## Schedule Reports

Reports can be run on demand, automatically on a regular schedule, or both. By default, the reports that come with ESM are not scheduled to run automatically.

Evaluate the reports that come with the foundations you have installed, and schedule the reports that are of interest to your organization and business objectives.

For instructions about how to schedule reports, see “Archiving Reports” in the *ESM User's Guide* or the Console Help.

## Default Trends Schedule

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

The standard content contains trends that monitor long-term conditions among the ArcSight foundations.

Based on the volume of data generated by some of these queries, only some of the trends are enabled by default at installation; the rest are disabled by default.

The 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 slower than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the Console.

ESM standard trends are listed below with their status on installation, and the time at which they are scheduled to run.

## ArcSight Administration Trends

Both ArcSight Administration trends are enabled by default.

ArcSight Administration Trends	Status	Schedule
Trend Queries	Enabled	4:00 a.m.
ASM Database Free Space	Enabled	4:30 a.m.
ArcSight User Login Trends – Hourly	Enabled	5:00 a.m.

## Configuration Monitoring Trends

Seven of the 13 Configuration Monitoring trends are enabled by default.

Configuration Monitoring Trends	Status	Schedule
Assets with Recent Configuration Modifications - Daily Trend	Enabled	12:40 a.m.
Host Configuration Modifications	Enabled	1:35 a.m.
Asset Startup and Shutdown Events - Daily Trend	Enabled	2:40 a.m.
Critical System Startup and Shutdown Events - Daily Trend	Disabled	N/A
Most Common Account Login Attempts - Daily Trend	Enabled	3:40 a.m.
User Account Login Failures	Enabled	4:40 a.m.
AAA User Account Creation	Disabled	N/A
AAA User Account Deletions	Disabled	N/A
Account Creation by Host	Disabled	N/A
Accounts Deleted by Host	Disabled	N/A
Local Windows User Creation - Disallowed Systems	Disabled	N/A
Password Modifications	Disabled	N/A
User Account Creation	Enabled	5:40 a.m.
User Account Modifications	Enabled	6:20 a.m.
User Removals	Enabled	1:15 a.m.
VPN User Account Creation	Disabled	N/A
Top Vulnerability Exposure of Critical Assets	Enabled	5:10 a.m.
Vulnerability Exposure by Asset Criticality (Snapshot)	Enabled	1:50 a.m. once a week
Vulnerability Exposure of Critical Assets (snapshot)	Enabled	3:30 a.m.

Configuration Monitoring Trends	Status	Schedule
Vulnerability Exposure of High and Very-High Criticality Assets by Zone - Daily Trend (Snapshot)	Disabled	N/A

## Intrusion Monitoring Trends

Eight of the 16 Intrusion Monitoring trends are enabled by default.

Intrusion Monitoring (8/16)	Status	Schedule
SANS Top 20 (v6.01) Attacked Systems	Disabled	N/A
Prioritized Attack Counts by Service	Disabled	N/A
Prioritized Attack Counts by Target Zone	Disabled	N/A
Inbound DoS Events	Disabled	N/A
Environment Status Events	Disabled	N/A
Port Scanning	Enabled	1:20 a.m.
Port Scanning Daily Top 20	Enabled	2:20 a.m.
Reconnaissance Activity	Disabled	N/A
Reconnaissance Types Detected	Disabled	N/A
Top 10 Reconnaissance Types Detected	Disabled	N/A
Zone Scanning Events by Priority	Enabled	4:20 a.m.
Brute Force Access Session Trends	Enabled	1:40 a.m.
Daily Top 10 Resource Access Trends	Disabled	N/A
Resource Access	Disabled	N/A
Asset Counts by Vulnerability (Snapshot)	Enabled	12:20 a.m. once a week
Prioritized Vulnerability Events by Zone	Enabled	5:20 a.m.
Top 10 Daily Vulnerability Events	Enabled	6:25 a.m.
Failed Logins per Hour	Enabled	6:00 a.m.
Top Users with Failed Logins per Day	Enabled	6:40 a.m.
Number of Vulnerabilities per Asset (Snapshot)	Enabled	3:20 a.m. once a week

## Network Monitoring Trends

All three Network Monitoring trends are disabled by default.

Network Monitoring	Status	Schedule
Inbound Traffic by Application Protocol	Disabled	N/A
Outbound Traffic by Application Protocol	Disabled	N/A
Overall Traffic	Disabled	N/A

## Workflow Trends

One Workflow trend is enabled by default, and the other is disabled by default.

Network Monitoring	Status	Schedule
Notification Events	Disabled	N/A
Notifications	Enabled	6:00 a.m.

## How to Enable/Disable Trends



If you wish to enable a disabled trend, you must first **change the default start date** in the Trend editor, then enable it.

If the start date is not changed, the trend will take the default start date (which is derived from when the trend was first installed), and backfill the data from that time. For example, if you enable the trend 6 months after the first install, these trends will try to get all the data for the last 6 months, which would cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

### To enable a disabled trend:

- 1 Edit the trend to change the default start date.
  - a Double-click the trend, or right-click it and select **Edit Trend** to open it in the Trend Editor in the Inspect/Edit panel.
  - b In the Trend editor, click the **Parameters** tab. In the *Query Parameters* section, find Start Time and uncheck the **Use Default** checkbox.
  - c In the *Value* drop-down menu, select a start date appropriate for the frequency at which the trend is scheduled to run. For example, if the trend is scheduled to run daily, select a start date of a week or less earlier than today. Keep in mind the data partitioning schedule your Manager uses to make sure the time frame you have specified provides adequate online access to the events. Click **Apply**.
- 2 Enable the trend.
  - ◆ If the Trend editor is still open, click the Attributes tab and check the **Enabled** checkbox. Click **OK** to apply changes and close the Trend editor.
  - ◆ If the Trend editor is closed, right-click the trend in the Navigator panel and select **Enable Trend**.

### To disable an enabled trend:

- In the Navigator panel, right-click the trend you want to enable and select **Disable Trend**.

## How to Monitor Trend Performance

The ArcSight Administration foundation contains resources that enable you to monitor the performance of your enabled trends. The Trends Status dashboard shows the run-time status for all enabled trends. The Trend reports show statistics about trend performance for all enabled trends.

## Getting Started Using Standard Content

Whatever your role in the security operations center, you can get started right away using the ESM standard content.

Each foundation is organized with content for different types of users.

- **Executive Summaries.** Executive summaries provide high-level analysis of event activity for management reports. These views show overall trends and long-term summaries.
- **Operational Summaries.** The operational summaries are intended for SOC operators and analysts for daily event monitoring and triage-level investigation.
- **Details.** The detailed content is intended for incident responders and analysts who need access to relevant event details in order to investigate situations that arise from monitoring reports in the operational summaries.
- **SANS Top 5 Reports.** Each foundation contains a set of reports that address the SANS Institute's list of recommendations of what every IT staff should know about their network at a minimum, based on the Top 5 Essential Log Reports.

## Monitoring with Standard Content

You can use standard content to begin monitoring your network immediately when SmartConnectors are added and basic configuration is complete.

### Active Channels

Each foundation provides high-level channels for observing general activity for its area of focus.

Foundation	Channel	Description
ArcSight System	System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	Today	Channel showing events received today since midnight. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
	All Events / Last 5 Minutes and Last Hour	Channel showing events received during the last five minutes or the last hour. The channel includes a sliding window that always displays exactly the last five minutes of event data.
	Core / Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing correlation events.

Foundation	Channel	Description
Configuration Monitoring	Operational Summaries / High-Priority Scan Events Directed Toward High-Criticality Assets	This channel shows scan results in real time to give you a view into any high-priority vulnerabilities detected on highly critical assets.
Intrusion Monitoring	Intrusion Monitoring - Significant Events	<p>This channel provides an overview of hostile, compromise or high priority events. It continuously monitors events matching:</p> <ul style="list-style-type: none"> <li>Not ArcSight Internal Events</li> <li>Priority greater than 8 or Category Significance Starts With /Compromise or /Hostile</li> </ul> <p>Uses the Business Impact Analysis Field Set (End Time, Business Role, Data Role, Attacker Zone Name, Target Host Name, Category Significance, Category Outcome and Priority).</p>
Network Monitoring	Argus Events	This active channel shows all the events coming from Argus SmartConnectors for the past 24 hours.
Workflow	Assigned Events	This channel shows events assigned today. The channel always displays events occurring since midnight of the current day up to the current time. A filter prevents the channel from showing correlated events. It shows only events that are not in closed stage and are assigned to a user.

Each foundation contains more channels that focus on events of different types. Explore the active channels to monitor the activity you are interested in.

For more about using active channels, see “Monitoring Active Channels” in the *ESM User's Guide* or the Console Help.

## Dashboards

Each foundation also includes general dashboards that provide a high-level view of activity for its area of focus.

Foundation	Dashboard	Description
Configuration Monitoring	Operational Summaries	This group contains four dashboards that provide an overview of configuration changes, database errors, host configuration modifications, and an overview of hosts with problems.



