



ArcSight Dashboard and User Management 1.1 User Guide

July 2020

Legal Notice

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/about/legal/>.

© Copyright 2020 Micro Focus or one of its affiliates.

Contents

About This Book	5
1 Welcome to ArcSight Fusion	7
Part I Creating and Using Dashboards	9
2 Viewing a Dashboard	11
View Data in a Dashboard	11
View a Different Dashboard	11
Favorite Dashboards	11
All Available Dashboards	11
3 Viewing Analyst and Entity Details	13
Case Overview by Owner	13
Review Entities	13
4 Managing Dashboards and Content	15
Change the Time Range of Data in a Dashboard	15
Mark a Dashboard as a Favorite	15
Specify a Default Dashboard	16
Create or Clone a Dashboard	16
Create a Dashboard	16
Clone a Dashboard	17
Edit the Dashboard	17
Add Widgets	17
Modify a Widget's Properties	17
Rearrange the Order of Widgets	18
Remove Widgets	18
Change the Dashboard's Name	18
Import and Export a Dashboard	18
Considerations for Importing a Dashboard	18
Import a Dashboard	19
Export a Dashboard	19
Display a Dashboard on the SOC Screen	19
Share a Dashboard	19
Understand the Provided Dashboards	20
How is My SOC Running?	20
Entity Priority	20
Health and Performance Monitoring	20
5 Configuring Widgets	21
Understand Widget Properties	21

Understand the Provided Widgets	23
Active List	23
Case Breakdown	23
Case Load	24
Case Timeline	24
Case Workflow Analysis	24
Database Event Ingestion Timeline	25
Database Storage Utilization	25
Entity Count Overview	25
Productivity	25
Threat Analysis Funnel	26
Part II Managing Users	27
6 Manage Your Profile	29
7 Managing Users and Groups of Users	31
Import Users from ESM	31
View Details of a Group	31
Create a New Group	31
Create a New User	32
View a User's Profile	32
Unlock the User's Account	32
Change the User's Password	33
Change the User's Status	33
Change the User's Roles or Permissions	33
Change the User's Group Assignments	33
8 Assigning Permissions to Roles and Users	35
Dashboard Permissions	35
Default Roles for the Dashboard	35
Create a Role with Permissions	36
View Details of a Role	36
Change Permissions for the Role	37
Add or Remove Users for the Role	37
Delete the Role	37

About This Book

This *User's Guide* provides concepts, use cases, and contextual help for the Dashboard and user management of the ArcSight Platform.

- ♦ [Part I, "Creating and Using Dashboards,"](#) on page 9
- ♦ [Part II, "Managing Users,"](#) on page 27

Intended Audience

This book provides information for individuals who use the Dashboard and manage users in the ArcSight Platform. These individuals have experience using the deployed products, such as ArcSight Enterprise Security Manager and ArcSight Intersect. For example, they tend to be familiar with managing security operation centers or performing duties of a security analyst or operator.

Additional Documentation

The Fusion documentation library includes the following resources:

- ♦ *Release Notes for ArcSight Platform*, which provides an overview of the products deployed in this suite and their latest features or updates
- ♦ *Technical Requirements for ArcSight Platform*, which provides information about the common hardware and software requirements for installing the CDF Management Portal and deployed components

For the most recent version of this guide and other ArcSight documentation resources, visit the [documentation for ArcSight Platform](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the [comment on this topic](#) link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care at <https://www.microfocus.com/support-and-services/>.

1 Welcome to ArcSight Fusion

ArcSight Fusion provides the common elements needed for the ArcSight Platform products deployed in a containerized environment: [user management](#), the [Dashboard](#), and other core services. You can add users and groups, as well as manage their roles and permissions. The Dashboard enables you to visualize, identify, and analyze potential threats by incorporating intelligence from the multiple layers of security sources that might be installed in your security environment:

- ◆ Real-time event monitoring and correlation with data from ArcSight Enterprise Security Manager (ESM)
- ◆ Analyzing end-user behavior with ArcSight Intersect
- ◆ Performing deep-dive investigations with ArcSight Recon

To help you get started, Fusion provides a set of out-of-the-box widgets and dashboards. Users can organize the widgets into personalized dashboards. You can also use the Widget SDK to create new widgets or modify the provided ones.

For information about deploying, configuring, and maintaining this product, see the [documentation for ArcSight Platform](#).

Creating and Using Dashboards

Select Dashboard

You can create one or more dashboards that incorporate widgets in your preferred arrangement. Depending on your role, you can create dashboards to be [shared](#) with specific [roles](#), and even identify which of those dashboards should be the [default landing page](#) for a role.

