ScienceLogic

Migration Guide for the New User Interface

SL1 version 11.3.0

Table of Contents

New Features in the SL1 User Interface 5
About This Guide 6
New Features in the SL1 User Interface 6
Login Process 6
Navigation Menus 6
Icons on the Left Navigation Bar 7
Icons 8
Filtering the Tables on Inventory Pages 9
Basic Search 9
Advanced Search 9
Bulk Actions in a List View 10
Custom Themes for the SL1 User Interface 10
New About and Help Pages 11
Events 11
Devices 12
Discovery and Credentials 13
Dashboards 14
Business Services 15
Machine Learning-based Anomaly Detection 16
Maps 17
Using the SL1 User Interface 19
Logging In and Out of the SL1 User Interface 20
The SL1 User Interface 20
The Classic User Interface 21
Using the Navigation Menus 22
Filtering Inventory Pages 22
Using Basic Search 23
Fields Used by an "ANY" Basic Search 25
Saving a Search 27
Performing an Advanced Search 27
Components of an Advanced Search 30
Fields 31
Operators 32
Values 33
Strings 34
Escape characters 34
Examples of Advanced Searches 35
Advanced Search Examples on the Devices Page 35
Advanced Search Examples on the Events Page 37
Advanced Search Examples for Dynamic Component Mapping (DCM) Scenarios 38
Scenario 1: vCenters 38
Search 1a 39
Search 1b 40
Scenario 2: SQL Servers 40
Searches 42
Performing Bulk Actions 43
Customizing the SL1 User Interface 44
Getting Help and More Information 44
The About Page 45
Tips and Best Practices for Using the Product Documentation 46

Events in the SL1 User Interface 49
Viewing the List of Events 50
Filtering the List of Events 53
Filtering Events by Organization and Service 53
Filtering Events by Severity 55
Filtering for Masked Events 57
Viewing Additional Data about an Event 59
Viewing Automation Actions 60
Using the Event Investigator 61
Using the Action Runner 62
Acknowledging and Clearing Events 64
Viewing and Editing Event Notes 65
Viewing the Event Policy 66
Suppressing and Unsuppressing an Event for a Device 67
Suppressing an Event 68
Suppressing an Event on Multiple Devices 68
Unsuppressing an Event 68
Unsuppressing All Instances of an Event 69
Enabling and Disabling Events 69
Disabling Events 70
Enabling Events 70
Event Throttling 70
Devices in the SL1 User Interface 72
Viewing Devices 73
Viewing Additional Data about a Device 75
Aligning a Device with a Different Organization 76
Adding Devices with Discovery 76
Using the Device Investigator 77
Using the Info Drawer on the Device Investigator Page 79
Running a Device Report 81
Using the Action Runner 82
Overview of the Device Investigator Tabs 84
The Investigator Tab 84
Adding and Removing Metrics on the Investigator Tab 86
Editing the Metric Panel Order on the Investigator Tab 87
Combining Charts on the Investigator Tab 89
Applying a Custom Device Investigator Layout to Other Devices 91
The Settings Tab 92
The Attributes Tab 96
The Changes Tab 97
The Collections Tab 98
The Configs Tab 99
The Events Tab 100
The Interfaces Tab 100
The Journals Tab 101
The Logs Tab 102
The Machine Learning Tab 103
The Map Tab 104
The Monitors Tab 104
The Notes Tab 105
The Ports Tab 107
The Processes Tab 107

The Redirects Tab 108
The Relationships Tab 109
The Schedules Tab 109
The Software Tab 110
The Thresholds Tab 111
The Tickets Tab 111
Assigning Icons to Devices 112

Chapter 1

New Features in the SL1 User Interface

Overview

This guide is intended for SL1 users who are migrating from the "classic " user interface for SL1 to the new user interface for SL1.

This chapter provides an overview of the features that are only available in the new SL1 user interface, and how those new features compare to features in the previous version of the user interface, where relevant. The topics in this chapter also contain links to the chapters of this guide that provide more information and procedures to help you make the transition from the "classic" user interface to the "new" user interface for SL1.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

About This Guide 6
New Features in the SL1 User Interface 6
Events 11
Devices 12
Discovery and Credentials 13
Dashboards 14
Business Services 15
Machine Learning-based Anomaly Detection 16
Maps 17

About This Guide

This guide assumes that the initial installation and configuration (deployment) of SL1 version 8.12.0 or later has been completed. SL1 8.12.0 was the first version of the that included content from both the "new" user interface and the "classic" user interface. For details on the initial configuration of SL1, see the ***Installation*** manual.

For the purpose of this guide and the SL1 product documentation in general, the new user interface for SL1 is called the ***SL1 user interface***. The new user interface is also sometimes called ***ap2***, which is short for "Admin Portal version 2". The previous version of the user interface is called the ***classic user interface*** in the SL1 product documentation.

New Features in the SL1 User Interface

The following sub-topics provide a very brief overview of each of the new features available in the SL1 user interface. Follow the links for detailed information and procedures for each new feature.

Login Process

In a browser, type the URL or IP address for your SL1 system, and then type the current user name and password you use with SL1. Click **Log In**.

> **TIP:** After you log in, if you can still see the horizontal NavBar or other features of the classic user interface in the SL1 user interface, click **[Refresh]** in your browser.

For more information, see *Logging In and Out of the SL1 User Interface*.

Navigation Menus

Starting with the 8.12.0 release of SL1, the SL1 user interface was upgraded to include content from both the "new" user interface (also called "ap2") and the "classic" user interface. This "unified" user interface provides a more streamlined method of navigation that uses two menus: a ***basic menu*** and an ***Advanced menu***.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ) at the top left of any SL1 page. Use the up and down arrow buttons ( ) to expand and contract the menu options.
- To view the **Advanced Menu** page, which contains links to *all* of the menu options, click the Advanced menu icon ( ) at the bottom left of any SL1 page. Use **[Ctrl]**+**[F]** in your browser to quickly find a page.

TIP: If you are familiar with the classic user interface, the **Advanced Menu** page will help you get used to the structure of the SL1 user interface.

TIP: The name of the SL1 page appears in the title bar of your browser, and the page title also appears in your browsing history to help you navigate through the pages you have visited.

Icons on the Left Navigation Bar

By default, the SL1 user interface displays the following icons, in the following order, on the left navigation bar:

- ***Dashboards*** (). Clicking this icon displays the **Dashboards** page, where you can view and define custom dashboard views. A dashboard view is a page that displays one or more graphical reports, called widgets. Each widget is displayed in its own customizable pane.
- ***Events*** (). Clicking this icon displays the **Events** page, which displays a list of all active events. An ***event*** is a message that is triggered when a specified condition is met. Among other things, an event can signal that a server has gone down, that a device is exceeding CPU or disk-space thresholds, that communication with a device has failed, or simply display the status of a managed entity.
- ***Devices*** (). Clicking this icon displays the **Devices** page, which allows you to view all of your managed devices in SL1 and also run a discovery to find more devices to monitor. You can select a device from the list on the **Devices** page to view detailed data on the **Device Investigator** page for that device.
- ***Business Services*** (). Clicking this icon displays the **Business Services** page, where you can create and manage business services for your company. Business services let you gauge the availability, health, and risk of your services and the devices that provide those services.
- ***Machine Learning*** (). Clicking this icon displays the **Machine Learning** page, which lets you enable anomaly detection. You can use machine learning-based anomaly detection to trigger events and automations in SL1. Machine learning-based anomaly detection is available only in SL1 Premium solutions; to upgrade, contact ScienceLogic Customer Support. You might not see this icon if your SL1 system is not configured for anomaly detection.
- ***Maps*** (). Clicking this icon displays the **Maps** page, where you can view, create, and manage relationship maps for the various elements in your SL1 environment.
- ***Setup and Config*** (). Clicking this icon displays the ***Setup and Config*** page, where you can access a variety of panes that let you get familiar with the SL1 user interface and discover devices in your environment so that you can start monitoring your devices, business services, and events.