Foundation	Dashboard	Description
Intrusion Monitoring	Operational Summaries / Security Activity Statistics	<p>This dashboard is a window into the health of common avenues for security threats on the network, including transport protocols, address spaces, application protocols, and statistics involving the top target and attacker IPs, among others.</p> <p>The Intrusion Monitoring foundation contains many other dashboards that provide general executive-level summaries, and more detailed views on different focus areas for operations and investigations.</p>
Network Monitoring	General	<p>The dashboards in the General group provide an overview of the top traffic to mail and web servers, and moving average statistics for TCP, UDP, ICMP, and SYN transport protocols.</p> <p>The Network Monitoring foundation contains many more dashboards that provide more detail about network health, including bandwidth usage, inbound and outbound traffic, and activity from firewalls, network devices, and VPNs.</p>

## Investigating with Standard Content

Each foundation contains resources that enable operators to view detailed activity and drill down, investigate, track, graph, map, and export, just to name a few.

Use **active channels** to view and sort event flows, investigate blocks of events, and drill down into single event details. For more about using active channels to investigate event activity, see “Monitoring Active Channels” in the *ESM User's Guide* or the Console Help.

Use **dashboards** to view activity from many perspectives in a single screen. Dashboards are also fully drill-down enabled. For more about investigating using dashboards, see “Using Dashboards” in the *ESM User's Guide* or the Console Help.

Use the Daily and Quarter Hourly **Pattern Discovery** profiles to find traffic patterns that are not easily detected using other methods. For more about investigating using Pattern Discovery, see “Pattern Discovery” in the *ESM User's Guide* or the Console Help.

## Reporting with Standard Content

ESM standard content supplies a robust set of reports for each ESM foundation. The reports for each foundation are organized into different levels of detail depending on who the reports are for as outlined in [“Getting Started Using Standard Content” on page 21](#).

Foundation	Reports
Common	The Common group contains a set of anti-virus reports that apply to all the foundations.

Foundation	Reports
Configuration Monitoring	<ul style="list-style-type: none"> <li>• <b>Detailed</b> reports concentrate on configuration changes by device and by user, inventories of applications and assets by role, and vulnerabilities by asset, asset type, asset criticality, and so on.</li> <li>• <b>Executive Summary</b> reports focus on overall host configurations by zone, role, criticality, data role, and operating system.</li> <li>• <b>Operational Summaries</b> provide summaries of host configuration modifications by Customer, OS, and over the last 30 days; top user login successes and failures over recent time periods; and asset restarts over recent time periods.</li> <li>• <b>SANS Top 5</b> Reports focus on SANS section 3: Unauthorized Changes to Users, Groups, and Services.</li> </ul>
Intrusion Monitoring	<ul style="list-style-type: none"> <li>• <b>Detailed</b> reports are organized into types of activity: anti-virus; attack monitoring; environment state for applications, operating systems, and services; reconnaissance attempts; access events; user activity through device type; vulnerability activity by asset and by vulnerability; and worm outbreak activity.</li> <li>• <b>Executive Summary</b> reports provide an overall Security Intelligence Status Report, and summary views by business role and systems that are subject to regulations, such as the Sarbanes-Oxley Act.</li> <li>• <b>Operational Summaries</b> provide mid-level summaries organized into device types, such as anti-virus, attack monitoring, and reconnaissance.</li> <li>• <b>SANS Top 5</b> Reports focus on SANS sections 1, 4, and 5: Attempts to Gain Access, Through Existing Accounts, Systems Most Vulnerable to Attack, and Suspicious or Unauthorized Network Traffic Patterns.</li> </ul>
Network Monitoring	<ul style="list-style-type: none"> <li>• <b>Detailed</b> reports provide views into traffic by host, by protocol, and by target, and activity over network devices and VPNs.</li> <li>• <b>Executive Summary</b> reports provide traffic summaries over daily, monthly, quarterly, and weekly time intervals.</li> <li>• <b>Operational Summaries</b> provide an overall traffic snapshot; bandwidth utilization statistics by device and by time interval; and statistics for inbound and outbound traffic by protocol and by host.</li> <li>• <b>SANS Top 5</b> Reports focus on SANS section 5: Suspicious or Unauthorized Network Traffic Patterns.</li> </ul>
Workflow	<ul style="list-style-type: none"> <li>• <b>Detailed</b> reports provide statistics for all cases, notifications, and notification action events.</li> <li>• <b>Executive Summary</b> reports provide overall case statistics, such as average time to case resolution, number of cases at each escalation stage, and cases as they affect operations.</li> <li>• <b>Operational Summaries</b> provide detailed case statistics, including trends over time, notifications that reach level 3, the status of notifications by user, and so on.</li> </ul>

## Chapter 2

# System and Core Content Resource Reference

---



The ArcSight System content consists of resources that ESM requires for basic security processing functionality, such as threat escalation and priority calculations, and basic throughput channels required for out-of-the-box functionality.

This content is installed automatically with ArcSight ESM so that these functions and the infrastructure that supports them are immediately available when you start up ESM for the first time. The system content infrastructure also serves the systems and solutions you deploy, and ArcSight content you create yourself.

Some of the system content is intended to be configured by you during setup time; others are write protected.

### System Content

System content is the basic framework of resources of all types, including network modeling, basic correlation, and monitoring, that support basic ESM function upon installation. Some resources contained in the `/ArcSight System/` directories are intended to be configured or modified as directed in [Chapter 1, Standard Content Overview and Setup, on page 1](#).

### Core Content

For some resources, the ArcSight System content includes a core directory, which contain resources that are required for basic ESM function, and are locked, so they cannot be deleted or renamed. Most of the Core content resources themselves are also locked, which further protects them from being modified or accidentally deleted. There are several filters in the Core content that can be configured as directed in ["Configure Asset Auto-Creation Filters" on page 9](#).

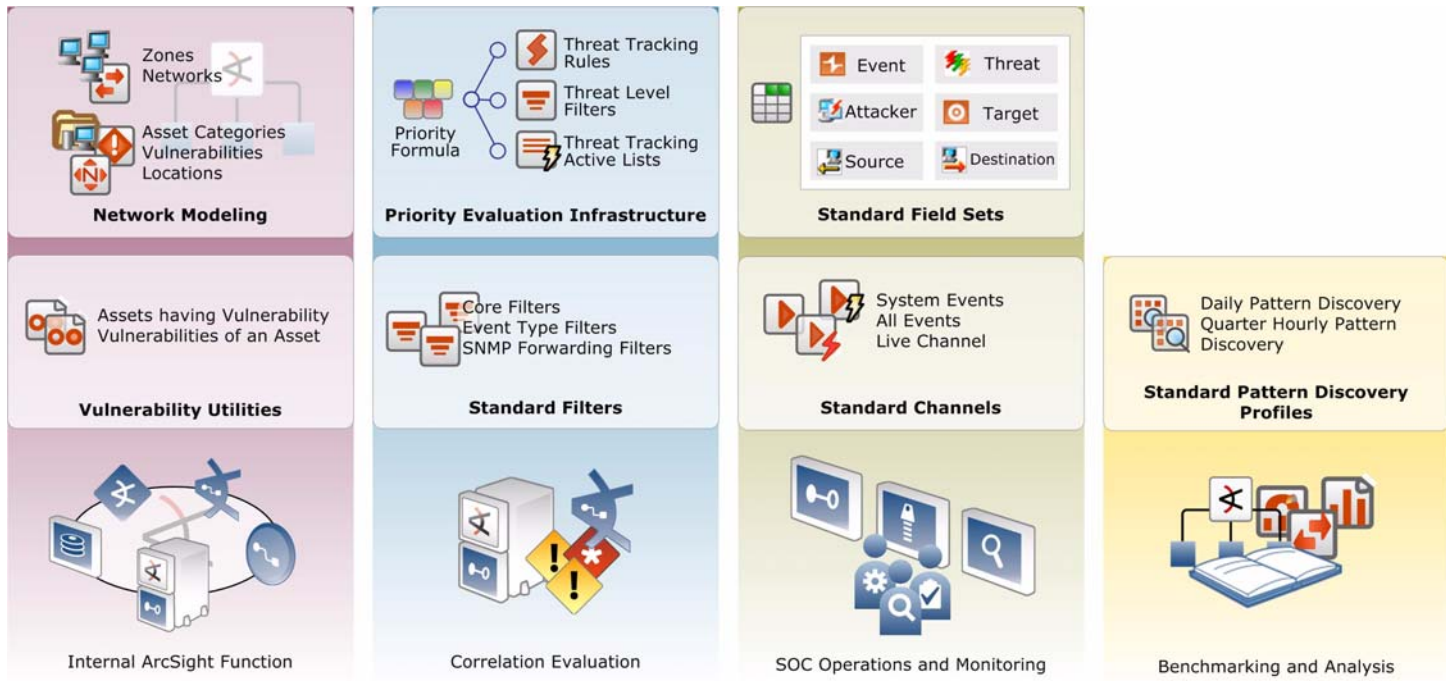
This chapter describes the system content that is automatically installed with ESM.

- ["System Content Overview" on page 26](#)
- ["Internal ArcSight Function" on page 26](#)
- ["Correlation Evaluation" on page 34](#)
- ["SOC Operations and Monitoring" on page 41](#)
- ["Benchmarking and Analysis" on page 45](#)
- ["Core Reports" on page 46](#)
- ["Standard Report Templates" on page 47](#)

## System Content Overview

The system content consists of a series of standard features and resources that support basic ESM function:

- Internal ArcSight Function
- Correlation Evaluation
- SOC Operations and Monitoring
- Benchmarking and Analysis



**Figure 2-1** The standard features included in the core content support basic ESM function.

## Internal ArcSight Function

The system content contains sets of resources that manage ESM's network modeling, vulnerability handling, and other internal ArcSight functions. These resources are leveraged by many basic systems and correlation use cases.

