ArcSight™ Standard Content Guide

for ArcSight Express™ v3.0

April 2012

ArcSight™
An HP Company

ArcSight™ Standard
Content Guide: ArcSight Express™ v3.0

Revision History

Date	Product Version	Description
04/23/2012	ArcSight Express v3.0	Resource descriptions and upgrade instructions.

Document template version: 1.0.2.8

Contact Information

Phone	1-866-535-3285 (North America) +44 (0)870 141 7487 (EMEA)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1: ArcSight Express Content 5

What is ArcSight Express Content? 5
How ArcSight Express Content Is Organized 6
Set Up Connectors and Model the Network 7
ArcSight Express-Related SmartConnectors 7
Network Modeling 8
Apply Standard Asset Categories to Assets 9
Categorize Internal Assets 9
Determine the Protected Network 9
Categorize Critical Assets 9
Create ArcSight Express Users 9
Configure Notification Destinations 10
Configure Asset Auto-Creation Filters 11
Configure Connector Asset Auto-Creation Controller Filter 11
Configure Device Asset Auto Creation Controller Filter 12
Configure Rules to Send Notifications and Open Cases 14
Schedule Reports 17
Tuning ArcSight Express Content 18

Chapter 2: Resource Reference 21

ArcSight Express 21
Anti-Virus 39
Case Tracking and Escalation 44
Database 49
Firewall 51
Identity Management 58
IDS-IPS 63
Network 67
Operating System 74
VPN 80
Vulnerabilities 87

Appendix A: Upgrading ArcSight Express Content 89

Preparing Existing Content for Upgrade 89

Configurations that Persist 89
Configurations that Require Restoration After Upgrade 90
Backing Up Existing Resources Before Upgrade 90
Running the Upgrade Script 91
Verifying and Reapplying Configurations After Upgrade 91
Verify Proper Function of Customer-Created Content 91
Fixing Invalid Resources 92

Index 93

Chapter 1

ArcSight Express Content

ArcSight Express v3.0 introduces the Correlation Optimized Retention and Retrieval Engine Storage (CORR-Engine Storage), a proprietary data storage and retrieval framework that receives and processes events at high rates, and performs high-speed searches. This provides a number of benefits, including increased performance and more compact data storage.

With some basic configuration done using the ArcSight 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.

"What is ArcSight Express Content?" on page 5

"How ArcSight Express Content Is Organized" on page 6

"Set Up Connectors and Model the Network" on page 7

"Apply Standard Asset Categories to Assets" on page 9

"Create ArcSight Express Users" on page 9

"Configure Notification Destinations" on page 10

"Configure Asset Auto-Creation Filters" on page 11

"Configure Rules to Send Notifications and Open Cases" on page 14

"Schedule Reports" on page 17

"Tuning ArcSight Express Content" on page 18

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 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.

How ArcSight Express Content Is Organized

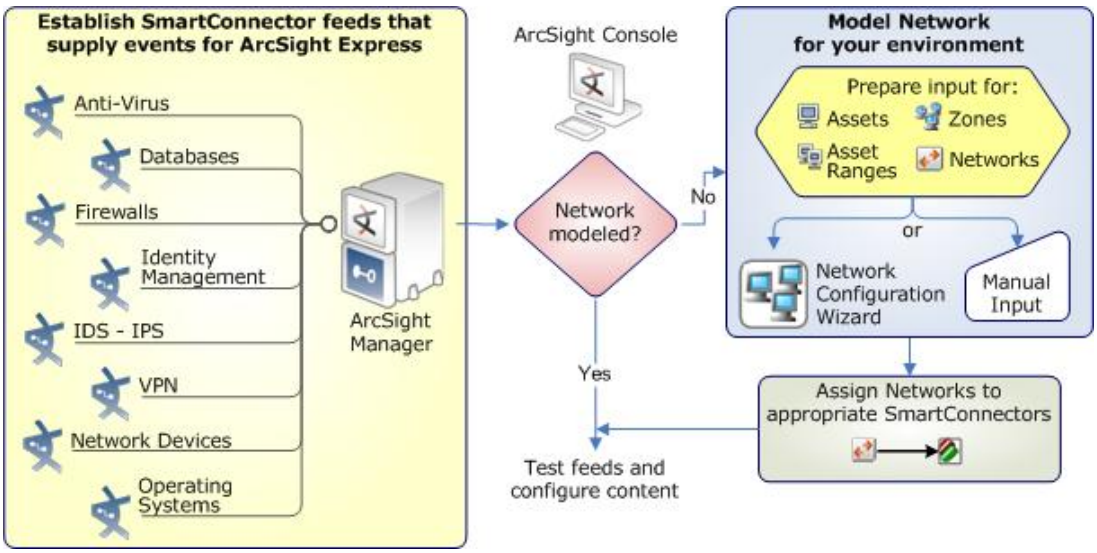
ArcSight Express content monitors and reports on activity relevant to the types of devices reporting into the Manager. The content is organized into the following device-specific groups:

Table 1-1 How ArcSight Express Content is Organized

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 following graphic outlines the process for establishing the feeds necessary to drive the ArcSight Express content.



Configuring ArcSight Express content starts with installing SmartConnectors and configuring zones and networks for devices that report to the Manager.

1. Establish relevant SmartConnector feeds.
2. Model the network.
3. Assign networks to the appropriate SmartConnectors.
4. Test feeds and configure content.

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.

Table 1-2 ArcSight Express-Related SmartConnectors

Device Group	Related Connectors
Anti-Virus	Most major anti-virus products, such as: • Symantec EndPoint Protection • TrendMicro • McAfee AV
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: • Juniper Netscreen • CheckPoint • Cisco PIX

Table 1-2ArcSight Express-Related SmartConnectors

Device Group	Related Connectors
Identity Management	Identity management content picks up from identity management systems, such as: • Juniper Steel-Belted Radius • Cisco Secure ACS • Windows AD
IDS - IPS	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: • ISS Site Protector • Symantec Network Security • Cisco IPS
Network	This content works on events from networking devices, such as: • Cisco IOS Devices • Juniper JunOS Devices
Operating System	This content picks up events from Windows and UNIX-based systems that generate relevant events and for which ArcSight supplies supported connectors, such as: • Linux OS Events (All major Versions) • MS Windows (2003/XP)
VPN	This content works on events from most VPN devices that report on errors, sessions established, and so on. For example: • Juniper/Netscreen VPN • Cisco VPN • CheckPoint VPN-1
Vulnerabilities	Vulnerability content relies on the device model, which can be populated one by one, or by a vulnerability scanner for which ArcSight supplies a Connector.

Network Modeling

ArcSight Express 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 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 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 9 before creating the comma-separated values lists to load into the network model.

For more about the network model and how to populate it, see the ESM User's Guide.

For more about the Network Modeling Wizard, see the ESM User's Guide.

To learn more about the architecture of network modeling tools, see Chapter 4, "ArcSight Network Model" in ESM 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 the ESM User's Guide.

For more about the Network Modeling Wizard, see the ESM User's Guide.

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 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/`

Determine 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 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 the ESM User's Guide.

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. However, the admin user can 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 14.

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**:

Table 1-3 Destination Editor Fields

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 for delivering notifications: • **Console** — Notification popup in this user's ArcSight account • **E-Mail** — User's email 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 email address.
User/Group	From the drop-down menu, select the individual user or user group who receives 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 ArcSight 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, the Manager would model a new Connector, which falsely clutters the network model with Connector nodes.

To limit how the Manager 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.

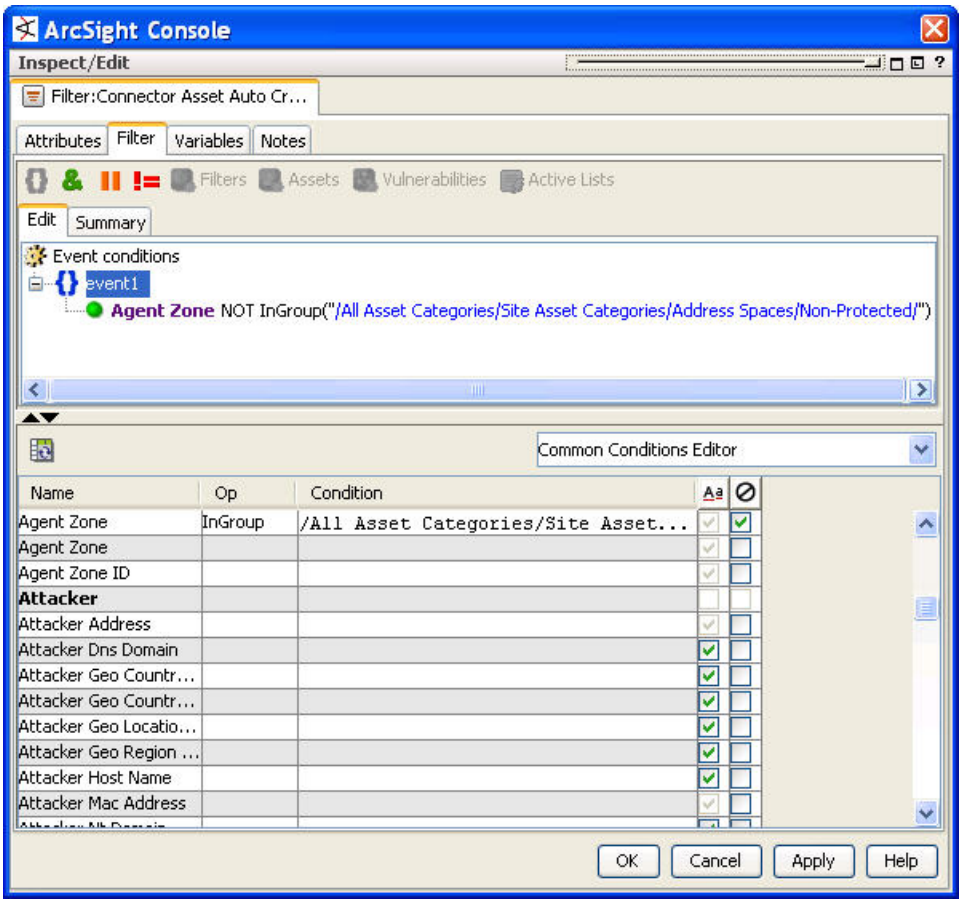
Configure Connector Asset Auto-Creation Controller Filter

The Asset Auto-Creation Events filter directs the Manager 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.



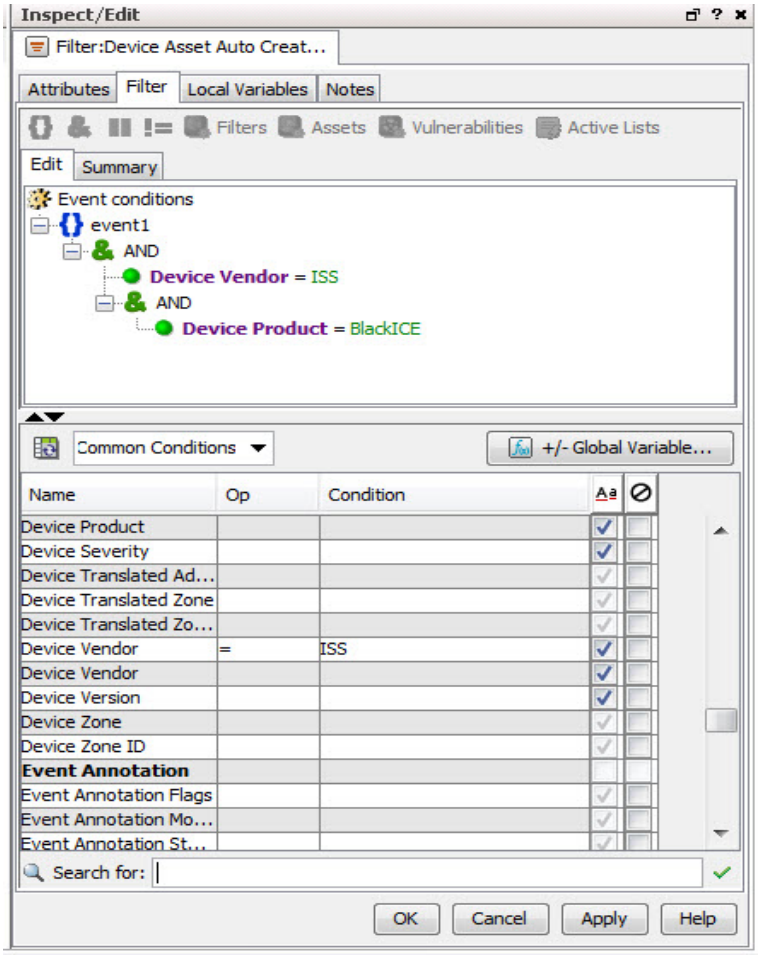
1. In the Navigator panel, navigate to the Connector Asset Auto Creation Controller filter (`All Filters/ArcSight System/Asset Auto Creation`) and double-click it to open it in the Inspect/Edit panel.
2. In the Filter editor in the Inspect/Edit panel, select the **Filter** tab. Delete the default condition `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 5 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 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 10, then enable the notification and case actions in the rules.

