

ArcSight™ Express Content Guide

Exploring ArcSight™ Express Content

ArcSight™ Express v4.5 SP1

April 17, 2009



ArcSight™ Express Content Guide: Exploring ArcSight™ Express 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
4/17/09	ArcSight Express v4.5 SP1	Released draft of document with resource descriptions and upgrade instructions.

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	support@arcsight.com
Support Web Site	https://support.arcsight.com
Customer Forum	https://forum.arcsight.com

Contents

About the ArcSight Express Content Guide	v
Who Should Read this Guide	v
Text Conventions	v
Related Documentation	vii
Feedback	vii
 Chapter 1: ArcSight Express Content	 1
What is ArcSight Express Content?	1
How ArcSight Express Is Organized	2
Set Up Connectors and Model the Network	2
ArcSight Express-Related SmartConnectors	3
Network Modeling	4
Apply Standard Asset Categories to Assets	5
Categorize Internal Assets	5
How ESM Determines the Protected Network	5
Categorize Critical Assets	5
Create ArcSight Express Users	5
Configure Notification Destinations	6
Configure Asset Auto-Creation Filters	7
Configure Connector Asset Auto-Creation Controller Filter	7
Configure Device Asset Auto Creation Controller Filter	8
Configure Rules to Send Notifications and Open Cases	10
Schedule Reports	13
Tuning ArcSight Express Content	14
 Chapter 2: Resource Reference	 17
Cross-Device	17
Cross-Device Presentation Resources	17
Cross-Device Data Processing Resources	20
Anti-Virus	20
Anti-Virus Presentation Resources	20
Anti-Virus Data Processing Resources	21
Case Management	22
Case Management Presentation Resources	22

Database	25
Database Presentation Resources	25
Database Data Processing Resources	25
Firewall	26
Firewall Presentation Resources	26
Firewall Data Processing Resources	27
Identity Management	30
Identity Management Presentation Resources	30
Identity Management Data Processing Resources	30
IDS-IPS	32
IDS-IPS Presentation Resources	32
IDS-IPS Data Processing Resources	33
Network	34
Network Presentation Resources	34
Network Data Processing Resources	35
Operating System	38
Operating System Presentation Resources	38
Operating System Data Processing Resources	39
VPN	41
VPN Presentation Resources	41
VPN Data Processing Resources	42
Vulnerabilities	44
Vulnerabilities Presentation Resources	44
Vulnerabilities Data Processing Resources	45
Appendix A: Upgrading ArcSight Express Content	47
Preparing Existing Content for Upgrade	47
Configurations that Persist	47
Configurations that Require Restoration After Upgrade	48
Backing Up Existing Resources Before Upgrade	48
About Running the Upgrade Script	49
Verifying and Reapplying Configurations After Upgrade	49
Verify Proper Function of Customer-Created Content	49
Fixing Invalid Resources	50
Index	51

About the ArcSight Express Content Guide

ArcSight Express is a Security Information and Event Management (SIEM) solution that leverages the correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers a streamlined, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports, included as part of ArcSight Express Content.

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

[“Text Conventions” on page v](#)

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

[“Feedback” on page vii](#)

Who Should Read this Guide

This guide is intended for ArcSight Express users, administrators, and security managers with the responsibility to plan, implement, maintain, and use ArcSight Express 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
Bold	<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">• Enter a value and click OK.

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">If the name of your active list entries text file is "<code>AdministrativeUsers.txt</code>," the script would look like this:
<i>Emphasis or BookName</i>	<p><i>Italics</i> indicates emphasis or a book name:</p> <ul style="list-style-type: none"><i>Do not</i> perform this procedure until you have backed up your data.For more information, see the <i>ArcSight Administrator's Guide</i>.
menu > submenu	<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">menu > submenu > submenu <p>For example:</p> <ul style="list-style-type: none">Authoring > Rules > Rule Actions > Updating Session Lists
tab subtab	<p>Vertical bars are used to separate multilevel editor-tab sequences.</p> <ul style="list-style-type: none">tab subtab subtab
/ Forward slash /	<p>Forward slashes are used to separate resource URI strings and other file paths.</p> <ul style="list-style-type: none">All Reports/System Reports/Asset/All Assets
<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=<password></code>, <code><password></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=<user_id> -- user_login=<user_login>}</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 Express Content Guide, ArcSight makes available the following ArcSight Express product documentation. Many of these documents are available for download from the ArcSight Express 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 ArcSight Express components and its network interfaces, and maintain ArcSight for ongoing operations.
ArcSight ESM Installation and Configuration Guide	Provides ArcSight Express deployment architecture and component setup instructions, and instructions about how to install the components included in the ArcSight Express appliance.
Getting Started with ArcSight Express	Printed instructions about how to install and boot up your ArcSight Express appliance.
ArcSight Express Upgrade Guide	Provides instructions about how to upgrade the ArcSight Express appliance.
ArcSight Express 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>.

Chapter 1

ArcSight Express Content

ArcSight Express is a Security Information and Event Management (SIEM) solution that provides the essentials for network perimeter and security monitoring by leveraging the superior correlation capabilities of ArcSight ESM in combination with an ArcSight Logger storage appliance. ArcSight Express delivers an easy-to-deploy, enterprise-level security monitoring and response system through a series of coordinated resources, such as dashboards, rules, and reports included as part of ArcSight Express Content.

The ESM portion of the ArcSight Express solution comes with a series of coordinated resource systems that address common enterprise network security and ArcSight administration tasks. These resource systems are referred to collectively as *ArcSight Express content*.

With some basic configuration done using the ESM Console, ArcSight Express content enables you to get started using ArcSight Express right away to effectively manage enterprise security operations without having to create additional resources.

The Logger storage portion of the ArcSight Express solution comes with basic system-level filters and foundation reports. For more information about the standard Logger filters and reports, see the *Logger Administrator's Guide*.

["What is ArcSight Express Content?" on page 1](#)
["How ArcSight Express Is Organized" on page 2](#)
["Set Up Connectors and Model the Network" on page 2](#)
["Apply Standard Asset Categories to Assets" on page 5](#)
["Create ArcSight Express Users" on page 5](#)
["Configure Notification Destinations" on page 6](#)
["Configure Asset Auto-Creation Filters" on page 7](#)
["Configure Rules to Send Notifications and Open Cases" on page 10](#)
["Schedule Reports" on page 13](#)
["Tuning ArcSight Express Content" on page 14](#)

What is ArcSight Express Content?

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

Users of the ArcSight Web interface leverage the active channels and dashboards to monitor the network, use the case tracking tools to investigate and resolve issues, and use the reports to communicate the condition of the network to key stakeholders at all levels of the enterprise.

The instructions in this topic describe how Administrators can configure the ArcSight Express content for the users of the ArcSight Web interface.

How ArcSight Express Is Organized

ArcSight Express content monitors and reports on activity relevant to the types of devices reporting into ESM. The content is organized into the following device-specific groups:

Function	Description
Cross-Device	Functions that apply to multiple kinds of devices, such as login attempts, bandwidth usage, and configuration changes.
Anti-Virus	Activity involving anti-virus devices, such as update status, virus activity, and configuration changes.
Case Management	Activity and notifications involving cases opened in ArcSight as a result of events that warrant investigation.
Database	Database activity, such as configuration changes, database logins, errors and warnings.
Firewall	Firewall activity, such as network logins and logouts, denied connections, bandwidth usage, and configuration changes.
Identity Management	User activity, such as logins, user session durations, and configuration changes in order to identify who is doing what activity on the network.
IDS-IPS	Activity involving Intrusion Detection and Prevention Systems, such as signature updates, alerts, and statistics.
Network	Activity involving network infrastructure, including system up/down status, configuration changes, bandwidth usage, and login events.
Operating System	Activity involving operating systems, such as user logins, and user modification events.
VPN	Activity involving VPN connections, including authentication errors, logins, and connection status.
Vulnerabilities	Resources that monitor and report on exposed vulnerabilities by asset.

Set Up Connectors and Model the Network

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

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

4 Test feeds and configure content

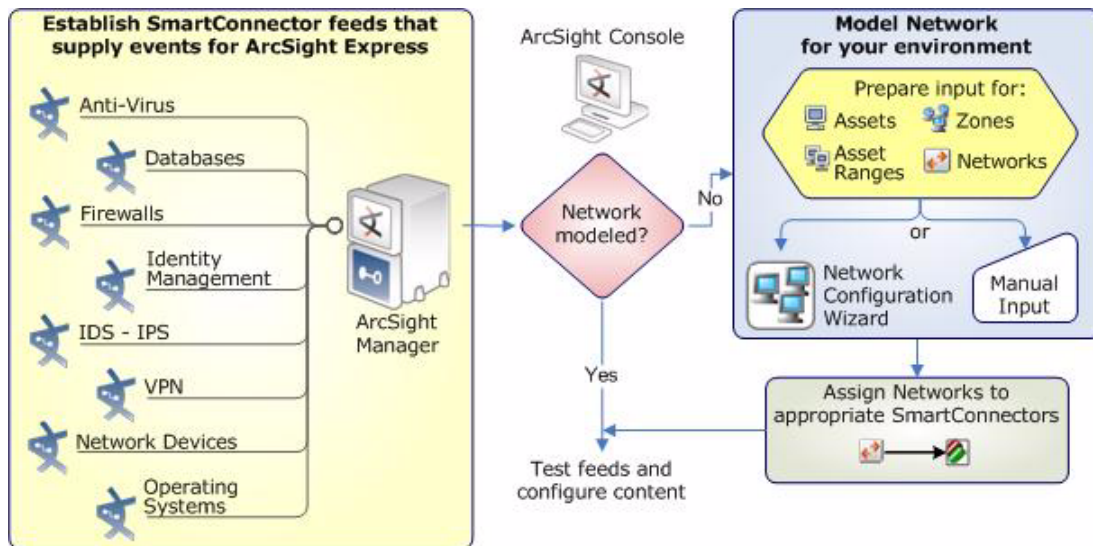


Figure 1-1 Configuring ArcSight Express content starts with installing SmartConnectors and configuring zones and networks for devices that report to ESM.

ArcSight Express-Related SmartConnectors

The ArcSight Express content is designed to address event throughput, network health, and basic security-related scenarios. The ArcSight Express content supports feeds from the following types of SmartConnectors.