### Network Modeling Standard Resources

The network model is a representation of the nodes on your network and certain characteristics of the network itself. For critical assets on the protected network, network modeling captures important facts that helps the system identify and classify the sources and destinations involved in your network traffic.

The ArcSight resources that make up the network model are assets, asset ranges, zones, and networks; assets, asset ranges, and zones are found in the Assets menu in the Console Navigator panel. For an overview of how to set these up for your environment, see [“Set Up Connectors and Model the Network”](#) on page 5.

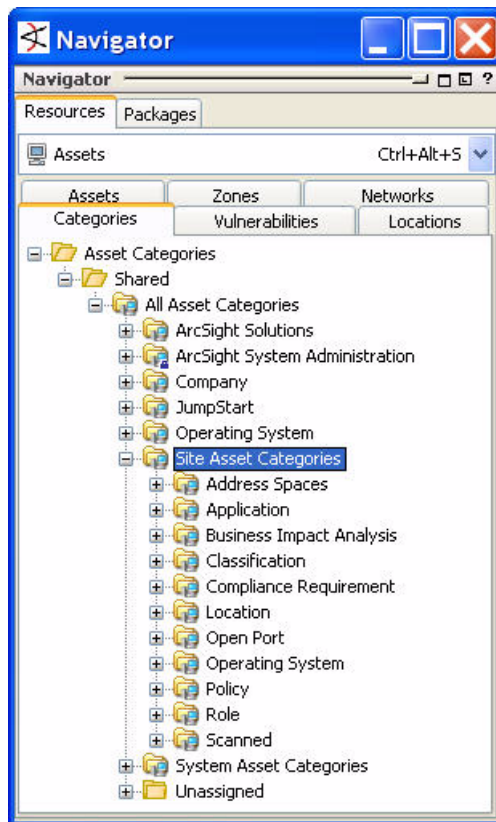
## Asset Categories

Asset categories are an extensible classification system stored as ArcSight resources. These classifications describe properties of an asset, such as the operating system running on it, key applications it hosts, its role in the enterprise, and any other properties you want to consider when evaluating threats or behaviors associated with the asset.

ArcSight ESM comes with a library of asset categories used by the standard content. Applying asset categories to the assets in your environment activates the standard content that uses these categories to apply criticality and business context to events. For an overview of how to set up asset categories, see [“Apply Standard Asset Categories to Assets” on page 7](#).

## Site Asset Categories

The Site asset categories provide a series of business-relevant categories, many of which are leveraged by the foundation packages.



The *Application*, *Open Port*, *Operating System* and *Scanned* asset categories are used by the scanner SmartConnector to automatically categorize assets. For example, Nessus can often identify the applications and operating systems a system runs, the vulnerabilities the system exposes, and keeps track of all the ports that were open on that system at the time of the last scan.

The foundations, such as the Intrusion Monitoring foundation, rely on the *Business Impact Analysis* categories, which includes the *Role* categories, the *Classification* category, and the *Compliance Requirements* categories.

ArcSight recommends that you add your own custom categories in the Site Asset Categories group. This group is specifically intended for you to extend with your own asset category system.



Although the Site Asset Categories group is not locked, you should retain the asset categories that are installed with ESM, since the foundations rely on many of them.

The Site Asset Categories are described below.

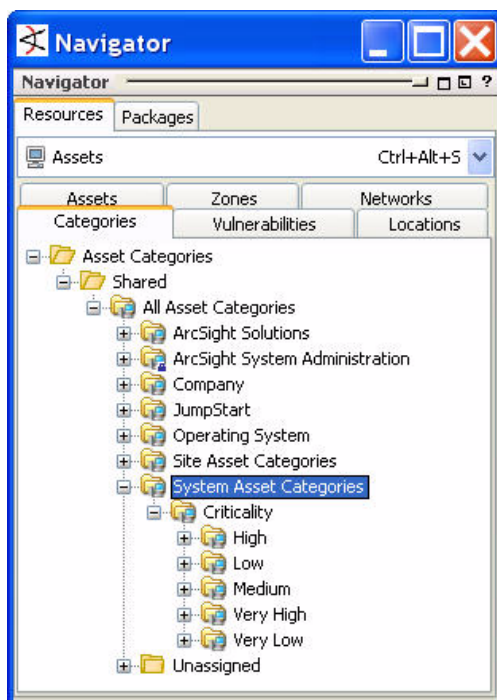
Asset Category	Description
Address Spaces	These categories include the Protected category, as well as some default categories used by zones (Dark for the Dark Address Space Zones, Protected for the Private Address Space Zones, etc.), and some potentially useful categories that can be attached to zones, like VPN and Wireless.
Application	These categories are maintained by scanner connectors.
Business Impact Analysis	This includes the Role categories and the Classification categories. This is used by the Intrusion Monitoring resources.
Location	Should be manually added to zones. For more about locations, see <a href="#">"Locations" on page 33</a> .
Open Ports	These categories are maintained by scanner connectors.
Operating System	These categories are maintained by scanner connectors.
Policy	This category should probably be manually added to systems that are significant relative to a company's computer use policy. Known malicious servers, porn, IRC servers, etc., could have assets created and have the disallowed servers category attached to them. Resources could then be written to notify or track connections to these servers.
Role	Common business and data roles, used by Business Impact Analysis.
Scanned	Maintained by scanner connectors. Each asset, when scanned, can be marked as scanned for open ports, scanned for vulnerabilities, or both. Note that the actual list of vulnerabilities found by a scanner are not listed under Asset Categories, but under Vulnerabilities. The Scanned asset category is used to determine whether, and what type of, a scan has (ever) been done.

## System Asset Categories

The System asset categories contain the Criticality asset categories, which are leveraged by the Priority Formula. The priority formula is discussed in more detail in ["Priority Evaluation Infrastructure" on page 34](#).



The Criticality asset categories are locked, and cannot be moved, renamed, or modified.



The *Criticality* asset categories tell ESM which events involve the highest priority assets in your network. Prioritizing assets using this rating system is central to how much of the standard content sorts events. To make the most out of ArcSight's standard content, you should classify your assets in these asset categories at set-up time, especially those that qualify as *High* and *Very High* Criticality. Events whose asset criticality is not set are registered by the system as *Criticality Unknown*. For more about how to configure your assets with these asset categories, see ["Categorize Critical Assets" on page 8](#).

## Vulnerabilities

A vulnerability is any hardware, firmware, or software state that leaves an asset open for potential exploitation. The *All Vulnerabilities* group provides a list of known vulnerabilities published by popular authorities.

These vulnerabilities are updated by the scanner SmartConnectors every time a scan is run. Not every vulnerability possible will be listed, only those found on the network by the scanner or those used explicitly by some part of the system content (such as the SANS Top 20 rules).

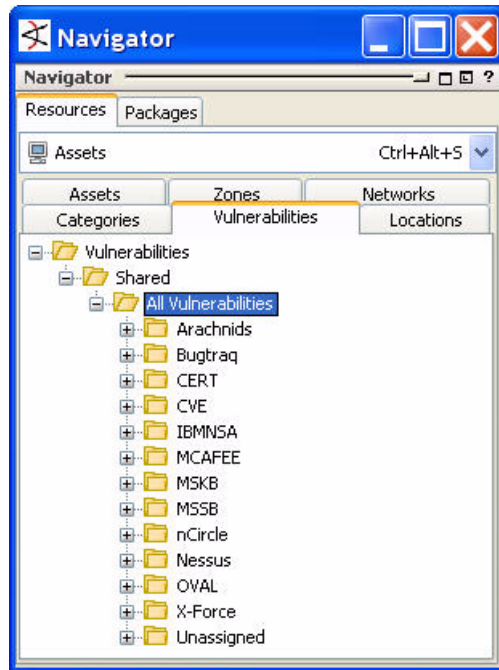
Not every vulnerability scanner will report all the possible names of a vulnerability. Most of the vulnerability publishers use their own vulnerability names, CVE name, and possibly CERT name. For example, if you use Nessus, the whole host of nCircle vulnerabilities will not also appear, unless you also have nCircle. Scanners are updated just like IDS and anti-virus engines, so if your scanner is not updated with the latest vulnerability profiles, the vulnerability list also will not be updated.

Vulnerability scans don't directly use the Vulnerabilities, but the scanner SmartConnectors do attach the vulnerabilities to the appropriate assets, much like they attach *Open Ports* categories to assets.



If assets have vulnerabilities associated with them, the standard resources that reference these vulnerabilities make it possible to monitor and track systems that expose certain vulnerabilities over time, and track the number of assets with vulnerabilities. With these vulnerability identifiers, you can also create your own vulnerability tracking content.

For more about how ESM uses vulnerabilities, see *ESM 101*.