TIP: To view a pop-out list of *additional* menu items on the left navigation bar, click the menu icon (). Click the left arrow icon ( ) to close the list of menu items.

Icons

The user interface includes many icons for quick and easy access to information. The SL1 user interface uses some of the same icons from the classic user interface along with a set of new icons.

The most common icons in the SL1 user interface include the following:

New User Interface Icons		Classic User Interface Icons	
	Expand the menu of options in the left navigation bar		Edit an object or policy
	Open the **Advanced Menu** page, which contains links to all pages		Delete an object
	Expand an item in a list or a menu, such as the Event Drawer or the ***More*** menu for the **Device Investigator** page		Access the Device Reports tools
	Close or collapse an item in a list or a menu		Access the Device Administration tools
	Open a context-sensitive menu or set of options		View information about an event
	Open a context-sensitive set of options for a specific item or widget		View information about an object
	When found on the top left of a list page, open the Select Column menu, where you can add or remove columns from the view		View the Notification Log
	When found at the end of a row, open a context-sensitive menu or set of options		Access Ticketing tools (often called the "life ring")
	Select one or more items in a list		Execute (usually Discovery)
	View masked events on the **Event Investigator** page		View a report
	Create an event note		Print a report
	Refresh the contents of a list		View log entries
	Close an item or a widget		View the calendar and define or edit a schedule
	Shows that a command or search is incorrectly formatted or incomplete		Export an object or policy
	Shows that a command or search is complete and formatted correctly		View raw logs

Filtering the Tables on Inventory Pages

In SL1, an ***inventory page*** is any page (or tab) that contains a table with a list of items that you work with, like the **Events** page or the **Devices** page. At the top of most inventory pages in the SL1 user interface are a set of filters for the columns in the table on that page.

On an inventory page, you can start typing filter text or select filter options in one or more of these filters to narrow down the items in the list to just the items you want to view.

As you type text in the ***Filter*** field at the top of a column, SL1 starts to filter the list to include only those elements that include your search terms.

For more information, see *Filtering Inventory Pages*.

Basic Search

At the top of most lists in the SL1 user interface, the ***Search*** field lets you look for specific elements in that list. The ***Search*** field contains a magnifying glass icon ( ) next to the words "Type to search" or "Search".

As you type text in the ***Search*** field, SL1 filters the list to include only those elements that include your search terms. When searching, SL1 considers all relevant columns for the search, including those that are not currently displayed on the page.

SL1 retains your search criteria on pages in the SL1 user interface even after you refresh the browser or navigate to another page and then return to the search page using the **[Back]** button in the browser.

For more information, see *Using Basic Search*.

Advanced Search

The SL1 user interface includes an Advanced Search option that lets you use customized search commands to search for data. The syntax for these Advanced Searches can be much more complex than a Basic Search, enabling you to find exactly what you need from a list of items.

Also, because the Basic Search only uses "AND" for multiple search criteria, you need to use an Advanced Search for an "OR" search using multiple search criteria, or if you want to create more complicated searches using Boolean Algebra.

At a minimum, an Advanced Search requires the following components, in the following order:

- A ***field***. The general type of data for which you are searching, such as a device name or an event message.
- An ***operator***. A word or symbol that specifies the relationship between the field and the value, such as equals or less than.
- A ***value***. A specific aspect or version of the field, such as a name or an amount. If a value is a string, it should be surrounded by "quotation marks" or 'apostrophes'.

TIP: As you type your Advanced Search, a red icon ( ) or a green icon ( ) appears at the end of the text field to show that your search is incorrectly or correctly formatted.

TIP: To view a list of all possible search commands in an Advanced Search, press **[Ctrl]** + **[Space]**.

Below are simple examples of Advanced Search syntax:

```
message contains 'risk is high'
organization has (company contains 'system')
attribute has (id = year and value = 2021)
name contains 'web_tier' and deviceClass has (description contains 'AppDynamics')
deviceClass has (description contains 'em7 admin portal')
```

TIP: You can type search commands in the ***Basic Search*** field and then click the gear icon ( ) and select *Advanced* to "translate" your basic search into an Advanced Search. You cannot go from an Advanced Search back to a Basic Search, however, without losing your search criteria.

For more information, see *Performing an Advanced Search*.

Bulk Actions in a List View

If a page in SL1 displays a list of items, and that page contains a checkbox ( ) to the left of each item in the list, you can select two or more items to perform bulk actions on all of the selected items at the same time.

To select all of the items on a page, click the checkbox at the top of the list. To clear all of the selected items, click the checkbox at the top again.

TIP: Pages that contain lists use "infinite scrolling", where the list continues to populate as you scroll toward the bottom of the list. The scrolling stops when you reach the end of the list.

For more information, see *Performing Bulk Actions*.

Custom Themes for the SL1 User Interface

You can customize the look and feel of your SL1 system by creating new themes. For example, you could create a theme that replaces the SL1 logo with your company's logo and updates the colors used in the user interface to match those used in your company's branding. You can also choose between a light theme or a dark theme.

For more information, see *Customizing the SL1 User Interface*.

New About and Help Pages

For more information about the components used by SL1, click your user name in the navigation bar at the top of any SL1 page and select *About*. The **About ScienceLogic** page appears, displaying the latest version numbers of the components used by SL1.

For product documentation about any page in SL1, click the **[Help]** button at the top right of any page in SL1. A product documentation topic specific to the current page appears in a new browser window:

NOTE: As of version 8.12.2 of SL1, ScienceLogic no longer updates the help content that appears when you click the **[Guide]** button in the classic the user interface. All help content is maintained in the online help, which is located at **https://docs.sciencelogic.com**.

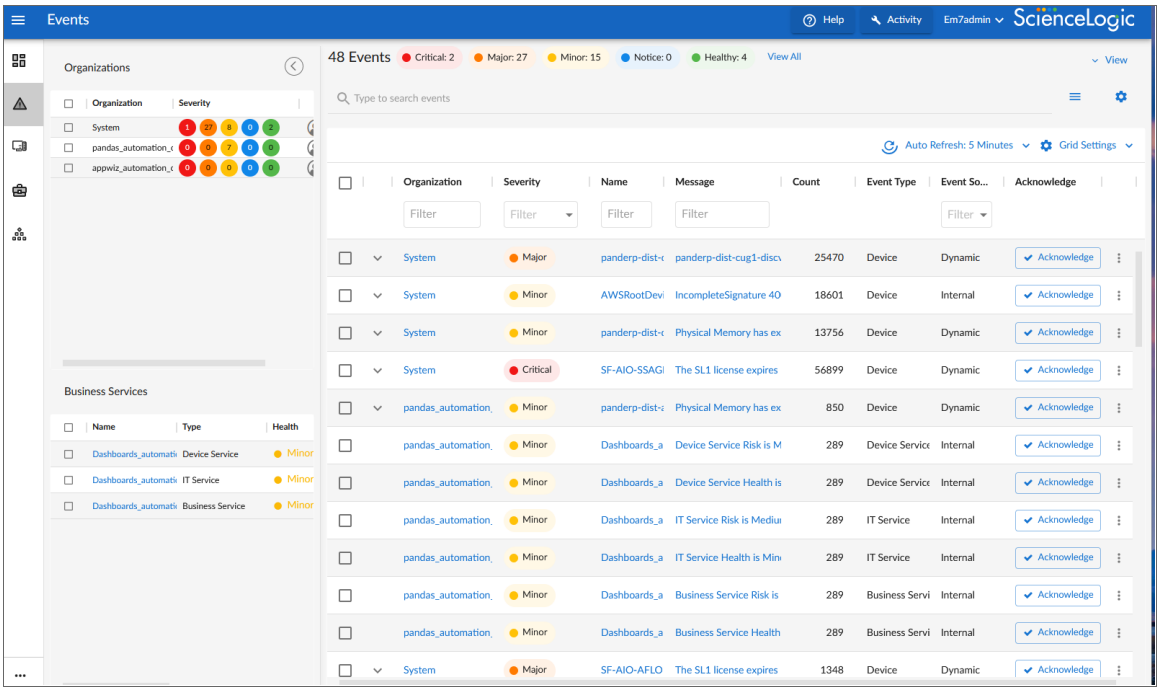
TIP: Click the **[Feedback]** button on the right side of the window to send comments directly to the ScienceLogic Documentation team, such as reporting typos, inaccuracies, questions, or other comments about that specific page in the Product Documentation.