- ◆ [Chapter 2, “Viewing a Dashboard,” on page 11](#)
- ◆ [Chapter 3, “Viewing Analyst and Entity Details,” on page 13](#)
- ◆ [Chapter 4, “Managing Dashboards and Content,” on page 15](#)
- ◆ [Chapter 5, “Configuring Widgets,” on page 21](#)

2 Viewing a Dashboard

Select **Dashboard**

The Dashboard automatically displays your [default dashboard](#) when you log in or select **Dashboard**. If you do not have a default dashboard, the Dashboard displays the list of available dashboards.

- ♦ [“View Data in a Dashboard” on page 11](#)
- ♦ [“View a Different Dashboard” on page 11](#)

While viewing a dashboard, you can [modify](#) its settings or [clone](#) it to [create](#) a new dashboard.

View Data in a Dashboard

Content in a dashboard depends on the widgets that it displays, as well as the dashboard’s specified [time range](#).

View a Different Dashboard

When viewing a dashboard, select **View All Dashboards**.

In the course of your day, you might need to switch among several dashboards. You can view the list of dashboards in two ways:

- ♦ [“Favorite Dashboards” on page 11](#)
- ♦ [“All Available Dashboards” on page 11](#)

The list indicates whether a dashboard is shared, for your personal use, or assigned as the default for a role. You can also see who owns each dashboard. An “out-of-the-box” label indicates that the dashboard is provided with the Dashboard. In general, out-of-the-box dashboards are available only to the Dashboard administrator because they require [configuration](#) before use.

Favorite Dashboards

You can [specify](#) which dashboards are your favorites.

All Available Dashboards

You can view the full list of available dashboards. A star beside the name indicates that you have [marked](#) that dashboard as a [favorite](#).

3 Viewing Analyst and Entity Details

Some of the widgets in the dashboard allow you to review activity associated with specific cases, case owners or owner groups, and entities.

- ♦ [“Case Overview by Owner” on page 13](#)
- ♦ [“Review Entities” on page 13](#)

Case Overview by Owner

Select an owner in a widget

You can review all cases [currently](#) assigned to a specific owner. When you select an owner in a widget, the Dashboard opens the **Case Overview by Owner** page. For each case, the table includes the following details:

- ♦ Severity of the case
- ♦ Current stage of the case
- ♦ Length of time that the case has been assigned to the owner
- ♦ Time since the case was created
- ♦ Time since the case was last updated

To determine when the owner received a particular case, hover over the **Owned** field. If you hover over the **Created** and **Last Updated** fields, the Dashboard shows the specific date and time that the case was created or last updated, respectively.

Review Entities

Select an entity in a widget

If your environment incorporates data from Intersect, you can select the entities in the [Entity Count Overview](#) widget to view their status and details.

4 Managing Dashboards and Content

Select Dashboard

You can [add](#), [remove](#), and [rearrange](#) the order of [widgets](#) in a dashboard. You can also [change the content](#) of a widget then save it with a unique name. To [edit](#) a dashboard, you must be currently viewing it.

- ♦ [“Change the Time Range of Data in a Dashboard” on page 15](#)
- ♦ [“Mark a Dashboard as a Favorite” on page 15](#)
- ♦ [“Specify a Default Dashboard” on page 16](#)
- ♦ [“Create or Clone a Dashboard” on page 16](#)
- ♦ [“Edit the Dashboard” on page 17](#)
- ♦ [“Import and Export a Dashboard” on page 18](#)
- ♦ [“Display a Dashboard on the SOC Screen” on page 19](#)
- ♦ [“Share a Dashboard” on page 19](#)
- ♦ [“Understand the Provided Dashboards” on page 20](#)

Change the Time Range of Data in a Dashboard

Select 

Most of the [widgets](#) in a dashboard display data according to the either a specified [Time range](#) or an [As of now](#) setting, which displays data based on the last time that you refreshed the browser. You can [configure](#) the time setting.

If you select a preset time, the Dashboard displays data starting from 12:00:00 a.m. of the first date in the range to 11:59:59 p.m. of the last date in the range. If the last date is the current date, then the Dashboard defaults to the current time or time of the last browser refresh. For example, the **Last 1 month** setting might be from 12:00:00 a.m. April 29 to 3:34 p.m. May 29. Note that the Dashboard does not display minutes and hours.

To display time values, the Dashboard uses your browser settings, such as your local time zone.