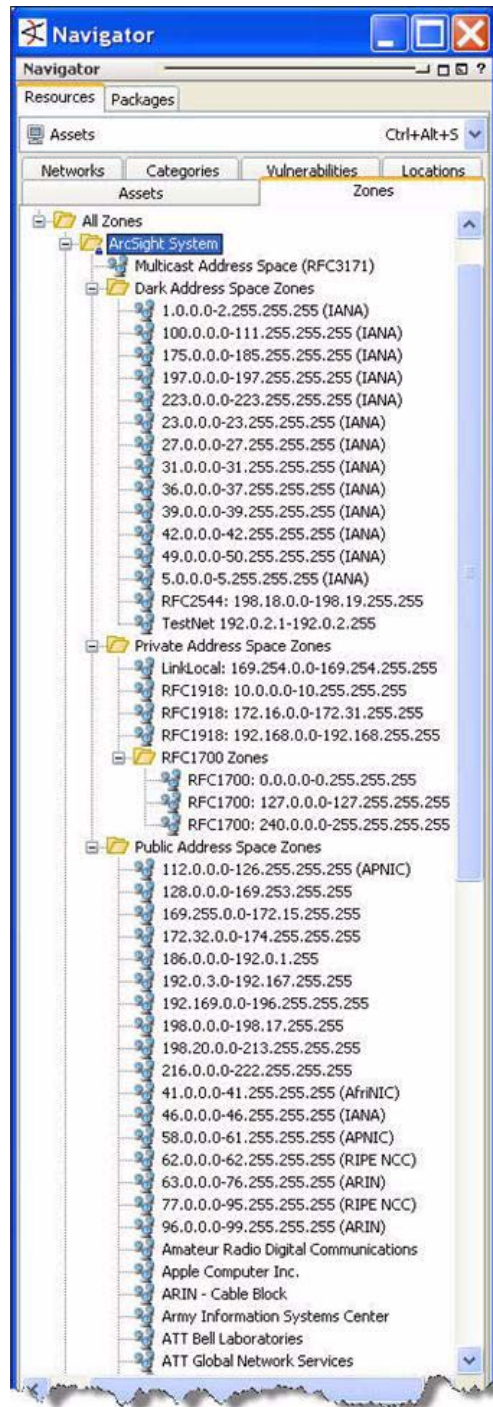
## Zones

A zone represents part of the network, and is identified by a contiguous block of IP addresses. Zones usually represent a functional group within the network or a subnet, such as a wireless LAN, the engineering network, the VPN or the DMZ. Zones are also how ESM resolves private networks whose IP ranges may overlap with other existing IP ranges.

Every asset or address range must have a zone associated with it. ESM comes configured with the standard global IP address ranges already grouped into zones, so if your network uses only these public IP addresses, ESM can resolve them without setting up any additional zones. However, if the devices reporting in to ESM are part of a subnet or contain



one or more private networks, you must set up zones so that ESM can resolve the IP addresses of those assets on your network.



**Multicast Address Space (RFC3171):**  
This zone represents addresses for hosts that have joined a Multicast group.

**Dark Address Space Zones:** These zones represent known dark address spaces. There should be no traffic to or from these ranges.

**Private Address Space Zones:** These zones represent any private address spaces used by ESM-monitored devices on your network.

**RFC1700 Zones:** These zones represent the IP address ranges reserved as the experimental block (also known as Class E—RFC 1700 [8]).

**Public Address Space Zones:** These zones represent known public address spaces. The owners of these ranges may have further subdivisions within their ranges. These organizations would use the Local Network to represent the subdivisions of their public address spaces.

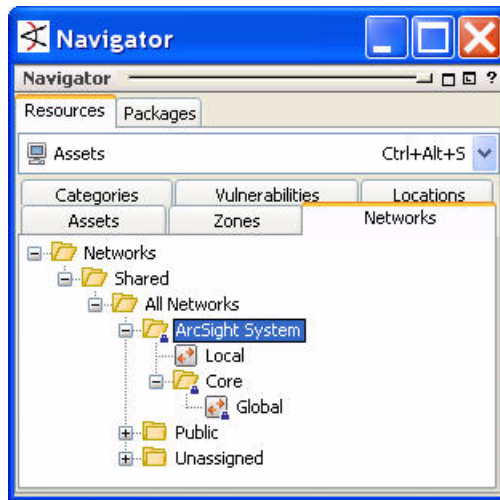
## Networks

The Network resource is a collection of zones. ArcSight uses Networks to differentiate between the private address spaces (zones) used in your network environment that overlap with other private address spaces, or those provided with ESM (ArcSight System zones).

For example, you would create unique Networks if your protected network uses Network Address Translation (NAT) and you have two or more NAT subnets that use the same private address space. You would also create unique Networks if your protected network uses a private address space that overlaps one of the Public Address Spaces provided by default with ESM.

ArcSight provides the *Local* Network for you to create separate Networks for your private address zones that overlap with other private address spaces in use on your ESM-monitored network, or any of the ArcSight System zones.

The *Global* Network is used by ESM to represent the default ArcSight System zones (described in [“Zones” on page 30](#)).



Network	Description
Local	The Local Network group is provided for you to create the Networks you need to differentiate custom zones with overlapping address spaces. Zone mappings in this Network will override the default zones in the Global Network.
Global	This Network contains the default zones provided with ESM. Use the Local Network to differentiate custom zones with overlapping address spaces.

## Locations

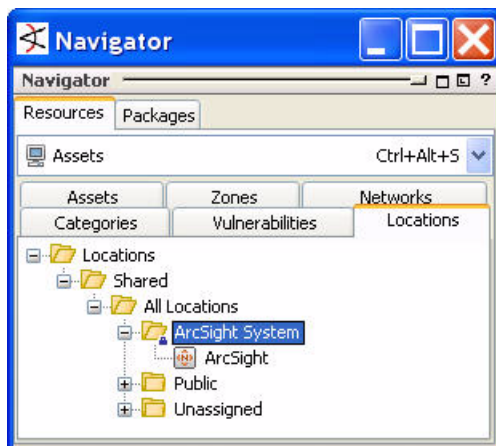
ArcSight provides a default location database that maps the IP addresses of event endpoints to its owning body for the block of IP addresses to which it belongs. This default location database is used by the Manager to find a latitude/longitude record (which also includes city, state, and country information) for each IP address in each endpoint reported by each event. This location data is used to populate the geographic map event graph available in the Viewer panel.

In some cases, the location mapping is inaccurate, or the IP address has no mapping at all, such as for private networks.

The location resource enables you to override the default location mapping provided automatically by the Manager by specifying the correct location for a known IP address whose mapping is wrong, and to specify locations for endpoints on private networks.

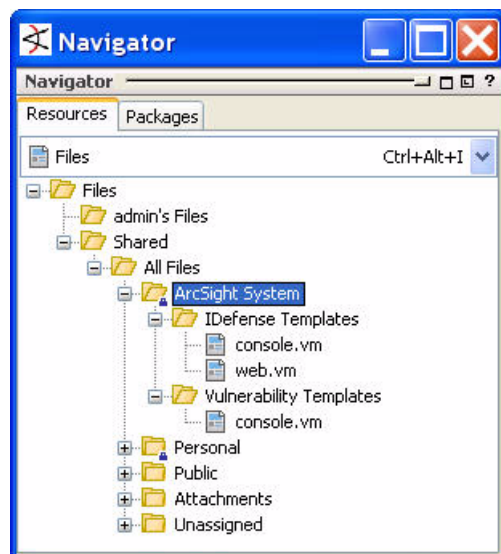
- If the override location is assigned to an **asset**, the location overrides the resolved longitude/latitude record from the internal database.
- If the location is assigned to a **zone**, it overrides the latitude/longitude record for all assets in that zone.
- If the location is assigned to a **network**, it overrides the latitude/longitude record for all zones in the network, and all the assets that belong on those zones.

If no override location is found, ESM uses the default location mapping, which is derived from ARIN records. The default ArcSight location is a placeholder.



## Files

The files in the ArcSight System group contain Velocity template macros for vulnerability data and IDefense data. The `.vm` files contain the variable names that correspond with the event fields and reference pages related to qualifying events, and can be configured with the event fields you want to display for these features.



If you have IDefense set up, you can use the *IDefense Templates* `console.vm` and `web.vm` to configure the event fields displayed in the event inspector for the ArcSight Console view and the ArcSight Web view. For more about IDefense setup, see the ArcSight Administrator's Guide Appendix A, *ArcSight Commands*.

The *Vulnerability Templates* `console.vm` file populates the reference pages and event inspector views with vulnerability mapping data. You can also configure the variables specified in these files to match the event fields you want to display for vulnerability mapping.

For more about how ESM uses velocity templates, see the topic *Velocity Templates* in ESM 101 and the Console Help.

## Correlation Evaluation

System content active lists and filters help drive parts of ArcSight's correlation engine.