For more information, see *Getting Help and More Information*.

Events

The **Events** page in the SL1 user interface displays a list of currently active events, from critical to healthy. From this page you can acknowledge, clear, and view more information about an event. You can also view events by organization to focus on only the events that are relevant to you.

To navigate to the **Events** page, click the Events icon (⚠) on the navigation bar:



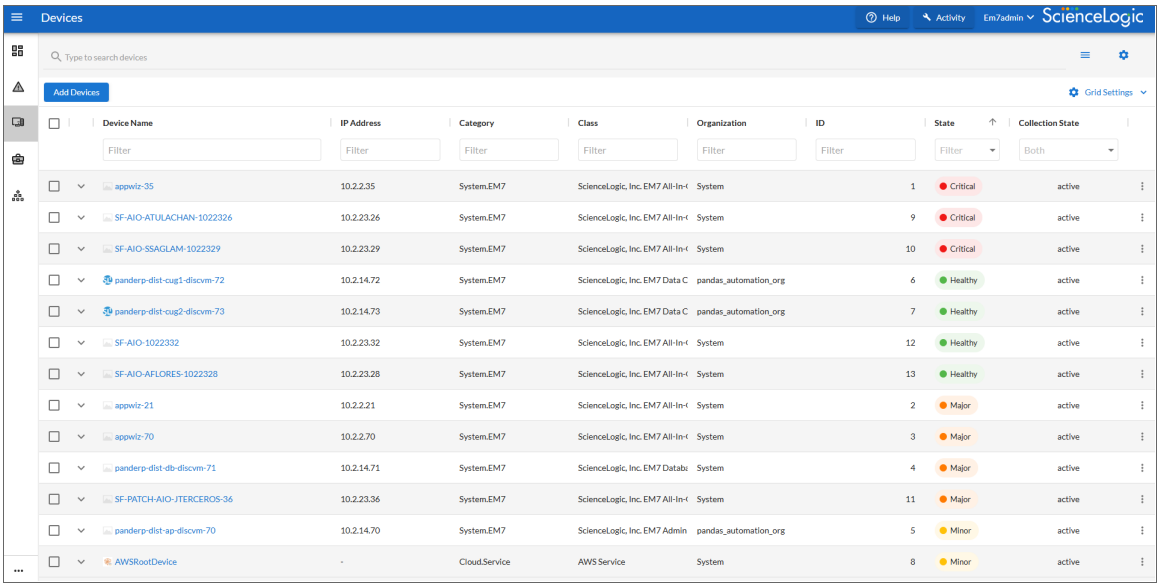
Each event includes a description of the problem, where the problem occurred (device, network hardware, software, policy violation), a pre-defined severity, the time of first occurrence, the time of most recent occurrence, and the age of the event.

For more information, see the *Events* chapter.

Devices

As part of monitoring your network, SL1 collects data using common networking protocols. Most collected data is associated with a ***device*** in SL1. A device in SL1 is a record that can represent physical network hardware, a component of a larger system, or any other entity about which you want to collect data. For example, you might configure a device record that represents a web site or a cloud service.

To navigate to the **Devices** page, click the Devices icon ( ) on the navigation bar:



SL1 allows you to monitor and manage hardware and applications within your network. SL1 provides a network-wide view through a "single pane of glass." This means that you can monitor status, create policies, define thresholds, and receive notifications, all through a single, browser-based application.

For more information, see the ***Devices*** chapter.

Discovery and Credentials

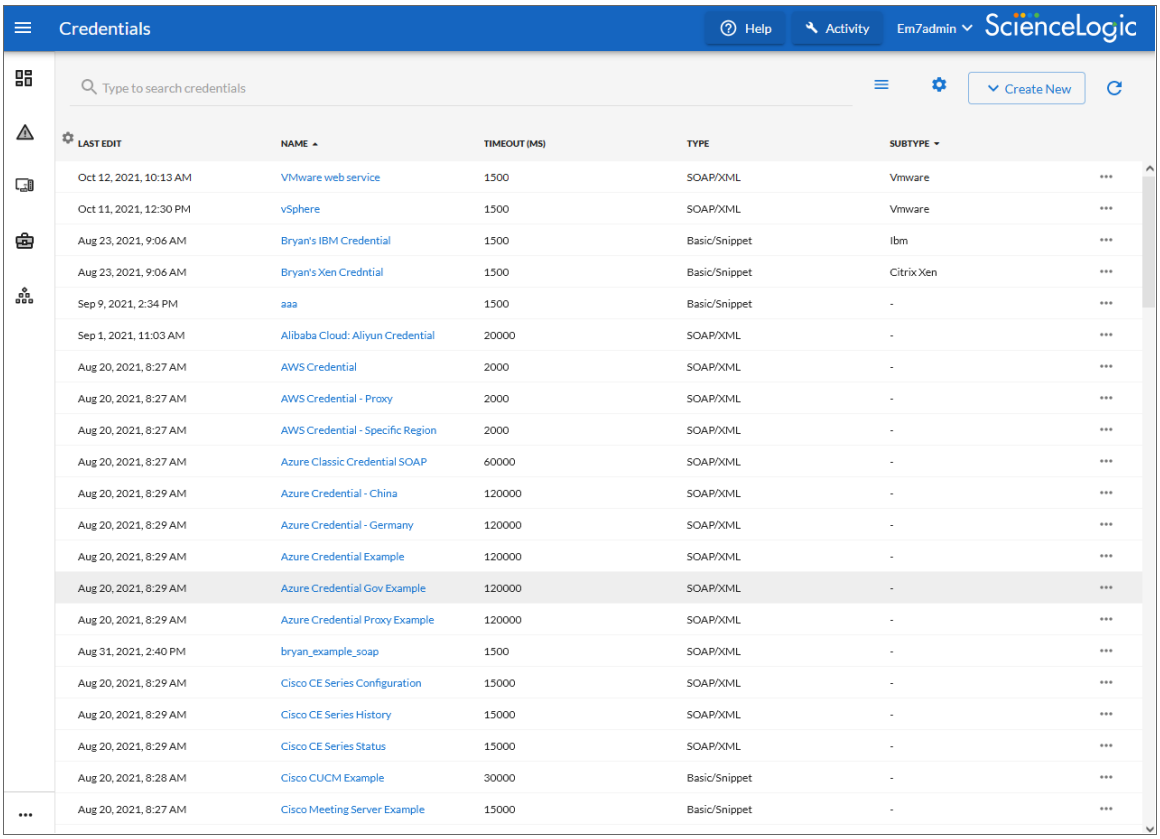
Discovery is the tool that automatically finds all the hardware-based devices, hardware components, and software applications in your network.

