

Standard Content Guide

Workflow

ArcSight ESM 6.5c

October 11, 2013



Copyright © 2013 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Follow this link to see a complete statement of copyrights and acknowledgements:

<http://www.hpenterprisesecurity.com/copyright>

Contact Information

| | |
|------------------------------|---|
| Phone | A list of phone numbers is available on the HP ArcSight Technical Support page: http://www8.hp.com/us/en/software-solutions/software.html?compURI=1345981#.URitMaVwpWI . |
| Support Web Site | http://support.openview.hp.com |
| Protect 724 Community | https://protect724.arcsight.com |

Revision History

| Date | Product Version | Description |
|-------------|--|-----------------------------|
| 10/11/2013 | Workflow content for ArcSight ESM 6.5c | Final revision for release. |

Contents

| | |
|---|-----------|
| Chapter 1: Workflow Overview | 5 |
| What is Standard Content | 5 |
| Standard Content Packages | 7 |
| Workflow Content | 7 |
| Chapter 2: Installation and Configuration | 9 |
| Installing the Workflow Package | 9 |
| Configuring Workflow Content | 10 |
| Modeling the Network | 10 |
| Categorizing Assets | 11 |
| Enabling Rules | 11 |
| Ensuring Filters Capture Relevant Events | 12 |
| Configuring Notification Destinations | 12 |
| Configuring Notifications and Cases | 12 |
| Scheduling Reports | 12 |
| Configuring Trends | 13 |
| Chapter 3: Workflow Content | 15 |
| Case Tracking and Escalation | 16 |
| Configuring the Case Tracking and Escalation Resource Group | 16 |
| Resources | 16 |
| Event Annotations and Tracking | 25 |
| Resources | 25 |
| Notification Tracking | 28 |
| Resources | 28 |
| Index | 41 |

Chapter 1

Workflow Overview

This chapter discusses the following topics.

["What is Standard Content" on page 5](#)

["Standard Content Packages" on page 7](#)

["Workflow Content" on page 7](#)

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.

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

Standard content consists of the following:

- **ArcSight Core Security** content is installed automatically with the ArcSight Manager and consists of key resources for monitoring Microsoft Windows, firewall, IPS and IDS, NetFlow, and other essential security information.
- **ArcSight Administration** content contains several packages that provide statistics about the health and performance of ArcSight products.
 - ◆ ArcSight Administration is installed automatically with the ArcSight Manager and is essential for managing and tuning the performance of content and components.
 - ◆ ArcSight Admin DB CORR is installed automatically with the ArcSight Manager for ArcSight ESM with CORR- (Correlation Optimized Retention and Retrieval) Engine and provides information on the health of the CORR-Engine.
 - ◆ ArcSight Content Management is an optional package that shows information about content package synchronization with the ESM Content Management feature. The information includes a history of content packages synchronized from a primary ESM source to multiple ESM destinations, and any common issues or errors encountered. You can install this package during ArcSight ESM installation or from the ArcSight Console any time after installation.

- ◆ ArcSight Search Filters is installed automatically with the ArcSight Manager for use in the ArcSight Command Center. You cannot edit or use these filters in the ArcSight Console. For information about the search filters, refer to the ArcSight Command Center User's Guide.



The ArcSight Admin DB CORR and ArcSight Search Filters content packages are installed automatically when you perform a new ArcSight ESM installation. However, when you upgrade your ArcSight ESM system, these content packages are not installed automatically. You can install these packages from the ArcSight Console any time after upgrade by right-clicking the package on the Packages tab in the Navigator and selecting Install Package.

Refer to the ArcSight ESM Upgrade Guide for information about upgrading ArcSight ESM.

