Standard Content Guide

Workflow

for ArcSight ESM™ 6.0c with CORR-Engine

September 14, 2012

ArcSight™
An HP Company

Standard Content Guide - Workflow

Revision History

Date	Product Version	Description
09/14/2012	Workflow Content for ESM 6.0c	Final revision for release.

Document template version: 2.1.1

Contact Information

Phone	1-866-535-3285 (North America) +44 203-564-1189 (EMEA) +49 69380789455 (Germany)
Support Web Site	http://support.openview.hp.com
Protect 724 Community	https://protect724.arcsight.com

Contents

Chapter 1

Workflow Overview

This chapter discusses the following topics.

What is Standard Content

Standard content is a series of coordinated resources (filters, rules, dashboards, reports, and so on) that address common security and management tasks. Standard content is designed to give you comprehensive correlation, monitoring, reporting, alerting, and case management out of the box with minimal configuration. The content provides a full spectrum of security, network, and configuration monitoring tasks, as well as a comprehensive set of tasks that monitor the health of the system.

The standard content is installed using a series of packages, some of which are installed automatically with the Manager to provide essential system health and status operations. The remaining packages are presented as install-time options organized by category.

Standard content consists of the following:

- **ArcSight System** content is installed automatically with the Manager and consists of resources required for basic security processing functions, such as threat escalation and priority calculations, as well as basic throughput channels required for out-of-the-box functionality.
- **ArcSight Administration** content is installed automatically with the Manager, and provides statistics about the health and performance of ArcSight products. ArcSight Administration is essential for managing and tuning the performance of content and components.
- **ArcSight Foundations** content (such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, NetFlow Monitoring, and Workflow) are presented as install-time options and provide a coordinated system of resources with real-time monitoring capabilities for a specific area of focus, as well as after-the-fact analysis in the form of reports and trends. You can extend these foundations with additional resources specific to your needs or you can use them as a template for building your own resources and tasks.
- **Shared Libraries -** ArcSight Administration and several of the ArcSight Foundations rely on a series of common resources that provide core functionality for common

security scenarios. Dependencies between these resources and the packages they support are managed by the Package resource.

- Anti-Virus content is a set of filters, reports, and report queries used by ArcSight Foundations, such as Configuration Monitoring and Intrusion Monitoring.
- Conditional Variable Filters are a library of filters used by variables in standard content report queries, filters, and rule definitions. The Conditional Variable Filters are used by ArcSight Administration and certain ArcSight Foundations, such as Configuration Monitoring, Intrusion Monitoring, Network Monitoring, and Workflow.
- Global Variables are a set of variables used to create other resources and to provide event-based fields that cover common event information, asset, host, and user information, and commonly used timestamp formats. The Global Variables are used by ArcSight Administration and certain ArcSight Foundations.
- Network filters are a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.

Standard Content Packages

Standard content comes in packages (`.arb` files) that are either installed automatically or presented as an install-time option. The following graphic outlines the packages.

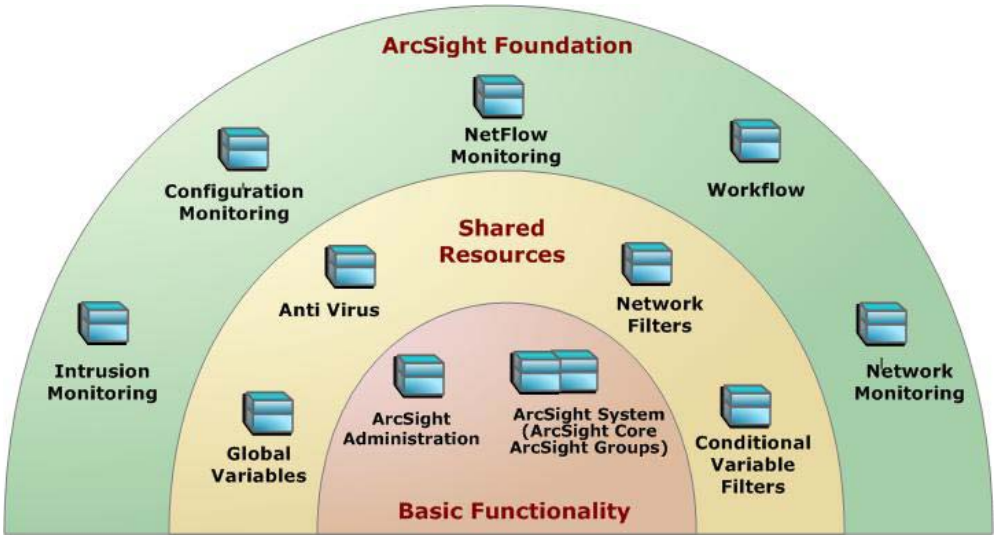

Figure 1-1 The ArcSight System and ArcSight Administration packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support ArcSight Administration and the ArcSight Foundation packages. The packages shown on top are ArcSight Foundations that address common network security and management scenarios.