Mark a Dashboard as a Favorite

To more quickly find a dashboard, you can add it to your [Favorites list](#).

While viewing a dashboard, select ☆.

Specify a Default Dashboard

Select ... > **Set as default for me**

When you log in, the Dashboard automatically displays the default dashboard that you have chosen or that an Administrator has [assigned](#) for your role. If no dashboard has been assigned to you or no default exists, you will see the list of available dashboards.

To override the default dashboard assigned to your role, you can specify any currently displayed dashboard as your preferred landing page.

Create or Clone a Dashboard

You can build as many dashboards that you need either by [creating a new](#) dashboard or [copying](#) a custom or out-of-the-box dashboard.

- ◆ [“Create a Dashboard” on page 16](#)
- ◆ [“Clone a Dashboard” on page 17](#)

Create a Dashboard

You can create as many dashboards as you need.

- 1 (Conditional) From within an existing dashboard, select ... > **Create new Dashboard**.
- 2 (Conditional) From the Dashboards list, select +.
- 3 Specify a **Title** for the new Dashboard.
The title can be a maximum of 150 characters, and must be unique.
- 4 To [add](#) a widget, select + beside **Main Context**.
- 5 [Choose](#) the widget that you want to add.
- 6 [Modify](#) the widget's [properties](#).
- 7 Continue to add widgets as needed.
- 8 [Arrange](#) the widgets how you prefer.
- 9 [Save](#) your changes.

Alternatively, you might choose to [clone](#) an existing dashboard or [import](#) a dashboard that someone else created.

Clone a Dashboard


To quickly [create](#) dashboards, you can copy an existing dashboard. For example, Inez Bates wants to customize an out-of-the-box dashboard and [share](#) it with her APJ analyst team. She clones the dashboard, then [modifies](#) some of the widgets to include only cases that the team owns.

By default, the Dashboard copies the name of the original version and adds “Copy of” to the name. You can change that title as part of the cloning process or [edit](#) the title later.

- 1 From within an existing dashboard, select ... > **Clone**.
- 2 Specify a unique name for the new dashboard.
- 3 (Optional) Indicate that you want to add the new dashboard to your [Favorites](#).
- 4 **Save** your changes.

Alternatively, you can [import](#) a dashboard that someone else created.


Edit the Dashboard

While viewing a dashboard, select 

You can only modify the configuration of the dashboard that you are currently viewing, such as changing widget properties or adding and removing widgets.

- ♦ [“Add Widgets” on page 17](#)
- ♦ [“Modify a Widget’s Properties” on page 17](#)
- ♦ [“Rearrange the Order of Widgets” on page 18](#)
- ♦ [“Remove Widgets” on page 18](#)
- ♦ [“Change the Dashboard’s Name” on page 18](#)

Add Widgets

While viewing a dashboard, select , then + in Main Context

To find an existing widget, you can search by its name or the tags assigned to it. After choosing the widget, you can [change its properties](#) to suit your dashboard.


To group widgets in sections under the **Main Context**, select **Nested Context** from the widget selector or select a context that has already been added to the dashboard. Then you can add widgets in that section. You can also change the name of the sections.

Modify a Widget’s Properties

While viewing a dashboard, select 


To edit the [settings](#) of a widget, select the widget. Make your changes in the **Widget Properties** pane. Then save your changes.

Rearrange the Order of Widgets

While viewing a dashboard, select 


To rearrange the order of [widgets](#) in a dashboard, simply drag each widget to the new location. Then save your changes.

Remove Widgets

While viewing a dashboard, select 

To remove a widget, select **X** within the widget's boundaries. Then save your changes to the dashboard.

Change the Dashboard's Name

While viewing a dashboard, select 

The title of a dashboard can be a maximum of 150 characters, and must be unique.

Import and Export a Dashboard

As an alternative to [sharing](#) or [copying](#) a dashboard, you can [export](#) the dashboard as a `json` file for other users to [import](#) to their Dashboard. The `json` file contains information about the dashboard's configuration and the included widgets. The file does not contain any data displayed in the dashboard. You can modify the exported `json` file or [edit](#) the imported dashboard.

For example, Inez Bates on the APJ analyst team really likes a dashboard that Murphy Buckley, on the EMEA team, made for his personal use. Murphy could [share](#) this dashboard with Inez. However, the widgets are configured for the AMS team's use, so the data would not be useful for Inez. Instead, Murphy exports the dashboard and sends the `json` file to Inez. She imports the dashboard, then [modifies](#) some of the widgets to point to cases that she and the APJ team own.