- **ArcSight System** content is installed automatically with the ArcSight 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 Foundation** content (such as Cisco Monitoring, Configuration Monitoring, Intrusion Monitoring, IPv6, NetFlow Monitoring, Network Monitoring, and Workflow) 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. You can install a Foundation during ArcSight ESM installation or from the ArcSight Console any time after installation.
- **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 content is 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 content is 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.
 - ◆ Monitoring Support Data content is a set of active lists that store mapping information for HTTP return status code classes, Cisco firewall syslog message types, and encoded logon types.
 - ◆ Network filters content is a set of filters required by ArcSight Administration and certain ArcSight Foundations, such as Intrusion Monitoring and Network Monitoring.



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

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.

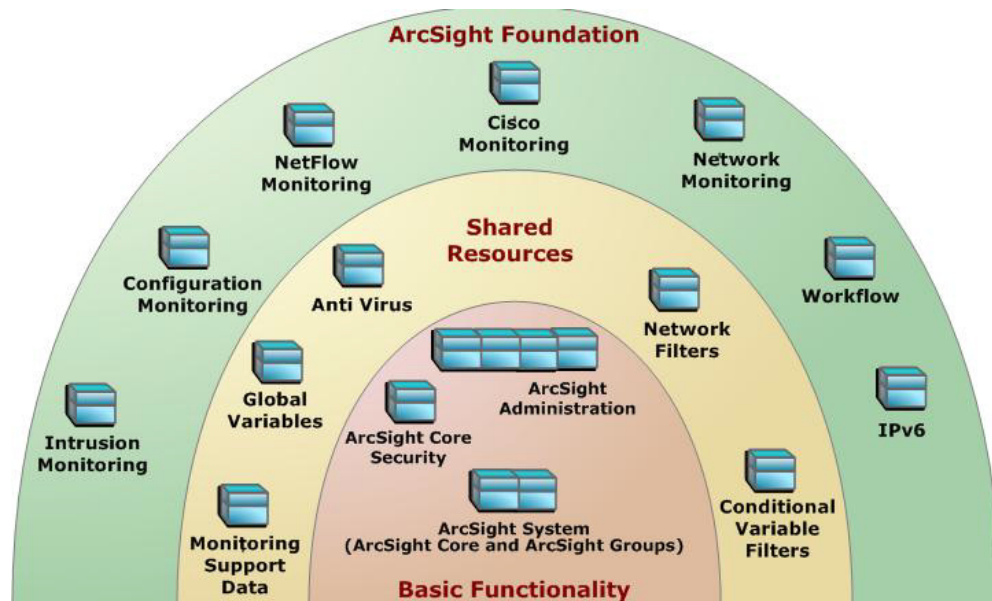


Figure 1-1 The ArcSight Core Security, ArcSight Administration, and ArcSight System packages at the base provide content required for basic ArcSight functionality. The common packages in the center contain shared resources that support multiple packages. The packages shown on top are ArcSight Foundations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

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



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.

ArcSight uses notifications and cases to enable security operators to coordinate and prioritize response to security events. Qualifying events in the other Foundation packages trigger notifications and cases that get escalated through the 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 notifications, cases, and incident response workflow, refer to the ESM 101 guide.

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

Chapter 2

Installation and Configuration

This chapter discusses the following topics.

[“Installing the Workflow Package” on page 9](#)

[“Configuring Workflow Content” on page 10](#)

Installing the Workflow Package

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

If you opted to exclude a Foundation package during ESM installation, the package is *imported* into the Packages tab in the Navigator panel automatically, but is not available in the resource view. The package icon in the package view appears 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 On the Navigator panel Packages tab, 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 On the Navigator Panel Packages tab, 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 Packages tab, and can be re-installed at another time.

To delete a package and remove it from the ArcSight Console and the ArcSight Database:

- 1** On the Navigator Panel Packages tab, navigate to the package you want to delete.
- 2** Right-click the package and select **Delete Package**.
- 3** When prompted for confirmation, click **Delete**.

The package is removed from the Navigator panel Packages tab.