## Priority Evaluation Infrastructure

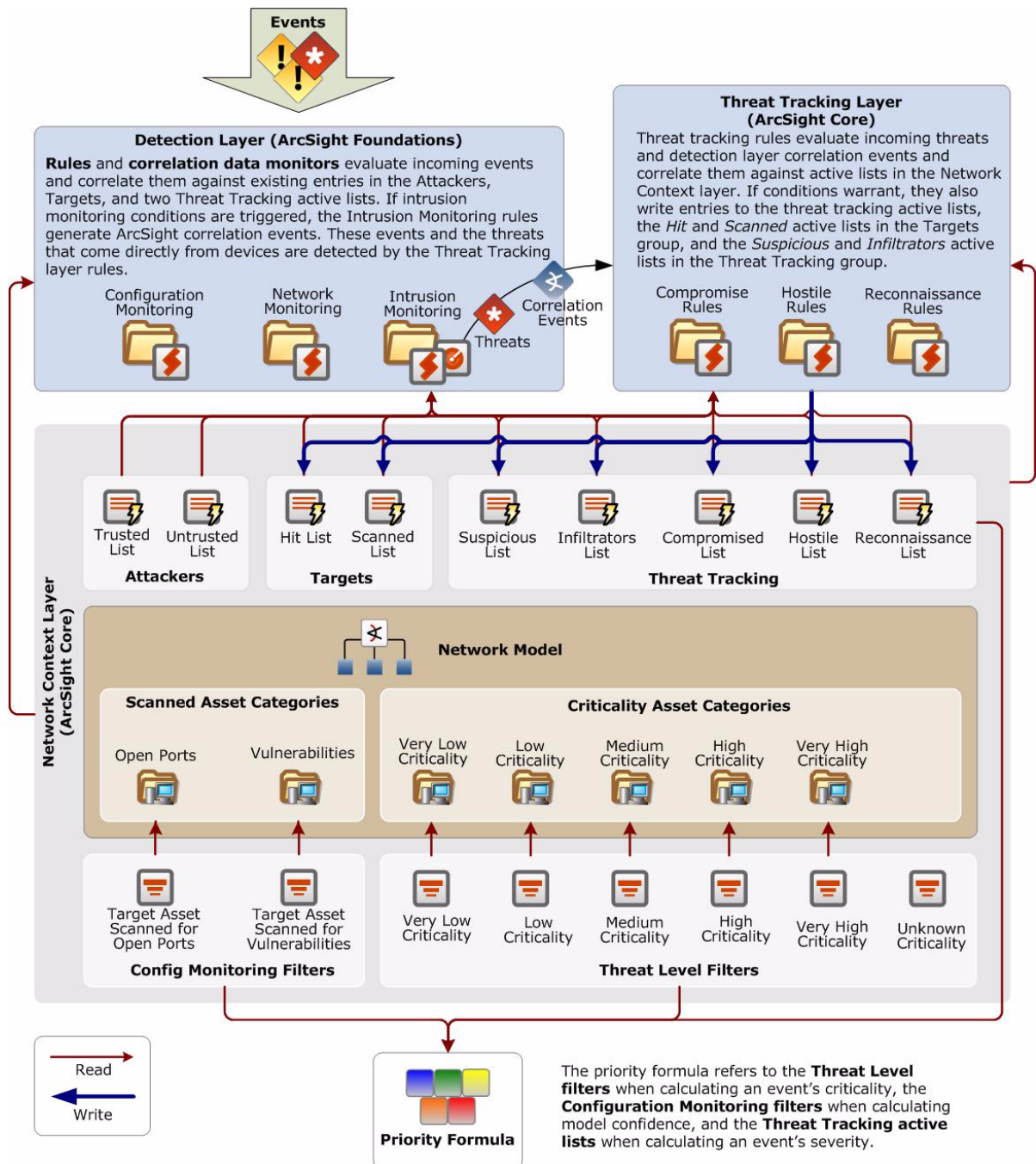
Priority evaluation is an automatic feature of ESM that is always "on," and is applied to all the events received by the ArcSight Manager. Calculating an event's priority signals to security operations personnel which events warrant further notice and in what order.

An event's priority is calculated by the priority formula, also referred to as the threat level formula. The priority formula is an algorithm made up of five criteria that each event is evaluated against to determine its relative importance, or priority, to your security operations.

The priority formula itself is managed and maintained on the Manager, and is supported by an infrastructure of network model classifications, active lists, filters, and rules that track

an event's classification based on specific conditions. These conditions are expressed in the threat tracking and priority evaluation resources included in the core content.

The diagram on the next page shows the layers of ArcSight resources that influence the priority evaluation process. The sections that follow describe the priority evaluation resources in more detail.



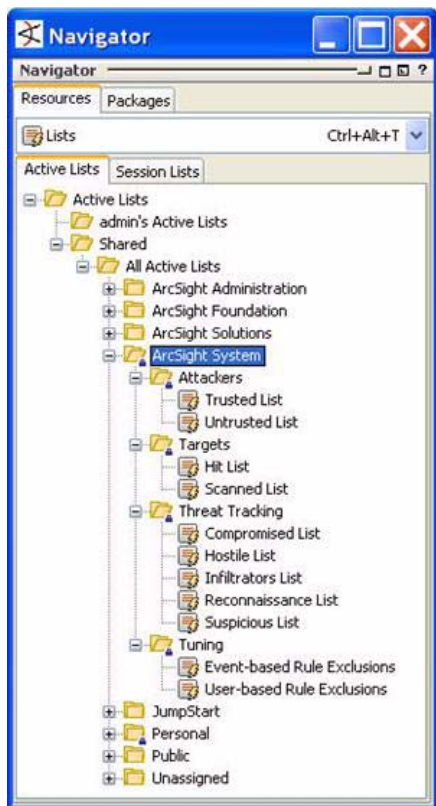
**Figure 2-2** Threat tracking and evaluation is based on the priority formula and managed through a multi-tiered infrastructure that tracks events and their priority based on aggregated conditions.



## Threat Escalation Active Lists

There are three groups of active lists that factor into priority evaluation:

- Attackers
- Targets
- Threat tracking
- Tuning



**Attackers:** These active lists contain entries written to them manually during configuration to indicate systems that should be included or excluded from consideration by ArcSight conditions expressed in rules, filters, and other resources.

**Targets:** These dynamic active lists contain entries written to them by the Threat Tracking rules, which look for events from systems that perform scans on protected network assets.

**Threat Tracking:** These dynamic active lists contain entries written to them by the Threat Tracking rules, which look for events from systems that exhibit compromised characteristics, either directly, or via correlation events generated by the Intrusion Monitoring foundation suite.

**Tuning:** These active lists are used to store specific event and user situations that are determined to be low or no risk in order to prevent false positives. These active lists support ArcSight Express content.

### Attackers Active Lists

The static active lists in the Attackers group, *Trusted* and *Untrusted*, act as a way to include or exclude the systems listed there in a condition statement, whether the condition is in a rule, filter, active list, report query, or other resource. These active lists should be configured during system setup. For instructions about how to configure active lists, see [“Configure Active Lists” on page 9](#).

Active List	Description
Trusted List	This is a list of systems (include the IP Address and Zone) that are trusted to perform activity, such as network mapping, vulnerability scans, port scans, etc., that would be considered suspicious or hostile from any other source. This can include permanent internal scanner devices or IP addresses of security consultants who are under contract to scan your network.

Active List	Description
Untrusted List	This is a list of systems that are known to be hostile or compromised. An ArcSight user could insert an external system that has successfully attacked internal assets, external systems that are known to be hostile based on a third-party blacklists, or internal systems that are known to be compromised (by an attacker, a worm, or some insider threat), and have not yet been recovered and cleaned up.

### Target Active Lists

The dynamic active lists in the Targets group, *Hit List* and *Scanned List*, act as a way to include or exclude the systems listed there in a condition statement, whether the condition is in a rule, filter, active list, report query, or other resource. These dynamic active lists are populated during run-time by rules triggered by qualifying events.

Active List	Description
Hit List	This list holds target asset data for assets that have been attacked, whether successfully or not. An asset's presence in this list does not mean that it has been compromised, but that a compromise attempt has been made.
Scanned List	This list holds target asset data for assets that have been scanned. Usually, the scanning system will be listed in the Reconnaissance List under Threat Tracking.

### Threat Tracking Active Lists

The threat tracking active lists correspond directly with the threat tracking rules *Compromise*, *Hostile*, and *Reconnaissance*. The threat tracking active list group also contains two active lists whose entries are read by rules in the intrusion monitoring foundation.

The threat tracking active lists are described below. These active lists are dynamically populated by rules, so no configuration is required, although you can manually configure the active lists with systems you know are compromised. For example, you might want to populate one or more of these lists manually during system testing.

Active List	Description
Compromised List	This list contains assets that have been successfully compromised.
Hostile List	This list contains attacker information on systems that have attempted to or successfully attack an asset.
Infiltrators List	This list contains attacker information on systems that have successfully attacked an asset.
Reconnaissance List	This list contains attacker information on systems that have exhibited reconnaissance activity against one or more assets on the network.
Suspicious List	This list contains attacker information on systems exhibiting suspicious behavior, such as attempting to open connections to other systems that shouldn't exist (systems with addresses in Dark Address Space), or systems that have been performing brute force logon attacks.

## System Filters

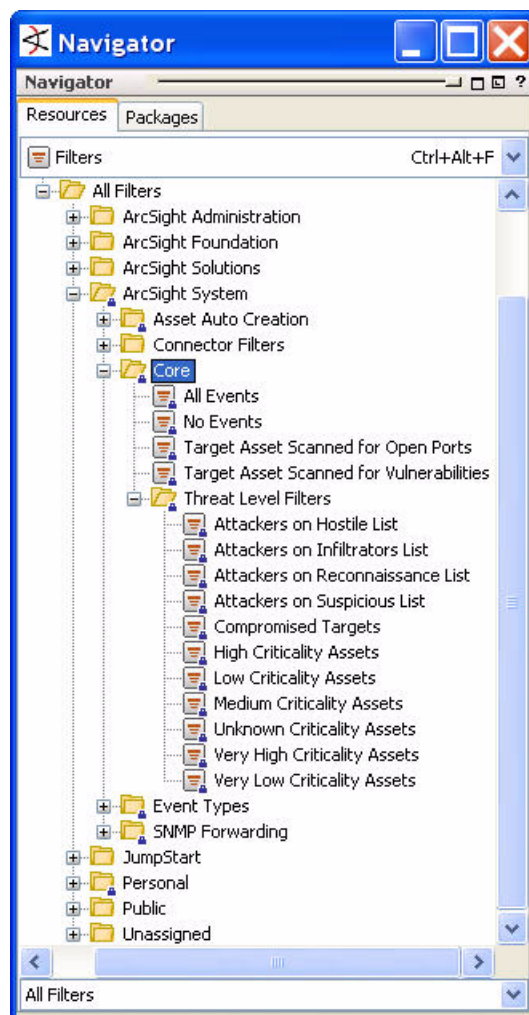
The filters contained in the ArcSight System filters group support various essential ArcSight functions.