You can use the Universal Discovery Framework process in SL1 that guides you through a variety of existing discovery types in additional to traditional SNMP discovery. This process, which is also called "guided discovery", lets you pick a discovery type based on the type of devices you want to monitor. The Universal Discovery workflow includes buttons for the following discovery types: Alibaba Cloud, Amazon Web Services, Microsoft Azure, Citrix, and IBM Cloud. The SNMP Discovery used in the classic user interface is also available, and is sometimes called "unguided" Discovery.

To run a Universal Discovery or an "unguided" Discovery, go to the **Devices** page ( ) and click the **[Add Devices]** button to start the Discovery wizard.

Credentials are access profiles (usually username, password, and any additional information required for access) that allow SL1 to retrieve information from devices and from software applications on devices. Discovery uses SNMP credentials to retrieve SNMP information during initial discovery and nightly auto-discovery. If SL1 can connect to a device with an SNMP credential, SL1 deems that device "manageable" in SL1.

To navigate to the **Credentials** page, go to Manage > Credentials:



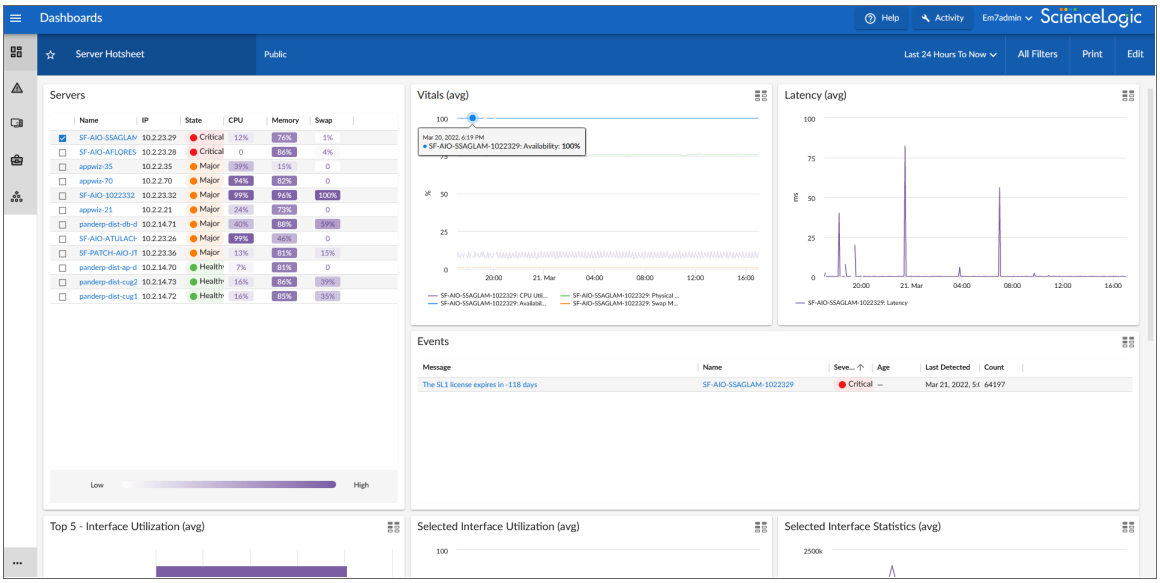
For each device, hardware component, or software application the discovery tool "discovers", the discovery tool can collect a list of open ports, DNS information, SSL certificates, list of network interfaces, device classes to align with the device, topology information, and basic SNMP information about the device.

For more information, see the ***Discovery and Credentials*** manual.

Dashboards

A ***dashboard*** is a page that displays one or more graphical reports, called ***widgets***. These widgets appear in their own pane, and display charts, tables, and text. To define a widget, you first select from a list of pre-defined widget definitions, and then customize what will be displayed by the selected widget by supplying values in the option fields provided by that widget.

To navigate to the **Dashboards** page, click the Dashboards icon ( ) on the navigation bar.



Access to dashboards is based on your login credentials, so you can view only dashboard data for which you have access. Also, some dashboards might be private instead of public.

TIP: If an item name displays as a hyperlink in a dashboard, you can click that link to go to the relevant detail or **Investigator** page for that item. You can click dashboard links to the **Investigator** pages for devices, events, and services.

NOTE: You cannot use dashboards and widgets that were created in the classic user interface in the SL1 user interface.

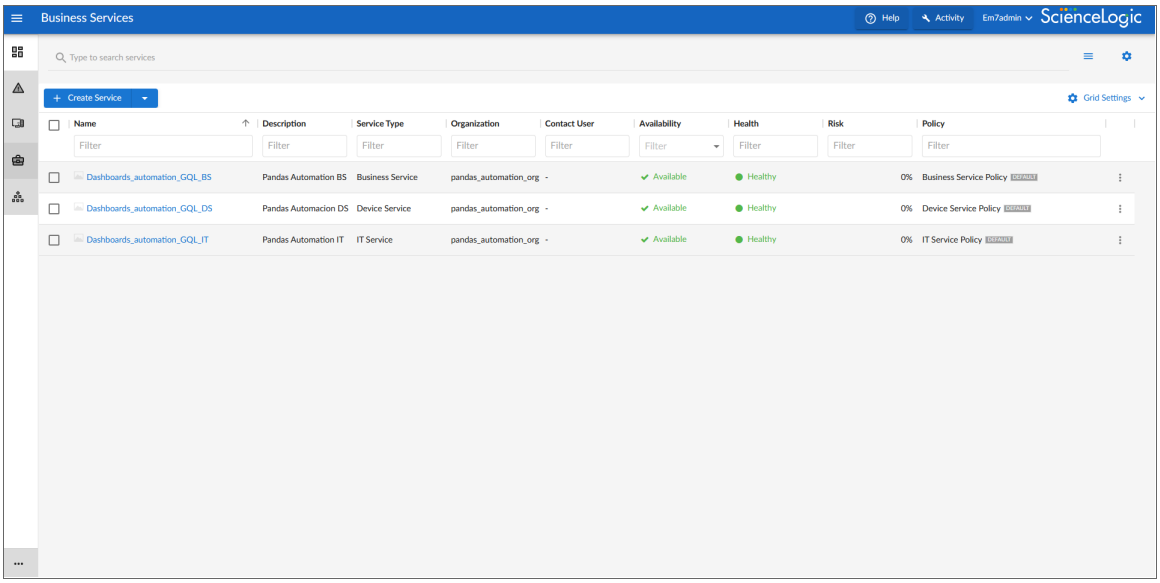
For more information, see the ***Dashboards*** manual.

Business Services

A ***business service*** includes one or more technical services that provide value to internal or external customers. Some examples of business services include verifying Internet access or website hosting, online banking, remote backups, and remote storage. Usually a business service includes an associated Service Level Agreement (SLA) that specifies the terms of the service.

NOTE: Business Services are only available in the SL1 user interface.

To navigate to the **Business Services** page, click the **Business Services** icon ( ) on the navigation bar:



You create the following types of services on the **Business Services** page, in the following order:

1. ***Device Service***. Monitors a set of related devices, such as all devices from a specific region.
2. ***IT Service***. Monitors a service that IT provides to your organization. An IT service is made up of one or more device services.
3. ***Business Service***. Monitors a service your organization provides to your customers. A business service is made up of one or more IT services.