- ♦ [“Considerations for Importing a Dashboard” on page 18](#)
- ♦ [“Import a Dashboard” on page 19](#)
- ♦ [“Export a Dashboard” on page 19](#)

Considerations for Importing a Dashboard

Changing the `json` file of a dashboard can cause problems either during import or within the Dashboard. Usually, you only need to change the name of the dashboard in the file. Before importing a dashboard, please review the following considerations:

- ♦ You cannot import a dashboard whose name already exists in your Dashboard environment. Ensure that you change the [title](#) of the dashboard in the `json` file.

NOTE: This caveat includes names of dashboards that other users have created and which you might not see in your list.

- ♦ You cannot import a dashboard if it contains widgets that do not exist in your Dashboard environment.

Import a Dashboard

When viewing the list of Dashboards, select ... > **Import Dashboard**. Then browse to the appropriate json file.

Export a Dashboard

When viewing a Dashboard, select ... > **Export Dashboard**.

Display a Dashboard on the SOC Screen

Like most software, the Dashboard will end a session that has been idle for a while. This is good for security. However, it can be inconvenient if you display a dashboard on the large monitors in your SOC. To avoid manually interacting with the browser or logging in regularly, you can use a plug-in that automatically refreshes all content in the browser tab that displays the dashboard.

- 1 Install an Auto Refresh add-on for your browser. There are free add-ons available for supported browsers.
- 2 Specify the time interval after which you want the browser tab to refresh automatically.
For instance, if you set the time for auto-refresh to five minutes, your browser tab will refresh automatically after an interval of five minutes.
- 3 (Optional) Minimize the left navigation pane.

Note that, when you refresh the tab, the Dashboard always updates to the latest data based on your chosen [time range](#).

Share a Dashboard

*You must have the **Share Dashboard** permission to perform this function*

Select ... > **Share**

You can share the currently displayed dashboard with one or more of your assigned [roles](#). If you have the **Manage Roles** permission, you can share the dashboard with any role.

Alternatively, if you cannot share a dashboard, you can [export](#) the dashboard for others to import and use.

NOTE: You cannot re-share a dashboard that has been shared with you.

Understand the Provided Dashboards

To help you get started, the Dashboard provides out-of-the-box dashboards with associated widgets. You will need to [configure the widgets](#) to ensure the dashboards display data appropriately for your environment.

- ◆ [“How is My SOC Running?” on page 20](#)
- ◆ [“Entity Priority” on page 20](#)
- ◆ [“Health and Performance Monitoring” on page 20](#)

Initially, the out-of-the-box dashboards are available to the administrative user created during the initial log in. This user can [share](#) these dashboards with SOC team members, who can then create their own [clones](#). Alternatively, administrators can create one or more clones based on these dashboards, then share the clones, and set [default dashboards](#) for roles.

How is My SOC Running?

The out-of-the-box dashboard, [How is my SOC running?](#), gives you an overview of the status and trends related to ESM case management. It includes the following widgets:

- ◆ [Case Breakdown](#)
- ◆ [Case Load](#)
- ◆ [Case Timeline](#)
- ◆ [Case Workflow Analysis](#)
- ◆ [Productivity](#)
- ◆ [Threat Analysis Funnel](#)

Entity Priority

The out-of-the-box dashboard, [Entity Priority](#), combines content from both Intersect and ESM to provide the status of users and entities at risk, including risk scores calculated by Intersect. It includes the following widgets:

- ◆ [Active Lists](#)
- ◆ [Entity Count Overview](#)

Health and Performance Monitoring

The out-of-the-box dashboard, [Health and Performance Monitoring](#), provides information about the status of the database installed with some components, such as ArcSight Recon and Intersect. It includes the following widgets:

- ◆ [Database Event Ingestion Timeline](#)
- ◆ [Database Storage Utilization](#)

5 Configuring Widgets

Widgets display data according to your specifications. You can filter content by specific case owners or groups, case severities, and sub-filters.

- ♦ [“Understand Widget Properties” on page 21](#)
- ♦ [“Understand the Provided Widgets” on page 23](#)

Understand Widget Properties

When you configure a widget, you might see a combination of the following properties:

Title and Subtitle

Specifies the name and an optional secondary name for a widget you want to add to your dashboard.

You can also specify whether the dashboard displays the title or subtitle.

In general, because you might have several variations of some widgets, it’s a good practice to title each widget according to your sub-filter criteria. For example, SOC Manager Franz Tupper creates a Case Breakdown widget for each of the SOC’s three owner groups: EMEA, AMS, and APJ. He names the widgets *Case Breakdown-EMEA*, *Case Breakdown-AMS*, and *Case Breakdown-APJ*.