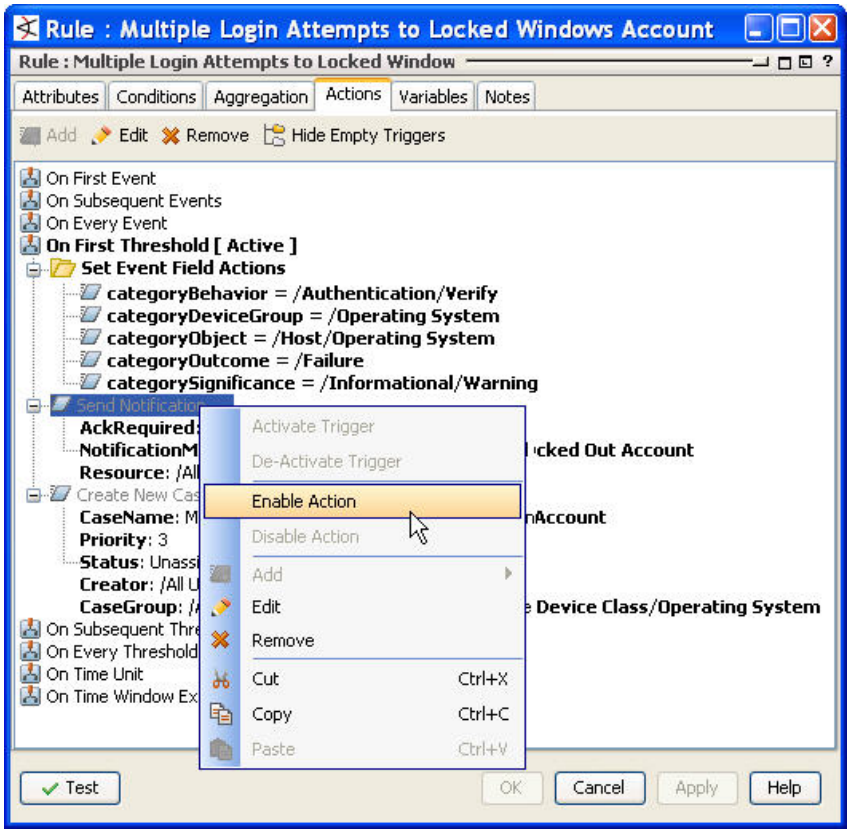
1 In the Navigator panel, navigate to each rule listed in "Configure Rules with Notifications to the Cert Team" on page 15 and "Configure Rules with Notifications to the SOC Operators" on page 16.

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 appears 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 5 for each rule listed in "Configure Rules with Notifications to the Cert Team" on page 15 and "Configure Rules with Notifications to the SOC Operators" on page 16.

For more about working with Rule actions in the Rules Editor, see the ESM User's Guide.

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.

Table 1-4 Configure Rules with Notifications to Cert Team URIs

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.

Table 1-5 Configure Rules with Notifications to the SOC Operators

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

Table 1-5 Configure Rules with Notifications to the SOC Operators

Rule URI	Rule Name
/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

Table 1-6 Reports on Cases

Report URI	Report Name
/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

Table 1-7 Reports on Notification

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

Table 1-8 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 the ESM User's Guide.

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 RuleExclusions are referenced by the user-based rules:

Table 1-9 Event-Based Rules and 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:

Table 1-10 Fields stored in Active Lists

Event-based Rule Exclusions	User-based Rule Exclusions
The following fields limit the rule exclusions to very specific events between two specific systems. • 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. • 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 displays the list of fields the active list saves from the selected event. If the selected event does not have a value for one or more of the fields, those fields 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 the ESM User's Guide.

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 5.

ArcSight Express

The ArcSight Express use case contains several useful resources for monitoring network and network security devices, as well as a way to configure some of these resources. This is a master use case, which contains other device monitoring use cases and can configure common elements used by all of these related use cases.

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Monitor Resources			
Last 5 Minutes	Channel showing events received during the last five minutes. The channel includes a sliding window that always displays exactly the last five minutres of event data.	Active Channel	/ArcSight Foundation/ArcSight Express/
Live	Live Channel showing events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data. A filter prevents the channel from showing events that contributed to the firing of a rule, commonly referred to as correlated events.	Active Channel	/ArcSight Foundation/ArcSight Express/
Reconnaissance Activity	Live Channel showing reconnaissance events received during the last two hours. The channel includes a sliding window that always displays exactly the last two hours of event data.	Active Channel	/ArcSight Foundation/ArcSight Express/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Correlated Alerts	This active channel shows all the rules that fired in the last 2 hours. The active channel uses the "ArcSight Express" field set which shows the End Time, Name, Attacker Address, Attacker User Name, Attacker User ID, Target Address, Target User Name, Target User ID, Target Port, and Priority.	Active Channel	/ArcSight Foundation/ArcSight Express/
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 Foundation/ArcSight Express/ Cross-Device/
Security Activity Statistics	This dashboard displays an overview of common attackers, targets, protocols, and activity by time.	Dashboard	/ArcSight Foundation/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 Foundation/ArcSight Express/ Cross-Device/
Configuration Changes Overview	This dashboard shows an overview of the successful configuration changes for databases, firewalls, VPN, and network devices.	Dashboard	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Current Event Sources	This dashboard displays information about the status of your ArcSight System's connectors, as well as the top devices (vendor and product) contributing events.	Dashboard	/All Dashboards/ArcSight Administration/Connectors/ System Health/
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 Foundation/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 Foundation/ArcSight Express/ Cross-Device/Login Tracking/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
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 Foundation/ArcSight Express/ Cross-Device/Top Activity/
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 Foundation/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 Foundation/ArcSight Express/ Cross-Device/Login Tracking/
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. This report shows you the applications that are consuming the most bandwidth.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/Bandwidth Tracking/
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 Foundation/ArcSight Express/ Cross-Device/Top Activity/
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 Foundation/ArcSight Express/ Cross-Device/User Change Tracking/
By User Account - Accounts Created	This report generates a table of all user accounts created in the last day.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/User Change Tracking/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
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 Foundation/ArcSight Express/ Cross-Device/Login 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). This report can be used to find highest bandwidth hosts.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/Bandwidth 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. This report allows you to find all the configuration changes made by a specific user.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/User Change 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 Foundation/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 Foundation/ArcSight Express/ Cross-Device/Login 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. This report allows you to quickly find all the configuration changes of a certain type.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/User Change Tracking/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
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 Foundation/ArcSight Express/ Cross-Device/Login Tracking/
Security Intelligence Status Report	The Security Intelligence Status Report displays 4 charts and 6 tables. The first table gives an hourly breakdown of the event counts by agent severity. The three tables below the Event Count by Agent Severity chart show the top events, top attacks and top firing rules. The three charts below the tables show the top attackers, top targets and top target ports. The three tables at the bottom of the page show the number of cases added and notifications sent, along with a list of assets and the vulnerabilities used to compromise them.	Report	/ArcSight Foundation/ArcSight Express/
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). This report can be used to find high bandwidth usage hours during the day.	Report	/ArcSight Foundation/ArcSight Express/ Cross-Device/Bandwidth Tracking/
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 Foundation/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 Foundation/ArcSight Express/ Cross-Device/Top Activity/
Library - Correlation Resources			

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
User Session (Accounting User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Juniper's Steel-Belted Radius product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Accounting User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Juniper's Steel-Belted Radius product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
Windows Account Created and Deleted within 1 Hour	This rule looks for Microsoft Windows account deletion events (Security:630). The rule fires if the user account that is being deleted is in the "Windows Created Accounts" active list (by default: active list's TTL = 1 hour). On first event, the user account is removed from the "Windows Created Accounts" active list, and the category significance is set to "/Suspicious".	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/
High Number of Connections	This rule looks for Firewall accept events for MSSQL, Terminal Services, and TFTP connections (destination ports by default: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule fires when 10 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
High Number of Denied Inbound Connections	This rule looks for inbound Firewall deny events. The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
User Session (Administrative User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Cisco's Secure ACS product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
User VPN Session Started	This rule looks for VPN user session start events, defined as a VPN access start event with user ID information. It then updates the User VPN Sessions list. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/VPN/
User Session (Normal User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports ActivCard's AAA Server Accounting product and Cisco's VPN products.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Administrative User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Cisco's Secure ACS product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
High Number of Denied Connections for A Source Host	This rule looks for Firewall deny events. The rule fires when 10 events coming from the same source host occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
Successful Windows Logout	This rule looks for Microsoft Windows successful user logout events. On first event, the "Login Count" in the "Windows Login Count" active list is decremented, and the device and agent severity is set to "Low".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/
Windows Account Locked Out	This rule looks for Microsoft Windows user account locked out events (Security:644). On first event, the user account is added in the "Windows Locked Out Accounts" active list, and the device and agent severity are set to "Medium". If the user account is already in the active list, the "Locked Count" is incremented.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
User Session (Normal User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports ActivCard's AAA Server Accounting product and Cisco's VPN products.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
Successful Windows Login	This rule looks for Microsoft Windows successful user login events. On first event, the user account is added in the "Windows Login Count" active list, and the device and agent severity is set to "Low". If the user is already in the active list, the "Login Count" is incremented.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/
Windows Account Locked Out Multiple Times	This rule looks for Microsoft Windows user account locked out events (Security:644). The rule fires if the "Locked Count" for that user account in the "Windows Locked Out Accounts" active list is equal or greater than 5. On first event, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/
User VPN Session Stopped	This rule looks for VPN user session stop (or terminate) events, defined as a VPN access stop event with user ID information. It then updates the User VPN Sessions list. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/VPN/
Multiple Login Attempts to Locked Windows Account	This rule looks for Microsoft Windows login attempts events targeting locked out accounts (Security:531). The rule fires when 5 events coming from the same host and targeting the same account occur in 2 minutes. On first threshold, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/
Windows Account Created	This rule looks for Microsoft Windows account creation events (Security:624). On first event, the user account is added in the "Windows Created Accounts" active list, and the device and agent severity is set to "Low".	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/Base Rules/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Multiple Windows Logins by Same User	This rule looks for Microsoft Windows successful user login events. The rule fires if the login count for that user in the "Windows Login Count" active list is equal or greater than 5 (by default: active list's TTL = 1 hour). On first event, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/
Library Resources			
User-based Rule Exclusions	This active list contains target user information of specific users to be excluded from certain rule conditions where the rule tracks user activity.	Active List	/ArcSight Foundation/ArcSight Express/Tuning
Event-based Rule Exclusions	This active list stores event information that is used to exclude specific events from specific systems to other specific systems that have been determined to be not relevant to the rules that would otherwise fire on these events.	Active List	/ArcSight Foundation/ArcSight Express/Tuning
Events per Address Space	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Most Frequent Ports	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Last 10 Zones Scanned	This data monitor shows the time and the target zone of the last 10 reconnaissance events to give an overview of the most recent scanning activity against the network.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Application Protocol Event Counts	This data monitor tracks the Application Protocol events by Customer Resource. It updates every 30 seconds. It uses 12 samples of 5 minute intervals, for a 1 hour time range. It requires a minimum of 10 events to maintain a group, aggregated event counts will be used when available for this determination.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Trojaned Machines	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Recent Events	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Last 10 Scanners	This data monitor shows the attacker zone and address, along with the time, of the last 10 reconnaissance events to give an overview of the most recent scanning activity against the network.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Top 10 Users with Failed Logins	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Last 10 Hosts Scanned	This data monitor shows the target zone and address, along with the time, of the last 10 reconnaissance events to give an overview of the most recent scanning activity against specific hosts.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Last 10 Database Configuration Changes	This data monitor shows the last 10 successful database configuration changes.	Data Monitor	/ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/ArcSight Express/ Cross-Device/Configuration Changes Overview/
Top Transport Protocols	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Top Event Sources	This data monitor tracks the most common event generating products and displays a listing of the top 20.	Data Monitor	/All Data Monitors/ArcSight Administration/Connectors/System Health/Current Event Sources/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Top Connectors	This data monitor provides a list of the top 10 ArcSight Connectors reporting events, minute-by-minute over the last 60 minutes, showing the connector name and ID (Agent Name and Agent ID fields), the total number of events reported, and a breakdown of the reported events by priority.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Worm Infected Machines	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Top 10 Zones Scanned	This data monitor shows the target zone of the 10 most frequent reconnaissance events within the last hour to give an overview of the most recent scanning activity against the network.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Reconnaissance/Reconnaissance in Progress/
Top Successful Attacks	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Top Firewall Blocked Machines	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Event Counts by Hour	This hourly counts data monitor collects the count of events at each priority level for each hour for the last 24 hours.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Security Activity Statistics/
Last Failed Logins	Shows the last 15 failed logins.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Top Categories	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Operational Summaries/Executive View Details/Attacked or Compromised Systems/
Port Monitor	No description available.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Security Activity/
Current Connector Status	This system attribute data monitor displays information about the connectors that are registered with the system and reporting events.	Data Monitor	/All Data Monitors/ArcSight Administration/Connectors/System Health/Connector Status/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Standard	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/
Security	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/
Categories	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/
Standard-MgrRcpt	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/
Cases	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/
ArcSight Express	This field set is used by the "Correlated Alerts" active channel and shows the End Time, Name, Attacker Address, Attacker User Name, Attacker User ID, Target Address, Target User Name, Target User ID, Target Port, and Priority.	Field Set	/ArcSight Foundation/ArcSight Express/
Event Inspector	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/
ArcSight Admin	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/
Internal-ExternalAssets.txt	This document recommends categorizing zones and assets as Protected so that systems can be determined to be internal or external.	File	/All Files/Public/
Failed Logins with Target Information	No description available.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Reconnaissance Events by Target	This filter matches events where the target address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	/ArcSight Foundation/Intrusion Monitoring/Reconnaissance/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Reconnaissance Events by Target Zone	This filter matches events where the target zone is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	/ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
Network Configuration Changes	This filter selects successful configuration changes events that match the "Network Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Firewall Deny	No description available.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Firewall Configuration Changes	This filter selects successful configuration changes events that match the "Firewall Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Reconnaissance Events by Attacker	This filter matches events where the attacker address is provided and the event matches the Reconnaissance Events (Internal Targets) filter.	Filter	/ArcSight Foundation/Intrusion Monitoring/Reconnaissance/
VPN Configuration Changes	This filter selects successful configuration changes events that match the "VPN Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
Non ArcSight Internal Event - Target Port Not Null	No description available.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/Targets/By Port or Protocol/
Backdoor Traffic	No description available.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Worm Traffic	No description available.	Filter	/ArcSight Foundation/Intrusion Monitoring/Worm Outbreak/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Reconnaissance Events (Internal Targets)	This filter selects events that match the ".../Boundary Filters/Internal Target," ".../Event Types/Not Correlated and Not Closed and Not Hidden," and ".../Event Types/Non-ArcSight Internal Events" filters and one or more conditions where the event name starts with Reconnaissance, the category significance is /Recon or the category technique starts with /Scan. This is the foundation filter for the other Reconnaissance filters, Reconnaissance Events by Attacker, Reconnaissance Events by Target and Reconnaissance Events by Target Zone.	Filter	/ArcSight Foundation/ArcSight Express/ Cross-Device/Event Types/
Successful Configuration Changes	This filter selects events with the category behavior of /Modify/Configuration and category outcome of /Success.	Filter	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Successful Attacks	This filter passes events that have a significance of compromise or hostile and an outcome of success.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Database Configuration Changes	This filter selects successful configuration changes events that match the "Database Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/Database/
Non ArcSight Internal Event with TargetPort Set	This filter passes events that have a Category Significance entry and a Target Port.	Filter	/ArcSight Foundation/Intrusion Monitoring/Attack Monitoring/
Login Event Audit	This query looks for all the successful and failed login attempts. The query selects the source and destination addresses, hosthames, and zones, the user name, the device group, and the outcome.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Successful Logins by Source Address (Chart)	This query looks for authentication successes events from login attempts. The query selects the count of failed login attempts by source address.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Failed Logins by Destination Address (Chart)	This query looks for authentication failures events from login attempts. The query selects the count of failed login attempts by destination address.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Bandwidth Usage by Protocol	This query selects the count of TotalBytes ('Bytes In' + 'Bytes Out') by protocol. The query looks for events where the 'Bytes In', 'Bytes Out', and 'Target Port' fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Assets Compromised Table Query	This query on events selects the Target Asset Name, the Vulnerability External ID (the vulnerability name), and a sum of the number of events reported for that asset/vulnerability pair for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Failed Login by User (Chart)	This query selects the count of failed login attempts per user.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Top Bandwidth Hosts	This query selects the count of TotalBytes ('Bytes In' + 'Bytes Out') for each host, and sorts them so that the hosts with the highest totals are reported first. The query looks for events where the 'Bytes In' and 'Bytes Out' fields are not empty and filters events using the "Bandwidth to or from External Systems" filter.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Failed Login Attempts	This query selects all the authentication failures from login attempts.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Password Changes	No description available.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Successful Login by User	This query looks for users with successful login attempts. The query selects the user name, the source and destination addresses, hostnames, and zones.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Bandwidth Usage per Hour	This query selects the count of TotalBytes ('Bytes In' + 'Bytes Out') per hour. The query looks for events where the 'Bytes In' and 'Bytes Out' fields are not empty and filters events using the Bandwidth to or from External Systems filter.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Configuration Changes	This query looks for all the successful configuration changes made to devices. The query selects the name, the user, the device, and the time the change was made.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Top Events Table Query	This query on events selects the event Name and sums the Aggregated Event Count for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
SIS-Top Targets Chart Query	This query on events selects the Target Zone Name, the Target Address and sums the Aggregated Event Count for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
SIS-Notifications Sent Table Query	This query on notifications selects the Group Name, the Escalation Level, the Acknowledgement Status and a count of the notifications for these conditions for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Failed Login by User	This query looks for users with failed login attempts. The query selects the user name, the source and destination addresses, hostnames, and zones, and the device group.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Successful Logins by Destination Address (Chart)	This query looks for authentication successes events from login attempts. The query selects the count of failed login attempts by destination address.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-TopTarget Ports Chart Query	This query on events selects the Target Port and sums the Aggregated Event Count for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
SIS-Top Firing Rules Table Query	This query on events selects the event Name and sums the Aggregated Event Count where the type is Correlation for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Failed Logins by Source Address (Chart)	This query looks for authentication failures events from login attempts. The query selects the count of failed login attempts by source address.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
By User Account - Accounts Created	This query selects events meeting the conditions Category Behavior = /Authentication/Add and Category Outcome = /Success, selecting End Time, Target User Name, Attacker User Name, Name, Target Zone Name and Target Host Name for the By User Account - Accounts Created report.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Top Attacks Table Query	This query on events selects the event Name and sums the Aggregated Event Count that have a category significance of /Compromise or /Hostile for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Failed Login Attempts (Chart)	This query selects the count of authentication failures from login attempts by hour.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Top Attackers Chart Query	This query on events selects the Attacker Zone Name, the Attacker address and sums the Aggregated Event Count for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Top Hosts by Number of Connections	This query selects host information and the number of events where the category behavior is /Access/Start and the category outcome is not /Failure.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Top IDS and IPS Alerts	This query looks for IDS and IPS alert events, selecting the device event class ID, the event name, the device vendor, the device product and a count on the end time of the event.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Failed Logins by Source-Destination Pair	This query looks for authentication failures events from login attempts. The query selects the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Event Count by Agent Severity Chart Query	This query on events selects the date, the Agent Severity and the number of events for each agent severity level for that day/hour for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Successful Logins by Source-Destination Pair	This query looks for authentication successes events from login attempts. The query selects the source zone, source address, source host name, destination zone, destination address, destination host name, user name, user ID, count of failed logins, and device group.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
Successful Login by User (Chart)	This query selects the count of successful login attempts per user.	Query	/ArcSight Foundation/ArcSight Express/ Cross-Device/
SIS-Cases Added Table Query	This query on cases selects the Stage, the Consequence Severity and a count of the cases with that pairing for use in the Security Intelligence Status Report.	Query	/ArcSight Foundation/ArcSight Express/Security Intelligence Status Report/
Vulnerabilities	The Vulnerabilties use case contains several useful resources for monitoring Security Assessment and vulnerability activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
Operating System	The Operating System use case contains several useful resources for monitoring Operating System activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
Database	The Database use case contains several useful resources for monitoring database activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
VPN	The VPN use case contains several useful resources for monitoring VPN activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
Network	The Network use case contains several useful resources for monitoring Network device activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
IDS - IPS	The IDS - IPS use case contains several useful resources for monitoring Intrusion Detection/Prevention System activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/