Device Group	Related Connectors
Anti-Virus	Most major anti-virus products, such as: <ul style="list-style-type: none"> • Symantec EndPoint Protection • TrendMicro • McAfee AV
Database	The database content for basic error reporting and user info that comes from most database connectors, such as: <ul style="list-style-type: none"> • Oracle 10g • MSSQL Server
Firewall	Firewall content picks up parsed and categorized events from specific firewalls, all-in-one devices, and client-side firewalls, such as those found on Windows. Examples include: <ul style="list-style-type: none"> • Juniper Netscreen • CheckPoint • Cisco PIX
Identity Management	Identity management content picks up from identity management systems, such as: <ul style="list-style-type: none"> • Juniper Steel-Belted Radius • Cisco Secure ACS • Windows AD

Device Group	Related Connectors
IDS - IPS	<p>This content picks up events from any IDS/IPS system for which ArcSight supplies a Connector, including combination devices that may generate events of these types. For example:</p> <ul style="list-style-type: none">• ISS Site Protector• Symantec Network Security• Cisco IPS
Network	<p>This content works on events from networking devices, such as:</p> <ul style="list-style-type: none">• Cisco IOS Devices• Juniper JunOS Devices
Operating System	<p>This content picks up events from Windows and Unix-based systems that generate relevant events and for which ArcSight supplies supported connectors, such as:</p> <ul style="list-style-type: none">• Linux OS Events (All major Versions)• MS Windows (2003/XP)
VPN	<p>This content works on events from most VPN devices that report on errors, sessions established, and so on. For example:</p> <ul style="list-style-type: none">• Juniper/Netscreen VPN• Cisco VPN• CheckPoint VPN-1
Vulnerabilities	<p>Vulnerability content relies on the ESM device model, which can be populated one by one, or by a vulnerability scanner for which ArcSight supplies a Connector.</p>

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 ESM standard asset categories is what activates much of the ArcSight Express 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 topic [“Apply Standard Asset Categories to Assets” on page 5](#) 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 ESM's network modeling tools, see Chapter 4, “ArcSight Network Model” in *ArcSight 101*.

Apply Standard Asset Categories to Assets

Once assets are added to the network model, or if you are adding them in bulk using the Network Modeling wizard, categorize relevant assets as internal to the network, and/or as critical assets.

Assets can be categorized individually using the Assets Editor, or in bulk using the Network Modeling wizard. Asset categories can also be applied to zones.

For more about asset categories and instructions about how to apply them using the Assets Editor, 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](#).

By default, the Private Address Space Zones are categorized as *Protected*. Assets within a zone that has been categorized do not inherit categories from the zone. For example, an asset with an IP address of 192.168.0.1 is not automatically categorized as *Protected*, but it belongs to one of the Private Address Spaces zones, so it is considered *Internal* because it belongs to a zone 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

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 asset category:

```
/All Asset Categories/System Asset Categories/Criticality/High
```

Create ArcSight Express Users

ArcSight Express comes configured with a custom user group called ArcSight Express. Add users to this group with ArcSight Web privileges.

- 1 In the Navigator panel, go to **Users > Shared > Custom User Groups**
- 2 Right click on ArcSight Express and select **New User**

- 3 For each user you add, provide a User ID and Password, and set the User Type to **Web User** and click **OK**.

For more about creating users, see “Managing Users” 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 ArcSight Express rules are triggered. By default, the notifications are disabled in the ArcSight Express 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 ArcSight Express rules, see [“Configure Rules to Send Notifications and Open Cases” on page 10](#).

The ArcSight Express 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.
Destination Type	From the drop-down menu, select the method by which the notification will be delivered: <ul style="list-style-type: none"> • Console — Notification popup in this user's ArcSight account • E-Mail — User's e-mail account • Pager — User's pager. Enter the pager's PIN number and service provider. • Cell Phone — Applicable for cell phones that receive e-mail. Enter the cell phone's e-mail address.
User/Group	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.

- 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 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 potentially cause a lot of unnecessary individual assets to be added to your asset model. For example, laptops with the intrusion detection system BlackICE from ISS can generate a new asset ID for that device every time the laptop logs onto the network. This situation also applies to VPN and wireless networks every time a device logs onto a new subnet.

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 clutters the network model with Connector nodes.

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.

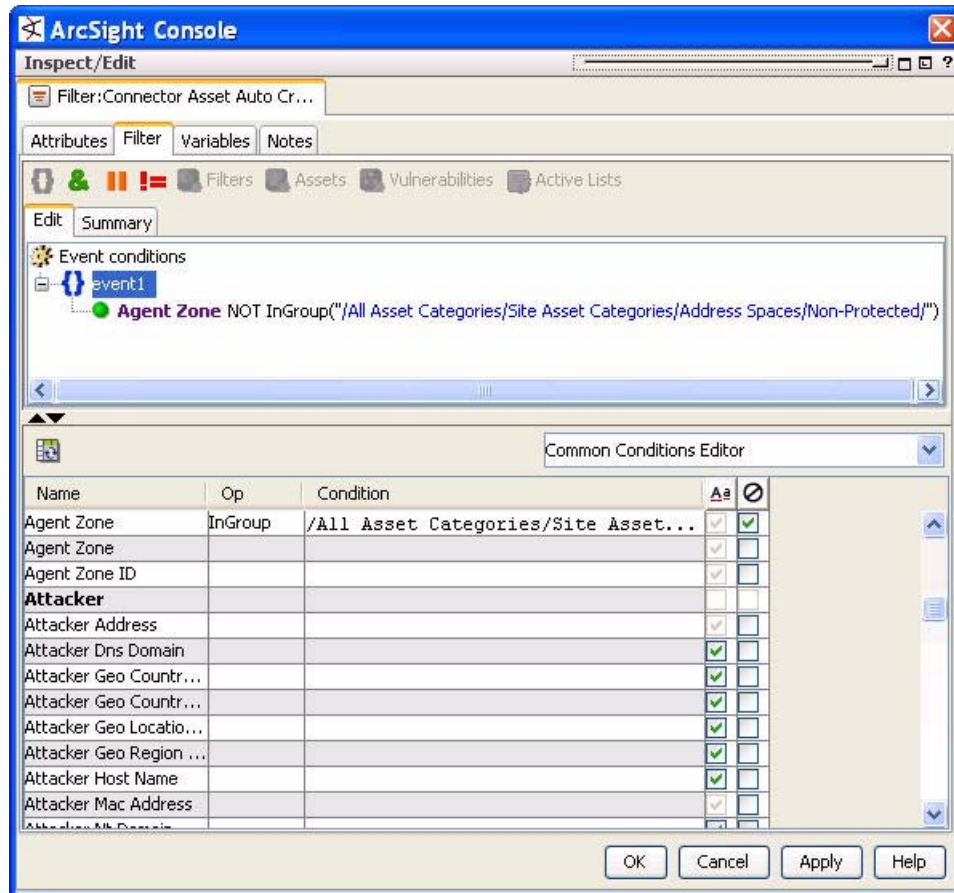
Configure Connector Asset Auto-Creation Controller Filter

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.



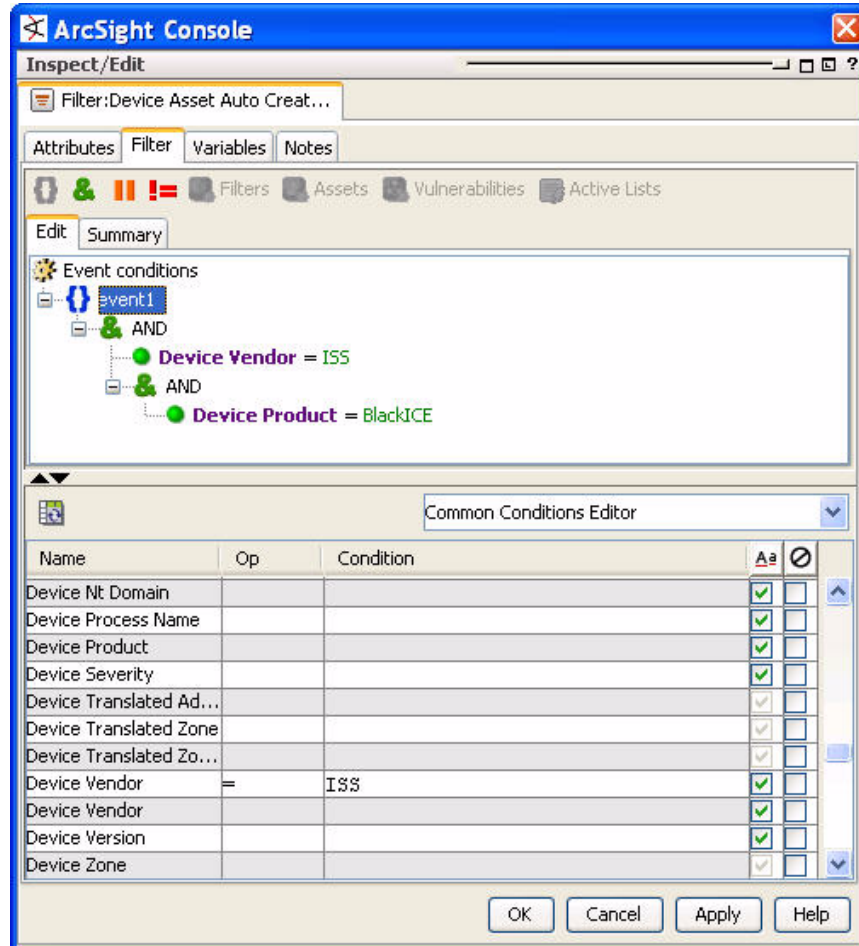
- 1 In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter ([All Filters/ArcSight System/Asset Auto Creation](#)) and double-click it to open it in the Inspect/Edit panel.
- 2 In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default 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 Rules to Send Notifications and Open Cases

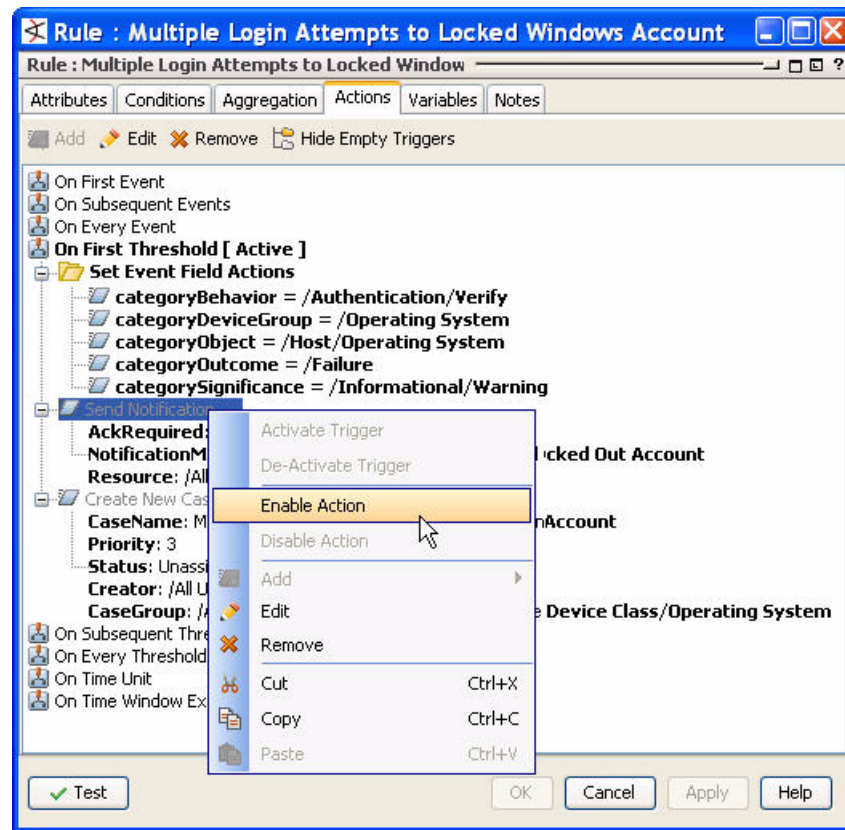
ArcSight Express depends on its rules to send notifications and open cases when conditions are met. Notifications and cases are how users can track and resolve the security issues that ArcSight Express is designed to find.