Depending on the options you install, you will see the ArcSight System resources, the ArcSight Administration resources, and some or all of the other package content.

The ArcSight Express package is present in ESM installations, but is not installed by default. The package offers an alternate view of the Foundation resources. You can install or uninstall the ArcSight Express package without impact to the system.

When creating your own packages, you can explicitly include or exclude system resources in the package. Exercise caution if you delete packages that might have system resources; for example, zones. Make sure the system resources either belong to a locked group or are themselves locked. For more information about packages, refer to the *ArcSight Console User's Guide*.

Workflow Content

The Workflow content is a system of active channels and reports that support incident response tracking by using the incident response system.

ESM uses notifications and cases to enable security operators to coordinate and prioritize response to security events. Qualifying events in the other ArcSight Foundation packages trigger notifications and cases that get escalated through ArcSight's incident response stages. The Workflow active channels and reports show the status of cases and notifications generated by these qualifying events.

For an overview on ESM notifications, cases, and incident response workflow, refer to the *ESM 101* guide.

This guide describes the Workflow content. For information about ArcSight System or ArcSight Administration content, refer to the Standard *Content Guide - ArcSight System and ArcSight Administration*. For information about an optional Foundation, refer to the Standard Content Guide for that Foundation. ArcSight ESM documentation is available on Protect 724 (https://protect724.arcsight.com).

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

For information about upgrading standard content, see Appendix A, Upgrading Standard Content, on page 139.

Installing the Workflow Package

The Workflow Foundation package is one of the standard content packages that are presented as install-time options. If you selected all the standard content packages to be installed at installation time, the packages and their resources will be installed in the ArcSight database and available in the Navigator panel resource tree. The package icon in the Navigator panel package view will appear blue.

If you opted to exclude any packages at installation time, the package is imported into the ESM package view in the Navigator panel, but is not available in the resource view. The package icon in the package view will appear grey.

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

To install a package that is imported, but not installed:

1. In the Navigator panel Package view, navigate to the package you want to install.
2. Right-click the package and select **Install Package**.
3. In the Install Package dialog, click **OK**.
4. When the installation is complete, review the summary report and click **OK**.

   The package resources are fully installed to the ArcSight database, the resources are fully enabled and operational, and available in the Navigator panel resource tree.

To uninstall a package that is installed:

1. In the Navigator Panel Package view, navigate to the package you want to uninstall.
2. Right-click the package and select **Uninstall Package**.
3. In the Uninstall Package dialog, click **OK**.

   The progress of the uninstall displays in the Progress tab of the Uninstalling Packages dialog. If a message displays indicating that there is a conflict, select an option in the Resolution Options area and click **OK**.

4 When uninstall is complete, review the summary and click **OK**.

The package is removed from the ArcSight database and the Navigator panel resource tree, but remains available in the Navigator panel package view, and can be re-installed at another time.

To delete a package and remove it from the Console and the database:

1 In the Navigator Panel Package view, navigate to the package you want to delete.

2 Right-click the package and select **Delete Package**.

3 When prompted for confirmation of the delete, click **Delete**.

The package is removed from the Navigator panel package view.

Configuring Workflow Content

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

Modeling the Network

A network model keeps track of the network nodes participating in the event traffic. Modeling your network and categorizing critical assets using the standard asset categories is what activates some of the standard content and makes it effective.

There are several ways to model your network. For information about populating the network model, refer to the *ArcSight Console User's Guide* or the ESM online Help. To learn more about the architecture of the ESM network modeling tools, refer to the *ESM 101* guide.

Categorizing Assets

After you have populated your network model with assets, apply the standard asset categories to activate standard content that uses these categories.

- Categorize all assets (or the zones to which the assets belong) that are internal to the network with the `/All Asset Categories/Site Asset Categories/Address Spaces/Protected` category.

  Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as *Protected*.

  

  Assets with a private IP address (such as 192.168.0.0) are considered *Protected* by the system, even if they are not categorized as such.

- Categorize all assets that are considered *critical* to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with the `/All Asset Categories/System Asset Categories/Criticality/High` or `Very High` category.

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

Asset categories can be assigned to assets, zones, asset groups, or zone groups. If assigned to a group, all resources under that group inherit the categories.

You can assign asset categories individually using the Asset editor or in a batch using the Network Modeling wizard. For information about how to assign asset categories using the Console tools, refer to the *ArcSight Console User's Guide* or the online Help.

For more about the Priority Formula and how it leverages these asset categories to help assign priorities to events, refer to the *ArcSight Console User's Guide* or the *ESM 101* guide.