Table 2-1 Resources that Support the ArcSight Express Use Case

Resource	Description	Type	URI
Firewall	The Firewall use case contains several useful resources for monitoring Firewall activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
Anti-Virus	The Anti-Virus use case contains several useful resources for monitoring anti-virus devices, virus and worm and other malware activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/
Case Tracking and Escalation	The Case Tracking and Escalation use case contains several useful resources for monitoring case workflow activity, from tracking the history of individual cases to being notified when a new case investigation has yet to be started within a policy time-frame.	Use Case	/ArcSight Foundation/ArcSight Express/
Identity Management	The Identity Management use case contains several useful resources for monitoring Identity Management activity, as well as a way to configure some of these resources.	Use Case	/ArcSight Foundation/ArcSight Express/

Anti-Virus

The Anti-Virus use case contains several useful resources for monitoring anti-virus devices, virus and worm and other malware activity, as well as a way to configure some of these resources.

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
Monitor Resources			
Anti-Virus Events	This active channel shows all the events coming from Anti-Virus Systems in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
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. This dashboard uses the Virus Activity by Zone and Virus Activity by Host data monitors.	Dashboard	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Anti-Virus/
Top Infected Systems	This report displays summaries of the systems reporting the most infections in the previous day.	Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Failed Anti-Virus Updates	This report displays a table with the Anti-Virus Vendor and Product name as well as the Host Name, Zone and IP Address of the host on which the update failed. The time (EndTime) at which the update failed is also displayed. This report runs against events that occurred yesterday.	Report	/ArcSight Foundation/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 Foundation/ArcSight Express/Anti-Virus/

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
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 Foundation/ArcSight Express/Anti-Virus/
Library Resources			
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 Foundation/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 Foundation/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 Foundation/ArcSight Express/Anti-Virus/Anti-Virus Overview/
Virus Activity by Host	This moving average data monitor shows the most active hosts with virus activity on the network.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Virus Activity Overview/
Virus Activity by Zone	This moving average data monitor shows the most active zones with virus activity on the network.	Data Monitor	/ArcSight Foundation/Intrusion Monitoring/Detail/Virus/Virus Activity Overview/
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 Foundation/ArcSight Express/Anti-Virus/Anti-Virus Overview/
Anti-Virus Events	This filter passes events with the category device group of /IDS/Host/Antivirus.	Filter	/ArcSight Foundation/ArcSight Express/Anti-Virus/

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
Virus Activity	This filter is looking for Virus Activity reported by either an IDS or a Anti Virus application. The filter classifies virus events in two ways. The first way is that the Category Object starts With /Vector/Virus or /Host/Infection/Virus. The second way is that the Category Behavior is /Found/Vulnerable, starts with /Modify/Content or /Modify/Attribute, and has a Category Device Group of /IDS/Host/Antirvirus and the Device Custom String1 is set to some value.	Filter	/ArcSight Foundation/ArcSight Express/Anti-Virus/
AV - Found Infected	This filter selects all events where the Category Device Group starts with /IDS/Host/Antivirus, the Category Outcome is /Failure and the Category Behavior is /Found/Vulnerable.	Filter	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Anti-Virus Errors	This filter passes events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success and the Category Significance starts with /Informational.	Filter	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Update Events	This filter passes events related to anti-virus product data file updates.	Filter	/ArcSight Foundation/ArcSight Express/Anti-Virus/
AV - Failed Updates	This filter selects all anti-virus update events (based on the Update Events filter), where the Category Outcome is /Failure.	Filter	/ArcSight Foundation/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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Infected Systems	This query selects data 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), and returns the host information and a count of the infections per host.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Top Infected Systems/
Failed Anti-Virus Updates	This query selects Device Vendor, Device Product Target Zone Name, Target Host Name, Target Address and Time (EndTime) from events that match the AV - Failed Updates filter.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Failed Anti-Virus Updates Chart	This query selects Target Zone Name and the sum of the Aggregated Event Count from events that match the anti-virus filter, AV - Failed Updates.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Virus Activity by Hour	This query selects data 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). It returns the time, priority, virus activity and a count of activity occurrances.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Virus Activity by Time/
Top Zones with Anti-Virus Errors	This query selects data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success and the Category Significance starts with /Informational. It returns zone and the number of times the error occurred.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Errors/

Table 2-2 Resources that Support the Anti-Virus Use Case

Resource	Description	Type	URI
Anti-Virus Errors	This query selects data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success and the Category Significance starts with /Informational. It returns the priority, vendor information, host information, error name and the number of times the error occurred.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Errors/
Update Summary Chart	This query selects Target Zone Name, Category Outcome and the sum of the Aggregated Event Count from events that match the anti-virus filter, Update Events.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Top Anti-Virus Errors	This query selects data from events where the Category Device Group is /IDS/Host/Antivirus, the Category Object starts with /Host/Application, the Category Outcome is not /Success and the Category Significance starts with /Informational. It returns error name and the number of times the error occurred.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Errors/
Top Infected Systems	This query selects data 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), and returns the host's zone and a count of the infections per zone.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/Top Infected Systems/
Update Summary	This query selects Target Zone Name, Target Host Name, Target Address, Device Vendor, Device Product, Category Outcome and the sum of the Aggregated Event Count from events that match the anti-virus filter, Update Events.	Query	/ArcSight Foundation/ArcSight Express/Anti-Virus/

Case Tracking and Escalation

The Case Tracking and Escalation use case contains several useful resources for monitoring case workflow activity, from tracking the history of individual cases to being notified when a new case investigation has yet to be started within a policy time-frame.