By default, the notifications and create case actions are disabled in the ArcSight Express 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 ArcSight Express rules to send notifications and open cases, first configure notification destinations as described in [“Configure Notification Destinations” on page 6](#), 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 11](#) and [“Configure Rules with Notifications to the SOC Operators” on page 12](#).
- 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 ArcSight Express 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 11](#) and [“Configure Rules with Notifications to the SOC Operators” on page 12](#).

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/ArcSight Express/Attack Monitoring/DoS/	High Number of IDS Alerts for DoS
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/	SYN Flood Detected by IDS and Firewall
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/	High Number of IDS Alerts for Backdoor
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/	Windows Account Created and Deleted within 1 Hour
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Login Attempts to Locked Windows Account
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	Multiple Windows Logins by Same User
/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/	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 ArcSight Express 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 ArcSight Express are not scheduled to run automatically.

You may want to schedule certain reports that are based on cases, notifications, assets (not based on events). These non-event-based reports cannot be run for the previous day or the previous week, which means that their output is always the “current” state.

An example of an asset-based report that you may want to schedule would be *Exposed Vulnerability Count by Critical Asset*.

Reports on cases

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases by Operational Impact
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Case Stage Counts
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	All Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Cases per Target
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Open Cases
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/	Today's Cases

Reports on notifications

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Statistics Summary
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Overview
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	All Level 3 Notifications
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notification Status Report
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Notifications By Acknowledgement Status
/All Reports/ArcSight Foundation/ArcSight Express/Case Management/Notifications/	Unacknowledged Level 3 Notifications

Reports on assets

Report URI	Report Name
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerabilities by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Asset
/All Reports/ArcSight Foundation/ArcSight Express/Vulnerabilities/	Exposed Vulnerability Count by Critical Asset

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

Tuning ArcSight Express Content

ArcSight Express content is designed to find activity of concern that the staff of your security operations center should be notified about so they can follow up. There may be times, however, that a situation is actually a benign or routine condition in your environment.

In such a case, ArcSight Express provides the following active lists where you can store specific event and user situations that are determined to be low or no risk:

- /All Active Lists/ArcSight System/Tuning/**Event-based Rule Exclusions**
- /All Active Lists/ArcSight System/Tuning/**User-based Rule Exclusions**

The entries in these active lists are ignored by the rules that reference them. The *Event-based Rule Exclusions* active list is referenced by the event-based rules, and the *User-based Rule Exclusions* are referenced by the user-based rules:

Event-Based Rules	User-Based Rules
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ High Number of IDS Alerts for DoS	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Logout
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/ SYN Flood Detected by IDS and Firewall	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/ Successful Windows Login
/All Rules/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/ High Number of IDS Alerts for Backdoor	/All Rules/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/ Multiple Windows Logins by Same User

These active lists store the following fields for the events and users:

Event-based Rule Exclusions	User-based Rule Exclusions
The following fields limit the rule exclusions to very specific events between two specific systems. <ul style="list-style-type: none"> • Device Event Class ID • Event Name • Attacker Zone Name • Attacker Address • Target Zone Name • Target Address 	The following fields limit the rule exclusions to user account activity that can be safely ignored. <ul style="list-style-type: none"> • Target NT Domain • Target User ID • Target User Name

There are three ways to add entries to these active lists:

- From an active channel
- Manually from the Active List editor
- In a batch from a CSV file

To add entries from an active channel:

- 1 In the active channel where the event appears, select and then right-click the event and select **Active List > Add to > Other...**
- 2 In the *Add to Active List* dialog box in the drop-down field, navigate to **/All Active Lists/ArcSight System/Tuning/Event-based Rule Exclusions** or **/All Active Lists/ArcSight System/Tuning/User-based Rule Exclusions** and click **OK**.
- 3 The *Add to Active List* dialog box will display the list of fields the active list will save from the selected event. If the selected event does not have a value for one or more of the fields, those fields will remain empty.

To add entries to these active lists manually:

- 1** In the Navigator panel, go to **Lists > Active Lists > All Active Lists > ArcSight System > Tuning**.
- 2** Right-click the active list you want to populate and select **Edit Active List**.
- 3** In the Active List Editor in the Inspect/Edit panel, click **Add Entry**.
- 4** In the ActiveList Entry Editor, enter the appropriate event or user details and click **Add**.
- 5** Repeat steps 3 and 4 for every event or user situation you want to exclude from the event or user-based rules.

To populate Active Lists from an imported CSV file:

- 1** In the Navigator panel, navigate to the active list you want to configure ([Lists > Active Lists](#)).
- 2** Generate a CSV file with the values with which you wish to populate the active list, and save it to a directory on the Console system.
- 3** Right-click the active list you wish to import the values into and select **Import CSV File...**
- 4** In the Open dialog box, navigate to and select the CSV file and click **Open**.

For more about working with active lists, see “Managing Active Lists” in the *ESM User's Guide* or the Console Help.

Chapter 2

Resource Reference

This chapter describes the resources included in ArcSight Express. For details about the devices that drive this content and instructions about setting up and configuring ArcSight Express content, see [Chapter 1, ArcSight Express Content, on page 1](#).

Cross-Device

The Cross-Device resources monitor and report on functions that apply to multiple kinds of devices, such as login attempts, bandwidth usage, and configuration changes.

Cross-Device Presentation Resources

Table 2-1 Information Presentation Resources for the Cross-Device Use Case

Resource	Description	Type	URI
Configuration Changes Overview	This dashboard shows an overview of the successful configuration changes for databases, firewalls, VPN, and network devices.	Dashboard	ArcSight Express/Cross-Device/
Reconnaissance in Progress	This dashboard displays the Top 10 Zones Scanned, the last 10 Zones Scanned, the Last 10 Hosts Scanned and the Last 10 Scanners data monitors to give an overview of the reconnaissance activity against the network.	Dashboard	ArcSight Express/Cross-Device/
Security Activity	This dashboard displays an overview of security activity, including suspicious network activity, failed log-ins, and common attacks on the network.	Dashboard	ArcSight Express/Cross-Device/
Security Activity Statistics		Dashboard	ArcSight Express/Cross-Device/
Bandwidth Usage by Hour	This report shows a summary of the bandwidth usage per hour in a chart. The chart shows the average bandwidth usage per hour for the past 24 hours (by default).	Report	ArcSight Express/Cross-Device/Bandwidth Tracking/

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol in a chart and a table. The chart shows the top 10 protocols with the highest bandwidth usage, and the table lists all the protocols sorted by bandwidth usage.	Report	ArcSight Express/Cross-Device/Bandwidth Tracking/
Top Bandwidth Hosts	This report shows a summary of the bandwidth usage by the top hosts in a chart. The chart shows the average bandwidth usage by host for the previous day (by default).	Report	ArcSight Express/Cross-Device/Bandwidth Tracking/
Failed Login Attempts	This report shows the count of authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Report	ArcSight Express/Cross-Device/Login Tracking/
Failed Logins by Destination Address	This report shows authentication failures from login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Report	ArcSight Express/Cross-Device/Login Tracking/
Failed Logins by Source Address	This report shows authentication failures from login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Report	ArcSight Express/Cross-Device/Login Tracking/
Failed Logins by User	This reports shows authentication failures from login attempts by user in a chart and a table. The chart shows the top 10 users with failed login attempts, and the table shows the details of the failed login attempts grouped and sorted by user.	Report	ArcSight Express/Cross-Device/Login Tracking/
Login Event Audit	This report shows all the successful and failed login events in a table. The table is sorted chronologically.	Report	ArcSight Express/Cross-Device/Login Tracking/
Successful Logins by Destination Address	This report shows authentication successes from login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Report	ArcSight Express/Cross-Device/Login Tracking/
Successful Logins by Source Address	This report shows authentication successes from login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Report	ArcSight Express/Cross-Device/Login Tracking/

Resource	Description	Type	URI
Successful Logins by User	This reports shows authentication successes from login attempts by user in a chart and a table. The chart shows the top users with successful login attempts, and the table shows the details of the successful login attempts grouped and sorted by user.	Report	ArcSight Express/Cross-Device/Login Tracking/
Top Alerts from IDS and IPS	This report shows the top alerts coming from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The report contains a chart and a table. The chart shows the top 10 alerts (signature ID), and the table shows the details of the top alerts.	Report	ArcSight Express/Cross-Device/Top Activity/
Top Attackers	This report displays a chart of the Attacker Zone Name, Attacker Address and the count of events where the category significance starts with /Compromise or /Hostile.	Report	ArcSight Express/Cross-Device/Top Activity/
Top Hosts by Number of Connections	This report shows a summary of the number of connections by the top hosts in a chart. The chart shows the number of connections by host for the previous day (by default).	Report	ArcSight Express/Cross-Device/Top Activity/
Top Targets	This report displays a 3D Stacking Bar Chart showing the Target Zone Name, Target Address and the sum of the Aggregated Event Count for events matching the Attack Events filter.	Report	ArcSight Express/Cross-Device/Top Activity/
By User Account - Accounts Created		Report	ArcSight Express/Cross-Device/User Change Tracking/
Configuration Changes by Type	This report shows recent configuration changes in a table. The table lists all the changes, grouped by type and user, and sorts them chronologically.	Report	ArcSight Express/Cross-Device/User Change Tracking/
Configuration Changes by User	This report shows recent configuration changes in a table. The table lists all the changes, grouped by user and type, and sorts them chronologically.	Report	ArcSight Express/Cross-Device/User Change Tracking/
Password Changes	This report shows password changes for the previous day in a table. The table groups the password changes by user and sort them chronologically.	Report	ArcSight Express/Cross-Device/User Change Tracking/

Cross-Device Data Processing Resources

Table 2-2 Data Processing Resources for the Cross-Device Use Case

Resource	Description	Type	URI
Last 10 Database Configuration Changes	This data monitor shows the last 10 successful database configuration changes.	Data Monitor	ArcSight Express/Cross-Device/Configuration Changes Overview/
Last 10 Firewall Configuration Changes	This data monitor shows the last 10 successful firewall configuration changes.	Data Monitor	ArcSight Express/Cross-Device/Configuration Changes Overview/
Last 10 Network Configuration Changes	This data monitor shows the last 10 successful configuration changes on network devices.	Data Monitor	ArcSight Express/Cross-Device/Configuration Changes Overview/
Last 10 VPN Configuration Changes	This data monitor shows the last 10 successful VPN configuration changes.	Data Monitor	ArcSight Express/Cross-Device/Configuration Changes Overview/

Anti-Virus

The Anti-Virus resources support monitoring and reporting on anti-virus activity, such as update status, virus activity, and configuration changes.