Enabling Rules

ESM rules trigger only if they are deployed in the `Real-Time Rules` group and are enabled. The Workflow rules are all deployed in the `Real-Time Rules` group by default but not all the rules are enabled.

To enable or disable a rule:

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

Ensuring Filters Capture Relevant Events

Standard content relies on specific event field values to identify events of interest. Although this method applies to most of the events and devices, be sure to test key filters to verify that they actually capture the required events.

To ensure that a filter captures the relevant events:

1. Generate or identify the required events and verify that they are being processed by viewing them in an active channel or query viewer.
2. Navigate to the appropriate filter, right-click the filter and choose **Create Channel with Filter**. If you see the events of interest in the newly created channel, the filter is functioning properly.

   If you do not see the events of interest:

   a. Verify that the configuration of the active channel is suitable for the events in question. For example, ensure that the event time is within the start and end time of the channel.

   b. Modify the filter condition to capture the events of interest. After applying the change, repeat Step 2 to verify that the modified filter captures the required events.

Configuring Notification Destinations

Configure notification destinations if you want to be notified when some of the standard content rules are triggered. By default, notifications are disabled in the standard content rules, so the admin user needs to configure the destinations *and* enable the notification in the rules. For details about enabling the notifications in rules, see Configuring Notifications and Cases, below.

Workflow rules reference the notification group SOC Operators. Add new destinations for notification levels 1, 2, and 3 as appropriate to the personnel in your security operations center. Refer to the *ArcSight Console User's Guide* or the ESM online Help for information on how to configure notification destinations.

Configuring Notifications and Cases

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

By default, the notifications and create case actions are disabled in the standard content rules that send notifications about security-related events to the Cert Team notification group.

To enable rules to send notifications and open cases, first configure notification destinations as described in Configuring Notification Destinations above, then enable the notification and case actions in the rules.

For more information about working with Rule actions in the Rules Editor, refer to the *ArcSight Console User's Guide* or the ESM online Help.

Scheduling Reports

You can run reports on demand, automatically on a regular schedule, or both. By default, reports are not scheduled to run automatically.

Evaluate the reports that come with Workflow, and schedule the reports that are of interest to your organization and business objectives. For instructions about how to schedule reports, refer to the *ArcSight Console User's Guide* or the online Help.

Configuring Trends

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

Workflow content includes several trends, some of which are enabled by default. These enabled trends are scheduled to run on an alternating schedule between the hours of midnight and 7:00 a.m., when network traffic is usually less busy than during peak daytime business hours. These schedules can be customized to suit your needs using the Trend scheduler in the ArcSight Console.

To disable or enable a trend, go to the **Trend** tab from the **Reports** drop-down list in the Navigator panel, right-click the trend, then select **Disable Trend** or **Enable Trend**.

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

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

Chapter 3

Workflow Content

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

Resource Group	Purpose
"Case Tracking and Escalation" on page 16	The Case Tracking and Escalation resources monitor 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.
"Event Annotations and Tracking" on page 25	The Event Annotations and Tracking resources provide analysts and team leaders with views of the events assigned to them for investigation or to be assigned.
"Notification Tracking" on page 28	The Notification Tracking resources provide insight into how notifications are being handled by the teams that are tasked with responding to them.

Case Tracking and Escalation

The Case Tracking and Escalation resources monitor 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.

Configuration

The Case Tracking and Escalation resource group requires the following configuration for your environment.

- In the **Case Escalation** active list, modify the **TTL** fields to match the maximum time that your organization allows a case to be in the Queued Stage.

  By default, the time frame to start the investigation of a newly opened case is set to one day.

  For information about how to edit active lists, refer to the *ArcSight Console User's Guide*.

Resources

The following table lists all the resources in the Case Tracking and Escalation resource group and any dependant resources.

Table 3-1 Resources in the Case Tracking and Escalation Group

Resource	Description	Type	URI
Monitor Resources			
Case Events	This active channel shows case audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/Cases and Notifications/
Case Times to Resolution	This resource has no description.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Stages	This dashboard displays information about the current state of open cases, showing the case stages for each case owner. A table is also provided to show more detailed open case information for each owner.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Status	This dashboard displays information about the current status of open cases, showing their impact and severity ratings. A table of recently closed cases is also provided.	Dashboard	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Open Cases by Stage	This query viewer displays a pie chart showing the number of open cases at each stage.	Query Viewer	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/

Resource	Description	Type	URI
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/Workflow/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Recently Closed Cases	This query viewer displays the most recently closed cases. Note: After a case is closed, if it is further modified, there might be multiple entries depending on the modifications. The Time Closed column shows the most recent modification of the closed case; this might not be the time when the case was initially closed.	Query Viewer	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/
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/Workflow/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
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/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/
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/Workflow/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
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/Workflow/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
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/Workflow/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
Average Time to Case Resolution - by User	This query viewer displays the average time taken to resolve cases that have been closed by each user during the reporting period.	Query Viewer	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/