Table 2-3 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
Monitor Resources			
Case Events	Live Channel showing case audit events received in the past 8 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/
Case Times to Resolution	No description available.	Dashboard	/ArcSight Foundation/ArcSight Express/Case Management/
Case Stages	This dashboard displays information about the current state of open cases, focusing on the case stages for each case owner. A details table is also provided to show more detailed open case information for each owner.	Dashboard	/ArcSight Foundation/ArcSight Express/Case Management/
Case Status	This dashboard displays information about the current status of open cases, focusing on the cases impact and severity ratings. A table of recently closde cases is also provided.	Dashboard	/ArcSight Foundation/ArcSight Express/Case Management/
Open Cases by Stage	This query view displays a pie chart showing the number of open cases at each stage.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Queued Stage Cases by Owner	This query viewer displays the number of cases in the Queued stage for each case owner.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Recently Closed Cases	This query viewer displays the most recently closed cases. Note that once a case is closed, if it is further modified, there may be multiple entries depending on the modificaitons. The 'Time Closed' column will show the most recent modification of the closed case, and may not be the time when the case was initially closed.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Average Time to Case Resolution - by Day	This query viewer displays the average time taken to resolve cases closed for each day of the reporting period.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case History/
Open Cases by Consequence Severity	This query viewer displays a pie chart showing the number of open cases at each Consequence Severity rating.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/

Table 2-3 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
Final Stage Cases by Owner	This query viewer displays the number of cases in the Final stage for each case owner.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Follow-Up Stage Cases by Owner	This query viewer displays the number of cases in the Follow-Up stage for each case owner.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Initial Stage Cases by Owner	This query viewer displays the number of cases in the Initial stage for each case owner.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Average Time to Case Resolution - by User	This query viewer the average time taken to resolve cases that have been closed by each user during the reporting period.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case History/
Average Time to Case Resolution - by Severity	This query viewer displays the severity and average time to resolution of all cases closed during the reporting period.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case History/
Maximum Time to Case Resolution - by User	This query viewer displays 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.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case History/
Open Cases	This query viewer displays open case information in a table.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Open Cases by Operational Impact	This query viewer displays a pie chart showing the number of open cases at each operational impact rating.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Open Cases by Associated Impact	This query viewer displays a pie chart showing the number of open cases at each associated impact rating.	Query Viewer	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Average Time to Case Resolution - By User	This report displays a chart and a table showing the average time taken to resolve cases that have been closed by each user during the reporting period.	Report	/ArcSight Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Resolution Times/

Table 2-3 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
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 during the reporting period.	Report	/ArcSight Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Resolution Times/
Case Stages Overview	This report displays four charts and a table. The four charts show the number of open cases in each stage by owner. The table shows a list of all open cases.	Report	/ArcSight Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Stages/
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 Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Resolution Times/
Case Status Overview	This report displays four charts and a table. The four charts show the number of open cases by stage, consequence severity, operational impact and associated impact. The table shows a list of recently closed cases.	Report	/ArcSight Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Status/
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 Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/Case Resolution Times/
Library Resources			
Case Escalation	This active list tracks case data on newly created cases that are still in the Queued stage. The default TTL is 1 day. If the case is not removed from the list (there is a rule that does that when the case stage is changed), a rule will detect this, put it back on the list and send a notification.	Active List	/ArcSight Foundation/ArcSight Express/Case Management/Case Tracking and Escalation/
Case	No description available.	Field Set	/ArcSight Foundation/Workflow/Inspect - Edit/
Cases	No description available.	Field Set	/ArcSight Foundation/ArcSight Express/Active Channel Only/

Table 2-3 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
Case Events	The case events filter selects events that are related to creating and updating cases.	Filter	/ArcSight Foundation/Workflow/
Case Monitoring Entry Expiration	This filter looks for audit events for the case escalation active list where a case entry has exipired (i.e., met the TTL condition).	Filter	/ArcSight Foundation/Workflow/Case Tracking and Escalation/
Average Time to Case Resolution - By User	This query on a case history trend selects the case owner, and the average time to resolve cases closed during the previous seven days.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case History/Case Resolution Times/
Recently Closed Cases	This query on a case tracking session list selects the most recently closed cases for display in a query viewer. Note that once a case is closed, if it is further modified, there may be multiple entries depending on the modificaitons. The 'Time Closed' column will show the most recent modification of the closed case, and may not be the time when the case was initially closed.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Final Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Final.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Open Cases Details	This query selects case information for cases where the stage is not closed.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Follow-Up Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Follow-Up.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Cases Open by Stage (Chart)	This query searches the cases for open cases, and counts the number of them at each stage. Note that an open case's stage is not Closed.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Open Cases by Associated Impact (Chart)	This query selects the number of open cases in the various associated impact ratings.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Queued Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Queued.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/

Table 2-3 Resources that Support the Case Tracking and Escalation Use Case

Resource	Description	Type	URI
Initial Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Initial.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Stages/
Open Cases by Consequence Severity (Chart)	This query selects the number of open cases in the various consequence severity ratings.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Average Time to Case Resolution - By Severity	This query on a case history trend selects the Consequence Severity, and the average time to resolve cases closed during the previous seven days.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case History/Case Resolution Times/
Average Time to Case Resolution - By Day	This query on a case history trend selects the Day of the Week, and the average time to resolve cases closed during the previous seven days.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case History/Case Resolution Times/
Maximum Time to Case Resolution - By User	This query on a case history trend selects case statistics for cases closed during the previous seven days.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case History/Case Resolution Times/
Trend on Case Audit Events	This query collects Time to Resolution (TTR) information from case audit events and stores them in a trend for case history reporting.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case History/
Open Cases by Operational Impact (Chart)	This query selects the number of open cases in the various operational impact ratings.	Query	/ArcSight Foundation/ArcSight Express/Case Management/Case Status/
Case Tracking	This session list contains case history information, monitoring the changes of the attributes in a case as it flows through the investigation and analysis. The attributes that are tracked are Case Name, Owner, Stage, Time To Resolution (TTR) in minutes, Ticket Type, Operational Impact, Security Classification, Consequence Severity, Associated Impact and Case URI.	Session List	/ArcSight Foundation/ArcSight Express/Case Management/

Database

The Database use case contains several useful resources for monitoring database activity, as well as a way to configure some of these resources.

Table 2-4 Resources that Support the Database Use Case

Resource	Description	Type	URI
Monitor Resources			
Database Events	This active channel shows all the events coming from Databases in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
Database Errors	This dashboard shows the most recent and top errors affecting database applications on the network.	Dashboard	/ArcSight Foundation/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 Foundation/ArcSight Express/Database/
Library Resources			
Last 10 Database Errors	This last n events data monitor displays the most recent database error events.	Data Monitor	/ArcSight Foundation/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 Foundation/ArcSight Express/Database/Database Errors/
Database Errors	This filter passes events with the category device group of /Application, category object of /Host/Application/Database and a category significance of /Informational/Warning or /Informational/Error.	Filter	/ArcSight Foundation/ArcSight Express/Database/
Database Configuration Changes	This filter selects successful configuration changes events that match the "Database Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/Database/
Database Events	This filter passes events with the category object of /Host/Application/Database.	Filter	/ArcSight Foundation/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 Foundation/ArcSight Express/Database/

Table 2-4 Resources that Support the Database Use Case

Resource	Description	Type	URI
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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Database/
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Database Errors and Warnings (Chart)	This query selects the count of database errors and warnings by event name.	Query	/ArcSight Foundation/ArcSight Express/Database/
Database Errors and Warnings	This query selects all the database errors and warnings events. The query returns the time, event name, result, user name, and category significance.	Query	/ArcSight Foundation/ArcSight Express/Database/

Firewall

The Firewall use case contains several useful resources for monitoring Firewall activity, as well as a way to configure some of these resources.

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
Monitor Resources			
Firewall Events	This active channel shows all the events coming from Firewalls in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/

Table 2-5 Resources that Support 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 Foundation/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 Foundation/ArcSight Express/Firewall/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/ArcSight Express/Firewall/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/ArcSight Express/Firewall/
Library - Correlation Resources			
High Number of Denied Connections for A Source Host	This rule looks for Firewall deny events. The rule fires when 10 events coming from the same source host occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
High Number of Connections	This rule looks for Firewall accept events for MSSQL, Terminal Services, and TFTP connections (destination ports by default: MSSQL=1433, Terminal Services=2289, TFTP=69). The rule fires when 10 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
High Number of Denied Inbound Connections	This rule looks for inbound Firewall deny events. The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Traffic Monitoring/
SYN Flood Detected by IDS or Firewall	This rule looks for SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/
Library Resources			
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Top 10 Hosts With Denied Outbound Connections	This data monitor shows the top 10 hosts with denied outbound connections.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Connection Overview/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
Top 10 Hosts With Denied Inbound Connections	This data monitor shows the top 10 hosts with denied inbound connections.	Data Monitor	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/Firewall Connection Overview/
Top 10 Users With Failed Logins	This data monitor shows the top 10 users with failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last 10 failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Top 10 Denied Ports (Inbound)	This data monitor shows the top 10 ports with denied inbound connections.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Connection Overview/
Failed Firewall Login Events	This filter selects firewall events with the category behavior of /Authentication/Verify and category outcome of /Failure.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Outbound Connections	This filter selects firewall events with the category behavior of /Access and category outcome of /Failure. The filter specifically looks for outbound events.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Firewall Configuration Changes	This filter selects successful configuration changes events that match the "Firewall Events" filter.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Firewall Login Events	This filter selects firewall events with the category behavior of /Authentication/Verify.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Inbound Connections	This filter selects firewall events with the category behavior of /Access and category outcome of /Failure. The filter specifically looks for inbound events.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/
Successful Firewall Login Events	This filter selects firewall events with the category behavior of /Authentication/Verify and category outcome of /Success.	Filter	/ArcSight Foundation/ArcSight Express/Firewall/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
Firewall Events	This filter passes events with the category device group of /Firewall.	Filter	/ArcSight Foundation/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 Foundation/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 Foundation/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 Foundation/ArcSight Express/Firewall/
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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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. This report shows you the applications that are consuming the most bandwidth.	Focused Report	/ArcSight Foundation/ArcSight Express/Firewall/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
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 Foundation/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). This report can be used to find high bandwidth usage hours during the day.	Focused Report	/ArcSight Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Database/
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 Foundation/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). This report can be used to find highest bandwidth hosts.	Focused Report	/ArcSight Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Firewall/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Firewall/
Denied Outbound Connections per Hour	This query selects the count of denied outbound connections per hour for each source zone.	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Inbound Connections per Hour	This query selects the count of denied inbound connections per hour for each source zone.	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Outbound Connections by Address	This query selects the count of denied outbound connections by local address (source zone, address, and hostname).	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Inbound Connections by Address	This query selects the count of denied inbound connections by foreign address (source zone, address, and hostname).	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Outbound Connections by Port	This query selects the count of denied outbound connections by destination port.	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Inbound Connections by Port	This query selects the count of denied inbound connections by destination port.	Query	/ArcSight Foundation/ArcSight Express/Firewall/
Denied Outbound Connections per Hour (Chart)	This query selects the count of denied outbound connections per hour.	Query	/ArcSight Foundation/ArcSight Express/Firewall/

Table 2-5 Resources that Support the Firewall Use Case

Resource	Description	Type	URI
Denied Inbound Connections per Hour (Chart)	This query selects the count of denied inbound connections per hour.	Query	/ArcSight Foundation/ArcSight Express/Firewall/

Identity Management

The Identity Management use case contains several useful resources for monitoring Identity Management activity, as well as a way to configure some of these resources.

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
Monitor Resources			
Identity Management Events	This active channel shows all the events coming from Identity Mangement Systems in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
Identity Management Overview	This dashboard displays information reported by Identity Management devices. Shown are the top users by number of connections and authentication failures by source and destination.	Dashboard	/ArcSight Foundation/ArcSight Express/Identity Managment/
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.	Report	/ArcSight Foundation/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. This report covers user VPN duration information for the previous day.	Report	/ArcSight Foundation/ArcSight Express/Identity Management/
Library - Correlation Resources			

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
User Session (Administrative User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Cisco's Secure ACS product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Accounting User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Juniper's Steel-Belted Radius product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Normal User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports ActivCard's AAA Server Accounting product and Cisco's VPN products.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Accounting User) Stopped	This rule looks for user session stop events reported by identity management devices, defined as a identity managment access stop event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Juniper's Steel-Belted Radius product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
User Session (Administrative User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports Cisco's Secure ACS product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
User Session (Normal User) Started	This rule looks for user session start events reported by identity management devices, defined as a identity managment access start event with user ID and session information. It then updates the Identity Management's User Sessions list. This rule supports ActivCard's AAA Server Accounting product and Cisco's VPN products.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Identity Management/
Library Resources			
Authentication Failures by Destination	This moving average data monitor displays the destination information of failed authentication attempts within five minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	/ArcSight Foundation/ArcSight Express/Identity Managment/Identity Management Overview/
Authentication Failures by Source	This moving average data monitor displays the source information of failed authentication attempts within five minute intervals over the last hour as reported by Identity Management devices.	Data Monitor	/ArcSight Foundation/ArcSight Express/Identity Managment/Identity Management Overview/
Top Users by Connection Count	This top value counts (bucketized) data monitor shows the top users by the number of connections in five minute intervals for the last hour, as reported by Identity Management devices.	Data Monitor	/ArcSight Foundation/ArcSight Express/Identity Managment/Identity Management Overview/
Identity Management Connection Start Events	This filter passes events where an Identity Management system has seen an access start event with valid user information.	Filter	/ArcSight Foundation/ArcSight Express/Identity Management/
Failed Identity Management Login Attempts	This filter passes events where an authentication attempt failed.	Filter	/ArcSight Foundation/ArcSight Express/Identity Management/
Identity Management Events	This filter passes events where the Category Device Group starts with /Identity Management.	Filter	/ArcSight Foundation/ArcSight Express/Identity Management/

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Firewall/
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Database/
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 Foundation/ArcSight Express/Identity Management/

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/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 Foundation/ArcSight Express/Firewall/
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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
Top Connection Durations	This query selects the user ID and average duration from the User Identity Management Sessions list and sorts them by the top duration.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Durations by User/
Closed Connection Durations	This query selects the user ID and the minimum, average, maximum and total durations, in minutes, for all user IDs with closes or terminated sessions in the User Sessions list.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Durations by User/

Table 2-6 Resources that Support the Identity Management Use Case

Resource	Description	Type	URI
Top Users by Connection Count	This query selects events where Category Behavior is /Access/Start, Category Behavior is /Authentication/Verify or Category Behavior or /Authorization/Verify, with user information available, returning the number of connections per user.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Counts by User/
Users with Open Connections	This query selects the user ID and the Identity Management device for each user in the User Sessions list where the user's entry has not been terminated (logged out or timed out) or expired (by default).	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Durations by User/
Users by Connection Count	This query selects events where Category Behavior is /Access/Start, Category Behavior is /Authentication/Verify or Category Behavior or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Counts by User/

IDS-IPS

The IDS - IPS use case contains several useful resources for monitoring Intrusion Detection/Prevention System activity, as well as a way to configure some of these resources.