Anti-Virus Presentation Resources

Table 2-3 Information Presentation Resources for the Anti-Virus Use Case

Resource	Description	Type	URI
Anti-Virus Overview	This dashboard give an overview of the top infections, the top infected systems, and the most recent and top Anti-Virus error events.	Dashboard	ArcSight Express/Anti-Virus/
Virus Activity Statistics	The Virus dashboard displays data monitors describing virus activity from two perspectives. The Virus Activity by Zone and Virus Activity by Host data monitors are moving average graphs grouping by the name of the virus, the target's zone resource and address and the customer resource.	Dashboard	ArcSight Express/Anti-Virus/

Resource	Description	Type	URI
Errors Detected in Anti-Virus Deployment	This report shows two charts and a table. The first chart displays the hosts reporting the most anti-virus errors for the previous day. The Second chart displays the most frequent anti-virus errors reported the previous day. The table shows a summary of information on the previous day's anti-virus errors, including the Anti-Virus product, host details, error information and the number of errors.	Report	ArcSight Express/Anti-Virus/
Failed Anti-Virus Updates	This report displays a table with the Device Vendor, Device Product Target Zone Name, Target Host Name, Target Address and Minute(EndTime) from yesterday.	Report	ArcSight Express/Anti-Virus/
Top Infected Systems	This report displays summaries of the systems reporting the most infections in the previous day.	Report	ArcSight Express/Anti-Virus/
Update Summary	This report displays a chart and a table. The chart shows a summary of the results of anti-virus update activity by zones. The table shows the details of anti-virus update activity. This report covers yesterday's events.	Report	ArcSight Express/Anti-Virus/
Virus Activity by Time	This report shows a chart and a table. The chart displays the malware activity by hour for the previous day. The table shows the malware activity by hour and priority for the previous day.	Report	ArcSight Express/Anti-Virus/

Anti-Virus Data Processing Resources

Table 2-4 Data Processing Resources for the Anti-Virus Use Case

Resource	Description	Type	URI
Last 10 Anti-Virus Errors	This data monitor tracks the last Anti-Virus error events, displaying the time of occurrence, the priority, the vendor information and the device information.	Data Monitor	ArcSight Express/Anti-Virus/Anti-Virus Overview/
Top 10 Anti-Virus Errors	This data monitor shows the top 10 systems with events matching the filter "AV - Found Infected" (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Anti-Virus/Anti-Virus Overview/

Resource	Description	Type	URI
Top 10 Infected Systems	This data monitor shows the top 10 systems with events matching the filter "AV - Found Infected" (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Anti-Virus/Anti-Virus Overview/
Top 10 Infections	This data monitor shows the top 10 systems with events matching the filter "AV - Found Infected" (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Anti-Virus/Anti-Virus Overview/
Configuration Changes by Type	This report shows a table that displays the configuration change name, the user making the change, device information and the time of the change for Anti-Virus configuration change events that were reported the previous day.	Focused Report	ArcSight Express/Anti-Virus/
Configuration Changes by User	This report shows a table that displays the user making the change, the configuration change name, device information and the time of the change for Anti-Virus configuration change events that were reported the previous day.	Focused Report	ArcSight Express/Anti-Virus/

Case Management

The Case Management resources support monitoring and reporting on activity and notifications involving cases opened in ArcSight as a result of activity that warrants investigation.

Case Management Presentation Resources

Table 2-5 Information Presentation Resources for the Case Management Use Case

Resource	Description	Type	URI
All Cases	This report displays a table showing the Name, Creator, Ticket Type, Stage, Security Classification and Consequence Severity of all the non-system cases in the system.	Report	ArcSight Express/Case Management/
Average Time to Case Resolution - By Day	This report displays a table and a chart showing the average time taken to resolve cases closed for each day of the reporting period.	Report	ArcSight Express/Case Management/
Average Time to Case Resolution - By Severity	This report displays a chart and a table, each showing the severity and average time to resolution of all cases closed in the last seven days.	Report	ArcSight Express/Case Management/

Resource	Description	Type	URI
Average Time to Case Resolution - By User	This report displays a chart and a table showing the average time taken, in minutes, to resolve cases that have been closed since the start time (midnight, seven days ago by default), for each user who closed cases during this time period.	Report	ArcSight Express/Case Management/
Case Stage Counts	This report displays a table showing the count of cases at each stage. Note, this report will include the count of all cases in the system, regardless of how long ago they were closed.	Report	ArcSight Express/Case Management/
Cases Overview	This report displays a chart and a table showing the count of cases at each stage and operational impact level.	Report	ArcSight Express/Case Management/
Cases by Operational Impact	This report displays a table and a chart showing the count of cases at each Operational Impact level. Note, this report will include the count of all cases in the system, regardless of how long ago they were closed.	Report	ArcSight Express/Case Management/
Cases per Target	This report displays a table showing the Attack Target, case Name, Security Classification and Consequence Severity at each Stage. Note, this report will include the count of all cases in the system, regardless of how long ago they were closed.	Report	ArcSight Express/Case Management/
Max Time to Case Resolution - By User	This report displays a chart and a table showing the maximum time taken, in minutes, to resolve cases that have been closed since the start time (midnight, seven days ago by default), grouped by Operational Impact for each user who closed cases during this time period.	Report	ArcSight Express/Case Management/
All Level 3 Notifications	This report displays a table showing the Event Name, Group Name, Create Time and ArcSight Severity of all notifications with Esc Level 3.	Report	ArcSight Express/Case Management/Notifications/
Notification Action Events	This report displays a table of the audit events related to notifications. The table includes the audit event Name, the severity, the time, the Acknowledgement Status (a variable), the User acknowledging or resolving the notification (a variable), the Destination Group (a variable) and the Notification Resource (a variable). Not all notification audit events populate all of these fields.	Report	ArcSight Express/Case Management/Notifications/
Notification Overview	This report displays a chart showing the number of notifications, grouped by ArcSight Severity, at each escalation level.	Report	ArcSight Express/Case Management/Notifications/

Resource	Description	Type	URI
Notification Statistics Summary	This report shows three charts and a table. Two of the three charts show notifications by escalation level and acknowledgement status, the third shows notifications with an escalation level of 3 and the destination groups to which they were sent. The table shows notification details, such as the destination group, the escalation level, acknowledgement status, and the creation time and notification event name.	Report	ArcSight Express/Case Management/Notifications/
Notification Status Report	This report displays a table showing the notifications generated for each notification (Destination) group, including the notification's creation time, escalation level and acknowledgement status.	Report	ArcSight Express/Case Management/Notifications/
Notifications By Acknowledgment Status	This report displays a chart and a table showing the counts of the notifications created yesterday, by acknowledgment status and ArcSight Severity.	Report	ArcSight Express/Case Management/Notifications/
Unacknowledged Level 3 Notifications	This report displays a table showing all the notifications, by ArcSight Severity, including their creation time and the notification (Destination) group responsible for them, that have not been acknowledged and are at escalation level 3.	Report	ArcSight Express/Case Management/Notifications/
Open Cases	This report displays a table showing the Name, Creator, Ticket Type, Stage, Security Classification, Consequence Severity, Create Time, Modification Time and Attack Target of all the open, non-system cases in the system.	Report	ArcSight Express/Case Management/
Today's Cases	This report displays a table showing the cases that have been generated since midnight this morning, including the case's Display ID, Name, Ticket Type, Stage, Operational Impact and who created the case.	Report	ArcSight Express/Case Management/

Database

The Database resources monitor and report on database activity, such as configuration changes, database logins, errors and warnings.

Database Presentation Resources

Table 2-6 Information Presentation Resources for the Database Use Case

Resource	Description	Type	URI
Database Errors	This dashboard shows the most recent and top errors affecting database applications on the network.	Dashboard	ArcSight Express/Database/
Database Errors and Warnings	This report shows recent database errors and warnings in a chart and a table. The chart shows the top 10 errors/warnings, and the table lists all the errors/warnings chronologically.	Report	ArcSight Express/Database/

Database Data Processing Resources

Table 2-7 Data Processing Resources for the Database Use Case

Resource	Description	Type	URI
Last 10 Database Errors	This last n events data monitor displays the most recent database error events.	Data Monitor	ArcSight Express/Database/Database Errors/
Top 10 Database Errors	This data monitor shows the top 10 systems with events matching the filter "AV - Found Infected" (the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure and the Category Behavior is /Found/Vulnerable).	Data Monitor	ArcSight Express/Database/Database Errors/
Configuration Changes by Type	This report shows recent database configuration changes in a table. The table lists all the changes, grouped by type, and sorts them chronologically.	Focused Report	ArcSight Express/Database/
Configuration Changes by User	This report shows recent database configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/Database/
Login Event Audit	This report shows all the successful and failed database login events in a table. The table is sorted chronologically.	Focused Report	ArcSight Express/Database/
Password Changes	This report shows database password changes for the previous day in a table. The table groups the password changes by user and sort them chronologically.	Focused Report	ArcSight Express/Database/

Firewall

The Firewall resources monitor and report on firewall activity, such as network logins and logouts, denied connections, bandwidth usage, and configuration changes.