Resource	Description	Type	URI
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/Workflow/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
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/Workflow/Case Tracking and Escalation/Case History/Case Times to Resolution Dashboard/
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/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/
Open Cases	This query viewer displays open case information in a table.	Query Viewer	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/Case Stages Dashboard/
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/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/
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/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
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/Workflow/Case Tracking and Escalation/Case History/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/Workflow/Case Tracking and Escalation/Case Stages/

Resource	Description	Type	URI
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/Workflow/Case Tracking and Escalation/Case History/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/Workflow/Case Tracking and Escalation/Case Status/
Open Cases	This report displays a table showing the name, creator, ticket type, stage, security classification, consequence severity, create time, modification time and attack target of all the open, non-system cases in the system.	Report	ArcSight Foundation/Workflow/Details/
TodaysCases'	This report displays a table showing the cases that have been generated since midnight this morning, including the case display ID, name, ticket type, stage, operational impact, and the user who created the case.	Report	ArcSight Foundation/Workflow/Operational Summaries/
All Cases	This report displays a table showing the name, creator, ticket type, stage, security classification, and consequence severity of all the non-system cases in the system.	Report	ArcSight Foundation/Workflow/Details/
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/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Library - Correlation Resources			
Case Deleted	This rule detects case audit events indicating that a case has been deleted without investigation. The rule removes the case from the active list for case tracking and escalation and sends a notification. This case is disabled by default.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/

Resource	Description	Type	URI
Track Deleted Case	This rule detects case audit events generated when a case is deleted. The rule then updates the case entry in a case history tracking session list and marks it as deleted.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Track New Case	This rule detects case audit events generated when a case is created. The rule then adds the case to a case history tracking session list.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Escalation	This rule tracks cases that have not yet been investigated when their entries expire from the case tracking and escalation active list. This case sends an escalation notification to the SOC Operators group and places the case information back on the active list. This rule is disabled by default.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Monitor New Case	This rule detects case audit events indicating that a case has been created. The rule adds the case to an active list for case tracking and escalation. This case is disabled by default.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Track Updated Case	This rule detects case audit events generated when a case is updated. If the case name, case owner, ticket type, stage, operational impact, security classification, consequence severity or associated impact attribute changes, the rule adds the case to a case history tracking session list.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Track Closed Case	This rule detects case audit events generated when a case is closed. A case is closed when the stage is changed to Closed. The rule then updates the case entry in a case history tracking session list. Note: You can re-open a case by changing the stage attribute.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case Investigation Started	This rule detects case audit events indicating that a case investigation has started. The rule then removes the case from the active list for case tracking and escalation. This rule is disabled by default.	Rule	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Library Resources			

Resource	Description	Type	URI
Case Escalation	This active list tracks case data on newly created cases that are still in the Queued stage. The default TTL is one day. If the case is not removed from the list, a rule will detect this, put it back on the list and send a notification.	Active List	ArcSight Foundation/Workflow/Case Tracking and Escalation/
DateTime	This variable returns the date and time in the year/month/day-hour:minute format. For example: 2009/10/03-00:43	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Month	This variable returns the numeric value of the month from the end time date field. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Minute	This variable returns the minute in a two-digit format. For example: 02	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
DateValue	This variable returns the date in the year/month/day format. For example: 2009/10/03	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Hour	This variable returns the hour in a two-digit format. For example: 02	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Day	This variable returns the day in a two-digit format. For example: 03	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
EndTimeValue	This variable returns the hour and minute in the hour:minute format. For example: 15:59	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Year	This variable returns the year. For example: 2002	Global Variable	ArcSight Foundation/Variables Library/Timestamp Formats/
Cases	This resource has no description.	Field Set	ArcSight Foundation/Workflow/Active Channels/
Case Owner Value is null''	This filter identifies the Device Custom String4 field in active list entry expired audit events for the case escalation active list where the owner of the case is not present.	Filter	ArcSight Foundation/Workflow/Conditional Variable Filters/

Resource	Description	Type	URI
Single-digit Minute	This filter supports the Minute variable by checking the end time to see if it is a single or double digit minute. The Minute variable prepends 0 to minutes with a single digit, so that the format is always mm.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Case Events	This filter identifies events that are related to creating and updating cases.	Filter	ArcSight Foundation/Workflow/
Single-digit Day	This filter identifies the Day variable by checking the end time to see if it is a single or double digit day. The Day variable prepends 0 to days with a single digit, so that the format is always DD (for example, the 1st displays as 01 instead of 1).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Single-digit Hour	This filter supports the Hour variable by checking the end time to see if it is a single or double digit hour. The Hour variable prepends 0 to hours with a single digit, so that the format is always MM (for example, 7:00 displays as 07 instead of 7).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Case Monitoring Entry Expiration	This filter identifies audit events for the case escalation active list where a case entry has expired (meets the TTL condition).	Filter	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case File Type	This filter identifies events in which the File Type field is Case.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Single-digit Month	This filter supports the Month variable by checking the end time to see if it is a single or double digit month. The Month variable prepends 0 to months with a single digit, so that the format is always MM (for example, July displays as 07 instead of 7).	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Timestamp/
Recently Closed Cases	This query on a case tracking session list selects the most recently closed cases for display in a query viewer. After a case is closed, if it is further modified, there may be multiple entries depending on the modifications. The Time Closed column shows the most recent modification of the closed case, which might not be the time when the case was initially closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/