## Core Filters

The Core filters group contains a series of filters used by essential out-of-the-box features, such as the ArcSight System, All Events, and Core active channels, and features of the priority formula.



All the filters in the Core filters group are locked, which means they cannot be modified, moved, or deleted.





The core filters are described in more detail below:

Filter	Description
All Events	Filter that matches all events.
No Events	This is a utility filter that will not match any events passing through the system.
Target Asset Scanned for Open Ports	This filter selects events where the Target Asset ID is categorized as scanned and showing open ports. This filter is used by the priority formula.
Target Asset Scanned for Vulnerabilities	This filter selects events where the Target Asset ID is categorized as scanned and showing vulnerabilities. This filter is used by the prioritization formula.
Attackers on Hostile List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Infiltrators List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Reconnaissance List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Attackers on Suspicious List	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.
Compromised Targets	This filter is used by the Threat Level Formula to determine whether an entity is in the relevant active list.

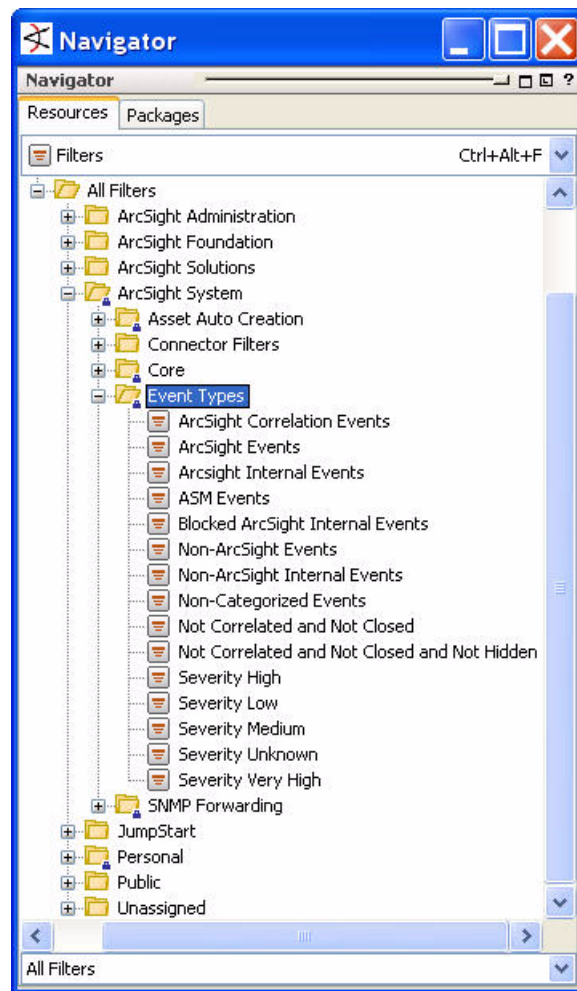
## Event Type Filters

The Event Type filters include all the different types of events that ArcSight identifies. These are used by the Priority Formula, the correlation engine, ArcSight administrative function, and many of the foundation resources.

For example, the Event Privileges tab in the User Groups access control list editor uses the All Events filter to set the Event Privileges that the different user groups, such as Operators and Analyzer Administrators. The Event Types filters are used to populate this list.



The Event Types filter group is locked, which means the group and its contents cannot be moved, added to, or deleted.



## SNMP Forwarding Filters

The System filters group also has a group that contains an SNMP Trap Sender filter. This filter is only needed if you have SNMP traps that forward events to a network management system, such as HP OpenView.

If you have SNMP forwarding enabled, this filter should be configured with the name of the filter whose events match the SNMP Trap Sender filter to forward events to the network management system. For instructions about how to configure this filter, see [“Configure SNMP Trap Forwarding Filter” on page 13](#).

For instructions about how to enable the SNMP trap sender on the ArcSight Manager, follow the instructions outlined in the *ArcSight Administrator's Guide* in chapter 4, *Configuration*.

## SOC Operations and Monitoring

The system content provides standard field sets and active channels to provide basic operations and monitoring functions out of the box.

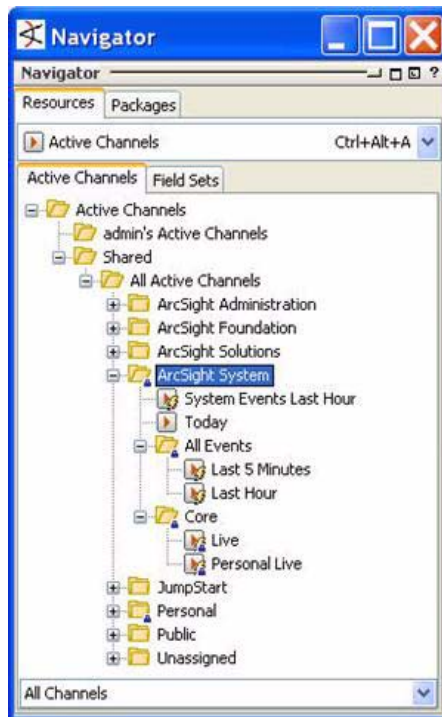
### System Active Channels

The system channels are a basic set of active channels that support out-of-the-box monitoring functionality.

At installation, these active channels verify feeds coming in from network devices through ArcSight SmartConnectors, and verify that the SmartConnector settings are correct.

During SOC operations and monitoring, these views can be a first place to start to observe the flow of events from the monitored devices on the network.

During incident investigation, these channels can provide a contextual launching place for drill-down and investigation into an event or series of events.



**ArcSight System:** These active channels show all ArcSight internal events, live events in the last hour, and all events from the past 24 hours.

**All Events:** These active channels are the default monitoring grids that display the flow of all events through the ArcSight system.

**Core:** The Live channel shows events received from devices during the last two hours. It filters out internal events and those that contributed to correlation events. The Personal Live channel also filters out events assigned to the current user.

## ArcSight System Active Channels

Active Channel	Description
System Events Last Hour	Channel showing all events generated by ArcSight during the last hour. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.
Today	Channel showing events received today since midnight. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.

## All Events Active Channels

The All Events active channels show all events: those generated by devices, and all those generated internally by ArcSight.

During installation, these channels are helpful to verify the complete throughput of events from devices as well as ArcSight internal events to verify that all feeds are being received as expected.

When an ArcSight admin creates new users, this channel can also be effective to test that the access control levels (ACLs) set for the user are showing the intended event data. Only event data that the user has permission to view should be available.

During content development, you can use this channel to test that your conditions find the intended event data and/or initiate the intended actions.

Active Channel	Description
Last 5 Minutes	Channel showing events received during the last five minutes. The channel includes a sliding window that always displays exactly the last five minutes of event data.
Last Hour	Channel showing events received during the last hour. The channel includes a sliding window that always displays exactly the hour of event data.

## Core Active Channels

The Core group contains the *Live* active channel, which shows a sliding window of the last two hours' events. To maximize performance and throughput, the channel shows aggregated events and correlation events generated by triggered rules rather than all the raw events that led up to them.

Active Channel	Description
Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.

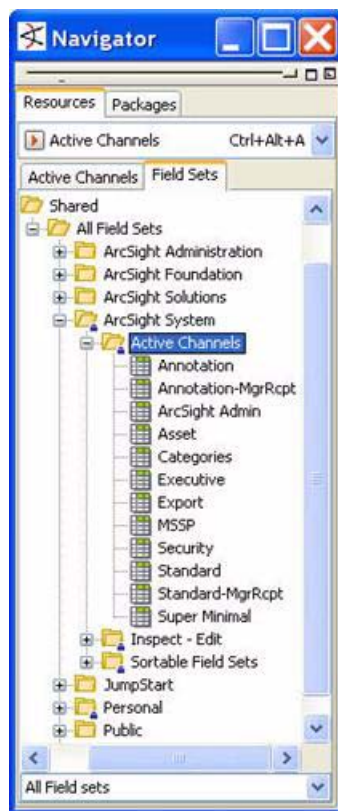
Active Channel	Description
Personal Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events. This channel also hides the events that have been assigned to the current user.

## System Field Sets

Field sets are collections of event fields stored as ArcSight resources that narrow the number of event fields displayed in certain situations, such as active channels and the common conditions editor in the Inspect/Edit panel.

### Active Channels

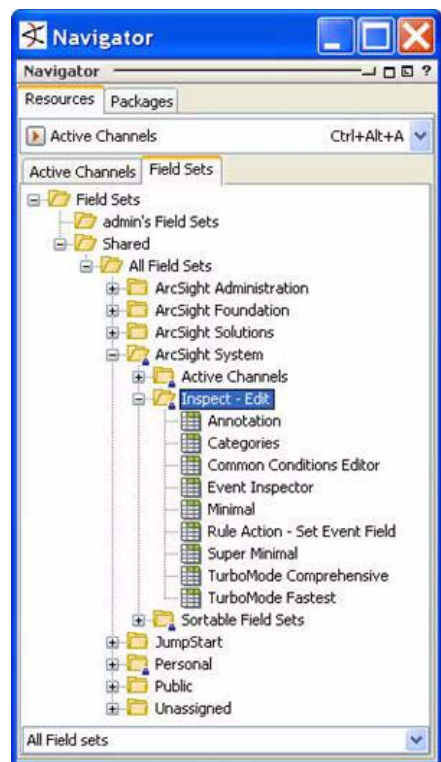
Event fields are displayed in active channels as column headers, for example *AssetID*, *Event Name*, and *Target User Name*. The standard field sets designed for active channels narrow the number of event fields displayed to those that are most pertinent to certain types of monitoring.