NOTE: Business Services and IT Services created in the classic SL1 user interface are *not* included in the new Business Services, and "classic" Business Services and IT Services are not related in any way to the new business services, IT services, and device services. For more information about the classic versions, see the ***Service Provider Utilities (formerly Business Services)*** and ***IT Services (Classic)*** manuals.

For more information, see the ***Business Services*** manual.

Machine Learning-based Anomaly Detection

Anomaly detection is a technique that uses machine learning to identify unusual patterns that do not conform to expected behavior.

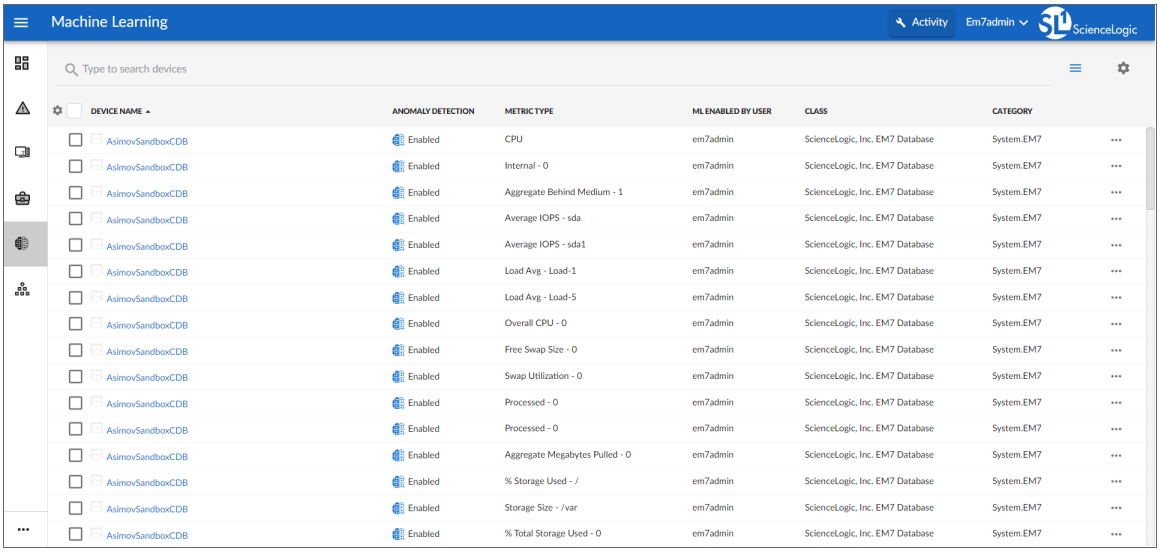
SL1 does this by collecting data for a particular metric over a period of time, learning the patterns of that particular device metric, and then choosing the best possible algorithm to analyze that data.

SL1 uses the resulting combination of collected data and the auto-selected algorithm to build a model that is unique to that specific device and metric. That model is then used to anticipate the expected behavior for that device metric. Anomalies are detected when the actual collected data value falls outside the boundaries of the expected value range.

SL1 then continuously refines the model as it collects more data.

TIP: Anomalies do not necessarily represent problems or events to be concerned about; rather, they represent unexpected behavior that you might want to investigate.

To navigate to the **Machine Learning** page, click the **Machine Learning** icon ( ) on the navigation bar:



NOTE: Anomaly detection and the **Machine Learning** page are only available in the SL1 user interface.

For more information, see the ***Machine Learning-based Anomaly Detection*** manual.

Maps

A ***map*** is a visual representation of the various devices and related elements, also called ***nodes***, in your environment that have been discovered by SL1. A map displays the important details about the nodes, their hierarchy, and the relationships associated with those nodes.

To view a map, click the **Maps** icon ( ) on the navigation bar, and then click the name of the map from the **Maps** page.

Maps can display business services, component maps (DCM, DCM+R), CDP topology, LLDP topology, Layer-2 topology, Layer-3 topology, and Virtual Infrastructure (VMware and virtual machines). You can also create your own maps with your most important devices, and add images, text, and shapes to customize your maps.

NOTE: Maps are only available in the SL1 user interface. They are directly related to "Classic Maps", which were called "Views" in the classic user interface. You can view HTML (non-Flash) versions of these Maps on the **Classic Maps** page (Maps > Classic Maps).

For more information, see the ***Maps*** manual.

Chapter 2

Using the SL1 User Interface

Overview

This chapter describes the key features of the SL1 user interface, including how to access SL1 and get help, how to perform basic and advanced searches, how to set user preferences, and more.

For more an overview of the SL1 user interface, view the video at https://sciencelogic.com/product/resources/navigate-the-sl1-ui.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Logging In and Out of the SL1 User Interface 20
Using the Navigation Menus 22
Filtering Inventory Pages 22
Using Basic Search 23
Performing an Advanced Search 27
Performing Bulk Actions 43
Customizing the SL1 User Interface 44
Getting Help and More Information 44

Logging In and Out of the SL1 User Interface

This topic covers how to access the different user interfaces for SL1: the "new" SL1 user interface and the "classic" user interface.

Starting with SL1 version 11.1.0, the SL1 user interface is the default user interface, not the classic.

NOTE: If your 11.1.0 or later SL1 system was installed using an ISO, the SL1 user interface is set as the default, but if your SL1 system was upgraded with a patch, the classic user interface will still be set as the default user interface. To change the default user interface (UI), edit the *New UI Default* option on to the **Behavior Settings** page (System > Settings > Behavior).

The SL1 User Interface

Starting with SL1 version 11.1.0, you no longer need to type **/ap2** at the end of the URL or IP address, such as **https://sl1.sciencelogic.com/ap2**, to get to the SL1 user interface. The **/ap2** is added to the IP address by default.

To log in to the SL1 user interface:

1. In a browser, type the URL or IP address for your SL1 system. The login page for SL1 appears.
2. Type the current user name and password you use with SL1 and click **Log In**. The SL1 login button displays a spinning status icon while you are being logged in.
3. If your company uses Single Sign-On (SSO) for authentication, you will be redirected to your company's SSO page, where you can log in to SL1 with your SSO credentials. When you log out, the logout screen redirects you to an SSO page instead of the typical login screen.
4. If you are logging in for the first time, you will be prompted to change your password. Type your username, your old password, and type your new password twice in the *New Password* and *Confirm Password* fields. Click **[Reset Password]**.
5. If your SL1 system is a Military Unique Deployment (MUD) system, a Disclaimer modal appears, and you will need to click **[OK]** after reading the text to use SL1.
6. For an Administrator user, the End User License Agreement (EULA) appears the first time the Administrator user logs in to SL1. The user must agree to the terms before using SL1.

TIP: If you can still see the horizontal NavBar or other features of the classic user interface in the SL1 user interface, click **[Refresh]** in your browser.

NOTE: A number of classic user interface pages exist within a frame in the new SL1 user interface, and these pages have the same appearance and functionality in both user interfaces. These pages will eventually be integrated into the SL1 user interface, and the corresponding GraphQL APIs for those feature are not yet available. If you navigated to a classic (framed) page in the SL1 user interface by typing **/em7** in the URL to go to the classic user interface, the top navigation might be missing from the classic user interface. To address this issue, navigate back to the new user interface, log out, and then log in to the classic user interface.

To log out of the SL1 user interface:

1. Click your user name in the navigation bar at the top of any SL1 page.
2. Click **Log off**. You are logged out, and a logoff page appears with the option to log in again.