Firewall Presentation Resources

Table 2-8 Information Presentation Resources for the Firewall Use Case

Resource	Description	Type	URI
Firewall Connection Overview	This dashboard shows an overview of all the denied connection events coming from firewalls. The dashboard displays the "Top 10 Denied Ports (Inbound)", "Top 10 Denied Ports (Outbound)", "Top 10 Hosts With Denied Inbound Connections", and "Top 10 Hosts With Denied Outbound Connections" data monitors.	Dashboard	ArcSight Express/Firewall/
Firewall Login Overview	This dashboard shows an overview of firewall logins. The dashboard displays the "Last 10 Failed Login Events", "Last 10 Successful Login Events", "Login Results", and "Top 10 Users With Failed Logins" data monitors.	Dashboard	ArcSight Express/Firewall/
Denied Inbound Connections by Address	This report shows a summary of the denied inbound traffic by foreign address in a chart and a table. The chart shows the top 10 addresses with the highest denied connections count, and the reports lists all the addresses sorted by connection count.	Report	ArcSight Express/Firewall/
Denied Inbound Connections by Port	This report shows a summary of the denied inbound traffic by destination port in a chart and a table. The chart shows the top 10 ports with the highest denied connections count, and the reports lists all the ports sorted by connection count.	Report	ArcSight Express/Firewall/
Denied Inbound Connections per Hour	This report shows a summary of the denied inbound traffic per hour in a chart and a table. The chart shows the total number of denied connections per hour for the previous day (by default), and the table shows the connection count per hour grouped by source zone.	Report	ArcSight Express/Firewall/
Denied Outbound Connections by Address	This report shows a summary of the denied outbound traffic by local address in a chart and a table. The chart shows the top 10 addresses with the highest denied connections count, and the reports lists all the addresses sorted by connection count.	Report	ArcSight Express/Firewall/

Resource	Description	Type	URI
Denied Outbound Connections by Port	This report shows a summary of the denied outbound traffic by destination port in a chart and a table. The chart shows the top 10 ports with the highest denied connections count, and the reports lists all the ports sorted by connection count.	Report	ArcSight Express/Firewall/
Denied Outbound Connections per Hour	This report shows a summary of the denied outbound traffic per hour in a chart and a table. The chart shows the total number of denied connections per hour for the previous day (by default), and the table shows the connection count per hour grouped by source zone.	Report	ArcSight Express/Firewall/

Firewall Data Processing Resources

Table 2-9 Data Processing Resources for the Firewall Use Case

Resource	Description	Type	URI
Top 10 Denied Ports (Inbound)	This data monitor shows the top 10 ports with denied inbound connections.	Data Monitor	ArcSight Express/Firewall/Firewall Connection Overview/
Top 10 Denied Ports (Outbound)	This data monitor shows the top 10 ports with denied outbound connections.	Data Monitor	ArcSight Express/Firewall/Firewall Connection Overview/
Top 10 Hosts With Denied Inbound Connections	This data monitor shows the top 10 hosts with denied inbound connections.	Data Monitor	ArcSight Express/Firewall/Firewall Connection Overview/
Top 10 Hosts With Denied Outbound Connections	This data monitor shows the top 10 hosts with denied outbound connections.	Data Monitor	ArcSight Express/Firewall/Firewall Connection Overview/
Last 10 Failed Login Events	This data monitor shows the last 10 failed firewall logins.	Data Monitor	ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful firewall logins.	Data Monitor	ArcSight Express/Firewall/Firewall Login Overview/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Express/Firewall/Firewall Login Overview/
Top 10 Users With Failed Logins	This data monitor shows the top 10 users with failed firewall logins.	Data Monitor	ArcSight Express/Firewall/Firewall Login Overview/

Resource	Description	Type	URI
Top Users by Login Activity	This top value counts data monitor shows the users with the most firewall login activity over the last 60 minutes.	Data Monitor	ArcSight Express/Firewall/Firewall Login Overview/
Bandwidth Usage by Protocol	This report shows a summary of the bandwidth usage by application protocol in a chart and a table. The chart shows the top 10 protocols with the highest bandwidth usage, and the table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/Firewall/
Bandwidth Usage per Hour	This report shows a summary of the bandwidth usage per hour in a chart. The chart shows the average bandwidth usage per hour for the previous day (by default).	Focused Report	ArcSight Express/Firewall/
Configuration Changes by Type	This report shows recent firewall configuration changes in a table. The table lists all the changes, grouped by type, and sorts them chronologically.	Focused Report	ArcSight Express/Firewall/
Configuration Changes by User	This report shows recent firewall configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/Firewall/
Failed Logins by Destination Address	This report shows authentication failures from login attempts to a firewall by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Firewall/
Failed Logins by Source Address	This report shows authentication failures from login attempts to a firewall by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Firewall/
Failed Logins by User	This reports shows authentication failures from firewall login attempts by user in a chart and a table. The chart shows the top 10 users with failed login attempts, and the table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Firewall/
Login Event Audit	This report shows all the successful and failed firewall login events in a table. The table is sorted chronologically. This report is a focused report based on the "Login Events" report.	Focused Report	ArcSight Express/Firewall/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from login attempts to a firewall by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Firewall/
Successful Logins by Source Address	This report shows authentication successes from login attempts to a firewall by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Firewall/
Successful Logins by User	This reports shows authentication successes from firewall login attempts by user in a chart and a table. The chart shows the top 10 users with successful login attempts, and the table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Firewall/
Top Bandwidth Hosts	This report shows a summary of the bandwidth usage reported by firewalls by the top hosts in a chart. The chart shows the average bandwidth usage by host for the previous day (by default).	Focused Report	ArcSight Express/Firewall/
Top Hosts by Number of Connections	This report shows a summary of the number of firewall connections by the top hosts in a chart. The chart shows the number of connections by host for the previous day (by default).	Focused Report	ArcSight Express/Firewall/

Identity Management

Identity Management resources monitor and report on user activity, such as logins, user session durations, and configuration changes in order to identify who is doing what activity on the network.

Identity Management Presentation Resources

Table 2-10 Information Presentation Resources for the Identity Management Use Case

Resource	Description	Type	URI
Connection Counts by User	This report shows count information about connections for each user reported by Identity Management devices. A summary of the Top Users by Connection Count is provided. Details of each user's connection counts are also provided, including connection, error and authentication failure counts.	Report	ArcSight Express/Identity Management/
Connection Durations by User	This report shows duration information about VPN connections for each user. A summary of the Top VPN Connection Duration by User is provided. Details of each user's connection durations are also provided, including minimum, average, maximum and total connection minutes. Also included are details of connections that are currently open at the time the report was run.	Report	ArcSight Express/Identity Management/

Identity Management Data Processing Resources

Table 2-11 Data Processing Resources for the Identity Management Use Case

Resource	Description	Type	URI
Configuration Changes by Type	This report shows recent identity management configuration changes in a table. The table lists all the changes, grouped by type (name), and sorts them chronologically.	Focused Report	ArcSight Express/Identity Management/
Configuration Changes by User	This report shows recent identity management configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/Identity Management/
Failed Login Attempts	This report shows the count of authentication failures from login attempts reported by identity management systems by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Express/Identity Management/

Resource	Description	Type	URI
Failed Logins by Destination Address	This report shows authentication failures from login attempts reported by identity management systems by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Identity Management/
Failed Logins by Source Address	This report shows authentication failures from login attempts reported by identity management systems by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Identity Management/
Failed Logins by User	This reports shows authentication failures from login attempts by user reported by identity management systems in a chart and a table. The chart shows the top users with failed login attempts, and the table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Identity Management/
Password Changes	This report shows identity management password changes for the previous day in a table. The table groups the password changes by user and sort them chronologically.	Focused Report	ArcSight Express/Identity Management/
Successful Logins by Destination Address	This report shows authentication successes from login attempts reported by identity management systems by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Identity Management/
Successful Logins by Source Address	This report shows authentication successes from login attempts reported by identity management systems by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Identity Management/
Successful Logins by User	This reports shows authentication successes from login attempts by user reported by identity management systems in a chart and a table. The chart shows the top users with successful login attempts, and the table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Identity Management/

IDS-IPS

The IDS-IPS resources monitor and report on activity involving Intrusion Detection and Prevention Systems, such as signature updates, alerts, and statistics.

IDS-IPS Presentation Resources

Table 2-12 Information Presentation Resources for the IDS - IPS Use Case

Resource	Description	Type	URI
IDS - IPS Overview	This dashboard shows an overview of IDS signatures. The dashboard shows the "Top 10 Signatures Destinations", "Top 10 Signature Sources", "Top 10 Signature Types", and "Top 10 Signatures" data monitors.	Dashboard	ArcSight Express/IDS - IPS/
Worm Outbreak Overview	This dashboard provides a view of worm activity across the network.	Dashboard	ArcSight Express/IDS - IPS/
Alert Counts by Device	This report shows the count of IDS and IPS alerts by device in a chart and a table. The chart shows the top 10 device addresses with highest counts, and the table shows the list of all the devices, grouped by device vendor and product, then sorted by count.	Report	ArcSight Express/IDS - IPS/
Alert Counts by Port	This report shows the count of IDS and IPS alerts by destination port in a chart and a table. The chart shows the top 10 ports with the highest counts, and the table shows the list of all the counts sorted by descending order.	Report	ArcSight Express/IDS - IPS/
Alert Counts by Severity	This report shows the total count of IDS and IPS alerts by severity (agent severity) in a chart and a table. The chart shows the count of alerts by severity, and the table shows the count of alerts by severity, device vendor, and device product.	Report	ArcSight Express/IDS - IPS/
Alert Counts by Type	This report shows the count of IDS and IPS alerts by type (category technique) in a chart and a table. The chart shows the top 10 alert counts, and the table shows the list of all the counts sorted by descending order.	Report	ArcSight Express/IDS - IPS/
Alert Counts per Hour	This report shows the total count of IDS and IPS alerts per hour in a chart. The chart shows the count of IDS and IPS alerts per hour for the past 24 hours (by default).	Report	ArcSight Express/IDS - IPS/

Resource	Description	Type	URI
Top Alert Destinations	This report shows the top IDS and IPS alert destinations per day in a chart and a table. The chart shows the top 10 IDS and IPS alert destination IP addresses, and the table shows the top alert destination IP addresses and zones, as well as the device vendor and product of the reporting device.	Report	ArcSight Express/IDS - IPS/
Top Alert Sources	This report shows the top IDS and IPS alert sources per day in a chart and a table. The chart shows the top 10 IDS and IPS alert source IP addresses, and the table shows the top alert source IP addresses and zones, as well as the device vendor and product of the reporting device.	Report	ArcSight Express/IDS - IPS/
Worm Infected Systems	This report presents a table of systems that have been infected by a worm. The table is sorted by the Attacker Zone Name, then by the Attacker Host Name and finally by the Attacker Address (for cases where the system does not have a host name).	Report	ArcSight Express/IDS - IPS/