**Active Channels:** These field sets provide a set of event fields limited to those that are most relevant to certain types of monitoring.

## Inspect - Edit Field Sets

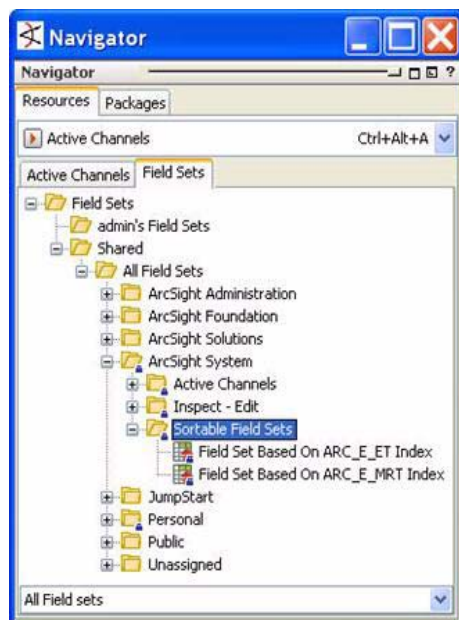
Event fields are also presented in groups in the Common Conditions Editor in the Inspect/Edit panel. The field sets designed for this use narrow the number of fields displayed to those that are applicable to certain kinds of correlation.



**Inspect - Edit:** These field sets provide a collection of event fields limited to those that are most relevant to certain types of correlation activities.

## Sortable Field Sets

Indexed sortable field sets are available in both active channels and the Common Conditions Editor.



**Sortable Field Sets:** These field sets contain only fields that are indexed, which enable an active channel column to be sorted by the entries in that column.

These field sets are used internally by ESM to keep track of fields that are indexed and can be used as a sorting criteria in channels and queries. Authors can refer to these field sets to determine whether a field they are using is indexed.

## Benchmarking and Analysis

ArcSight provides Pattern Discovery, a benchmarking and analysis add-on module. As part of the standard content, ArcSight includes two Pattern Discovery profiles. These profiles will be active only if you have the Pattern Discovery module installed.

### Pattern Discovery Profiles

Pattern Discovery is ArcSight's separately licensed data mining module. Pattern Discovery automatically identifies patterns that occur in an event flow that you didn't know to look for. Pattern Discovery can be used for benchmarking, that is, identifying patterns of normal activity that you can then filter out, and it can be used as a regular diligence check on historical data flows to ensure you're not missing anything in your daily operations.

To support these functions, the system content provides the following two Pattern Discovery profiles:

- Daily Pattern Discovery
- Quarter Hourly Pattern Discovery

The Daily Pattern Discovery profile can be used as a daily check for any patterns of activity that may have been overlooked during real-time operations.

The Quarter Hourly Pattern Discovery can be used as an investigation tool.

Both profiles can be used for benchmarking to find normal activity patterns that can be filtered out when building your own correlation content.

For more about Pattern Discovery, see the *ArcSight Pattern Discovery Guide* or call Customer Support (see ["Feedback" on page ix](#)).

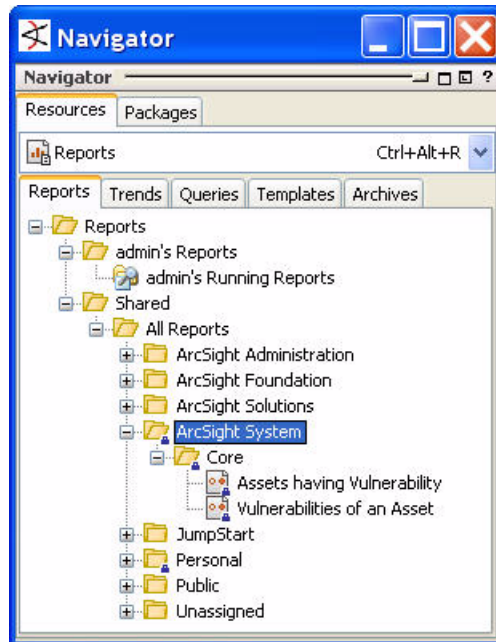
## Core Reports

The Core reports group contains two special reports that are used internally by the ArcSight vulnerability update structure.



These reports cannot be scheduled, and are not intended to be run as stand-alone reports.

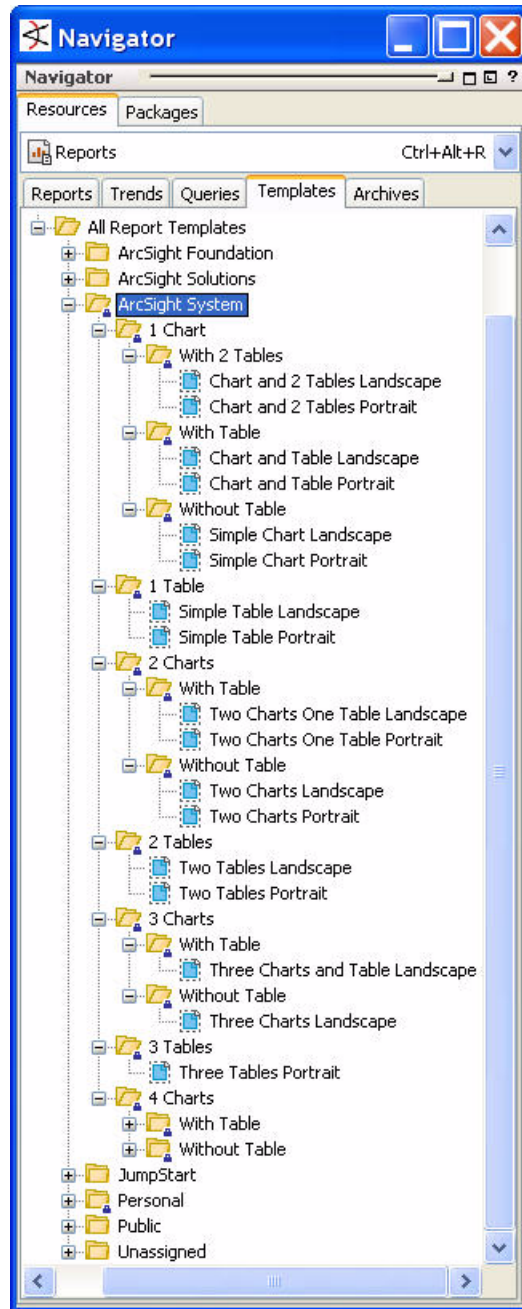
The Assets Having Vulnerability report lists all the assets that expose a particular vulnerability. The Vulnerabilities of an Asset report lists all the vulnerabilities exposed by a particular asset.





## Standard Report Templates

ESM 4.0 is installed with a series of standard report templates, which define the layout of the reports contained in the System and Foundation content. These templates are also available for you to use for reports you create.



The report templates' parent groups are locked, which means you cannot move, rename, or delete the report templates. You can perform some minimal customizations, however, as directed in the following sections.

## Customize Branding in Standard Templates

By default, the standard ArcSight report templates are branded with the ArcSight logo. You can customize this branding with your own corporate logo.

### To change the company logo branding:

- 1 Right-click the standard report template you wish to customize and select **Edit Template**.
- 2 In the Report Template editor in the Inspect/Edit panel, click **Open in Designer**.
- 3 In the Report Designer, select, then right-click the ArcSight logo and select **Properties**.
- 4 In the Image Properties dialog, select the Image tab and click **Browse**.
- 5 Browse to the image file you wish to use and click **Open**, then **OK**.
- 6 Save and close the report template (**File > Save**, or **Ctrl + S**).

## Making Custom Modifications to Standard Templates

It is possible to make other custom modifications to a standard template. Before you do however, be aware of the following:



- If you remove an element (such as a chart, table, text box for title) in the report template, all the reports that use this template will also lose their link to that element. The report will not be broken, but the link between the query and the deleted chart, table, or text box, will be broken.
- If you add an element (such as a chart or table) to the report template, all the reports using this template will need to be modified or updated to make use of the new element. If they are not updated, the element will appear empty. If you add a new text box to the template, the default text is set in the report template, so any reports linked to the template will automatically display the new text box and the default text.
- Renaming an element in a report template will also break the links between the queries and the elements they are linked to (charts and tables).

The things you can safely change without breaking any report elements include:

- Move, resize elements (such as the size of the chart)
- Change the default parameters of an element (such as default text in a text box, colors for the charts, default font sizes for tables, and so on)

Follow these tips when modifying a standard template.

- Make a copy of the template you want to customize and make modifications to the copy.
- Use a resource graph to view what reports the template supports.
- After making modifications to the copy, go to the reports the template supports and point the report to the new modified template.



Note that any changes made directly to a standard template will likely be overridden during future upgrades.

# Upgrading ArcSight Standard Content

---

This topic applies if you are upgrading from ArcSight ESM version 4.0 SPX to ArcSight ESM v4.5 SP1. For a complete description of the changes available in ArcSight ESM v4.5 SP1, see the *Release Notes for ArcSight ESM v4.5 SP1*.