Severity

Specifies the categories of importance, or severity, assigned to the affected cases. For example, in ESM, some cases might be categorized as *Catastrophic* or *Marginal*.

When selected for **Group by**, you can add sub-filters by specifying the type of **Cases**, **Assigned Owners**, or **Assigned Owner Groups** that you also want to view.

Assigned Owners

Indicates that you want to display data based on the individuals assigned to the affected cases. You can specify the **Owners** that you want to include.

If you do not specify an owner, the Dashboard includes data for all owners. If you specify more than five owners, the Dashboard displays data for the top five selected owners. Then adds an **Other** category that totals the values for all other selected owners.

When selected for **Group by**, you can add sub-filters by specifying the type of **Cases** and **Importance** categories that you also want to view.

Assigned Owner Groups

Indicates that you want to display data based on the owner groups, or teams, assigned to the affected cases. The widget also displays all cases assigned to the individuals and child groups within the owner groups. You can specify the **Owner Groups** that you want to include.

If you do not specify an owner group, the Dashboard includes data for all groups, and thus all owners. If you specify more than five owner groups, the Dashboard displays data for the top five selected groups. Then adds an **Other** category that totals the values for all other selected owner groups.

When selected for **Group by**, you can add sub-filters by specifying the type of **Cases** and **Severity** categories that you also want to view.

Assigned Cases

*Applies only when you specify **Severity for Group by**.*

Indicates whether a sub-filter includes cases assigned to the specified owners.

To include specific owners or owner groups, select **Owners** then add the names that you want to include. Otherwise, the Dashboard displays data for all assigned cases.

In general, to view sub-filter data, you might hover over the visual in the widget or drill down into the data.

Unassigned Cases

*Applies only when you specify **Severity for Group by**.*

Indicates whether a sub-filter includes unassigned cases.

Target for Case Closure

*Applies only to the **Productivity and Case Load** widgets.*

Specifies the number of cases per week that you expect each owner group (Productivity widget) or owner (Case Load) to close.

Time Range

Specifies the start and end dates for the data that you want to view:

- ◆ **Dashboard's default** tells the widget to use the **time range** set for the dashboard.
- ◆ **As of now** tells the widget to use the most recent data retrieved from the data source.

Data updates each time you **refresh the browser**, unless you have specified a **Custom** time range.

NOTE: You can set a **maximum time range** to limit the amount of data that the Dashboard can collect from its data sources. For example, you can specify 365 days of data. For more information, see the *Administrator Guide* in the [documentation for ArcSight Fusion](#).

NOTE: To assign or change the severity or owner of a case, use the ArcSight Console or Command Center.

Understand the Provided Widgets

The Dashboard ships with several widgets designed to help you manage your security operations. When you [create or modify](#) a dashboard, you can choose from the full set of widgets and [configure](#) them as needed.

The Dashboard provides the following out-of-the-box widgets:

- ◆ [“Active List” on page 23](#)
- ◆ [“Case Breakdown” on page 23](#)
- ◆ [“Case Load” on page 24](#)
- ◆ [“Case Timeline” on page 24](#)
- ◆ [“Case Workflow Analysis” on page 24](#)
- ◆ [“Database Event Ingestion Timeline” on page 25](#)
- ◆ [“Database Storage Utilization” on page 25](#)
- ◆ [“Entity Count Overview” on page 25](#)
- ◆ [“Productivity” on page 25](#)
- ◆ [“Threat Analysis Funnel” on page 26](#)

Active List

Requires data collection from Intersect and ESM

To watch for suspicious activity associated with entities and users, add **Active List** widgets to your dashboard. Each widget displays the top five at-risk entities or users, based on the specified **Active list**, **Field**, and **Entity type** settings.

The available active lists correspond to active lists in ESM. For example, you might have watch lists for privileged or administrative users or vulnerable hosts. If an active list entry matches an entity or user in Intersect, then the widget also shows the Intersect risk score for that entry.

Case Breakdown

Requires data collection from ESM

The **Case Breakdown** widget displays the number or percentage of cases by their **Severity**, **Owners**, or **Owner Groups**. The widget always shows data **As of Now**, regardless of the [specified time range](#) for the dashboard.

By default, the widget shows data for total open, assigned cases. The widget displays a maximum of six data points, which comprise the top five objects associated with the specified filter plus an *Other* object that combines the rest of the cases. For example, if you have seven case owners, the widget shows specific values for the five owners with the largest quantity of cases, then groups the total number of cases for the other two owners in the Other category.