Resource	Description	Type	URI
Average Time to Case Resolution - By User	This query returns the case owner and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Final Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Final.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/
Open Cases Details	This query returns case information for cases where the stage is not closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/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/Workflow/Case Tracking and Escalation/Case Stages/
Open Cases by Associated Impact (Chart)	This query returns the number of open cases in the various associated impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Cases Open by Stage (Chart)	This query searches the cases for open cases and counts the number of them at each stage. Note: The stage for an open case is not Closed.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/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/Workflow/Case Tracking and Escalation/Case Stages/
TodaysCases'	This query returns the display ID, name, creator, ticket type, stage and operational impact, ordered by operational impact, of all cases created so far today that are not system cases.	Query	ArcSight Foundation/Workflow/Operational Summaries/
All Cases	This query returns the name, creator, ticket type, stage, security classification, and consequence severity, ordered by ticket type and stage, of all cases that are not system cases.	Query	ArcSight Foundation/Workflow/Details/
Open Cases by Consequence Severity (Chart)	This query returns the number of open cases in the various consequence severity ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
Initial Stage Cases by Owner (Chart)	This query counts the number of cases for each owner where the stage is Initial.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Stages/

Resource	Description	Type	URI
Average Time to Case Resolution - By Severity	This query returns the consequence severity and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Average Time to Case Resolution - By Day	This query returns the day of the week and the average time to resolve cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Maximum Time to Case Resolution - By User	This query returns case statistics for cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Open Cases by Operational Impact (Chart)	This query returns the number of open cases in the various operational impact ratings.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/
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/Workflow/Case Tracking and Escalation/Case History/
Maximum Time to Case Resolution - By User Chart	This query returns case statistics for cases closed during the previous seven days.	Query	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/Case Resolution Times/
Open Cases	This query returns the name, creator, ticket type, stage, security classification, consequence severity, create time, modification time, and attack target, ordered by ticket type and stage, of all cases that are not system cases and not in the Closed Stage.	Query	ArcSight Foundation/Workflow/Details/
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.	Session List	ArcSight Foundation/Workflow/Case Tracking and Escalation/
Case History Data	This trend stores case information from audit events resulting from case audit events for case history reporting.	Trend	ArcSight Foundation/Workflow/Case Tracking and Escalation/Case History/

Event Annotations and Tracking

The Event Annotations and Tracking resources provide analysts and team leaders with views of the events assigned to them for investigation or to be assigned.

Resources

The following table lists all the resources in the Event Annotations and Tracking resource group and any dependant resources.

Table 3-2 Resources in the Event Annotations and Tracking Group

Resource	Description	Type	URI
Monitor Resources			
YesterdaysAssignedEvents'	The active channel shows events assigned yesterday. The active channel displays events occurring since midnight of the previous day up to midnight of the day the channel was opened. A filter prevents the channel from showing correlated events. The active channel shows only events that are not in the Closed stage and are assigned to a user.	Active Channel	ArcSight Foundation/Workflow/
Assigned Events	This active channel shows events assigned in the past eight hours. A filter prevents the channel from showing correlated events. The active channel shows only events that are not in the Closed stage and are assigned to a user.	Active Channel	ArcSight Foundation/Workflow/
My Open Events	This active channel shows events received since the beginning of the week. The channel displays events received since the beginning of the week up to the time the channel was opened. A filter prevents the channel from showing correlated events. It shows only events that are not in the Closed stage and are assigned to the current user.	Active Channel	ArcSight Foundation/Workflow/
My Live Events	This active channel shows events assigned to me over the last two hours. The channel includes a sliding window that always displays events occurring over the last two hours. A filter prevents the channel from showing correlated events. The active channel shows only events that are not in the Closed stage and are assigned to the current user.	Active Channel	ArcSight Foundation/Workflow/