Table 2-7 Resources that Support the IDS - IPS Use Case

Resource	Description	Type	URI
Monitor Resources			
IDS - IPS Events	This active channel shows all the events coming from Intrusion Detection Systems (IDS) in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
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 Foundation/ArcSight Express/IDS - IPS/
Worm Outbreak Overview	This dashboard provides a view of worm activity across the network.	Dashboard	/ArcSight Foundation/ArcSight Express/IDS - IPS/

Table 2-7 Resources that Support the IDS - IPS Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/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). The parameters are set so that the user can change the start and end times of the event query. The row limit is also modifiable, so that more or fewer systems are shown. Also, the Filter By parameter is available so that the user can create an additional filter to limit the report to specific systems (i.e., filter by zone, asset criticality, etc.). Changing the Filter By parameter will cause the query to select events that match both the selected filter and the Worm Traffic filter (Worm Traffic AND <selected filter>).	Report	/ArcSight Foundation/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 Foundation/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 Foundation/ArcSight Express/IDS - IPS/

Table 2-7 Resources that Support the IDS - IPS Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/ArcSight Express/IDS - IPS/
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 Foundation/ArcSight Express/IDS - IPS/
Library - Correlation Resources			
High Number of IDS Alerts for DoS	This rule looks for Denial of Service (DoS) alerts from Intrusion Detection Systems (IDS). The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/
SYN Flood Detected by IDS or Firewall	This rule looks for SYN flood alerts from Intrusion Detection Systems (IDS) or firewalls. The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/DoS/
High Number of IDS Alerts for Backdoor	This rule looks for Backdoor alerts from Intrusion Detection Systems (IDS). The rule fires when 20 events from the same device occur in 2 minutes.	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/Malware Activity/
Library Resources			
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 Foundation/ArcSight Express/IDS - IPS/Worm Outbreak Overview/
Top 10 Alert Types	This data monitor shows the top 10 IDS alert types.	Data Monitor	/ArcSight Foundation/ArcSight Express/IDS - IPS/IDS - IPS Overview/

Table 2-7 Resources that Support 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 Foundation/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 Foundation/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 Foundation/ArcSight Express/IDS - IPS/Worm Outbreak Overview/
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 Foundation/ArcSight Express/IDS - IPS/Worm Outbreak Overview/
Top 10 Alerts	This data monitor shows the top 10 IDS alerts.	Data Monitor	/ArcSight Foundation/ArcSight Express/IDS - IPS/IDS - IPS Overview/
Worm Outbreak	This filter only passes events with a name of Worm Outbreak Detected and the type Correlation.	Filter	/ArcSight Foundation/ArcSight Express/IDS - IPS/Worm Outbreak/
Target Port Activity By Attacker	No description available.	Filter	/ArcSight Foundation/ArcSight Express/IDS - IPS/Worm Outbreak/
IDS -IPS Events	This filter passes Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) events.	Filter	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Worm Activity	No description available.	Filter	/ArcSight Foundation/ArcSight Express/IDS - IPS/Worm Outbreak/
Top 10 Targets	This report shows the top 10 targets in a chart.	Focused Report	/ArcSight Foundation/ArcSight Express/IDS - IPS/
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 Foundation/ArcSight Express/IDS - IPS/

Table 2-7 Resources that Support the IDS - IPS Use Case

Resource	Description	Type	URI
Top 10 Attackers	This report shows the top 10 attackers in a chart.	Focused Report	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Top Alert Sources	This query selects the count of IDS and IPS alerts by source address, zone, device vendor, and device product.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts by Port	This query selects the count of IDS and IPS alerts by destination port.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts by Severity (Chart)	This query selects the count of IDS and IPS alerts by severity (agent severity).	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts by Type	This query selects the count of IDS and IPS alerts by type (category technique).	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts by Severity	This query selects the count of IDS and IPS alerts by severity (agent severity), device vendor, and device product.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Top Alert Destinations	This query selects the count of IDS and IPS alerts by destination address, zone, device vendor, and device product.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts by Device	This query selects the count of IDS and IPS alerts by device vendor, product, zone, address, and hostname.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Worm Infected Systems	This query selects the Attacker Zone Name, Attacker Host Name and Attacker Address from events matching the Worm Traffic filter.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/
Alert Counts per Hour	This query selects the count of IDS and IPS alerts per hour.	Query	/ArcSight Foundation/ArcSight Express/IDS - IPS/

Network

The Network use case contains several useful resources for monitoring Network device activity, as well as a way to configure some of these resources.

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Monitor Resources			

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Network Events	This active channel shows all the events coming from Networking Systems in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
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 Foundation/ArcSight Express/Network/
Network Status Overview	This dashboard displays data monitors related to network device errors, network interfaces and critical network events.	Dashboard	/ArcSight Foundation/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. Use this report to help determine whether SNMP accounts are targets of brute force attacks, and which devices are exhibiting the most SNMP authentication falure activity.	Report	/ArcSight Foundation/ArcSight Express/Network/
Device Events	This report shows information regarding events on network devices.	Report	/ArcSight Foundation/ArcSight Express/Network/
Device Interface Down Notifications	This report shows a table displaying the network devices that report a down link.	Report	/ArcSight Foundation/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 Foundation/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 Foundation/ArcSight Express/Network/

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Device Interface Status Messages	This report shows a table displaying the network devices reporting link status changes.	Report	/ArcSight Foundation/ArcSight Express/Network/
Library Resources			
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 Foundation/ArcSight Express/Network/Network Status Overview/
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 Foundation/ArcSight Express/Network/Network Status 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 Foundation/ArcSight Express/Network/Network Status 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 Foundation/ArcSight Express/Network/Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful firewall logins.	Data Monitor	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/Firewall Login 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 Foundation/ArcSight Express/Network/Network Status Overview/
Top 10 Users With Failed Logins	This data monitor shows the top 10 users with failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last 10 failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Critical Network Events	This filter selects critical events related to network devices.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Network Events	This filter passes events with the category object starts with /Network or the category device group starts with /Network Equipment.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Network Login Events	This filter selects events with the category behavior of /Authentication/Verify and category device group starting with /Network.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Successful Network Login Events	This filter selects events with the category behavior of /Authentication/Verify, category outcome of /Success, and category object starting with /Network.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Network Device Interface Status Events	This filter selects events related to device interfaces, ports or links. VPN events are excluded.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Network Error Events	This filter selects events related to network device errors.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Failed Network Login Events	This filter selects events with the category behavior of /Authentication/Verify, category outcome of /Failure, and category object starting with /Network.	Filter	/ArcSight Foundation/ArcSight Express/Network/
Network Device Interface Down Messages	This filter selects device interface events stating that an interface, port or link is down. VPN events are excluded.	Filter	/ArcSight Foundation/ArcSight Express/Network/
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 Foundation/ArcSight Express/Firewall/

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/ArcSight Express/Firewall/

Table 2-8 Resources that Support the Network Use Case

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. This report shows you the applications that are consuming the most bandwidth.	Focused Report	/ArcSight Foundation/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). This report can be used to find highest bandwidth hosts.	Focused Report	/ArcSight Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Database/
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). This report can be used to find high bandwidth usage hours during the day.	Focused Report	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Firewall/

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Device Events	This query selects base events where the device group is /Network Equipment or the device group is /Operating System and the object starts with /Network.	Query	/ArcSight Foundation/ArcSight Express/Network/
SNMP Authentication Failures by Device	This query looks for events where authentication or authorization failures using SNMP. It returns the device information sorted by count, from highest to lowest.	Query	/ArcSight Foundation/ArcSight Express/Network/Device SNMP Authentication Failures/
Device SNMP Authentication Failures by User	This query looks for events where authentication or authorization failures using SNMP. It returns user information sorted by count, from highest to lowest.	Query	/ArcSight Foundation/ArcSight Express/Network/Device SNMP Authentication Failures/
Device Critical Events	This query selects critical base events where the device group is /Network Equipment or the device group is /Operating System and the object starts with /Network.	Query	/ArcSight Foundation/ArcSight Express/Network/
Top Device System Authentication Events	This query selects base authentication events where the device group is /Network Equipment or the device group is /Operating System and the object starts with /Network.	Query	/ArcSight Foundation/ArcSight Express/Network/
Device SNMP Authentication Failures	This query looks for events where authentication or authorization failures using SNMP.	Query	/ArcSight Foundation/ArcSight Express/Network/Device SNMP Authentication Failures/
Device Interface Down Notifications	This query selects device information from network device events regaring network interfaces that are not VPN interfaces where a link has been reported to be down and the inbound or outbound interface is defined.	Query	/ArcSight Foundation/ArcSight Express/Network/
Device Errors	This query selects base error events where the device group is /Network Equipment or the device group is /Operating System and the object starts with /Network.	Query	/ArcSight Foundation/ArcSight Express/Network/

Table 2-8 Resources that Support the Network Use Case

Resource	Description	Type	URI
Device Interface Status Messages	This query selects device information from network device events regaring network interfaces that are not VPN interfaces where a link has been reported to be up or down and the inbound or outbound interface is defined.	Query	/ArcSight Foundation/ArcSight Express/Network/

Operating System

The Operating System use case contains several useful resources for monitoring Operating System activity, as well as a way to configure some of these resources.

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
Monitor Resources			
Operating System Events	This active channel shows all the events coming from Operating Systems in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
Operating System Login Overview	This dashboard shows an overview of operating system 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 Foundation/ArcSight Express/Operating System/
Login Errors by User	This report shows a summary of the operating system login errors by username in a chart and a table. The chart shows the top 10 users with failed logins, and the table shows the details of the failed logins for each username (time, event name, source, destination).	Report	/ArcSight Foundation/ArcSight Express/Operating System/
User Administration	This report shows a summary of user and user group creation, modification, and deletion in a chart and a table. The chart shows the count of users (or user groups) that have been recently created or deleted, and the table shows a detailed list of all these users and user groups.	Report	/ArcSight Foundation/ArcSight Express/Operating System/
Library - Correlation Resources			

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
Successful Windows Logout	This rule looks for Microsoft Windows successful user logout events. On first event, the "Login Count" in the "Windows Login Count" active list is decremented, and the device and agent severity is set to "Low".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/
Windows Account Locked Out	This rule looks for Microsoft Windows user account locked out events (Security:644). On first event, the user account is added in the "Windows Locked Out Accounts" active list, and the device and agent severity are set to "Medium". If the user account is already in the active list, the "Locked Count" is incremented.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/
Windows Account Created and Deleted within 1 Hour	This rule looks for Microsoft Windows account deletion events (Security:630). The rule fires if the user account that is being deleted is in the "Windows Created Accounts" active list (by default: active list's TTL = 1 hour). On first event, the user account is removed from the "Windows Created Accounts" active list, and the category significance is set to "/Suspicious".	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/
Successful Windows Login	This rule looks for Microsoft Windows successful user login events. On first event, the user account is added in the "Windows Login Count" active list, and the device and agent severity is set to "Low". If the user is already in the active list, the "Login Count" is incremented.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/Base Rules/
Windows Account Locked Out Multiple Times	This rule looks for Microsoft Windows user account locked out events (Security:644). The rule fires if the "Locked Count" for that user account in the "Windows Locked Out Accounts" active list is equal or greater than 5. On first event, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
Multiple Login Attempts to Locked Windows Account	This rule looks for Microsoft Windows login attempts events targeting locked out accounts (Security:531). The rule fires when 5 events coming from the same host and targeting the same account occur in 2 minutes. On first threshold, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/
Windows Account Created	This rule looks for Microsoft Windows account creation events (Security:624). On first event, the user account is added in the "Windows Created Accounts" active list, and the device and agent severity is set to "Low".	Rule	/ArcSight Foundation/ArcSight Express/Attack Monitoring/Suspicious Activity/Base Rules/
Multiple Windows Logins by Same User	This rule looks for Microsoft Windows successful user login events. The rule fires if the login count for that user in the "Windows Login Count" active list is equal or greater than 5 (by default: active list's TTL = 1 hour). On first event, the category significance is set to "/Informational/Warning".	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/Brute Force/
Library Resources			
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Failed Login Events	This data monitor shows the last 10 failed firewall logins.	Data Monitor	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/Firewall Login Overview/
Last 10 Successful Login Events	This data monitor shows the last 10 successful firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall 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 Foundation/ArcSight Express/Network/Login Overview/

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
Successful Windows Logout	This filter looks for successful Windows logout events (Device Event Class ID = Security:538). The filter specifically looks for the following types of logouts: console (2), lock (7), and remote (10).	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
Successful Windows Login	This filter looks for successful Windows login events (Device Event Class ID = Security:528). The filter specifically looks for the following types of logins: console (2), lock (7), and remote (10).	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
Operating System Events	This filter passes events with the category device group of /Operating System.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
LockedCount is NULL	This filter is designed for conditional expression variables. It passes events where the "LockedCount" is NULL. "LockedCount" is a variable used in the "Windows Account Locked Out" rule and will retrieve the number of times a Windows account has been locked out from the "Windows Locked Out Accounts" active list.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
Operating System Login Events	This filter selects operating system events with the category behavior of /Authentication/Verify.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
Failed Operating System Login Events	This filter selects operating system events with the category behavior of /Authentication/Verify and category outcome of /Failure.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
LoginCount is NULL or 0	This filter is designed for conditional expression variables. It passes events where the "LoginCount" is NULL or equal to 0. "LoginCount" is a variable used in the "Successful Windows Login" and "Successful Windows Logout" rules and will retrieve the number of successful Windows logins from the "Windows Login Count" active list.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/
Successful Operating System Login Events	This filter selects operating system events with the category behavior of /Authentication/Verify and category outcome of /Success.	Filter	/ArcSight Foundation/ArcSight Express/Operating System/

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Database/
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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Firewall/
Failed Logins by User	This report 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 Foundation/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 Foundation/ArcSight Express/Firewall/

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
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 Foundation/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 Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Identity Management/
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 Foundation/ArcSight Express/Firewall/
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 Foundation/ArcSight Express/Database/
User Administration (Chart)	This query selects the count of user (and user group) creations, modifications, and deletions.	Query	/ArcSight Foundation/ArcSight Express/Operating System/
Login Errors by User	This query looks for operating system login errors. The query selects the user name, the event name, the source and destination addresses, hostnames, and zones.	Query	/ArcSight Foundation/ArcSight Express/Operating System/

Table 2-9 Resources that Support the Operating System Use Case

Resource	Description	Type	URI
User Administration	This query looks for user (and user group) creation, modification, and deletion of events.	Query	/ArcSight Foundation/ArcSight Express/Operating System/
Login Errors by User (Chart)	This query selects the count of operating system login errors by username.	Query	/ArcSight Foundation/ArcSight Express/Operating System/

VPN

The VPN use case contains several useful resources for monitoring VPN activity, as well as a way to configure some of these resources.