The Classic User Interface

To log in to the classic user interface for SL1:

1. In a browser, type the URL or IP address for your SL1 system, followed by **/em7**. The login page for the classic user interface appears.
2. Type the current user name and password you use with SL1 and click **Log In**.

TIP: You can log out of the classic user interface by typing **/em7/logout.em7** at the end of the URL or IP address.

3. To switch to the SL1 user interface while you are using the classic user interface, type **/** at the end of the URL or IP address for your SL1 system and press **[Enter]**. The login page of the SL1 user interface appears.
4. To switch to the classic user interface while you are using the SL1 user interface, type **/em7** at the end of the URL or IP address for your SL1 system and press **[Enter]**. The login page for the classic user interface appears.
5. To make the classic user interface the default interface, go to the **Behavior Settings** page (System > Settings > Behavior) and unselect the *New UI Default* option.

TIP: If you need to run both the classic and SL1 user interfaces simultaneously, you can open the classic and the SL1 version in two different browsers, or you can open private or incognito browser windows and then log in to the two user interfaces.

Using the Navigation Menus

Starting with the 8.12.0 release of SL1, the SL1 user interface was upgraded to include content from both the "new" user interface (also called "ap2") and the "classic" user interface. This "unified" user interface provides a more streamlined method of navigation that uses two menus: a ***basic menu*** and an ***Advanced menu***.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ) at the top left of any SL1 page. Use the up and down arrow buttons ( ) to expand and contract the menu options.
- To view the **Advanced Menu** page, which contains links to *all* of the menu options, click the Advanced menu icon ( ) at the bottom left of any SL1 page. Use **[Ctrl]**+**[F]** in your browser to quickly find a page.

TIP: If you are familiar with the classic user interface, the **Advanced Menu** page will help you get used to the structure of the SL1 user interface.

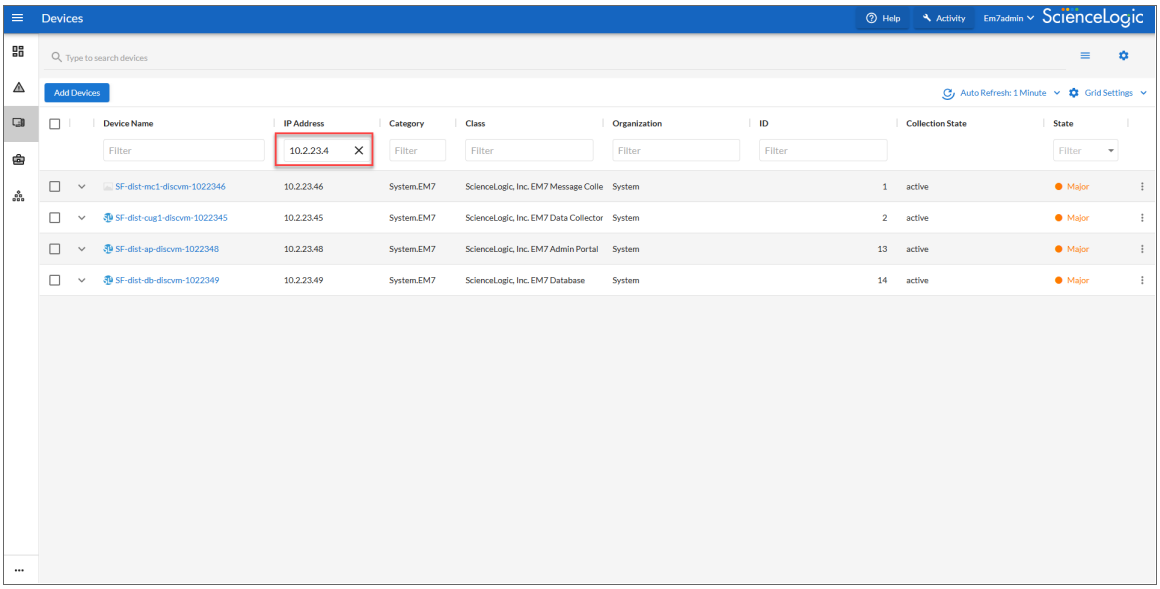
TIP: The name of the SL1 page appears in the title bar of your browser, and the page title also appears in your browsing history to help you navigate through the pages you have visited.

Filtering Inventory Pages

In SL1, an ***inventory page*** is any page (or tab) that contains a table with a list of items that you work with, like the **Events** page or the **Devices** page. At the top of most inventory pages in the SL1 user interface are a set of filters for the columns in the table on that page.

On an inventory page, you can start typing filter text or select filter options in one or more of these filters to narrow down the items in the list to just the items you want to view.

In the following image, the user is filtering the **Devices** inventory page by typing part of an IP address in the filter for the **IP Address** column:



As you type text in the ***Filter*** field at the top of a column, SL1 starts to filter the list to include only those elements that include your search terms.

Some filters, like the **State** filter, let you click a drop-down arrow to select search options from a drop-down menu. Also, any filters related to date and time let you click a calendar icon () to select a date or a date range, and a clock icon (), where relevant, to select a time or a time range.

NOTE: If you were using a version of SL1 from before version 11.2.0, any list and column preferences you had configured will *not* be retained with the new features for inventory pages after you upgrade to 11.2.0 or later. This includes customizations such as which columns are visible, column widths, column order, and other customizations.

SL1 retains your search filters on pages in the SL1 user interface even after you refresh the browser or navigate to another page and then return to the page where you created your search.

For more information, see the ***Introduction to SL1*** manual

Using Basic Search

At the top of most lists in the SL1 user interface, the ***Search*** field lets you look for specific elements in that list. The ***Search*** field contains a magnifying glass icon () next to the words "Type to search" or "Search".

As you type text in the ***Search*** field, SL1 filters the list to include only those elements that include your search terms. When searching, SL1 considers all relevant columns for the search, including those that are not currently displayed on the page.

SL1 retains your search criteria on pages in the SL1 user interface even after you refresh the browser or navigate to another page and then return to the search page using the **[Back]** button in the browser.

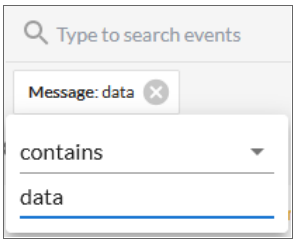
> **TIP:** After you type search commands in the ***Search*** field, you can click the gear icon (⚙) and select *Advanced* to "translate" your basic search into an Advanced Search. For more information, see *Performing an Advanced Search*.

To use the ***Search*** field:

1. Click the ***Search*** field and start typing search text. As you type, SL1 provides potential matching values in a drop-down menu and starts filtering the list with your search text.

   > **TIP:** For example, if you start searching for "database" by typing *data*, a drop-down list appears with a list of columns that might contain that word, and the list is filtered by items that have "data" in one of their fields.

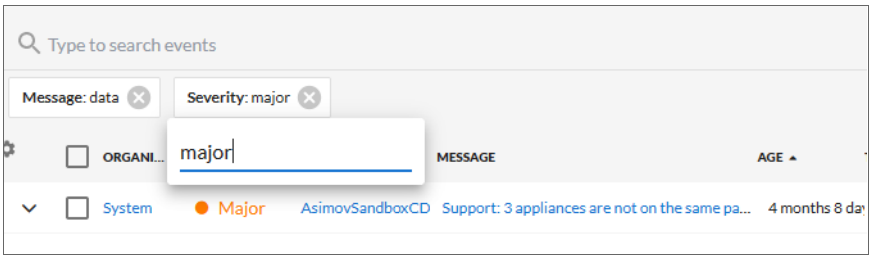
2. If you select one of the suggested search criteria from the list, such as *message*, a ***criteria button*** displays under the ***Search*** field. You can click the criteria button and edit the search text under the button, if needed:



   > **TIP:** If you select the *ANY* option from the drop-down menu, the search looks through all relevant columns for matches to your search text. SL1 uses different search criteria for an "ANY" search, depending on the page you are currently on in SL1. For more information, see *Fields Used by an "ANY" Basic Search*.