Resource	Description	Type	URI
Queued Events Previous Night Shift	This active channel shows events received yesterday between 4:00 p.m. and midnight. A filter prevents the channel from showing correlated events. The active channel shows only events that are in the Queued stage.	Active Channel	ArcSight Foundation/Workflow/
My Events Today	This active channel shows events assigned to me today. The active channel displays events occurring since midnight of the day the channel was up to the time the channel was opened. A filter prevents the channel from showing correlated events. The active channel shows only events that are not in the Closed stage and are assigned to the current user.	Active Channel	ArcSight Foundation/Workflow/
Queued Events Previous Day	This active channel shows events received during the previous day. A filter prevents the channel from showing correlated events. The active channel shows only events that are in Queued stage.	Active Channel	ArcSight Foundation/Workflow/
Live Queued Events	This active channel shows events received within the last two hours that have not been reviewed. A filter prevents the channel from showing correlated events. The active channel shows only events that are in Queued stage.	Active Channel	ArcSight Foundation/Workflow/
Queued Events Previous Morning Shift	This active channel shows events received yesterday between 12:00 a.m. and 8:00 a.m. A filter prevents the channel from showing correlated events. The active channel shows only events that are in the Queued stage.	Active Channel	ArcSight Foundation/Workflow/
Queued Events Previous Daytime Shift	This active channel shows events received yesterday between 8:00 a.m. and 4:00 p.m. A filter prevents the channel from showing correlated events. The active channel shows only events that are in Queued stage.	Active Channel	ArcSight Foundation/Workflow/
Library Resources			
Annotation-MgrRcpt	This resource has no description.	Field Set	ArcSight System/Event Field Sets/Active Channels
Assigned Events	This filter identifies events that have been assigned to a user.	Filter	ArcSight Foundation/Workflow/
ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types

Resource	Description	Type	URI
Closed Events	This filter identifies non-internal, non-correlated events that are in the closed stage.	Filter	ArcSight Foundation/Workflow/
Non-ArcSight Internal Events	This resource has no description.	Filter	ArcSight System/Event Types
Not Correlated and Not Closed	This resource has no description.	Filter	ArcSight System/Event Types
ASM Events	This resource has no description.	Filter	ArcSight System/Event Types
Closed	This stage indicates that the event is closed.	Stage	/
Queued	This stage indicates that event has not been inspected.	Stage	/

Notification Tracking

The Notification Tracking resources provide insight into how notifications are being handled by the teams that are tasked with responding to them.

Resources

The following table lists all the resources in the Notification Tracking resource group and any dependant resources.

Table 3-3 Resources in the Notification Tracking Group

Resource	Description	Type	URI
Monitor Resources			
Notification Events	This active channel shows notification audit events received within the past eight hours.	Active Channel	ArcSight Foundation/Workflow/Cases and Notifications/
Level 3 Notifications - Weekly Trend	This report shows a chart of notification severities, a chart of notification destination groups, and a table showing the combined details and event names of the notifications charted by day for the previous week.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notifications By Acknowledgement Status	This report displays a chart and a table showing the counts of the notifications created yesterday, by acknowledgment, status, and ArcSight severity.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Statistics Summary	This report shows three charts and a table. Two of the three charts show notifications by escalation level and acknowledgement status, the third shows notifications with an escalation level of 3 and the destination groups to which they were sent. The table shows notification details, such as the destination group, the escalation level, acknowledgement status, and the creation time and notification event name.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications - Quarterly Trend	This report shows a chart of notification severities, a chart of notification destination groups, and a table showing the combined details and event names of the notifications charted by week for the last three months.	Report	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Status by User Overview - Quarterly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level for each month over the last three months. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
All Level 3 Notifications	This report displays a table showing the event name, group name, create time, and ArcSight severity of all notifications with escalation level 3.	Report	ArcSight Foundation/Workflow/Details/
Notification Status by User Overview - Monthly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level per week for the previous month. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Action Events	This report displays a table of the audit events related to notifications. The table includes the audit event name, the severity, the time, the acknowledgement status (a variable), the user acknowledging or resolving the notification (a variable), the destination group (a variable) and the notification resource (a variable). Not all notification audit events populate all of these fields. Note: This report does not populate all values when running in Turbo Mode Fastest. Device Custom fields (used by the variables in this report's query) are not included in Turbo Mode Fastest.	Report	ArcSight Foundation/Workflow/Details/
Notification Status Report	This report displays a table showing the notifications generated for each notification (Destination) group, including the notification creation time, escalation level, and acknowledgement status.	Report	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Escalation Level Event Overview - Quarterly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level for the quarter. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Unacknowledged Level 3 Notifications	This report displays a table showing all the notifications by ArcSight severity (including creation times and the notification (Destination) groups responsible for them) that have not been acknowledged and are at escalation level 3.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status - Quarterly Trend	This report shows a chart of notification acknowledgement status, a chart of notification severities, a chart of notification destination groups, a chart of notification escalation levels, and a table showing the combined details of the notifications charted for the previous three months.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Event Overview - Weekly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level per day. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Overview	This report displays a chart showing the number of notifications, grouped by ArcSight severity, at each escalation level.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status - Weekly Trend	This report shows a chart of notification acknowledgement status, a chart of notification severities, a chart of notification destination groups, a chart of notification escalation levels, and a table showing the combined details of the notifications charted for the previous week.	Report	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Status by User Overview - Weekly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level per day for the previous week. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status - Monthly Trend	This report shows a chart of notification acknowledgement status, a chart of notification severities, a chart of notification destination groups, a chart of notification escalation levels, and a table showing the combined details of the notifications charted for the previous month.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications - Monthly Trend	This report shows a chart of notification severities, a chart of notification destination groups, and a table showing the combined details and event names of the notifications charted by week for the previous month.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Event Overview - Monthly Trend	This report displays a table and chart of notification escalation events from the Notification Events trend. The chart shows a summary of the number of events for each escalation level per week. The table shows the details of the escalation events.	Report	ArcSight Foundation/Workflow/Operational Summaries/
Library Resources			
Notifications	This field set tracks events related to the sending and acknowledgement of notifications.	Field Set	ArcSight Foundation/Workflow/Active Channels/
Notification Event has Rule Name	This filter identifies notification events that have a Device Custom String 3 label set as Rule Name.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has User Name	This filter identifies notification events that have an attacker user name to represent the user who acknowledged or resolved a notification.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Destination Group	This filter identifies notification events that have a Device Custom String 4 label set as Group.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/