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” on page 10](#)
- [“Categorizing Assets” on page 11](#)
- [“Enabling Rules” on page 11](#)
- [“Ensuring Filters Capture Relevant Events” on page 12](#)
- [“Configuring Notification Destinations” on page 12](#)
- [“Configuring Notifications and Cases” on page 12](#)
- [“Scheduling Reports” on page 12](#)
- [“Configuring Trends” on page 13](#)

Modeling the Network

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

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

Categorizing Assets

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

| Asset Category | Description |
|---|--|
| /Site Asset Categories/ Address Spaces/Protected | <p>Categorize all assets (or the zones to which the assets belong) that are internal to the network with this asset category.</p> <p>Internal Assets are assets inside the company network. Assets that are not categorized as internal to the network are considered to be external. Make sure that you also categorize assets that have public addresses but are controlled by the organization (such as web servers) as <i>Protected</i>.</p> <p>Note: Assets with a private IP address (such as 192.168.0.0) are considered <i>Protected</i> by the system, even if they are not categorized as such.</p> |
| /System Asset Categories/ Criticality/High | <p>Categorize all assets that are considered <i>critical</i> to protect (including assets that host proprietary content, financial data, cardholder data, top secret data, or perform functions critical to basic operations) with this asset category.</p> <p>The asset categories most essential to basic event processing are those used by the Priority Formula to calculate the criticality of an event. Asset criticality is one of the four factors used by the Priority Formula to generate an overall event priority rating.</p> |
| /System Asset Categories/ Criticality/Very High | See /System Asset Categories/Criticality/High |

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

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

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

Enabling Rules

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 and all the rules are enabled.

To 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 disable.
- 3 Right-click the rule and select **Disable 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 SOC Operators notification group. 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 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 SOC Operators 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.

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.

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**.



Caution

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 back fills the data from that time. For example, if you enable the trend six months after the first install, these trends try to get all the data for the last six months, which might cause performance problems, overwhelm system resources, or cause the trend to fail if that event data is not available.

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.

Configuring the Case Tracking and Escalation Resource Group

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 that Support 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/Case Tracking and Escalation/ |
| 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/ |

| Resource | Description | Type | URI |
|--|--|--------------|--|
| Open Cases by Stage | This query viewer shows the number of open cases at each stage. | Query Viewer | ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/Case Status Dashboard/ |
| 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 shows 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/ |

| Resource | Description | Type | URI |
|---|---|--------------|--|
| 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/ |
| 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 shows 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 shows 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 shows the average time taken to resolve cases that have been closed by each user during the reporting period. | Report | ArcSight Foundation/Workflow/Operational Summaries |
| Average Time to Case Resolution - By Severity | This report shows the severity and average time to resolution of all cases closed during the reporting period. | Report | ArcSight Foundation/Workflow/Executive Summaries |
| Case Stages Overview | This report shows the number of open cases in each stage by owner and lists 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 shows the average time taken to resolve cases closed for each day of the reporting period. | Report | ArcSight Foundation/Workflow/Operational Summaries |
| Case Status Overview | This report shows the number of open cases by stage, consequence severity, operational impact, and associated impact. A table shows a list of recently closed cases. | Report | ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/ |
| Open Cases | This report shows the name, creator, ticket type, stage, security classification, consequence severity, creation time, modification time, and attack target of all the open, non-system cases in the system. | Report | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| Cases Created Today | This report shows the cases that have been generated since midnight this morning. | Report | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| All Cases | This report shows the name, creator, ticket type, stage, security classification, and consequence severity of all the non-system cases in the system. | Report | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| Max Time to Case Resolution - By User | This report shows 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/Operational Summaries |
| 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. | Rule | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| 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/ |

| Resource | Description | Type | URI |
|----------------------------|--|-----------------|--|
| 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. | 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. | 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. | Rule | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| 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 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 |

| Resource | Description | Type | URI |
|--------------------------|--|-----------------|---|
| 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: 00:10 | 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 field set contains several fields related to case information associated with case management events. | 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/Case Tracking and Escalation/ |
| 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/Conditio nal Variable Filters/Timestamp |
| Case Events | This filter identifies events related to creating and updating cases. | Filter | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |

| Resource | Description | Type | URI |
|---|--|--------|--|
| 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 HH (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 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 | ArcSight Foundation/Workflow/Case Tracking and Escalation/Case Status/ |
| 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/ |

| Resource | Description | Type | URI |
|---|--|-------|---|
| 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/ |
| Cases Created Today | This query returns all cases created so far today that are not system cases. | Query | ArcSight Foundation/Workflow/Case Tracking and Escalation/ |
| 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/Case Tracking and Escalation/ |
| 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/ |
| 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/ |

| Resource | Description | Type | URI |
|---|--|-----------------|---|
| 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/Case Tracking and Escalation/ |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |
| Four Charts and Table Landscape | This template is designed to show four charts and a table. The orientation is landscape. | Report Template | ArcSight System/4 Charts/With Table |
| Simple Table Landscape | This template is designed to show a table. The orientation is landscape. | Report Template | ArcSight System/1 Table |
| Chart and Table Portrait | This template is designed to show one chart and a table. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With Table |
| Case Tracking | This session list contains case history information, monitoring the changes of the attributes in a case as it flows through 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 that Support the Event Annotations and Tracking Group

| Resource | Description | Type | URI |
|-----------------------------|--|----------------|----------------------------------|
| Monitor Resources | | | |
| Yesterday's Assigned Events | 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. 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/ |
| 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. 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 the 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 the 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 the 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 filter selects events that are internal events generated by the ArcSight ESM system. | Filter | ArcSight System/Event Types |
| Closed Events | This filter identifies non-internal, non-correlated events that are in the closed stage. | Filter | ArcSight Foundation/Workflow/ |

| Resource | Description | Type | URI |
|-------------------------------|--|--------|-----------------------------|
| Non-ArcSight Internal Events | This filter selects events that are not internal events generated by the ArcSight ESM system. | Filter | ArcSight System/Event Types |
| Not Correlated and Not Closed | This resource has no description. | Filter | ArcSight System/Event Types |
| ASM Events | This filter selects ArcSight System Monitoring events generated by the local ESM system (in an hierarchical deployment). | Filter | ArcSight System/Event Types |
| Closed | This stage indicates that the event is closed. | Stage | /All Stages |
| Queued | This stage indicates that the event has not been inspected. | Stage | /All Stages |

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 that Support 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/System Notifications and Escalation/ |
| 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 Acknowledgment Status | This report displays a chart and a table showing the counts of the notifications created yesterday, by acknowledgment, status, and ArcSight severity. | Report | ArcSight 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 groups responsible for them (including creation times and the notification (destination) 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/System Notifications and Escalation/ |
| All Events | This filter matches 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 Acknowledge 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/ |
| Simple Table Portrait | This template is designed to show a table. The orientation is portrait. | Report Template | ArcSight System/1 Table |
| Four Charts and Table Landscape | This template is designed to show four charts and a table. The orientation is landscape. | Report Template | ArcSight System/4 Charts/With Table |
| Simple Chart Portrait | This template is designed to show one chart. The orientation is portrait. | Report Template | ArcSight System/1 Chart/Without Table |
| Chart and Table Landscape | This template is designed to show one chart and a table. The orientation is landscape. | Report Template | ArcSight System/1 Chart/With Table |
| Simple Table Landscape | This template is designed to show a table. The orientation is landscape. | Report Template | ArcSight System/1 Table |
| Chart and Table Portrait | This template is designed to show one chart and a table. The orientation is portrait. | Report Template | ArcSight System/1 Chart/With Table |
| Two Charts One Table Portrait | This template is designed to show two charts and a table. The orientation is portrait. | Report Template | ArcSight System/2 Charts/With Table |
| Three Charts and Table Landscape | This template is designed to show three charts and a table. The orientation is landscape. | Report Template | ArcSight System/3 Charts/With Table |
| 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/ |

| Resource | Description | Type | URI |
|---------------------|--|-------|---|
| 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