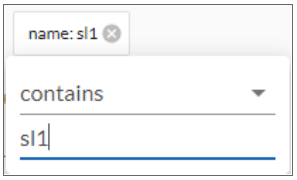
   > **NOTE:** If you are unable to paste a copied string of text in the ***Search*** field, make sure that your copied text does not contain any hidden special characters.

3. To edit the search criteria for your current search even further, click the criteria button and click the *contains* field. You can choose from additional search operators in the drop-down that appears, such as *begins with*, *is null*, *equal to*, and *not equal to*.
4. You can add another set of search criteria to an existing search by typing additional text in the ***Search*** field, and then selecting additional fields from the drop-down list. The new search terms are added to a second criteria button:



> **TIP:** The search criteria button under the ***Search*** field also displays the search operator and value for the search as hovertext.

5. Alternately, you can click the menu icon (☰) to the right of the ***Search*** field to open a menu containing related search criteria. Select an element from the list of criteria and type additional search information in the criteria button that appears under the ***Search*** field:



> **TIP:** If you select a date-related search criteria from the list of criteria, you can use a drop-down calendar to select a specific date and time.

6. To *remove* a search criteria, click the close icon (⊗) on the criteria button under the ***Search*** field.
7. To switch to an Advanced Search, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. For more information, see *Advanced Search*.
8. To quickly clear a search, click the gear icon (⚙) to the right of the ***Search*** field and select *Clear*.
9. To save a search so you can use it again, see *Saving a Basic Search*.

Fields Used by an "ANY" Basic Search

If you type search criteria into a ***Search*** field at the top of a page in SL1 and then select the *ANY* option from the drop-down menu, the search looks through *all* relevant columns for matches to your search text.

SL1 uses different search criteria for an "ANY" search, depending on the page you are currently on in SL1. For example, an "ANY" search on the **Dashboards** page searches for the search criteria in the Dashboard ID or Dashboard Name fields, while an "ANY" search on the **Devices** page searches for the search criteria in the Device Name, Hostname, Device Class, Collector Group, Organization, and additional fields. See the table below for details.

To see which fields SL1 is using for a search, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. The syntax of the Basic Search is converted into an Advanced Search, which lists the relevant fields being searched by SL1.

The following table lists the fields that are used by an "ANY" search, based on the page you are on in SL1:

Page in SL1 user interface	Fields searched by SL1 for that page
Main Pages	
Dashboards	Dashboard ID, Dashboard Name
Events	Event Message, Aligned Resource Name, Aligned Organization, Aligned Sub-entity Name, Device Name, Hostname, Device Class Logical Name, Device Class Description, Device Collector Group, Device Class, Device Group ID, Device Group Name, Device Class Category
Devices, Machine Learning, Device Services	Device Name, Hostname, Device Class Logical Name, Device Class Description, Device Class, Device Group, Device Class Category Name, Collector Group ID, Collector Group Name, Aligned Organization, Machine Learning Policy
Business Services and IT Services	Service Type, Service ID, Service Name, Service Label, Service Policy Name, Aligned Organization
Maps	Map Name, Map Description
Secondary Pages	
Agents	Agent Nickname, Agent Operating System, Hostname
Business Service Templates	Business Service Template Name, Business Service Template Descriptions
Credentials	Credential Name
Custom Attributes	Custom Attribute Label, Custom Attribute Name
Device Categories	Device Category Name
Device Classes	Device Class Name, Device Class Description, Virtual Type, Logical Name, Device Category Name
Discovery Sessions	Discovery Session Name, Aligned Collector Name, Aligned Organization
Event Policies	Event Policy Name
Subscription Usage (Current License Usage)	License Type, Device Name, Aligned Organization, Device Class Category Name

If a page from the SL1 user interface is not listed in the above table, then SL1 only uses the relevant Name field on that page for an "ANY" search.

Saving a Search

If you are creating a complicated search using Basic Search or Advanced Search, or if you have a search that you use on a regular basis, you can save that search criteria so you can quickly use it again later.

To save a search:

1. After you have created a Basic or Advanced Search, click the gear icon (⚙) to the right of the ***Search*** field and select *Save*. A **Save Search** window appears.
2. In the ***Search Name*** field, type the name of your search and click **[Save]**. The search is added to the list of saved searches.

To use a saved search:

1. Click the gear icon (⚙) to the right of the ***Search*** field and select *Saved Searches*. An **Apply Search** window appears.
2. From the ***Select a search*** drop-down, select the search you want to use and click **[Apply]**. That search is applied to the current list.

> **NOTE:** By default, saved searches apply only to *your* user profile, and they are not shared with other users.

To share a saved search:

1. Create a Basic Search and change it to an Advanced Search by clicking the gear icon (⚙) to the right of the ***Search*** field and selecting *Advanced*.
2. Copy the Advanced Search code from the ***Search*** field and paste it into the relevant documentation so you can share the search with other users.

Performing an Advanced Search

The SL1 user interface includes an Advanced Search option that lets you use customized search commands to search for data. The syntax for these Advanced Searches can be much more complex than a Basic Search, enabling you to find exactly what you need from a list of items.

Also, because the Basic Search only uses "AND" for multiple search criteria, you need to use an Advanced Search for an "OR" search using multiple search criteria, or if you want to create more complicated searches using Boolean Algebra.

At a minimum, an Advanced Search requires the following components, in the following order:

- A ***field***. The general type of data for which you are searching, such as a device name or an event message.
- An ***operator***. A word or symbol that specifies the relationship between the field and the value, such as equals or less than.

- A ***value***. A specific aspect or version of the field, such as a name or an amount. If a value is a string, it should be surrounded by "quotation marks" or 'apostrophes'.

TIP: As you type your Advanced Search, a red icon ( ) or a green icon ( ) appears at the end of the text field to show that your search is incorrectly or correctly formatted.

TIP: To view a list of all possible search commands in an Advanced Search, press **[Ctrl]** + **[Space]**.

The Advanced Search fields and values vary based on the page you are on in the SL1 user interface. For more information about fields, operators, and values, see *Components of an Advanced Search*.

Below are simple examples of Advanced Search syntax:

```
message contains 'risk is high'
organization has (company contains 'system')
attribute has (id = year and value = 2021)
name contains 'web_tier' and deviceClass has (description contains 'AppDynamics')
deviceClass has (description contains 'em7 admin portal')
```

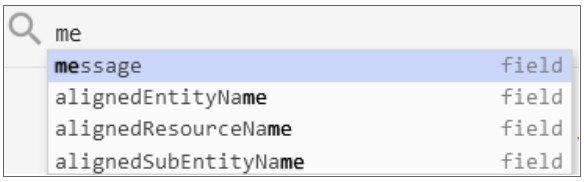
For additional examples, including examples with more complex syntax, see *Examples of Advanced Searches*.

TIP: You can type search commands in the ***Search*** field for a Basic Search, and then click the gear icon ( ) and select *Advanced* to "translate" your basic search into an Advanced Search. You cannot go from an Advanced Search back to a Basic Search, however, without losing your search criteria.