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Monitor Resources			
VPN Events	This active channel shows all VPN activity in the last 2 hours.	Active Channel	/ArcSight Foundation/ArcSight Express/Device Class Event Channels/
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 Foundation/ArcSight Express/VPN/
VPN Connection Statistics	This dashboard displays data monitors related to VPN Servers, including connection status counts and authentication errors.	Dashboard	/ArcSight Foundation/ArcSight Express/VPN/
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 Foundation/ArcSight Express/VPN/

Table 2-10 Resources that Support the VPN 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.	Report	/ArcSight Foundation/ArcSight Express/Identity Management/
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 Foundation/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 Foundation/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 Foundation/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 Foundation/ArcSight Express/VPN/
Library - Correlation Resources			
User VPN Session Stopped	This rule looks for VPN user session stop (or terminate) events, defined as a VPN access stop event with user ID information. It then updates the User VPN Sessions list. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/VPN/
User VPN Session Started	This rule looks for VPN user session start events, defined as a VPN access start event with user ID information. It then updates the User VPN Sessions list. This rule supports Cisco VPN products, Nokia's Security Platform product and Nortel's VPN product.	Rule	/ArcSight Foundation/ArcSight Express/Session Monitoring/VPN/
Library Resources			

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Last 10 Failed Login Events	This data monitor shows the last 10 failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall 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 Foundation/ArcSight Express/Network/Login Overview/
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 Foundation/ArcSight Express/VPN/VPN Connection Statistics/
Last 10 Successful Login Events	This data monitor shows the last 10 successful firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
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 Foundation/ArcSight Express/VPN/VPN Connection Statistics/
Top 10 Users With Failed Logins	This data monitor shows the top 10 users with failed firewall logins.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
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 Foundation/ArcSight Express/VPN/VPN Connection Statistics/
Login Results	This data monitor shows the number of firewall logins (attempt, success, failure) in a pie chart.	Data Monitor	/ArcSight Foundation/ArcSight Express/Firewall/Firewall Login Overview/
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 Foundation/ArcSight Express/VPN/VPN Connection Statistics/
VPN Events	This filter passes events with the category device group of /VPN.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
VPN Login Events	This filter selects VPN events with the category behavior of /Authentication/Verify.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
Failed VPN Connection Events	This filter selects unsuccessful VPN events where the behavior is /Access/Start.	Filter	/ArcSight Foundation/ArcSight Express/VPN/

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Successful VPN Connection Events	This filter selects successful VPN events where the behavior is /Access/Start.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
Successful VPN Login Events	This filter selects VPN events with the category behavior of /Authentication/Verify and category outcome of /Success.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
Failed VPN Login Events	This filter selects VPN events with the category behavior of /Authentication/Verify and category outcome of /Failure.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
VPN Authentication Errors	This filter selects VPN authentication error events, where an authentication error event is defined as having the category behavior of /Authentication/Verify and the category significance of /Informational/Error.	Filter	/ArcSight Foundation/ArcSight Express/VPN/
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 Foundation/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 Foundation/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). This report can be used to find high bandwidth usage hours during the day.	Focused Report	/ArcSight Foundation/ArcSight Express/Firewall/

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
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 Foundation/ArcSight Express/Firewall/
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. This report shows you the applications that are consuming the most bandwidth.	Focused Report	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/
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 Foundation/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 Foundation/ArcSight Express/Database/
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 Foundation/ArcSight Express/Firewall/

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
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. This report allows you to find all the configuration changes made by a specific user.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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). This report can be used to find highest bandwidth hosts.	Focused Report	/ArcSight Foundation/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 Foundation/ArcSight Express/Firewall/
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. This report allows you to quickly find all the configuration changes of a certain type.	Focused Report	/ArcSight Foundation/ArcSight Express/Anti-Virus/
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 Foundation/ArcSight Express/Firewall/
Connections Accepted by Address	Selects the device zone, address, host name and a count of VPN devices with successful connections.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connections Accepted by Address/

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Top Connections Denied by Address	Selects the device zone, address and a count to show the top VPN devices with denied connections.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connections Denied by Address/
Authentication Errors	This query selects VPN authentication events where there has been an error. It returns the user information, the host information, the error, the time (within an hour) and the number of times the error occurred in the hour.	Query	/ArcSight Foundation/ArcSight Express/VPN/
Closed VPN Connection Durations	This query selects the user ID and the minimum, average, maximum and total durations, in minutes, for all user IDs with closes or terminated VPN sessions in the User VPN Sessions list.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connection Durations by User/
Users by Connection Count	This query selects events where Category Behavior is /Access/Start, Category Behavior is /Authentication/Verify or Category Behavior or /Authorization/Verify, with user information available, returning user and host information and the number of VPN connections.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Counts by User/
Top Connections Accepted by Address	Selects the device zone, address and a count to show the top VPN devices with successful connections.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connections Accepted by Address/
Top Users by Connection Count	This query selects events where Category Behavior is /Access/Start, Category Behavior is /Authentication/Verify or Category Behavior or /Authorization/Verify, with user information available, returning the number of connections per user.	Query	/ArcSight Foundation/ArcSight Express/Identity Management/Connection Counts by User/
Connections Denied by Address	Selects the device zone, address, host name and a count of VPN devices with denied connections.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connections Denied by Address/
Top VPN Connection Durations	This query selects the user ID and average duration from the User VPN Sessions list and sorts them by the top duration.	Query	/ArcSight Foundation/ArcSight Express/VPN/Connection Durations by User/
Connections Denied by Hour	Selects the device zone, address, host name and a count of VPN devices with denied connections.	Query	/ArcSight Foundation/ArcSight Express/VPN/

Table 2-10 Resources that Support the VPN Use Case

Resource	Description	Type	URI
Users with Open VPN Connections	This query selects the user ID and the VPN device for each user in the User VPN Sessions list where the user's entry has not been terminated (logged out or timed out) or expired (by default).	Query	/ArcSight Foundation/ArcSight Express/VPN/Connection Durations by User/

Vulnerabilities

The Vulnerabilties use case contains several useful resources for monitoring Security Assessment and vulnerability activity, as well as a way to configure some of these resources.

Table 2-11 Resources that Support the Vulnerabilities Use Case

Resource	Description	Type	URI
Monitor Resources			
Exposed Vulnerabilities by Asset	This report shows a table of exposed vulnerabilities by asset.	Report	/ArcSight Foundation/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 Foundation/ArcSight Express/Vulnerabilities/
Library Resources			
Exposed Vulnerability Count by Critical Asset	This report shows a table of exposed vulnerabilities on assets categorized as high criticality.	Focused Report	/ArcSight Foundation/ArcSight Express/Vulnerabilities/
Exposed Vulnerability Count by Asset	No description available.	Query	/ArcSight Foundation/ArcSight Express/Vulnerabilities/
Top 10 Assets by Exposed Vulnerability Counts	No description available.	Query	/ArcSight Foundation/ArcSight Express/Vulnerabilities/
Exposed Vulnerabilities by Asset	No description available.	Query	/ArcSight Foundation/ArcSight Express/Vulnerabilities/

Appendix A

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 HP SSO website. 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 89
"Running the Upgrade Script" on page 91
"Verifying and Reapplying Configurations After Upgrade" on page 91

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 Connector Asset Auto-Creation Controller Filter" on page 11.
- Any configurations made to ArcSight-supplied **rules**, such as those described in "Configure Rules to Send Notifications and Open Cases" on page 14.
- 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 90 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**.

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 92.

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 89 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 5.

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 92, below.

Fixing Invalid Resources

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

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

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

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

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

Index

A

active channels
- Anti-Virus Events 39
- Case Events 45
- Correlated Alerts 22
- Database Events 50
- Firewall Events 51
- Identity Management Events 58
- IDS - IPS Events 63
- Last 5 Minutes 21
- Live 21
- Network Events 68
- Operating System Events 74
- Reconnaissance Activity 21
- VPN Events 80

active lists
- Case Escalation 47
- Event-based Rule Exclusions 29
- User-based Rule Exclusions 29

Alert Counts by Device query 67
Alert Counts by Device report 64
Alert Counts by Port query 67
Alert Counts by Port report 64
Alert Counts by Severity (Chart) query 67
Alert Counts by Severity query 67
Alert Counts by Severity report 65
Alert Counts by Type query 67
Alert Counts by Type report 65
Alert Counts per Hour query 67
Alert Counts per Hour report 64
Anti-Virus Errors filter 42
Anti-Virus Errors query 44
Anti-Virus Events active channel 39
Anti-Virus Events filter 41
Anti-Virus Overview dashboard 40
Anti-Virus use case 39
Application Protocol Event Counts data monitor 29
ArcSight Admin field set 32
ArcSight Express
- device list 7

ArcSight Express field set 32
asset auto-creation filters
- connector 11
- device 12

Authentication Errors query 86
Authentication Errors report 81
Authentication Failures by Destination data monitor 60
Authentication Failures by Source data monitor 60
AV - Failed Updates filter 42
AV - Found Infected filter 42
Average Time to Case Resolution - By Day query 49
Average Time to Case Resolution - by Day query viewer 45
Average Time to Case Resolution - By Day report 47
Average Time to Case Resolution - By Severity query 49
Average Time to Case Resolution - by Severity query viewer 46
Average Time to Case Resolution - By Severity report 47
Average Time to Case Resolution - By User query 48
Average Time to Case Resolution - by User query viewer 46
Average Time to Case Resolution - By User report 46

B

Backdoor Traffic filter 33
Bandwidth Usage by Hour report 25
Bandwidth Usage by Protocol focused report 55, 72, 84
Bandwidth Usage by Protocol query 35
Bandwidth Usage by Protocol report 23
Bandwidth Usage per Hour focused report 56, 72, 83
Bandwidth Usage per Hour query 35
By User Account - Accounts Created query 37
By User Account - Accounts Created report 23

C

Case Escalation active list 47
Case Events active channel 45
Case Events filter 48
Case field set 47
Case Monitoring Entry Expiration filter 48
Case Stages dashboard 45
Case Stages Overview report 47
Case Status dashboard 45
Case Status Overview report 47
Case Times to Resolution dashboard 45
Case Tracking and Escalation use case 39
Case Tracking session list 49
Cases field set 32, 47
Cases Open by Stage (Chart) query 48
Categories field set 32
Closed Connection Durations query 62
Closed VPN Connection Durations query 86
configuration
- connector asset auto-creation filter 11
- device asset auto-creation filter 12
- schedule reports 17
- set up connectors and model the network 7

Configuration Changes by Type focused report 43, 51, 57, 61, 71, 78, 85
Configuration Changes by Type report 24
Configuration Changes by User focused report 42, 51, 55, 62, 71, 78, 85
Configuration Changes by User report 24
Configuration Changes Overview dashboard 22

Configuration Changes query 36
Connection Counts by User report 58, 81
Connection Durations by User report 58
Connections Accepted by Address query 85
Connections Accepted by Address report 81
Connections Denied by Address query 86
Connections Denied by Address report 81
Connections Denied by Hour query 86
Connections Denied by Hour report 81
Correlated Alerts active channel 22
Critical Network Events filter 70
Current Connector Status data monitor 31
Current Event Sources dashboard 22