A

active channels

- Assigned Events 25
- Case Events 16
- Live Queued Events 26
- My Events Today 26
- My Live Events 25
- My Open Events 25
- Notification Events 28
- Queued Events Previous Day 26
- Queued Events Previous Daytime Shift 26
- Queued Events Previous Morning Shift 26
- Queued Events Previous Night Shift 26
- Yesterday'sAssignedEvents 25

active lists

- Case Escalation 20
- general configuration 12

All Cases query 23

All Cases report 19

All Events filter 32

All Level 3 Notifications query 36

All Level 3 Notifications report 29

Annotation-MgrRcpt field set 26

ArcSight Administration overview 5

ArcSight Core Security overview 5

ArcSight Foundations overview 6

ArcSight Internal Events filter 26

ArcSight System overview 6

ASM Events filter 27

Assigned Events active channel 25

Assigned Events filter 26

Average Time to Case Resolution - By Day query 23

Average Time to Case Resolution - by Day query viewer 17

Average Time to Case Resolution - By Day report 19

Average Time to Case Resolution - By Severity query 23

Average Time to Case Resolution - by Severity query viewer 18

Average Time to Case Resolution - By Severity report 18

Average Time to Case Resolution - By User query 22

Average Time to Case Resolution - by User query viewer 18

Average Time to Case Resolution - By User report 18

C

Case Deleted rule 19

Case Escalation active list 20

Case Escalation rule 20

Case Events active channel 16

Case Events filter 21

Case File Type filter 22

Case History Data trend 24

Case Investigation Started rule 20

Case Monitoring Entry Expiration filter 22

Case Owner Value is null filter 21

Case Stages dashboard 16

Case Stages Overview report 18

Case Status dashboard 16

Case Status Overview report 19

Case Times to Resolution dashboard 16

Case Tracking and Escalation resource group 16

Case Tracking session list 24

Cases Created Today query 23

Cases Created Today report 19

Cases field set 21

Cases Open by Stage (Chart) query 23

Chart and Table Landscape report template 38

Chart and Table Portrait report template 24, 38

Closed Events filter 26

Closed stage 27

configuration

active lists 12

content packages 7

D

dashboards

Case Stages 16

Case Status 16

Case Times to Resolution 16

DateTime global variable 20

DateValue global variable 21

Day global variable 21

E

EndTimeValue global variable 21

Event Annotations and Tracking resource group 25

F

field sets

Annotation-MgrRcpt 26

Cases 21

Notifications 31

filters

All Events 32

ArcSight Internal Events 26

ASM Events 27

Assigned Events 26

Case Events 21

Case File Type 22

- Case Monitoring Entry Expiration 22
- Case Owner Value is null 21
- Closed Events 26
- Non-ArcSight Internal Events 27
- Not Correlated and Not Closed 27
- Notification Event has Acknowledgement Status 32
- Notification Event has Configuration Resource 32
- Notification Event has Destination Group 31
- Notification Event has Rule Name 31
- Notification Event has User Name 31
- Notification Events 32
- Single-digit Day 22
- Single-digit Hour 22
- Single-digit Minute 21
- Single-digit Month 22
- Final Stage Cases by Owner (Chart) query 22
- Final Stage Cases by Owner query viewer 17
- Follow-Up Stage Cases by Owner (Chart) query 23
- Follow-Up Stage Cases by Owner query viewer 17
- Four Charts and Table Landscape report template 24, 38

G

- global variables
 - DateTime 20
 - DateValue 21
 - Day 21
 - EndTimeValue 21
 - Hour 21
 - Minute 21
 - Month 21
 - Year 21

H

- Hour global variable 21

I

- Initial Stage Cases by Owner (Chart) query 23
- Initial Stage Cases by Owner query viewer 17