You can [change the widget’s properties](#) to view cases in a different state, such as cases created by specific analysts. For example, SOC Manager Franz Tupper wants to view all cases created by his Level 1 analysts. He sets the filter to **Assigned Owners**, and in the sub-filters specifies Jin Stafford, Neve Marshall, Troy Leach, and Chole Gay as **Owners**. Then he selects **Created** for the state that he

wants to analyze. The widget will display the quantity and percentage of cases created by each analyst. Because Franz has configured the dashboard to [automatically refresh](#), he sees in real-time when the analysts add new cases.

If you don't specify an owner or owner group, the widget displays data for all cases.

Case Load

Requires data collection from ESM

To help managers balance the amount of work assigned to case owner, the **Case Load** widget provides several case management metrics:

- ♦ Average number of cases each owner closes per week
- ♦ Estimation of the time required to close all cases currently assigned to the owner based on the time elapsed since the cases were opened
- ♦ Projection of the number of cases per severity that the owner might not be able to close, based on the configured target, the time elapsed since the cases were opened, and the average velocity of the owner. This assumes that owners work on cases in severity order, from highest to lowest.

By default, the widget shows the data for total open, assigned cases for the top three members of the group based on their average number of cases per week. You can filter the data by specific **Owner Groups**. The metrics are based on the specified [time range](#) and the [target](#) number of cases that you expect the owners to close per **Severity**.

For best use of this widget, we recommend that you create one Case Load widget per owner group. In this way, you will see details for members of the owner group.

Case Timeline

Requires data collection from ESM

The **Case Timeline** widget shows changes in the volume of cases over a [specified time range](#). By default, the widget filters the data according to the **Severity** category assigned in ESM. However, you can also choose to view trends for other case states, such as cases **Closed** by specific **Owners** or **Owner Groups**.

To observe the breakdown of cases associated with a specific date, you can hover over any location within the timeline. You can also zoom in to view a particular time range, either using the magnifier icons or by clicking and dragging within the graph.

Case Workflow Analysis

Requires data collection from ESM

The **Case Workflow Analysis** widget helps you compare the current volume of cases per stage with how the cases transitioned among the stages. In the widget, the width of the lines indicates the average time cases have taken to move from stage to stage during the [specified time range](#). The diameter of each circle, except for the *Closed* stage, represents the total number of cases currently at that stage, based on the last refresh of data from the source.

NOTE: The widget does not represent backward transitions. For example, a case moves from *Final* back to *Follow-up* during the specified time range.

By default, the widget shows data for total open, assigned cases. You can also choose to filter the data by **Severity**, **Owners**, or **Owner Groups**.

Database Event Ingestion Timeline

To help SOC managers and IT administrators monitor the rate of event ingestion into the database, use the **Database Event Ingestion Timeline** widget. Due to differences in how quickly an event from different sources arrives at the database for storage, the moment when a database stores an event differs from when the event occurred. This widget measures when the database receives the event data.

Database Storage Utilization

To help SOC Managers and IT Administrators ensure that disk use does not overload the database nodes, the **Database Storage Utilization** widget displays storage utilization data for up to five database nodes. In general, most administrators keep disk usage below 60 percent per node, thus ensuring space for temporary activity required by some query execution operators.

If the database cluster has more than five nodes in the cluster, you might specify the nodes with the least amount of free space available. In this way, you can monitor the nodes at most risk of running out space. For each node, you can compare the percent and quantity of space used to the total amount. You can also monitor the throughput and latency of the database per second.

Entity Count Overview

Requires data collection from Interset

To help identify users and entities currently at risk, the **Entity Count Overview** widget shows the number of entities by entity type that you monitor, then indicates which have high risk scores [As of Now](#). You can select an entity to [review its details](#).

Productivity

Requires data collection from ESM

To help managers optimize analyst activity for the [specified time range](#), the **Productivity** widget incorporates several elements related to SOC productivity:

Case Closure Velocity

Shows the current rate of case closure per week based on the [target](#) velocity for all owners and owner groups. For example, you might expect teams to close at least 5 cases per week. The dotted line in the graph represents the target.

The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were created.

Highest Velocity

Represents the owner that currently has the fastest closure rate per week. You can also see the total number of cases assigned to the owner by severity.

The trend indicates whether the velocity fails to meet or exceeds the target rate compared to the previous week. The velocity is based on when cases were assigned to the owner.