D

dashboards
- Anti-Virus Overview 40
- Case Stages 45
- Case Status 45
- Case Times to Resolution 45
- Configuration Changes Overview 22
- Current Event Sources 22
- Database Errors 50
- Firewall Connection Overview 52
- Firewall Login Overview 52
- Identity Management Overview 58
- IDS - IPS Overview 63
- Network Login Overview 68
- Network Status Overview 68
- Operating System Login Overview 74
- Reconnaissance in Progress 22
- Security Activity 22
- Security Activity Statistics 22
- Virus Activity Statistics 40
- VPN Connection Statistics 80
- VPN Login Overview 80
- Worm Outbreak Overview 63

data monitors
- Application Protocol Event Counts 29
- Authentication Failures by Destination 60
- Authentication Failures by Source 60
- Current Connector Status 31
- Devices with High Error Rates 69
- Event Counts by Hour 31
- Events per Address Space 29
- Last 10 Anti-Virus Errors 41
- Last 10 Critical Network Events 69
- Last 10 Database Configuration Changes 30
- Last 10 Database Errors 50
- Last 10 Failed Login Events 54, 69, 76, 82
- Last 10 Firewall Configuration Changes 30
- Last 10 Hosts Scanned 30
- Last 10 Interface Down Messages 69
- Last 10 Interface Status Messages 69
- Last 10 Network Configuration Changes 30
- Last 10 Scanners 30
- Last 10 Successful Login Events 54, 69, 76, 82
- Last 10 VPN Configuration Changes 30
- Last 10 Zones Scanned 29
- Last Failed Logins 31
- Login Results 53, 69, 76, 82
- Most Frequent Ports 29
- Port Monitor 31
- Recent Events 30
- Target Port Activity by Attacker 66
- Top 10 Alert Destinations 66
- Top 10 Alert Sources 66
- Top 10 Alert Types 65
- Top 10 Alerts 66
- Top 10 Anti-Virus Errors 41
- Top 10 Database Errors 50
- Top 10 Denied Ports (Inbound) 54
- Top 10 Denied Ports (Outbound) 54
- Top 10 Hosts With Denied Inbound Connections 54
- Top 10 Hosts With Denied Outbound Connections 53
- Top 10 Infected Systems 41
- Top 10 Infections 41
- Top 10 Users With Failed Logins 54, 69, 76, 82
- Top 10 Users with Failed Logins 30
- Top 10 Zones Scanned 31
- Top Categories 31
- Top Connectors 31
- Top Event Sources 30
- Top Firewall Blocked Machines 31
- Top Successful Attacks 31
- Top Transport Protocols 30
- Top Users by Connection Count 60
- Top Users by Login Activity 69, 76, 82
- Top VPN Servers with Authentication Errors 82
- Top VPN Servers with Denied Connections 82
- Top VPN Servers with Successful Connections 82
- Top VPN Users with Authentication Errors 82
- Trojaned Machines 29
- Virus Activity by Host 41
- Virus Activity by Zone 41
- Worm Activity Status 66
- Worm Infected Machines 31
- Worm Infected Systems 65

Database Configuration Changes filter 34, 50
Database Errors and Warnings (Chart) query 51
Database Errors and Warnings query 51
Database Errors and Warnings report 50
Database Errors dashboard 50
Database Errors filter 50
Database Events active channel 50
Database Events filter 50
Database use case 38
Denied Inbound Connections by Address query 57
Denied Inbound Connections by Address report 53
Denied Inbound Connections by Port query 57
Denied Inbound Connections by Port report 52
Denied Inbound Connections filter 54
Denied Inbound Connections per Hour (Chart) query 58
Denied Inbound Connections per Hour query 57
Denied Inbound Connections per Hour report 52
Denied Outbound Connections by Address query 57
Denied Outbound Connections by Address report 53
Denied Outbound Connections by Port query 57
Denied Outbound Connections by Port report 52
Denied Outbound Connections filter 54
Denied Outbound Connections per Hour (Chart) query 57
Denied Outbound Connections per Hour query 57
Denied Outbound Connections per Hour report 52
Device Critical Events query 73
Device Critical Events report 68
Device Errors query 73
Device Errors report 68

Device Events query 73
Device Events report 68
Device Interface Down Notifications query 73
Device Interface Down Notifications report 68
Device Interface Status Messages query 74
Device Interface Status Messages report 69
Device SNMP Authentication Failures by User query 73
Device SNMP Authentication Failures query 73
Device SNMP Authentication Failures report 68
Devices with High Error Rates data monitor 69

E

Errors Detected in Anti-Virus Deployment report 40
Event Counts by Hour data monitor 31
Event Inspector field set 32
Event-based Rule Exclusions active list 29
Events per Address Space data monitor 29
Exposed Vulnerabilities by Asset query 87
Exposed Vulnerabilities by Asset report 87
Exposed Vulnerability Count by Asset query 87
Exposed Vulnerability Count by Asset report 87
Exposed Vulnerability Count by Critical Asset focused report 87

F

Failed Anti-Virus Updates Chart query 43
Failed Anti-Virus Updates query 43
Failed Anti-Virus Updates report 40
Failed Firewall Login Events filter 54
Failed Identity Management Login Attempts filter 60
Failed Login Attempts (Chart) query 37
Failed Login Attempts focused report 61, 79
Failed Login Attempts query 35
Failed Login Attempts report 23
Failed Login by User (Chart) query 35
Failed Login by User query 36
Failed Logins by Destination Address (Chart) query 34
Failed Logins by Destination Address focused report 55, 61, 72, 78, 83
Failed Logins by Destination Address report 23
Failed Logins by Source Address (Chart) query 36
Failed Logins by Source Address focused report 55, 61, 71, 79, 85
Failed Logins by Source Address report 24
Failed Logins by Source-Destination Pair query 37
Failed Logins by User focused report 57, 62, 71, 78, 83
Failed Logins by User report 24
Failed Logins with Target Information filter 32
Failed Network Login Events filter 70
Failed Operating System Login Events filter 77
Failed VPN Connection Events filter 82
Failed VPN Login Events filter 83
field sets
  ArcSight Admin 32
  ArcSight Express 32
  Case 47
  Cases 32, 47
  Categories 32
  Event Inspector 32
  Security 32
  Standard 32
  Standard-MgrRcpt 32
files
  Internal-ExternalAssets.txt 32
filters
  Anti-Virus Errors 42
  Anti-Virus Events 41
  AV - Failed Updates 42
  AV - Found Infected 42
  Backdoor Traffic 33
  Case Events 48
  Case Monitoring Entry Expiration 48
  Critical Network Events 70
  Database Configuration Changes 34, 50
  Database Errors 50
  Database Events 50
  Denied Inbound Connections 54
  Denied Outbound Connections 54
  Failed Firewall Login Events 54
  Failed Identity Management Login Attempts 60
  Failed Logins with Target Information 32
  Failed Network Login Events 70
  Failed Operating System Login Events 77
  Failed VPN Connection Events 82
  Failed VPN Login Events 83
  Firewall Configuration Changes 33, 54
  Firewall Deny 33
  Firewall Events 55
  Firewall Login Events 54
  Identity Management Connection Start Events 60
  Identity Management Events 60
  IDS -IPS Events 66
  LockedCount is NULL 77
  LoginCount is NULL or 0 77
  Network Configuration Changes 33
  Network Device Interface Down Messages 70
  Network Device Interface Status Events 70
  Network Error Events 70
  Network Events 70
  Network Login Events 70
  Non ArcSight Internal Event - Target Port Not Null 33
  Non ArcSight Internal Event with TargetPort Set 34
  Operating System Events 77
  Operating System Login Events 77
  Reconnaissance Events (Internal Targets) 34
  Reconnaissance Events by Attacker 33
  Reconnaissance Events by Target 32
  Reconnaissance Events by Target Zone 33
  Successful Attacks 34
  Successful Configuration Changes 34
  Successful Firewall Login Events 54
  Successful Network Login Events 70
  Successful Operating System Login Events 77
  Successful VPN Connection Events 83
  Successful VPN Login Events 83
  Successful Windows Login 77
  Successful Windows Logout 77
  Target Port Activity By Attacker 66
  Update Events 42
  Virus Activity 42
  VPN Authentication Errors 83
  VPN Configuration Changes 33
  VPN Events 82
  VPN Login Events 82
  Worm Activity 66
  Worm Outbreak 66
  Worm Traffic 33

Final Stage Cases by Owner (Chart) query 48
Final Stage Cases by Owner query viewer 46
Firewall Configuration Changes filter 33, 54
Firewall Connection Overview dashboard 52
Firewall Deny filter 33
Firewall Events active channel 51
Firewall Events filter 55
Firewall Login Events filter 54
Firewall Login Overview dashboard 52
Firewall use case 39
focused reports
    Bandwidth Usage by Protocol 55, 72, 84
    Bandwidth Usage per Hour 56, 72, 83
    Configuration Changes by Type 43, 51, 57, 61, 71, 78, 85
    Configuration Changes by User 42, 51, 55, 62, 71, 78, 85
    Exposed Vulnerability Count by Critical Asset 87
    Failed Login Attempts 61, 79
    Failed Logins by Destination Address 55, 61, 72, 78, 83
    Failed Logins by Source Address 55, 61, 71, 79, 85
    Failed Logins by User 57, 62, 71, 78, 83
    Login Event Audit 51, 56, 72, 78, 84
    Password Changes 50, 61, 79, 84
    Successful Logins by Destination Address 56, 61, 72, 79, 84
    Successful Logins by Source Address 56, 62, 70, 79, 84
    Successful Logins by User 56, 62, 71, 78, 85
    Top 10 Alerts 66
    Top 10 Attackers 67
    Top 10 Targets 66
    Top Bandwidth Hosts 56, 72, 85
    Top Hosts by Number of Connections 55, 71, 84
Follow-Up Stage Cases by Owner (Chart) query 48
Follow-Up Stage Cases by Owner query viewer 46

H

High Number of Connections rule 26, 53
High Number of Denied Connections for A Source Host rule 27, 53
High Number of Denied Inbound Connections rule 26, 53
High Number of IDS Alerts for Backdoor rule 65
High Number of IDS Alerts for DoS rule 65

I

Identity Management Connection Start Events filter 60
Identity Management Events active channel 58
Identity Management Events filter 60
Identity Management Overview dashboard 58
Identity Management use case 39
IDS - IPS Events active channel 63
IDS - IPS Overview dashboard 63
IDS - IPS use case 38
IDS -IPS Events filter 66
Infected Systems query 43
Initial Stage Cases by Owner (Chart) query 49
Initial Stage Cases by Owner query viewer 46
Internal-ExternalAssets.txt file 32

L

Last 10 Anti-Virus Errors data monitor 41
Last 10 Critical Network Events data monitor 69
Last 10 Database Configuration Changes data monitor 30
Last 10 Database Errors data monitor 50
Last 10 Failed Login Events data monitor 54, 69, 76, 82
Last 10 Firewall Configuration Changes data monitor 30
Last 10 Hosts Scanned data monitor 30
Last 10 Interface Down Messages data monitor 69
Last 10 Interface Status Messages data monitor 69
Last 10 Network Configuration Changes data monitor 30
Last 10 Scanners data monitor 30
Last 10 Successful Login Events data monitor 54, 69, 76, 82
Last 10 VPN Configuration Changes data monitor 30
Last 10 Zones Scanned data monitor 29
Last 5 Minutes active channel 21
Last Failed Logins data monitor 31
Live active channel 21
LockedCount is NULL filter 77
Login Errors by User (Chart) query 80
Login Errors by User query 79
Login Errors by User report 74
Login Event Audit focused report 51, 56, 72, 78, 84
Login Event Audit query 34
Login Event Audit report 22
Login Results data monitor 53, 69, 76, 82
LoginCount is NULL or 0 filter 77

M

Max Time to Case Resolution - By User report 47
Maximum Time to Case Resolution - By User query 49
Maximum Time to Case Resolution - by User query viewer 46
Most Frequent Ports data monitor 29
Multiple Login Attempts to Locked Windows Account rule 28, 76
Multiple Windows Logins by Same User rule 29, 76

N

Network Configuration Changes filter 33
Network Device Interface Down Messages filter 70
Network Device Interface Status Events filter 70
Network Error Events filter 70
Network Events active channel 68
Network Events filter 70
Network Login Events filter 70
Network Login Overview dashboard 68
network modeling
    ArcSight Express 7
Network Status Overview dashboard 68
Network use case 38
Non ArcSight Internal Event - Target Port Not Null filter 33
Non ArcSight Internal Event with TargetPort Set filter 34

O

Open Cases by Associated Impact (Chart) query 48
Open Cases by Associated Impact query viewer 46
Open Cases by Consequence Severity (Chart) query 49
Open Cases by Consequence Severity query viewer 45

Open Cases by Operational Impact (Chart) query 49
Open Cases by Operational Impact query viewer 46
Open Cases by Stage query viewer 45
Open Cases Details query 48
Open Cases query viewer 46
Operating System Events active channel 74
Operating System Events filter 77
Operating System Login Events filter 77
Operating System Login Overview dashboard 74
Operating System use case 38

P

Password Changes focused report 50, 61, 79, 84
Password Changes query 35
Password Changes report 23
Port Monitor data monitor 31
protected network
    how ArcSight determines 9