L

- Level 3 Notifications - Monthly Trend query 38
- Level 3 Notifications - Monthly Trend report 31
- Level 3 Notifications - Quarterly Trend query 32
- Level 3 Notifications - Quarterly Trend report 28
- Level 3 Notifications - Weekly Trend query 33
- Level 3 Notifications - Weekly Trend report 28
- Level 3 Notifications by Destination Group - Monthly Trend query 35
- Level 3 Notifications by Destination Group - Quarterly Trend query 33
- Level 3 Notifications by Destination Group - Weekly Trend query 33
- Level 3 Notifications by Severity - Monthly Trend query 34
- Level 3 Notifications by Severity - Quarterly Trend query 37
- Level 3 Notifications by Severity - Weekly Trend query 35
- Level 3 Notifications Overview Chart query 33
- Live Queued Events active channel 26

M

- Max Time to Case Resolution - By User report 19
- Maximum Time to Case Resolution - By User Chart query 24
- Maximum Time to Case Resolution - By User query 24
- Maximum Time to Case Resolution - by User query viewer 18
- Minute global variable 21
- Monitor New Case rule 20
- Month global variable 21
- My Events Today active channel 26
- My Live Events active channel 25
- My Open Events active channel 25

N

- Non-ArcSight Internal Events filter 27
- Not Correlated and Not Closed filter 27
- Notification Action Events query 34
- Notification Action Events report 29
- Notification Escalation Level Event Overview - Monthly Trend report 31
- Notification Escalation Level Event Overview - Quarterly Trend report 30
- Notification Escalation Level Event Overview - Weekly Trend report 30
- Notification Escalation Level Events Overview Chart - Monthly Trend query 36
- Notification Escalation Level Events Overview Chart - Quarterly Trend query 35
- Notification Escalation Level Events Overview Chart - Weekly Trend query 33
- Notification Escalation Level Events Overview Table - Monthly Trend query 38
- Notification Escalation Level Events Overview Table - Quarterly Trend query 35
- Notification Escalation Level Events Overview Table - Weekly Trend query 36
- Notification Event has Acknowledgement Status filter 32
- Notification Event has Configuration Resource filter 32
- Notification Event has Destination Group filter 31
- Notification Event has Rule Name filter 31
- Notification Event has User Name filter 31
- Notification Events - Trend query 37
- Notification Events active channel 28
- Notification Events filter 32
- Notification Events trend 39
- Notification Overview query 35
- Notification Overview report 30
- Notification Statistics Summary report 28
- Notification Status - Monthly Trend report 31
- Notification Status - Quarterly Trend report 30
- Notification Status - Weekly Trend report 30
- Notification Status by User Chart query 36
- Notification Status by User Overview - Monthly Trend report 29
- Notification Status by User Overview - Quarterly Trend report 29
- Notification Status by User Overview - Weekly Trend report 31
- Notification Status by User Table - Monthly Trend query 37
- Notification Status by User Table - Quarterly Trend query 35

Notification Status by User Table - Weekly Trend query 36
 Notification Status Report query 33
 Notification Status Report report 29
 Notification Tracking resource group 28
 Notifications - Trend query 32
 Notifications by Acknowledgement Status Chart - Monthly Trend query 35
 Notifications by Acknowledgement Status Chart - Quarterly Trend query 34
 Notifications by Acknowledgement Status Chart - Weekly Trend query 34
 Notifications By Acknowledgement Status Chart query 32
 Notifications By Acknowledgement Status query 33
 Notifications By Acknowledgement Status report 28
 Notifications by Destination Group Chart - Monthly Trend query 37
 Notifications by Destination Group Chart - Quarterly Trend query 32
 Notifications by Destination Group Chart - Weekly Trend query 36
 Notifications by Escalation Level Chart - Monthly Trend query 37
 Notifications by Escalation Level Chart - Quarterly Trend query 37
 Notifications by Escalation Level Chart - Weekly Trend query 37
 Notifications by Severity Chart - Monthly Trend query 32
 Notifications by Severity Chart - Quarterly Trend query 33
 Notifications by Severity Chart - Weekly Trend query 34
 Notifications field set 31
 Notifications Status Table - Monthly Trend query 34
 Notifications Status Table - Quarterly Trend query 34
 Notifications Status Table - Weekly Trend query 36
 Notifications trend 38