Productivity by Owner Groups

Lists the owner groups that currently have the highest average number of cases closed per week. It also identifies which owner in the group has the highest velocity.

You can observe the average number of cases closed and whether the rate is trending up or down. The colored bar indicates the volume of cases by severity.

By default, the widget displays data according to the [specified time range](#).

Threat Analysis Funnel

Requires data collection from ESM

The **Threat Analysis Funnel** provides the SOC Manager an overview for the volume of events in the [specified time range](#) that transition from initial analysis of events from source devices through correlation to case creation. The widget also shows the **percent** of change between each state.

Analyzed

Shows the number of **events**, from source devices, that would need to be handled manually without the use of ArcSight correlation.

Found

Indicates the reduction in the number of items that you would need to handle manually. This data includes the **correlation events** generated by rules that monitor events from source device as well as events created by ArcSight components. For typical correlation rule configurations, the data usually represents a reduction in the number of items. However, it is possible for an increase to occur in unusual configurations.

Created

Represents the number of **cases** created within the time range, based on correlation event activity, content or systems detecting what's significant, and manual assessments.



Managing Users

As an end-user or the manager of an end-user, you can change the user password, as well as view the assigned permissions, roles, and groups.

As a product administrator, you can add users or groups of users; create roles; and assign permissions to the roles, users, and groups. The Dashboard provides five default roles with appropriate permissions to use the product.

- ♦ [Chapter 6, “Manage Your Profile,” on page 29](#)
- ♦ [Chapter 7, “Managing Users and Groups of Users,” on page 31](#)
- ♦ [Chapter 8, “Assigning Permissions to Roles and Users,” on page 35](#)

6 Manage Your Profile

Select *[your_ID]* > **My Profile**

When viewing your user profile, you can perform the following actions:

- ◆ Reset your password
- ◆ Change your contact information
- ◆ View your assigned [roles](#), permissions, and [groups](#)

7 Managing Users and Groups of Users

You must have the **System Administrator** or **Manage Roles** permission to perform these functions

To more efficiently manage your users, you can organize them into groups then assign permissions to those groups. If you already have groups of users in ESM, you can import them to the Dashboard. Alternatively, you can manually create users.

- ♦ [“Import Users from ESM” on page 31](#)
- ♦ [“View Details of a Group” on page 31](#)
- ♦ [“Create a New Group” on page 31](#)
- ♦ [“Create a New User” on page 32](#)
- ♦ [“View a User’s Profile” on page 32](#)

Import Users from ESM

To help you get started, you can import users already authorized for ESM. You need to have at least one [role](#) available in the Dashboard to assign to these users.

- 1 Click **ADMIN** > **Account Groups** > **Import Users**.
- 2 Select the [role](#) that you want to assign to the imported users.
- 3 Select **IMPORT USERS**.

View Details of a Group

When you view the details of a user group, you can also modify the group’s settings and permissions.

- 1 Click **ADMIN** > **Account Groups** > *group_name*.
- 2 (Optional) [Change](#) the roles and users within the group.

Create a New Group

- 1 Click **ADMIN** > **Account Groups** > **Create User**.
- 2 Specify the email ID and name of the user.
- 3 Select the groups to which you want to add the user.
- 4 Assign the role that includes appropriate permissions.
- 5 Click **Save**.
- 6 Under **Account Groups**, click **All Users**.
- 7 Select the user you just created.

- 8 Click **RESET PASSWORD**.
- 9 Set the password and click **SAVE**.

Create a New User

Users must have at least one role to ensure that they can login.

- 1 Click **ADMIN > Account Groups > Create User**.
- 2 Specify the email ID and name of the user.
- 3 Select the groups to which you want to add the user.
- 4 Assign the role that includes Dashboard permissions.
- 5 Click **Save**.
- 6 Select **Account Groups > Search Users**.
- 7 Select the user that you just created.
- 8 Click **RESET PASSWORD**.
- 9 Set the password and click **SAVE**.

View a User's Profile

The user profile provides basic details about the user. If you are the user's manager, you can modify the user's account. You must also have appropriate permissions to make the modifications.

- 1 To find the user, perform one of the following actions:
 - ♦ Click **ADMIN > Account Groups > Search Users**.
 - ♦ Click **ADMIN > Account Groups > *group_name***.
- 2 Select the user that you want to view.
- 3 (Optional) Modify the user's profile in one of the following ways:
 - ♦ [Unlock the user's account](#)
 - ♦ [Reset the password](#)
 - ♦ [Activate or deactivate the user](#)
 - ♦ [Change roles or permissions](#)
 - ♦ [Change group assignments](#)

Unlock the User's Account

In the notification pane, select **Unlock**.