IDS-IPS Data Processing Resources

Table 2-13 Data Processing Resources for the IDS - IPS Use Case

Resource	Description	Type	URI
Top 10 Alert Destinations	This data monitor shows the top 10 destination hosts with IDS alert counts.	Data Monitor	ArcSight Express/IDS - IPS/IDS - IPS Overview/
Top 10 Alert Sources	This data monitor shows the top 10 source hosts with IDS alert counts.	Data Monitor	ArcSight Express/IDS - IPS/IDS - IPS Overview/
Top 10 Alert Types	This data monitor shows the top 10 IDS alert types.	Data Monitor	ArcSight Express/IDS - IPS/IDS - IPS Overview/
Top 10 Alerts	This data monitor shows the top 10 IDS alerts.	Data Monitor	ArcSight Express/IDS - IPS/IDS - IPS Overview/
Target Port Activity by Attacker	This Data monitor is used in conjunction with the Worm Outbreak detected rule and the possible network sweep rule to detect worm outbreaks before an IDS signature is released.	Data Monitor	ArcSight Express/IDS - IPS/Worm Outbreak Overview/

Resource	Description	Type	URI
Worm Activity Status	This last n events data monitor shows the most recent events related to worm activity in the network zones.	Data Monitor	ArcSight Express/IDS - IPS/Worm Outbreak Overview/
Worm Infected Systems	This Last State data monitor displays the status of systems that have been infected in the course of a worm outbreak.	Data Monitor	ArcSight Express/IDS - IPS/Worm Outbreak Overview/
Top 10 Alerts	This report shows the top alerts coming from Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) in a chart and a table. The chart shows the top 10 alerts (signature IDs), and the table shows the details of the top alerts.	Focused Report	ArcSight Express/IDS - IPS/
Top 10 Attackers	This report shows the top 10 attackers in a chart.	Focused Report	ArcSight Express/IDS - IPS/
Top 10 Targets	This report shows the top 10 targets in a chart.	Focused Report	ArcSight Express/IDS - IPS/

Network

The Network resources monitor and report on activity involving network infrastructure, including system up/down status, configuration changes, bandwidth usage, and login events.

Network Presentation Resources

Table 2-14 Information Presentation Resources for the Network Use Case

Resource	Description	Type	URI
Network Login Overview	This dashboard shows an overview of logins on network devices. The dashboard displays the "Last 10 Failed Login Events", "Last 10 Successful Login Events", "Login Results", and "Top 10 Users With Failed Logins" data monitors.	Dashboard	ArcSight Express/Network/
Network Status Overview	This dashboard displays data monitors related to network device errors, network interfaces and critical network events.	Dashboard	ArcSight Express/Network/
Device Critical Events	This report shows information regarding critical events on network devices. These critical events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/
Device Errors	This report shows information regarding system errors on network devices. These events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/

Resource	Description	Type	URI
Device Events	This report shows information regarding events on network devices. These events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/
Device Interface Down Notifications	This report shows a table displaying the network devices that report a down link.	Report	ArcSight Express/Network/
Device Interface Status Messages	This report shows a table displaying the network devices reporting link status changes.	Report	ArcSight Express/Network/
Device SNMP Authentication Failures	This report shows summaries of SNMP authentication failures by device or by user. A table details the failed user SNMP authentication attempts for the devices. Two charts give an overview of the users or devices with the most SNMP authentication failures.	Report	ArcSight Express/Network/

Network Data Processing Resources

Table 2-15 Data Processing Resources for the Network Use Case

Resource	Description	Type	URI
Last 10 Failed Login Events	This data monitor shows the last 10 failed logins on network devices.	Data Monitor	ArcSight Express/Network/Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful logins on network devices.	Data Monitor	ArcSight Express/Network/Login Overview/
Login Results	This data monitor shows the number of logins on network devices (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Express/Network/Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top 10 users with failed logins on network devices.	Data Monitor	ArcSight Express/Network/Login Overview/
Top Users by Login Activity	This top value counts data monitor shows the users with the most network login activity over the last 60 minutes.	Data Monitor	ArcSight Express/Network/Login Overview/
Devices with High Error Rates	This moving average data monitor tracks network device error rates over the last hour. Devices that show up, when this data monitor is displayed in a dashboard or in the resulting correlation events, have reported at least 3 errors within a five minute period.	Data Monitor	ArcSight Express/Network/Network Status Overview/

Resource	Description	Type	URI
Last 10 Critical Network Events	This Last N Events data monitor displays the last 10 events reported by network devices with an agent severity of high or very high.	Data Monitor	ArcSight Express/Network/Network Status Overview/
Last 10 Interface Down Messages	This Last N Events data monitor displays the last 10 events reported by network devices related to down network interfaces, ports or links.	Data Monitor	ArcSight Express/Network/Network Status Overview/
Last 10 Interface Status Messages	This Last N Events data monitor displays the last 10 events reported by network devices related to network interfaces, ports or links.	Data Monitor	ArcSight Express/Network/Network Status Overview/
Bandwidth Usage by Protocol	This report shows a summary of network bandwidth usage by application protocol in a chart and a table. The chart shows the top 10 protocols with the highest bandwidth usage, and the table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/Network/
Bandwidth Usage per Hour	This report shows a summary of network bandwidth usage per hour in a chart. The chart shows the average bandwidth usage per hour for the past 24 hours (by default).	Focused Report	ArcSight Express/Network/
Configuration Changes by Type	This report shows recent network configuration changes in a table. The table lists all the changes, grouped by type (name), and sorts them chronologically.	Focused Report	ArcSight Express/Network/
Configuration Changes by User	This report shows recent network configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/Network/
Failed Logins by Destination Address	This report shows authentication failures from network login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Network/
Failed Logins by Source Address	This report shows authentication failures from network login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Network/
Failed Logins by User	This reports shows authentication failures from network login attempts by user in a chart and a table. The chart shows the top 10 users with failed login attempts, and the table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Network/

Resource	Description	Type	URI
Login Event Audit	This report shows all the successful and failed Network login events in a table. The table is sorted chronologically.	Focused Report	ArcSight Express/Network/
Successful Logins by Destination Address	This report shows authentication successes from network login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Network/
Successful Logins by Source Address	This report shows authentication successes from network login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Network/
Successful Logins by User	This reports shows authentication successes from Network login attempts by user in a chart and a table. The chart shows the top users with successful login attempts, and the table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/Network/
Top Bandwidth Hosts	This report shows a summary of the bandwidth usage reported by network devices by the top hosts in a chart. The chart shows the average bandwidth usage by host for the previous day (by default).	Focused Report	ArcSight Express/Network/
Top Hosts by Number of Connections	This report shows a summary of the number of network connections by the top hosts in a chart. The chart shows the number of connections by host for the previous day (by default).	Focused Report	ArcSight Express/Network/

Operating System

The Operating System resources monitor and report on activity involving operating systems, such as user logins, and user modification events.

Operating System Presentation Resources

Table 2-16 Information Presentation Resources for the Network Use Case

Resource	Description	Type	URI
Network Login Overview	This dashboard shows an overview of logins on network devices. The dashboard displays the "Last 10 Failed Login Events", "Last 10 Successful Login Events", "Login Results", and "Top 10 Users With Failed Logins" data monitors.	Dashboard	ArcSight Express/Network/
Network Status Overview	This dashboard displays data monitors related to network device errors, network interfaces and critical network events.	Dashboard	ArcSight Express/Network/
Device Critical Events	This report shows information regarding critical events on network devices. These critical events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/
Device Errors	This report shows information regarding system errors on network devices. These events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/
Device Events	This report shows information regarding events on network devices. These events could be indications of hardware failure, resource exhaustion, configuration issues or attacks.	Report	ArcSight Express/Network/
Device Interface Down Notifications	This report shows a table displaying the network devices that report a down link.	Report	ArcSight Express/Network/
Device Interface Status Messages	This report shows a table displaying the network devices reporting link status changes.	Report	ArcSight Express/Network/
Device SNMP Authentication Failures	This report shows summaries of SNMP authentication failures by device or by user. A table details the failed user SNMP authentication attempts for the devices. Two charts give an overview of the users or devices with the most SNMP authentication failures.	Report	ArcSight Express/Network/

Operating System Data Processing Resources

Table 2-17 Data Processing Resources for the Operating System Use Case

Resource	Description	Type	URI
Last 10 Failed Login Events	This data monitor shows the last 10 failed operating system logins.	Data Monitor	ArcSight Express/Operating System/Operating System Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful operating system logins.	Data Monitor	ArcSight Express/Operating System/Operating System Login Overview/
Login Results	This data monitor shows the number of operating system logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Express/Operating System/Operating System Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top 10 users with failed operating system logins.	Data Monitor	ArcSight Express/Operating System/Operating System Login Overview/
Top Users by Login Activity	This top value counts data monitor shows the users with the most operating system login activity over the last 60 minutes.	Data Monitor	ArcSight Express/Operating System/Operating System Login Overview/
Configuration Changes by Type	This report shows recent operating system configuration changes in a table. The table lists all the changes, grouped by type, and sorts them chronologically.	Focused Report	ArcSight Express/Operating System/
Configuration Changes by User	This report shows recent operating system configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/Operating System/
Failed Login Attempts	This report shows the count of operating system authentication failures from login attempts by hour in a chart and the details of all the authentication failures in a table.	Focused Report	ArcSight Express/Operating System/
Failed Logins by Destination Address	This report shows authentication failures from operating system login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/Operating System/

Resource	Description	Type	URI
Failed Logins by Source Address	This report shows authentication failures from operating system login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/Operating System/
Failed Logins by User	This report shows a summary of the failed operating system logins by username in a chart and a table. The chart shows the top 10 usernames with failed logins, and the table shows the details of the successful logins for each username (time, source, destination).	Focused Report	ArcSight Express/Operating System/
Login Event Audit	This report shows all the successful and failed operating system login events in a table. The table is sorted chronologically.	Focused Report	ArcSight Express/Operating System/
Password Changes	This report shows operating system password changes for the previous day in a table. The table groups the password changes by user and sort them chronologically.	Focused Report	ArcSight Express/Operating System/
Successful Logins by Destination Address	This report shows authentication successes from operating system login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/Operating System/
Successful Logins by Source Address	This report shows authentication successes from operating system login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/Operating System/
Successful Logins by User	This report shows a summary of the successful operating system logins by username in a chart and a table. The chart shows the top 10 usernames with successful logins, and the table shows the details of the successful logins for each username (time, source, destination).	Focused Report	ArcSight Express/Operating System/

VPN

The VPN resources monitor and report on activity involving VPN connections, including authentication errors, logins, and connection status.