Resource	Description	Type	URI
Notification Event has Configuration Resource	This filter identifies notification events that have a Device Custom String 2 label set as Configuration Resource.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Event has Acknowledgement Status	This filter identifies notification events that have a Device Custom String 6 label set as Acknowledgement Status.	Filter	ArcSight Foundation/Common/Conditional Variable Filters/Case and Notification/
Notification Events	This filter identifies events that are related to sending and acknowledging notifications.	Filter	ArcSight Foundation/Workflow/
All Events	This filter identifies all events.	Filter	ArcSight System/Core
Notifications by Destination Group Chart - Quarterly Trend	This query returns the month, destination group, and the sum of the count of the events in the Notification trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Severity Chart - Monthly Trend	This query returns the week, severity, and sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications - Trend	This query returns the notification creation time, acknowledgement status, ArcSight severity, the name of the event that caused the notification to be sent, the destination group name, and the number of notifications sent. This query populates the Notifications trend.	Query	ArcSight Foundation/Workflow/Operational Summaries/Trends/
Notifications By Acknowledgement Status Chart	This query returns the acknowledgement status, ArcSight severity, and number of notifications (count of Notification ID), of all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications - Quarterly Trend	This query returns the month, destination group, severity, acknowledgement status, event name, and the sum of the count of the events in the Notifications trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Level 3 Notifications by Destination Group - Quarterly Trend	This query returns the month, destination group, and the sum of the count of the events in the Notifications trend where the Notification Escalation Level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications - Weekly Trend	This query returns the day, destination group, severity, acknowledgement status, event name, and the sum of the count of the events in the Notification trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Events Overview Chart - Weekly Trend	This query returns the day, escalation level, and the sum of the count of the events in the Notification trend where the escalation level is not null (there is a value for the Escalation Level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status Report	This query returns the group name, event name, creation time, escalation level, and acknowledgement status, ordered by the creation time, for all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Severity Chart - Quarterly Trend	This query returns the month, severity, and the sum of the count of the events in the Notification trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications By Acknowledgement Status	This query returns the acknowledgement status, ArcSight severity, and the number of notifications (count of Notification ID), for all notifications created yesterday.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications by Destination Group - Weekly Trend	This query returns the day, destination group, and the sum of the count of the events in the Notifications trend where the Notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications Overview Chart	This query retrieves notification information (the destination group, severity, and count), for all notifications with an escalation level of 3.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notifications Status Table - Monthly Trend	This query returns the week, escalation level, acknowledgement status, severity, destination group, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications by Severity - Monthly Trend	This query returns the week, severity, and the sum of the count of the events in the Notification trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Severity Chart - Weekly Trend	This query returns the day, severity, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Acknowledgement Status Chart - Quarterly Trend	This query returns the month, acknowledgement status, and sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Acknowledgement Status Chart - Weekly Trend	This query returns the day, acknowledgement status, and the sum of the count of the events in the Notification trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Action Events	This query returns audit events related to notifications. The query makes extensive use of variables and Device Custom Strings to display relevant information. Note: Device Custom fields are not included in Turbo Mode Fastest.	Query	ArcSight Foundation/Workflow/Details/
Notifications Status Table - Quarterly Trend	This query returns the month, escalation level, acknowledgement status, severity, destination group, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Escalation Level Events Overview Chart - Quarterly Trend	This query returns the month, escalation level, and the sum of the count of the events in the Notification Events trend where the Escalation Level is not null (there is a value for the Escalation Level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status by User Table - Quarterly Trend	This query returns the user, month, acknowledgement status, destination group, notification resource, and the sum of the count of the events in the Notifications trend where the acknowledgement status is not null (there is a value for the Acknowledgement Status field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Overview	This query returns the escalation level, ArcSight severity, and the number of notifications (count of Notification IDs), ordered by escalation level and ArcSight severity, of all notifications.