O

Open Cases by Associated Impact (Chart) query 23
 Open Cases by Associated Impact query viewer 18
 Open Cases by Consequence Severity (Chart) query 23
 Open Cases by Consequence Severity query viewer 17
 Open Cases by Operational Impact (Chart) query 24
 Open Cases by Operational Impact query viewer 18
 Open Cases by Stage query viewer 17
 Open Cases Details query 23
 Open Cases query 24
 Open Cases query viewer 18
 Open Cases report 19

P

packages
 deleting 10
 installing 9
 uninstalling 9

Q

queries
 All Cases 23
 All Level 3 Notifications 36
 Average Time to Case Resolution - By Day 23
 Average Time to Case Resolution - By Severity 23

Average Time to Case Resolution - By User 22
 Cases Created Today 23
 Cases Open by Stage (Chart) 23
 Final Stage Cases by Owner (Chart) 22
 Follow-Up Stage Cases by Owner (Chart) 23
 Initial Stage Cases by Owner (Chart) 23
 Level 3 Notifications - Monthly Trend 38
 Level 3 Notifications - Quarterly Trend 32
 Level 3 Notifications - Weekly Trend 33
 Level 3 Notifications by Destination Group - Monthly Trend 35
 Level 3 Notifications by Destination Group - Quarterly Trend 33
 Level 3 Notifications by Destination Group - Weekly Trend 33
 Level 3 Notifications by Severity - Monthly Trend 34
 Level 3 Notifications by Severity - Quarterly Trend 37
 Level 3 Notifications by Severity - Weekly Trend 35
 Level 3 Notifications Overview Chart 33
 Maximum Time to Case Resolution - By User 24
 Maximum Time to Case Resolution - By User Chart 24
 Notification Action Events 34
 Notification Escalation Level Events Overview Chart - Monthly Trend 36
 Notification Escalation Level Events Overview Chart - Quarterly Trend 35
 Notification Escalation Level Events Overview Chart - Weekly Trend 33
 Notification Escalation Level Events Overview Table - Monthly Trend 38
 Notification Escalation Level Events Overview Table - Quarterly Trend 35
 Notification Escalation Level Events Overview Table - Weekly Trend 36
 Notification Events - Trend 37
 Notification Overview 35
 Notification Status by User Chart 36
 Notification Status by User Table - Monthly Trend 37
 Notification Status by User Table - Quarterly Trend 35
 Notification Status by User Table - Weekly Trend 36
 Notification Status Report 33
 Notifications - Trend 32
 Notifications By Acknowledgement Status 33
 Notifications By Acknowledgement Status Chart 32
 Notifications by Acknowledgement Status Chart - Monthly Trend 35
 Notifications by Acknowledgement Status Chart - Quarterly Trend 34
 Notifications by Acknowledgement Status Chart - Weekly Trend 34
 Notifications by Destination Group Chart - Monthly Trend 37
 Notifications by Destination Group Chart - Quarterly Trend 32
 Notifications by Destination Group Chart - Weekly Trend 36
 Notifications by Escalation Level Chart - Monthly Trend 37
 Notifications by Escalation Level Chart - Quarterly Trend 37
 Notifications by Escalation Level Chart - Weekly