VPN Presentation Resources

Table 2-18 Information Presentation Resources for the VPN Use Case

Resource	Description	Type	URI
VPN Connection Statistics	This dashboard displays data monitors related to VPN Servers, including connection status counts and authentication errors.	Dashboard	ArcSight Express/VPN/
VPN Login Overview	This dashboard shows an overview of VPN logins. The dashboard displays the "Last 10 Failed Login Events", "Last 10 Successful Login Events", "Login Results", and "Top 10 Users With Failed Logins" data monitors.	Dashboard	ArcSight Express/VPN/
Authentication Errors	This report shows errors generated by a VPN connection attempt. The address is the IP address of the VPN connection source. This report can be used to see which users are having difficulties using or setting up their VPN clients.	Report	ArcSight Express/VPN/
Connection Counts by User	This report shows count information about VPN connections for each user. A summary of the Top Users by Connection Count is provided. Details of each user's connection counts are also provided, including connection count and systems accessed.	Report	ArcSight Express/VPN/
Connections Accepted by Address	This report shows successful VPN connection data. A chart summarizes the top VPN device addresses with successful connections. A table shows details of the successful connections.	Report	ArcSight Express/VPN/
Connections Denied by Address	This report shows denied VPN connection data. A chart summarizes the top VPN device addresses with denied connections. A table shows details of the denied connections.	Report	ArcSight Express/VPN/
Connections Denied by Hour	This report shows denied VPN connection data. A chart summarizes the number of denied connections for each hour. A table shows details of the denied connections by hour.	Report	ArcSight Express/VPN/

Resource	Description	Type	URI
Top Users by Average Session Length	This report shows duration information about VPN connections for each user. A summary of the Top VPN Connection Duration by User is provided. Details of each user's connection durations are also provided, including minimum, average, maximum and total connection minutes. Also included are details of connections that are currently open at the time the report was run.	Report	ArcSight Express/VPN/

VPN Data Processing Resources

Table 2-19 Data Processing Resources for the VPN Use Case

Resource	Description	Type	URI
Top VPN Servers with Authentication Errors	This Top Value Counts data monitor tracks the number of VPN authentication error events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Express/VPN/VPN Connection Statistics/
Top VPN Servers with Denied Connections	This Top Value Counts data monitor tracks the number of failed VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Express/VPN/VPN Connection Statistics/
Top VPN Servers with Successful Connections	This Top Value Counts data monitor tracks the number of successful VPN connection events for each VPN server every five minutes for an hour.	Data Monitor	ArcSight Express/VPN/VPN Connection Statistics/
Top VPN Users with Authentication Errors	This Top Value Counts data monitor tracks the number of VPN authentication error events for each VPN user (including the VPN server), every five minutes for an hour.	Data Monitor	ArcSight Express/VPN/VPN Connection Statistics/
Last 10 Failed Login Events	This data monitor shows the last 10 failed VPN logins.	Data Monitor	ArcSight Express/VPN/VPN Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful VPN logins.	Data Monitor	ArcSight Express/VPN/VPN Login Overview/
Login Results	This data monitor shows the number of VPN logins (attempt, success, failure) in a pie chart.	Data Monitor	ArcSight Express/VPN/VPN Login Overview/
Top 10 Users With Failed Logins	This data monitors shows the top 10 users with failed VPN logins.	Data Monitor	ArcSight Express/VPN/VPN Login Overview/
Top Users by Login Activity	This top value counts data monitor shows the users with the most VPN login activity over the last 60 minutes.	Data Monitor	ArcSight Express/VPN/VPN Login Overview/

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This report shows a summary of VPN bandwidth usage by application protocol in a chart and a table. The chart shows the top 10 protocols with the highest bandwidth usage, and the table lists all the protocols sorted by bandwidth usage.	Focused Report	ArcSight Express/VPN/
Bandwidth Usage per Hour	This report shows a summary of VPN bandwidth usage per hour in a chart. The chart shows the average bandwidth usage per hour for the past 24 hours (by default).	Focused Report	ArcSight Express/VPN/
Configuration Changes by Type	This report shows recent VPN configuration changes in a table. The table lists all the changes, grouped by type (name), and sorts them chronologically.	Focused Report	ArcSight Express/VPN/
Configuration Changes by User	This report shows recent VPN configuration changes in a table. The table lists all the changes, grouped by user, and sorts them chronologically.	Focused Report	ArcSight Express/VPN/
Failed Logins by Destination Address	This report shows authentication failures from VPN login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with failed login attempts, and the table shows the count of authentication failures by destination-source pair and by user.	Focused Report	ArcSight Express/VPN/
Failed Logins by Source Address	This report shows authentication failures from VPN login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with failed login attempts, and the table shows the count of authentication failures by source-destination pair and by user.	Focused Report	ArcSight Express/VPN/
Failed Logins by User	This reports shows authentication failures from VPN login attempts by user in a chart and a table. The chart shows the top 10 users with failed login attempts, and the table shows the details of the failed login attempts grouped and sorted by user.	Focused Report	ArcSight Express/VPN/
Login Event Audit	This report shows all the successful and failed VPN login events in a table. The table is sorted chronologically.	Focused Report	ArcSight Express/VPN/
Password Changes	This report shows VPN password changes for the previous day in a table. The table groups the password changes by user and sort them chronologically.	Focused Report	ArcSight Express/VPN/

Resource	Description	Type	URI
Successful Logins by Destination Address	This report shows authentication successes from VPN login attempts by destination address in a chart and a table. The chart shows the top 10 destination addresses with successful login attempts, and the table shows the count of authentication successes by destination-source pair and by user.	Focused Report	ArcSight Express/VPN/
Successful Logins by Source Address	This report shows authentication successes from VPN login attempts by source address in a chart and a table. The chart shows the top 10 source addresses with successful login attempts, and the table shows the count of authentication successes by source-destination pair and by user.	Focused Report	ArcSight Express/VPN/
Successful Logins by User	This reports shows authentication successes from VPN login attempts by user in a chart and a table. The chart shows the top users with successful login attempts, and the table shows the details of the successful login attempts grouped and sorted by user.	Focused Report	ArcSight Express/VPN/
Top Bandwidth Hosts	This report shows a summary of the VPN bandwidth usage by the top hosts in a chart. The chart shows the average bandwidth usage by host for the previous day (by default).	Focused Report	ArcSight Express/VPN/
Top Hosts by Number of Connections	This report shows a summary of the number of VPN connections by the top hosts in a chart. The chart shows the number of connections by host for the previous day (by default).	Focused Report	ArcSight Express/VPN/

Vulnerabilities

The Vulnerabilities resources monitor and report on exposed vulnerabilities by asset.

Vulnerabilities Presentation Resources

Table 2-20 Information Presentation Resources for the Vulnerabilities Use Case

Resource	Description	Type	URI
Exposed Vulnerabilities by Asset		Report	ArcSight Express/Vulnerabilities/
Exposed Vulnerability Count by Asset	This report shows a table that lists the count of vulnerabilities per asset and a chart that displays the 10 assets with the most exposed vulnerabilities.	Report	ArcSight Express/Vulnerabilities/

Vulnerabilities Data Processing Resources

Table 2-21 Data Processing Resources for the Vulnerabilities Use Case

Resource	Description	Type	URI
Exposed Vulnerability Count by Critical Asset		Focused Report	ArcSight Express/Vulnerabilities/

Upgrading ArcSight Express Content

This topic applies if you have an ArcSight Express appliance with a software version previous to v4.5 SP1. The ArcSight Express v4.5 SP1 software release contains fixes and enhancements to content and the user interface. For a complete description of the changes available in ArcSight Express v4.5 SP1, see the *Release Notes for ArcSight Express v4.5 SP1*.

The ArcSight Express appliance is upgraded using a self-extracting upgrade file downloaded from the ArcSight Customer Support web site. The software upgrade process is described in the tech note *Upgrading ArcSight Express v4.5 GA to v4.5 SP1*.

This appendix describes how to prepare ArcSight Express 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 47](#)

[“About Running the Upgrade Script” on page 49](#)

[“Verifying and Reapplying Configurations After Upgrade” on page 49](#)

Preparing Existing Content for Upgrade

The majority of ArcSight Express 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 7](#).
- Any configurations made to ArcSight-supplied **rules**, such as those described in [“Configure Rules to Send Notifications and Open Cases” on page 10](#).
- Modifications made directly to ArcSight Express 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 48](#) 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 *AE 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 Script

After copying the configured resources, you are ready to run the upgrade RPM script using the process described in tech note *Upgrading ArcSight Express v4.5 GA to v4.5 SP1*.

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

For more about fixing invalid resources after the upgrade, see ["Fixing Invalid Resources" on page 50](#).

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 47](#) 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 Express 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 Express v4.5 SP1 content.

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

Verify Proper Function of Customer-Created Content

It is possible during upgrade that updates to the ArcSight Express 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 Express 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 50](#), 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

- Alert Counts by Device report 32
- Alert Counts by Port report 32
- Alert Counts by Severity report 32
- Alert Counts by Type report 32
- Alert Counts per Hour report 32
- All Cases report 22
- All Level 3 Notifications report 33
- Anti-Virus Overview dashboard 20
- ArcSight Express
 - Device list 3
- Asset Auto-Creation Filter
 - Connector 7
 - Device 8
- Asset Modeling
 - Protected Network 5
- Authentication Errors report 41
- Average Time to Case Resolution - By Day report 22
- Average Time to Case Resolution - By Severity report 22
- Average Time to Case Resolution - By User report 23

B

- Bandwidth Usage by Hour report 17
- Bandwidth Usage by Protocol focused report 28, 36, 43
- Bandwidth Usage by Protocol report 18
- Bandwidth Usage per Hour focused report 28, 36, 43
- By User Account - Accounts Created report 19

C

- Case Stage Counts report 23
- Cases by Operational Impact report 23
- Cases Overview report 23
- Cases per Target report 23
- Configuration
 - Connector Asset Auto-Creation Filter 7
 - Device Asset Auto-Creation Filter 8
 - schedule reports 13
 - set up connectors and model the network 2
- Configuration Changes by Type focused report 22, 25, 28, 30, 36, 39, 43
- Configuration Changes by Type report 19
- Configuration Changes by User focused report 22, 25, 28, 30, 36, 39, 43
- Configuration Changes by User report 19
- Configuration Changes Overview dashboard 17
- Connection Counts by User report 30, 41
- Connection Durations by User report 30
- Connections Accepted by Address report 41
- Connections Denied by Address report 41