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Events Overview Table - Quarterly Trend	This query returns the month, escalation level, destination group, acknowledgement status, notification resource, and the sum of the count of the events in the Notifications trend where the escalation level is not null (there is a value for the escalation level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications by Severity - Weekly Trend	This query returns the day, severity, and the sum of the count of the events in the Notifications trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications by Destination Group - Monthly Trend	This query returns the week, destination group, and the sum of the count of the events in the Notifications trend where the Notification Escalation Level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Acknowledgement Status Chart - Monthly Trend	This query returns the week, acknowledgement status, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Status by User Chart	This query retrieves the user, acknowledgement status, and the sum of the count of the events in the Notification Events trend where the acknowledgement status is not null (there is a value for the Acknowledgement Status field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
All Level 3 Notifications	This query returns the event name, group name, create time, escalation level, and ArcSight severity, ordered by creation time, of all notifications with an escalation level of 3.	Query	ArcSight Foundation/Workflow/Details/
Notification Status by User Table - Weekly Trend	This query returns the user, day, acknowledgement status, destination group, notification resource, and the sum of the count of the events in the Notification Events trend where the acknowledgement status is not null (there is a value for the Acknowledgement Status field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Events Overview Chart - Monthly Trend	This query returns the week, escalation level, and the sum of the count of the events in the Notification Events trend where the escalation level is not null (there is a value for the Escalation Level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Destination Group Chart - Weekly Trend	This query returns the day, destination group, and the sum of the count of the events in the Notification trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Escalation Level Events Overview Table - Weekly Trend	This query returns the day, escalation level, destination group, acknowledgement status, notification resource, and the sum of the count of the events in the Notification trend where the escalation level is not null (there is a value for the Escalation Level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications Status Table - Weekly Trend	This query returns the day, escalation level, acknowledgement status, severity, destination group, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notifications by Escalation Level Chart - Quarterly Trend	This query returns the month, escalation level, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Escalation Level Chart - Monthly Trend	This query returns the week, escalation level, and the sum of the count of the events in the Notifications trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Events - Trend	This query returns the acknowledgement status, destination group, escalation level, notification resource, rule name, user, and the number of notification events where the event matches the Notification Events filter.	Query	ArcSight Foundation/Workflow/Operational Summaries/Trends/
Level 3 Notifications by Severity - Quarterly Trend	This query returns the month, severity and the sum of the count of the events in the Notifications trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Destination Group Chart - Monthly Trend	This query returns the week, destination group, and the sum of the count of the events in the Notification trend where the notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications by Escalation Level Chart - Weekly Trend	This query returns the day, escalation level, and the sum of the count of the events in the trend where the Notification was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notification Status by User Table - Monthly Trend	This query returns the user, week, acknowledgement status, destination group, notification resource, and the sum of the count of the events in the Notification Events trend where the Acknowledgement Status is not null (there is a value for the Acknowledgement Status field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Unacknowledged Level 3 Notifications	This query returns the event name, create time, ArcSight severity and group name, of all notifications with an escalation level of 3 and an acknowledgement status that is neither Acknowledged or Resolved.	Query	ArcSight Foundation/Workflow/Operational Summaries/

Resource	Description	Type	URI
Notification Escalation Level Events Overview Table - Monthly Trend	This query on the Notification Events trend selects the week, escalation level, destination group, acknowledgement status, notification resource, and the sum of the count of the events in the trend where the escalation level is not null (there is a value for the Escalation Level field).	Query	ArcSight Foundation/Workflow/Operational Summaries/
Level 3 Notifications - Monthly Trend	This query returns the week, destination group, severity, acknowledgement status, event name, and the sum of the count of the events in the Notification trend where the notification escalation level is 3 and it was created within the time range specified.	Query	ArcSight Foundation/Workflow/Operational Summaries/
Notifications	This trend returns the notification creation time, acknowledgement status, ArcSight severity, the name of the event that caused the notification to be sent, the destination group name, and the number of notifications sent.	Trend	ArcSight Foundation/Workflow/Operational Summaries/
Notification Events	This trend returns the acknowledgement status, destination group, escalation level, notification resource, rule name, user, and the number of notification events sent on a daily basis.	Trend	ArcSight Foundation/Workflow/Operational Summaries/

Index

G

H

I

L

M

N

O

P

Q

R

S

T

U

Y