ArcSight ESM is upgraded using the process described in the tech note *Upgrading ArcSight ESM v4.0 SP3 to v4.5 SP1*. If you run a multiple-Manager environment, also see the tech note *Upgrading Hierarchical or Other Multi-Manager ArcSight™ ESM Installations to v4.5 SP1*.

This appendix describes how to prepare ArcSight ESM standard content for the upgrade process, and how to verify content and reapply affected configurations after the software upgrade process is completed.

[“Preparing Existing Content for Upgrade” on page 49](#)

[“About Running the Upgrade Installer” on page 51](#)

[“Verifying and Reapplying Configurations After Upgrade” on page 51](#)

## Preparing Existing Content for Upgrade

The majority of ArcSight ESM standard content does not need configuration, and does not require special preparation for upgrade. Upgrade preparation is recommended only for content that has been configured *and* whose configurations are not preserved after the upgrade.

This topic describes which configurations are preserved during the upgrade, and which resources require reconfiguration after the software upgrade. It then describes how to back up the resources that require reconfiguration to help facilitate the process of restoring the configurations after the software upgrade is complete.

## Configurations that Persist

The following resource configurations are preserved during the upgrade process. No restoration is required to these resources after the upgrade.

- Asset modeling done to network assets, including:
  - ◆ Assets and asset groups and their settings
  - ◆ Asset categories applied to assets and asset groups
  - ◆ Locations
  - ◆ Networks

- ◆ Vulnerabilities applied to assets
- ◆ Custom zones
- SmartConnectors
- Users and user groups
- Active list entries
- Report schedules
- Notification destinations and priority settings
- Cases
- Custom content added by the customer or ArcSight Professional Services. Custom content is considered to be any resource created from scratch or copied and modified from ArcSight-supplied content.

## Configurations that Require Restoration After Upgrade

The following resources require restoration after upgrade.

- Any configurations made to ArcSight-supplied **filters**, such as those described in [“Configure Asset Auto-Creation Filters” on page 9](#).
- Any configurations made to ArcSight-supplied **rules**, such as those described in [“Configure Rules to Send Notifications and Open Cases” on page 15](#).
- Modifications made directly to ArcSight ESM system and core content not already described in this document.

## Backing Up Existing Resources Before Upgrade

To help the process of reapplying configurations to resources that require it after upgrade, back up the resources you identified in [“Configurations that Require Restoration After Upgrade” on page 50](#) by creating a copy of them in a user-defined group. Once copied and saved to a user-defined directory, the content is considered custom content, which is preserved during the upgrade process. After upgrade, you can reference these copies while reapplying the configurations in the v4.5 SP1 environment. This process is described in the following section.



### Copy and paste configurations from the old resources to the new

Instead of overwriting the new resources with the backed up copies of the old ones, copy and paste configurations from the old resources one by one into the new ones. This will ensure that you preserve your configurations without overwriting any improvements provided in the v4.5 SP1 content.

To create a backup copy of the resources that require restoration after upgrade, do this:

- 1 For each resource type (filters, rules, active lists), create a new group under your personal group. Name it in a way that identifies what it contains, such as *ESM v4.5 Backup*.
  - ◆ Right-click your group name and select **New Group**.
- 2 Copy the resources into the new group. Repeat this process for every resource type you want to back up.
  - ◆ Select the resources you want to back up and drag them into the backup folder you created in [Step 1](#). In the *Drag & Drop Options* dialog box, select **Copy**.

## About Running the Upgrade Installer

After copying the configured resources, you are ready to run the upgrade installer using the process described in tech note *Upgrading ArcSight ESM v4.0 SP3 to v4.5 SP1*. (If you run a multiple-Manager environment, see the tech note *Upgrading Hierarchical or Other Multi-Manager ArcSight™ ESM Installations to v4.5 SP1*).

During the upgrade process, the upgrade installer performs a resource validation check. If any resource is found to have an invalid condition or to be in an invalid state, the condition is added to the upgrade report.

The upgrade installer also gives you the choice to save the reason the resource was invalid in the database (**Persist conflicts to the database=TRUE**). If you choose this option, the upgrade installer:

- Saves the reason the resource was found to be invalid in the database, so you can generate a list of invalid resources, which you can use later to manually repair the problems.
- Disables the resource, so it does not try to evaluate live events in its invalid state.

If you choose not to save the reasons the resource was invalid in the database (**Persist conflicts to the database=FALSE**), the invalid resources remain enabled, which means they try to evaluate the event stream in their invalid state.



If you choose not to persist conflicts to the database and disable invalid resources, the Manager could throw exceptions when the invalid resources try to evaluate live events.

For more about fixing invalid resources after the upgrade, see [“Fixing Invalid Resources” on page 52](#).

## Verifying and Reapplying Configurations After Upgrade

After the upgrade is complete, do the following checks to verify that all your content has been successfully transferred to the v4.5 SP1 environment.

- 1 Verify that your configured ArcSight-supplied resources listed in the section [“Configurations that Persist” on page 49](#) retained their configurations as expected.
- 2 Reapply configurations to the resources that require restoration.

One resource at a time, copy and paste the configurations preserved in the copied version of the resources from the previous version into the new resources installed with the ArcSight ESM v4.5 SP1 upgrade. Copying your configurations one resource at a time instead of overwriting the new resources with the old will ensure that you retain your configurations without overwriting any improvements provided with the ArcSight ESM v4.5 SP1 content.

For instructions about what resources require configurations specific to your environment, see [Chapter 1, Standard Content Overview and Setup, on page 1](#).

## Verify Proper Function of Customer-Created Content

It is possible during upgrade that updates to the ArcSight standard content could cause resources you created to work in a way that is not intended. This case may show

symptoms such as a rule getting triggered too often, or a rule that should be getting triggered is not getting triggered at all.

For example, this could happen if you have a rule that uses an ArcSight System filter whose conditions have been changed such that rule matches more events than you expect, or doesn't match the events you expect. Another example is a moving average data monitor whose threshold has been changed.

To verify that the custom content you created that depends on ArcSight-supplied content works as expected, go through the following checks:

- **Trigger matching events.** Send events that you know should trigger the content through the system using the Replay with Rules feature. For more about this feature and how it's been enhanced for v4.0, see the online Help topic *Verifying Rules with Events*.
- **Check Live Events.** Check the Live or All Events active channel to verify if the correlation event is triggered, and check that data monitors you created are returning the expected output based on the test events you send through.
- **Verify notification destinations.** Verify that notifications are sent to the recipients in your notification destinations as expected.
- **Verify active lists.** Check that any active lists you have created to support your content are gathering the replay with rules data as expected.
- **Repair any invalid resources.** During the upgrade process, the resource validator identifies any resources that are rendered invalid (conditions that no longer work) during the upgrade. Find invalid resources and fix their conditions as appropriate. For more about invalid resources, see ["Fixing Invalid Resources" on page 52](#), below.

## Fixing Invalid Resources



During the upgrade process, the content is run through a resource validator, which verifies that the values expressed in the resource's condition statement still apply to the resource in its new format, and that any resources upon which it depends are still present and also valid. The resource validator is run on any resource that contains a condition statement, or populates the asset model:

- Active channels
- Filters
- Data Monitors
- Rules
- Report queries and schedules
- Assets and Asset ranges
- Zones

It is possible that during upgrade, the condition statement for a customer-created or modified resource can become invalid. For example, if there are two assets with the same IP address in the same zone, the resource validator will mark one of those resources invalid.

To fix an invalid resource, use the report generated by the upgrade process to locate the resources and understand what needs to be fixed.

When the problem that makes the resource invalid is fixed, the system automatically re-validates the resource when the fix is applied. If the resource was disabled, the system automatically re-enables the resource.

# Index

---

## A

- Active Channels
  - System Active Channels 41
- Active Lists
  - General Configuration 9
- active lists
  - general configuration 15, 17
- Asset Categories
  - Criticality 8
- Asset Modeling
  - Protected Network 7

## C

- Configuration
  - Active Lists 9
  - Report Templates 48
- configuration
  - active lists 15, 17
  - Asset Auto-Creation Filters 9
  - Connector Asset Auto-Creation Filter 10
  - Device Asset Auto-Creation Filter 12
  - SNMP Trap Forwarding Filter 13
- Core Content
  - About 25

## D

- Device List
  - Standard Content 6

## E

- Event Type Filters 39

## F

- Files 34
- Foundations 2

## L

- Locations 33

## N

- Network Modeling
  - What is 7

## P

- Pattern Discovery Profiles 45

- Priority Formula 34

- Criticality Asset Categories 8

## R

- Report Templates 47
  - Customize Branding in 48
- Resources
  - Shared Resources 4

## S

- SmartConnectors
  - For Standard Content 6
- SNMP Forwarding Filters 40
- Standard Content
  - Device List 6
  - Foundations 2
- System Content 3
  - About 25
  - Active Channels 41
    - Field Sets 43
  - Asset Categories 27
    - Site Asset Categories 27
    - System Asset Categories 28
  - Files 34
  - Filters 38
    - Event Type Filters 39
    - SNMP Forwarding Filters 40
  - Locations 33
  - Overview 26
  - Priority Formula 34
  - Reports
    - Core Reports 46
    - Vulnerabilities 29
- Sytsem Content
  - Reports
    - Report Templates 47

## T

- Threat Level Formula. See Priority Formula
- Trends
  - About 17
  - Enabling and Disabling 20

## U

- Upgrading ArcSight Express Content 49
  - After Upgrade 51
  - Preparing for Upgrade 49

**V**

Vulnerabilities 29