- Connections Denied by Hour report 41

D

dashboards

- Anti-Virus Overview 20
- Configuration Changes Overview 17
- Database Errors 25
- Firewall Connection Overview 26
- Firewall Login Overview 26
- IDS - IPS Overview 32
- Network Login Overview 34, 38
- Network Status Overview 34, 38
- Reconnaissance in Progress 17
- Security Activity 17
- Security Activity Statistics 17
- Virus Activity Statistics 20
- VPN Connection Statistics 41
- VPN Login Overview 41
- Worm Outbreak Overview 32

data monitors

- Devices with High Error Rates 35
- Last 10 Anti-Virus Errors 21
- Last 10 Critical Network Events 36
- Last 10 Database Configuration Changes 20
- Last 10 Database Errors 25
- Last 10 Failed Login Events 27, 35, 39, 42
- Last 10 Firewall Configuration Changes 20
- Last 10 Interface Down Messages 36
- Last 10 Interface Status Messages 36
- Last 10 Network Configuration Changes 20
- Last 10 Successful Login Events 27, 35, 39, 42
- Last 10 VPN Configuration Changes 20
- Login Results 27, 35, 39, 42
- Target Port Activity by Attacker 33
- Top 10 Alert Destinations 33
- Top 10 Alert Sources 33
- Top 10 Alert Types 33
- Top 10 Alerts 33
- Top 10 Anti-Virus Errors 21
- Top 10 Database Errors 25
- Top 10 Denied Ports (Inbound) 27
- Top 10 Denied Ports (Outbound) 27
- Top 10 Hosts With Denied Inbound Connections 27
- Top 10 Hosts With Denied Outbound Connections 27
- Top 10 Infected Systems 22
- Top 10 Infections 22
- Top 10 Users With Failed Logins 27, 35, 39, 42
- Top Users by Login Activity 28, 35, 39, 42
- Top VPN Servers with Authentication Errors 42
- Top VPN Servers with Denied Connections 42

- Top VPN Servers with Successful Connections 42
- Top VPN Users with Authentication Errors 42
- Worm Activity Status 34
- Worm Infected Systems 34
- Database Errors and Warnings report 25
- Database Errors dashboard 25
- Denied Inbound Connections by Address report 26
- Denied Inbound Connections by Port report 26
- Denied Inbound Connections per Hour report 26
- Denied Outbound Connections by Address report 26
- Denied Outbound Connections by Port report 27
- Denied Outbound Connections per Hour report 27
- Device Critical Events report 34, 38
- Device Errors report 34, 38
- Device Events report 35, 38
- Device Interface Down Notifications report 35, 38
- Device Interface Status Messages report 35, 38
- Device SNMP Authentication Failures report 35, 38
- Devices with High Error Rates data monitor 35

E

- Errors Detected in Anti-Virus Deployment report 21
- Exposed Vulnerabilities by Asset report 44
- Exposed Vulnerability Count by Asset report 44
- Exposed Vulnerability Count by Critical Asset focused report 45

F

- Failed Anti-Virus Updates report 21
- Failed Login Attempts focused report 30, 39
- Failed Login Attempts report 18
- Failed Logins by Destination Address focused report 28, 31, 36, 39, 43
- Failed Logins by Destination Address report 18
- Failed Logins by Source Address focused report 28, 31, 36, 40, 43
- Failed Logins by Source Address report 18
- Failed Logins by User focused report 28, 31, 36, 40, 43
- Failed Logins by User report 18
- Firewall Connection Overview dashboard 26
- Firewall Login Overview dashboard 26
- focused reports
 - Bandwidth Usage by Protocol 28, 36, 43
 - Bandwidth Usage per Hour 28, 36, 43
 - Configuration Changes by Type 22, 25, 28, 30, 36, 39, 43
 - Configuration Changes by User 22, 25, 28, 30, 36, 39, 43
 - Exposed Vulnerability Count by Critical Asset 45
 - Failed Login Attempts 30, 39
 - Failed Logins by Destination Address 28, 31, 36, 39, 43
 - Failed Logins by Source Address 28, 31, 36, 40, 43
 - Failed Logins by User 28, 31, 36, 40, 43
 - Login Event Audit 25, 28, 37, 40, 43
 - Password Changes 25, 31, 40, 43
 - Successful Logins by Destination Address 29, 31, 37, 40, 44
 - Successful Logins by Source Address 29, 31, 37, 40, 44
 - Successful Logins by User 29, 31, 37, 40, 44
 - Top 10 Alerts 34
 - Top 10 Attackers 34

- Top 10 Targets 34
- Top Bandwidth Hosts 29, 37, 44
- Top Hosts by Number of Connections 29, 37, 44

I

- IDS - IPS Overview dashboard 32

L

- Last 10 Anti-Virus Errors data monitor 21
- Last 10 Critical Network Events data monitor 36
- Last 10 Database Configuration Changes data monitor 20
- Last 10 Database Errors data monitor 25
- Last 10 Failed Login Events data monitor 27, 35, 39, 42
- Last 10 Firewall Configuration Changes data monitor 20
- Last 10 Interface Down Messages data monitor 36
- Last 10 Interface Status Messages data monitor 36
- Last 10 Network Configuration Changes data monitor 20
- Last 10 Successful Login Events data monitor 27, 35, 39, 42
- Last 10 VPN Configuration Changes data monitor 20
- Login Event Audit focused report 25, 28, 37, 40, 43
- Login Event Audit report 18
- Login Results data monitor 27, 35, 39, 42

M

- Max Time to Case Resolution - By User report 23

N

- Network Login Overview dashboard 34, 38
- Network Modeling
 - ArcSight Express 2
- Network Status Overview dashboard 34, 38
- Notification Action Events report 23
- Notification Overview report 23
- Notification Statistics Summary report 24
- Notification Status Report report 24
- Notifications By Acknowledgement Status report 24

O

- Open Cases report 24

P

- Password Changes focused report 25, 31, 40, 43
- Password Changes report 19
- Protected Network
 - How ArcSight determines 5

R

- Reconnaissance in Progress dashboard 17
- Reports
 - scheduling 13
- reports
 - Alert Counts by Device 32
 - Alert Counts by Port 32
 - Alert Counts by Severity 32
 - Alert Counts by Type 32
 - Alert Counts per Hour 32
 - All Cases 22

All Level 3 Notifications 23
 Authentication Errors 41
 Average Time to Case Resolution - By Day 22
 Average Time to Case Resolution - By Severity 22
 Average Time to Case Resolution - By User 23
 Bandwidth Usage by Hour 17
 Bandwidth Usage by Protocol 18
 By User Account - Accounts Created 19
 Case Stage Counts 23
 Cases by Operational Impact 23
 Cases Overview 23
 Cases per Target 23
 Configuration Changes by Type 19
 Configuration Changes by User 19
 Connection Counts by User 30, 41
 Connection Durations by User 30
 Connections Accepted by Address 41
 Connections Denied by Address 41
 Connections Denied by Hour 41
 Database Errors and Warnings 25
 Denied Inbound Connections by Address 26
 Denied Inbound Connections by Port 26
 Denied Inbound Connections per Hour 26
 Denied Outbound Connections by Address 26
 Denied Outbound Connections by Port 27
 Denied Outbound Connections per Hour 27
 Device Critical Events 34, 38
 Device Errors 34, 38
 Device Events 35, 38
 Device Interface Down Notifications 35, 38
 Device Interface Status Messages 35, 38
 Device SNMP Authentication Failures 35, 38
 Errors Detected in Anti-Virus Deployment 21
 Exposed Vulnerabilities by Asset 44
 Exposed Vulnerability Count by Asset 44
 Failed Anti-Virus Updates 21
 Failed Login Attempts 18
 Failed Logins by Destination Address 18
 Failed Logins by Source Address 18
 Failed Logins by User 18
 Login Event Audit 18
 Max Time to Case Resolution - By User 23
 Notification Action Events 23
 Notification Overview 23
 Notification Statistics Summary 24
 Notification Status Report 24
 Notifications By Acknowledgement Status 24
 Open Cases 24
 Password Changes 19
 Successful Logins by Destination Address 18
 Successful Logins by Source Address 18
 Successful Logins by User 19
 Today'sCases' 24
 Top Alert Destinations 33
 Top Alert Sources 33
 Top Alerts from IDS and IPS 19
 Top Attackers 19
 Top Bandwidth Hosts 18
 Top Hosts by Number of Connections 19
 Top Infected Systems 21
 Top Targets 19
 Top Users by Average Session Length 42
 Unacknowledged Level 3 Notifications 24
 Update Summary 21

Virus Activity by Time 21
 Worm Infected Systems 33

S

Security Activity dashboard 17
 Security Activity Statistics dashboard 17
 SmartConnectors
 for ArcSight Express content 3
 Successful Logins by Destination Address focused report 29, 31, 37, 40, 44
 Successful Logins by Destination Address report 18
 Successful Logins by Source Address focused report 29, 31, 37, 40, 44
 Successful Logins by Source Address report 18
 Successful Logins by User focused report 29, 31, 37, 40, 44
 Successful Logins by User report 19

T

Target Port Activity by Attacker data monitor 33
 TodaysCasesreport 24
 Top 10 Alert Destinations data monitor 33
 Top 10 Alert Sources data monitor 33
 Top 10 Alert Types data monitor 33
 Top 10 Alerts data monitor 33
 Top 10 Alerts focused report 34
 Top 10 Anti-Virus Errors data monitor 21
 Top 10 Attackers focused report 34
 Top 10 Database Errors data monitor 25
 Top 10 Denied Ports (Inbound) data monitor 27
 Top 10 Denied Ports (Outbound) data monitor 27
 Top 10 Hosts With Denied Inbound Connections data monitor 27
 Top 10 Hosts With Denied Outbound Connections data monitor 27
 Top 10 Infected Systems data monitor 22
 Top 10 Infections data monitor 22
 Top 10 Targets focused report 34
 Top 10 Users With Failed Logins data monitor 27, 35, 39, 42
 Top Alert Destinations report 33
 Top Alert Sources report 33
 Top Alerts from IDS and IPS report 19
 Top Attackers report 19
 Top Bandwidth Hosts focused report 29, 37, 44
 Top Bandwidth Hosts report 18
 Top Hosts by Number of Connections focused report 29, 37, 44
 Top Hosts by Number of Connections report 19
 Top Infected Systems report 21
 Top Targets report 19
 Top Users by Average Session Length report 42
 Top Users by Login Activity data monitor 28, 35, 39, 42
 Top VPN Servers with Authentication Errors data monitor 42
 Top VPN Servers with Denied Connections data monitor 42
 Top VPN Servers with Successful Connections data monitor 42
 Top VPN Users with Authentication Errors data monitor 42

U

Unacknowledged Level 3 Notifications report 24
Update Summary report 21
Upgrading ArcSight Express Content 47
 After Upgrade 49
 Preparing for Upgrade 47

V

Virus Activity by Time report 21

Virus Activity Statistics dashboard 20
VPN Connection Statistics dashboard 41
VPN Login Overview dashboard 41

W

Worm Activity Status data monitor 34
Worm Infected Systems data monitor 34
Worm Infected Systems report 33
Worm Outbreak Overview dashboard 32