Q

queries
    Alert Counts by Device 67
    Alert Counts by Port 67
    Alert Counts by Severity 67
    Alert Counts by Severity (Chart) 67
    Alert Counts by Type 67
    Alert Counts per Hour 67
    Anti-Virus Errors 44
    Authentication Errors 86
    Average Time to Case Resolution - By Day 49
    Average Time to Case Resolution - By Severity 49
    Average Time to Case Resolution - By User 48
    Bandwidth Usage by Protocol 35
    Bandwidth Usage per Hour 35
    By User Account - Accounts Created 37
    Cases Open by Stage (Chart) 48
    Closed Connection Durations 62
    Closed VPN Connection Durations 86
    Configuration Changes 36
    Connections Accepted by Address 85
    Connections Denied by Address 86
    Connections Denied by Hour 86
    Database Errors and Warnings 51
    Database Errors and Warnings (Chart) 51
    Denied Inbound Connections by Address 57
    Denied Inbound Connections by Port 57
    Denied Inbound Connections per Hour 57
    Denied Inbound Connections per Hour (Chart) 58
    Denied Outbound Connections by Address 57
    Denied Outbound Connections by Port 57
    Denied Outbound Connections per Hour 57
    Denied Outbound Connections per Hour (Chart) 57
    Device Critical Events 73
    Device Errors 73
    Device Events 73
    Device Interface Down Notifications 73
    Device Interface Status Messages 74
    Device SNMP Authentication Failures 73
    Device SNMP Authentication Failures by User 73
    Exposed Vulnerabilities by Asset 87
    Exposed Vulnerability Count by Asset 87
    Failed Anti-Virus Updates 43
    Failed Anti-Virus Updates Chart 43
    Failed Login Attempts 35
    Failed Login Attempts (Chart) 37
    Failed Login by User 36
    Failed Login by User (Chart) 35
    Failed Logins by Destination Address (Chart) 34
    Failed Logins by Source Address (Chart) 36
    Failed Logins by Source-Destination Pair 37
    Final Stage Cases by Owner (Chart) 48
    Follow-Up Stage Cases by Owner (Chart) 48
    Infected Systems 43
    Initial Stage Cases by Owner (Chart) 49
    Login Errors by User 79
    Login Errors by User (Chart) 80
    Login Event Audit 34
    Maximum Time to Case Resolution - By User 49
    Open Cases by Associated Impact (Chart) 48
    Open Cases by Consequence Severity (Chart) 49
    Open Cases by Operational Impact (Chart) 49
    Open Cases Details 48
    Password Changes 35
    Queued Stage Cases by Owner (Chart) 48
    Recently Closed Cases 48
    SIS-Assets Compromised Table Query 35
    SIS-Cases Added Table Query 38
    SIS-Event Count by Agent Severity Chart Query 37
    SIS-Notifications Sent Table Query 36
    SIS-Top Attackers Chart Query 37
    SIS-Top Attacks Table Query 37
    SIS-Top Events Table Query 36
    SIS-Top Firing Rules Table Query 36
    SIS-Top Target Ports Chart Query 36
    SIS-Top Targets Chart Query 36
    SNMP Authentication Failures by Device 73
    Successful Login by User 35
    Successful Login by User (Chart) 38
    Successful Logins by Destination Address (Chart) 36
    Successful Logins by Source Address (Chart) 34
    Successful Logins by Source-Destination Pair 38
    Top 10 Assets by Exposed Vulnerability Counts 87
    Top Alert Destinations 67
    Top Alert Sources 67
    Top Anti-Virus Errors 44
    Top Bandwidth Hosts 35
    Top Connection Durations 62
    Top Connections Accepted by Address 86
    Top Connections Denied by Address 86
    Top Device System Authentication Events 73
    Top Hosts by Number of Connections 37
    Top IDS and IPS Alerts 37
    Top Infected Systems 44
    Top Users by Connection Count 63, 86
    Top VPN Connection Durations 86
    Top Zones with Anti-Virus Errors 43
    Trend on Case Audit Events 49
    Update Summary 44
    Update Summary Chart 44
    User Administration 80
    User Administration (Chart) 79
    Users by Connection Count 63, 86
    Users with Open Connections 63
    Users with Open VPN Connections 87
    Virus Activity by Hour 43
    Worm Infected Systems 67
query viewers

Average Time to Case Resolution - by Day 45
Average Time to Case Resolution - by Severity 46
Average Time to Case Resolution - by User 46
Final Stage Cases by Owner 46
Follow-Up Stage Cases by Owner 46
Initial Stage Cases by Owner 46
Maximum Time to Case Resolution - by User 46
Open Cases 46
Open Cases by Associated Impact 46
Open Cases by Consequence Severity 45
Open Cases by Operational Impact 46
Open Cases by Stage 45
Queued Stage Cases by Owner 45
Recently Closed Cases 45
Queued Stage Cases by Owner (Chart) query 48
Queued Stage Cases by Owner query viewer 45

R

Recent Events data monitor 30
Recently Closed Cases query 48
Recently Closed Cases query viewer 45
Reconnaissance Activity active channel 21
Reconnaissance Events (Internal Targets) filter 34
Reconnaissance Events by Attacker filter 33
Reconnaissance Events by Target filter 32
Reconnaissance Events by Target Zone filter 33
Reconnaissance in Progress dashboard 22
reports
Alert Counts by Device 64
Alert Counts by Port 64
Alert Counts by Severity 65
Alert Counts by Type 65
Alert Counts per Hour 64
ArcSight Express, scheduling 17
Authentication Errors 81
Average Time to Case Resolution - By Day 47
Average Time to Case Resolution - By Severity 47
Average Time to Case Resolution - By User 46
Bandwidth Usage by Hour 25
Bandwidth Usage by Protocol 23
By User Account - Accounts Created 23
Case Stages Overview 47
Case Status Overview 47
Configuration Changes by Type 24
Configuration Changes by User 24
Connection Counts by User 58, 81
Connection Durations by User 58
Connections Accepted by Address 81
Connections Denied by Address 81
Connections Denied by Hour 81
Database Errors and Warnings 50
Denied Inbound Connections by Address 53
Denied Inbound Connections by Port 52
Denied Inbound Connections per Hour 52
Denied Outbound Connections by Address 53
Denied Outbound Connections by Port 52
Denied Outbound Connections per Hour 52
Device Critical Events 68
Device Errors 68
Device Events 68
Device Interface Down Notifications 68
Device Interface Status Messages 69
Device SNMP Authentication Failures 68
Errors Detected in Anti-Virus Deployment 40
Exposed Vulnerabilities by Asset 87
Exposed Vulnerability Count by Asset 87
Failed Anti-Virus Updates 40
Failed Login Attempts 23
Failed Logins by Destination Address 23
Failed Logins by Source Address 24
Failed Logins by User 24
Login Errors by User 74
Login Event Audit 22
Max Time to Case Resolution - By User 47
Password Changes 23
Security Intelligence Status Report 25
Successful Logins by Destination Address 24
Successful Logins by Source Address 25
Successful Logins by User 22
Top Alert Destinations 65
Top Alert Sources 64
Top Alerts from IDS and IPS 23
Top Attackers 23
Top Bandwidth Hosts 24
Top Hosts by Number of Connections 25
Top Infected Systems 40
Top Targets 25
Top Users by Average Session Length 80
Update Summary 41
User Administration 74
Virus Activity by Time 40
Worm Infected Systems 64
rules
High Number of Connections 26, 53
High Number of Denied Connections for A Source Host 27, 53
High Number of Denied Inbound Connections 26, 53
High Number of IDS Alerts for Backdoor 65
High Number of IDS Alerts for DoS 65
Multiple Login Attempts to Locked Windows Account 28, 76
Multiple Windows Logins by Same User 29, 76
Successful Windows Login 28, 75
Successful Windows Logout 27, 75
SYN Flood Detected by IDS or Firewall 53, 65
User Session (Accounting User) Started 26, 59
User Session (Accounting User) Stopped 26, 59
User Session (Administrative User) Started 26, 59
User Session (Administrative User) Stopped 27, 59
User Session (Normal User) Started 27, 60
User Session (Normal User) Stopped 28, 59
User VPN Session Started 27, 81
User VPN Session Stopped 28, 81
Windows Account Created 28, 76
Windows Account Created and Deleted within 1 Hour 26, 75
Windows Account Locked Out 27, 75
Windows Account Locked Out Multiple Times 28, 75

S

Security Activity dashboard 22
Security Activity Statistics dashboard 22
Security field set 32
Security Intelligence Status Report report 25
session lists
Case Tracking 49

SIS-Assets Compromised Table Query query 35
SIS-Cases Added Table Query query 38
SIS-Event Count by Agent Severity Chart Query query 37
SIS-Notifications Sent Table Query query 36
SIS-Top Attackers Chart Query query 37
SIS-Top Attacks Table Query query 37
SIS-Top Events Table Query query 36
SIS-Top Firing Rules Table Query query 36
SIS-Top Target Ports Chart Query query 36
SIS-Top Targets Chart Query query 36
SmartConnectors
    for ArcSight Express content 7
SNMP Authentication Failures by Device query 73
Standard field set 32
Standard-MgrRcpt field set 32
Successful Attacks filter 34
Successful Configuration Changes filter 34
Successful Firewall Login Events filter 54
Successful Login by User (Chart) query 38
Successful Login by User query 35
Successful Logins by Destination Address (Chart) query 36
Successful Logins by Destination Address focused report 56, 61, 72, 79, 84
Successful Logins by Destination Address report 24
Successful Logins by Source Address (Chart) query 34
Successful Logins by Source Address focused report 56, 62, 70, 79, 84
Successful Logins by Source Address report 25
Successful Logins by Source-Destination Pair query 38
Successful Logins by User focused report 56, 62, 71, 78, 85
Successful Logins by User report 22
Successful Network Login Events filter 70
Successful Operating System Login Events filter 77
Successful VPN Connection Events filter 83
Successful VPN Login Events filter 83
Successful Windows Login filter 77
Successful Windows Login rule 28, 75
Successful Windows Logout filter 77
Successful Windows Logout rule 27, 75
SYN Flood Detected by IDS or Firewall rule 53, 65

T

Target Port Activity by Attacker data monitor 66
Target Port Activity By Attacker filter 66
Top 10 Alert Destinations data monitor 66
Top 10 Alert Sources data monitor 66
Top 10 Alert Types data monitor 65
Top 10 Alerts data monitor 66
Top 10 Alerts focused report 66
Top 10 Anti-Virus Errors data monitor 41
Top 10 Assets by Exposed Vulnerability Counts query 87
Top 10 Attackers focused report 67
Top 10 Database Errors data monitor 50
Top 10 Denied Ports (Inbound) data monitor 54
Top 10 Denied Ports (Outbound) data monitor 54
Top 10 Hosts With Denied Inbound Connections data monitor 54
Top 10 Hosts With Denied Outbound Connections data monitor 53
Top 10 Infected Systems data monitor 41
Top 10 Infections data monitor 41
Top 10 Targets focused report 66
Top 10 Users With Failed Logins data monitor 54, 69, 76, 82
Top 10 Users with Failed Logins data monitor 30
Top 10 Zones Scanned data monitor 31
Top Alert Destinations query 67
Top Alert Destinations report 65
Top Alert Sources query 67
Top Alert Sources report 64
Top Alerts from IDS and IPS report 23
Top Anti-Virus Errors query 44
Top Attackers report 23
Top Bandwidth Hosts focused report 56, 72, 85
Top Bandwidth Hosts query 35
Top Bandwidth Hosts report 24
Top Categories data monitor 31
Top Connection Durations query 62
Top Connections Accepted by Address query 86
Top Connections Denied by Address query 86
Top Connectors data monitor 31
Top Device System Authentication Events query 73
Top Event Sources data monitor 30
Top Firewall Blocked Machines data monitor 31
Top Hosts by Number of Connections focused report 55, 71, 84
Top Hosts by Number of Connections query 37
Top Hosts by Number of Connections report 25
Top IDS and IPS Alerts query 37
Top Infected Systems query 44
Top Infected Systems report 40
Top Successful Attacks data monitor 31
Top Targets report 25
Top Transport Protocols data monitor 30
Top Users by Average Session Length report 80
Top Users by Connection Count data monitor 60
Top Users by Connection Count query 63, 86
Top Users by Login Activity data monitor 69, 76, 82
Top VPN Connection Durations query 86
Top VPN Servers with Authentication Errors data monitor 82
Top VPN Servers with Denied Connections data monitor 82
Top VPN Servers with Successful Connections data monitor 82
Top VPN Users with Authentication Errors data monitor 82
Top Zones with Anti-Virus Errors query 43
Trend on Case Audit Events query 49
Trojaned Machines data monitor 29

U

Update Events filter 42
Update Summary Chart query 44
Update Summary query 44
Update Summary report 41
Upgrading ArcSight Express Content 89
    After Upgrade 91
    Preparing for Upgrade 89
use cases
    Anti-Virus 39
    Case Tracking and Escalation 39
    Database 38
    Firewall 39
    Identity Management 39
    IDS - IPS 38

Network 38
Operating System 38
VPN 38
Vulnerabilities 38
User Administration (Chart) query 79
User Administration query 80
User Administration report 74
User Session (Accounting User) Started rule 26, 59
User Session (Accounting User) Stopped rule 26, 59
User Session (Administrative User) Started rule 26, 59
User Session (Administrative User) Stopped rule 27, 59
User Session (Normal User) Started rule 27, 60
User Session (Normal User) Stopped rule 28, 59
User VPN Session Started rule 27, 81
User VPN Session Stopped rule 28, 81
User-based Rule Exclusions active list 29
Users by Connection Count query 63, 86
Users with Open Connections query 63
Users with Open VPN Connections query 87

V

Virus Activity by Host data monitor 41
Virus Activity by Hour query 43
Virus Activity by Time report 40
Virus Activity by Zone data monitor 41
Virus Activity filter 42
Virus Activity Statistics dashboard 40
VPN Authentication Errors filter 83
VPN Configuration Changes filter 33
VPN Connection Statistics dashboard 80
VPN Events active channel 80
VPN Events filter 82
VPN Login Events filter 82
VPN Login Overview dashboard 80
VPN use case 38
Vulnerabilities use case 38

W

Windows Account Created and Deleted within 1 Hour rule 26, 75
Windows Account Created rule 28, 76
Windows Account Locked Out Multiple Times rule 28, 75
Windows Account Locked Out rule 27, 75
Worm Activity filter 66
Worm Activity Status data monitor 66
Worm Infected Machines data monitor 31
Worm Infected Systems data monitor 65
Worm Infected Systems query 67
Worm Infected Systems report 64
Worm Outbreak filter 66
Worm Outbreak Overview dashboard 63
Worm Traffic filter 33