- Trend 37
- Notifications by Severity Chart - Monthly Trend 32
- Notifications by Severity Chart - Quarterly Trend 33
- Notifications by Severity Chart - Weekly Trend 34
- Notifications Status Table - Monthly Trend 34
- Notifications Status Table - Quarterly Trend 34
- Notifications Status Table - Weekly Trend 36
- Open Cases 24
- Open Cases by Associated Impact (Chart) 23
- Open Cases by Consequence Severity (Chart) 23
- Open Cases by Operational Impact (Chart) 24
- Open Cases Details 23
- Queued Stage Cases by Owner (Chart) 23
- Recently Closed Cases 22
- Trend on Case Audit Events 24
- Unacknowledged Level 3 Notifications 37
- query viewers
 - Average Time to Case Resolution - by Day 17
 - Average Time to Case Resolution - by Severity 18
 - Average Time to Case Resolution - by User 18
 - Final Stage Cases by Owner 17
 - Follow-Up Stage Cases by Owner 17
 - Initial Stage Cases by Owner 17
 - Maximum Time to Case Resolution - by User 18
 - Open Cases 18
 - Open Cases by Associated Impact 18
 - Open Cases by Consequence Severity 17
 - Open Cases by Operational Impact 18
 - Open Cases by Stage 17
 - Queued Stage Cases by Owner 17
 - Recently Closed Cases 17
- Queued Events Previous Day active channel 26
- Queued Events Previous Daytime Shift active channel 26
- Queued Events Previous Morning Shift active channel 26
- Queued Events Previous Night Shift active channel 26
- Queued stage 27
- Queued Stage Cases by Owner (Chart) query 23
- Queued Stage Cases by Owner query viewer 17

R

- Recently Closed Cases query 22
- Recently Closed Cases query viewer 17
- report templates
 - Chart and Table Landscape 38
 - Chart and Table Portrait 24, 38
 - Four Charts and Table Landscape 24, 38
 - Simple Chart Portrait 38
 - Simple Table Landscape 24, 38
 - Simple Table Portrait 24, 38
 - Three Charts and Table Landscape 38
 - Two Charts One Table Portrait 38
- reports
 - All Cases 19
 - All Level 3 Notifications 29
 - Average Time to Case Resolution - By Day 19
 - Average Time to Case Resolution - By Severity 18
 - Average Time to Case Resolution - By User 18
 - Case Stages Overview 18
 - Case Status Overview 19
 - Cases Created Today 19
 - Level 3 Notifications - Monthly Trend 31
 - Level 3 Notifications - Quarterly Trend 28
 - Level 3 Notifications - Weekly Trend 28
 - Max Time to Case Resolution - By User 19

- Notification Action Events 29
- Notification Escalation Level Event Overview - Monthly Trend 31
- Notification Escalation Level Event Overview - Quarterly Trend 30
- Notification Escalation Level Event Overview - Weekly Trend 30
- Notification Overview 30
- Notification Statistics Summary 28
- Notification Status - Monthly Trend 31
- Notification Status - Quarterly Trend 30
- Notification Status - Weekly Trend 30
- Notification Status by User Overview - Monthly Trend 29
- Notification Status by User Overview - Quarterly Trend 29
- Notification Status by User Overview - Weekly Trend 31
- Notification Status Report 29
- Notifications By Acknowledgement Status 28
- Open Cases 19
- Unacknowledged Level 3 Notifications 30
- resource group
 - Case Tracking and Escalation 16
 - Event Annotations and Tracking 25
 - Notification Tracking 28
- rules
 - Case Deleted 19
 - Case Escalation 20
 - Case Investigation Started 20
 - Monitor New Case 20
 - Track Closed Case 20
 - Track Deleted Case 19
 - Track New Case 19
 - Track Updated Case 20

S

- session lists
 - Case Tracking 24
- shared libraries 6
- Simple Chart Portrait report template 38
- Simple Table Landscape report template 24, 38
- Simple Table Portrait report template 24, 38
- Single-digit Day filter 22
- Single-digit Hour filter 22
- Single-digit Minute filter 21
- Single-digit Month filter 22
- stages
 - Closed 27
 - Queued 27

T

- Three Charts and Table Landscape report template 38
- Track Closed Case rule 20
- Track Deleted Case rule 19
- Track New Case rule 19
- Track Updated Case rule 20
- Trend on Case Audit Events query 24
- trends
 - Case History Data 24
 - Notification Events 39
 - Notifications 38
- Two Charts One Table Portrait report template 38

U

Unacknowledged Level 3 Notifications query 37
Unacknowledged Level 3 Notifications report 30

Y

Year global variable 21
Yesterday's Assigned Events active channel 25