The system locks a user's account after three attempts to log into the system with the wrong credentials. When a user's account is locked, the **User Details** tab displays a notification.

Change the User's Password

To reset a user's password, you must have the *Change User Password* permission. When you reset a user's password the user receives a notification email automatically. The email does not include the new password. You must provide the new password to the user directly.

Change the User's Status

Adjust the **User Status** toggle switch. You must have the *Activate/Deactivate Users* permission.

A deactivated user cannot log into the system. .

Change the User's Roles or Permissions

You must have the *Assign Roles to Users* permission. Unless you have the *Group Manager* permission, you can only assign those roles that you currently have.

- 1 In the user's profile, select **Roles & Permissions**.
- 2 Select **Assign/Remove Roles**.
- 3 Change the user's roles, then select **Save**.

Each **role** has a defined set of permissions. To change a user's permissions, you must change the assigned role or the permissions associated with a role.

Change the User's Group Assignments

You must have the *Assign Users to Groups* permission. Unless you have the *Group Manager* permission, you can only assign those **groups** in which you are currently a member.

- 1 In the user's profile, select **Groups**.
- 2 Select **Add/Remove**.
- 3 Change the user's group assignments.

8

Assigning Permissions to Roles and Users

You must have the **System Administrator** permission to perform these functions.

The Dashboard includes a set of permissions and roles that you can assign to your users or user groups. You can also create new roles.

- ◆ [“Dashboard Permissions” on page 35](#)
- ◆ [“Default Roles for the Dashboard” on page 35](#)
- ◆ [“Create a Role with Permissions” on page 36](#)
- ◆ [“View Details of a Role” on page 36](#)

Dashboard Permissions

The following table lists the permissions available for using the Dashboard:

Permission	Allows users to...
Access Dashboard	<ul style="list-style-type: none">◆ View dashboards owned by or shared with the user◆ Modify, delete, and export dashboards owned by the user◆ Create or clone dashboards◆ Import dashboards◆ Set a dashboard as a personal default dashboard
Share a Dashboard	<ul style="list-style-type: none">◆ Perform all actions associated with the Access Dashboard permission◆ With the Manage Role permission, share the current dashboard with any role◆ Without the Manage Role permission, share the current dashboard with any of the roles associated with the user’s role

If your environment includes Intersect, users created with Dashboard permissions automatically receive the *Default Tenant* status in Intersect. These users can view content in widgets that display data from Intersect.

NOTE: Intersect users that have the *Administrative Tenant* status only cannot view content in widgets that display data from Intersect.

Default Roles for the Dashboard

The Dashboard provides the following roles by default:

Role	Permissions
System Admin	All Admin and both Dashboard permissions
Admin	All Admin and both Dashboard permissions
Analyst L1	Manage Roles and both Dashboard permissions
Guest	Dashboard permissions
User	Dashboard permissions

However, you can [create new roles](#) that reflect your organization's needs.

Create a Role with Permissions

You can group multiple permissions into a role and assign the relevant role to Dashboard users. A user must have at least one role.

- 1 Click **ADMIN > Roles > Create Role**.
- 2 In the field in the upper left corner, specify a name for the role.
- 3 Press **Enter**.
- 4 Select the [permissions](#) that you want to apply to the new role.
- 5 To add users to the role, complete the following steps:
 - 5a Select the **USERS** tab.
 - 5b Select **Assign role to users**.
 - 5c Choose the users you want to add to the role.
 - 5d **Save** your changes.

View Details of a Role

When you view the details of a role, you can also modify the role's settings and permissions.

- 1 Click **ADMIN > Roles > role_name**.
- 2 (Optional) Modify the user's profile in one of the following ways:
 - ♦ [Change the set of permissions](#)
 - ♦ [Add or remove users](#)
 - ♦ [Delete the role](#)

Change Permissions for the Role

You can only assign permissions that you have yourself.

- 1 While viewing a role, select **Permissions**.
- 2 In the **Permissions** tab, select the permissions that you want to add or remove.
You might need to scroll the page to see the full set of available permissions.

Add or Remove Users for the Role

You can add or remove multiple users in a role.

- 1 While viewing a role, select **Users**.
- 2 In the **Users** tab, select **Assign Role to Users**.
- 3 Select the users that you want to assign to or remove from the role.

You can also add or remove roles for a [specific user](#).

Delete the Role

While viewing a role, select **Delete Role**.

You can delete any role except the *System Admin* role.