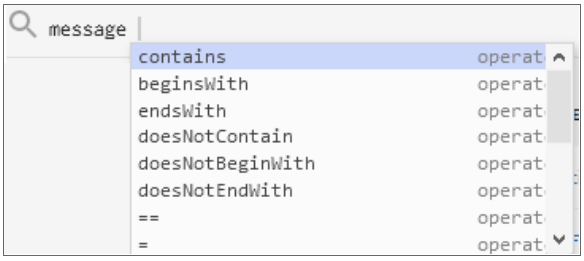
To create an Advanced Search:

1. Click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. The search type changes from Basic to Advanced (note the change in font style).

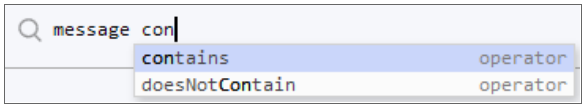
2. Start typing a field name for your search. As you type, SL1 displays a list of available fields in a drop-down menu:



3. Select or type a field name.
4. To view a list of all possible search commands at any point in an Advanced Search, press **[Ctrl+Space]**. For example, the following operator options appear if you press **[Ctrl+Space]** after typing "message" and inserting a space:



5. Select or type an operator name. If you are typing, SL1 provides a list of available options.



> **TIP:** As you type your search command, a red icon ( ) appears at the end of the text field if your command is incorrectly formatted or incomplete. Click the red icon to view additional details.

6. Type a value to complete your search, and type additional search commands as needed. When your search is complete and formatted correctly, a green icon ( ) appears at the end of the text field:

7. Click the **[Search]** button. The results of your search appear.

> **NOTE:** Even if you have correct search syntax, SL1 will save your search query only *after* you click **[Search]**. For example, some pages, such as a Device Service search, might not show all of the search results until you click **[Search]**.

8. To clear a search, click the gear icon (⚙) to the right of the ***Search*** field and select *Clear*.
9. You can save an Advanced Search to use later. By default, saved searches apply only to *your* user profile, and they are not shared with other users. For more information, see ***Saving a Search***.

Components of an Advanced Search

At the minimum, an Advanced Search requires the following components, in the following order:

- A ***field***. The general type of data for which you are searching, such as a device name or event message.
- An ***operator***. A word or symbol that specifies the relationship between the field and the value, such as equals or less than.
- A ***value***. A specific aspect or version of the field, such as a name or an amount. You must use either "quotation marks" or 'apostrophes' for your search strings, and strings are not case-sensitive.

You can also include the operators "and" or "or" to your search command. Basic Search in SL1 uses only "AND" searches, unless you specify "Any" in your Basic Search.

NOTE: When SL1 evaluates an Advanced Search command, it evaluates the "OR" expressions first, followed by the "AND" filters.

For example, the following search command looks for events that have a status of Critical *and* contain a message with the word "error":

```
status = critical and message contains 'error'
```

The following search command looks for devices with a name of "device-name" *or* messages containing the word "error":

```
name = "device-name" or message contains "error"
```

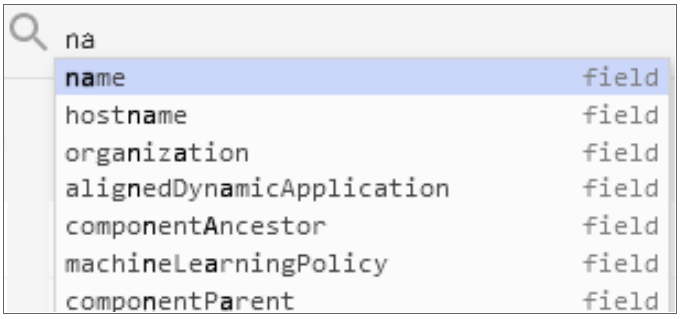
You can use parentheses ( ) to group expressions and to ensure that the expressions are evaluated in the correct order. The following search command looks for either devices with a name of "device-name" and a status of Critical, *or* devices with a name of "device-name" and a status of Major:

```
(name = "device-name" and status = critical) or (name = "device-name" and status =
Major)
```

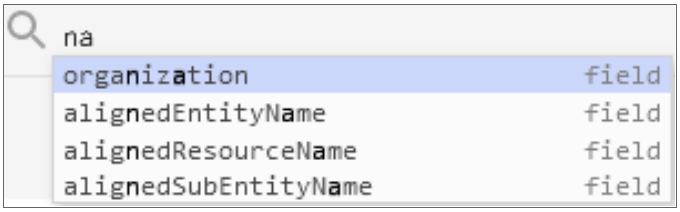
TIP: Searches in SL1 are *not* case-sensitive, so you can use any combination of upper-case and lower-case letters.

Fields

For most searches, you start your search command with a field name. When you start typing in an Advanced Search field, SL1 provides a list of potential fields in a drop-down menu that you can select for your search command:



The list of potential fields depends upon the page you are currently on in SL1. The example above is from the **Advanced Search** field on the **Devices** page. If you typed the same letters in the **Advanced Search** field on the **Events** page, the drop-down menu would look like this:



The following table lists some of the more common fields, along with how to use them and examples of search commands that use those fields:

Field name	Purpose	Example
`alignedResourceName`	Search for the name of a device aligned with an event.	`alignedResourceName contains "lab"`
`asset`	Search for an asset aligned with a device.	`asset has (assetTag contains 1)`
`attribute`	Search for devices based on custom attributes. In the example, the custom attribute is "year" and the value is "2021".	`attribute has (id = year and value = 2021)`
`dateCreated`	Search for the date and time a device was created.	`dateCreated isNotNull`
`deviceClass`	Search for devices belonging to a device class.	`deviceClass has (class contains 'Cisco')`
`deviceGroup`	Search for devices belonging to	`deviceGroup has (name contains`

Field name	Purpose	Example
	a device group.	"Network")
hostname	Search for a device hostname	device has (hostname = "srv")
id	Search for the unique numeric ID assigned by SL1.	id contains "10"
isAcknowledged	Search for events that have or have not been acknowledged.	isAcknowledged = true
message	Search for details about an event message.	message contains "problem"
name	Search for the name of the device.	name = "server"
organization	Search for the organization to which the device is assigned.	organization has (company = "System") organization has (company doesNotContain 'ABC Systems')
severity	Search for the severity of an event; severities range from 0 to 4, from Healthy to Critical.	severity in 3,4 Searches for all Major and Critical events.
state	Search for the state of a device; states range from 0 to 4: Healthy, Notice, Minor, Major, and Critical.	state in 0,1,2 Searches for all devices with a state of Healthy, Notice, and Minor.
suppressGroup	Hide data related to the specified group.	suppressGroup = sciencelogic

Operators

For most searches, you follow a field with an operator. The operator establishes a relationship between the field and the value that comes after the operator.

TIP: The list of available operators changes based on the page where you are making your search.

The following table lists some of the more common operators, along with how to use them and examples of search commands that use those operators:

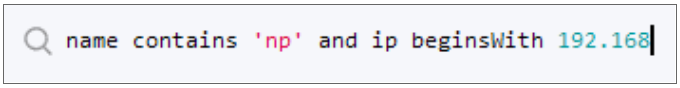
Operator name	Purpose	Example
and	Include two or more search criteria before producing search results	deviceClass has (description contains 'rds instance') and name contains 'wordpress'
or	Include at least one of multiple search criteria.	name = "server" or message contains "error"
=, ==, eq	The field and the value are equal.	name == 'ECS 23' and ip doesNotContain '.'

Operator name	Purpose	Example
<>, !=, neq	The field and the search value are *not* equal.	field != abc
<, lt	The field is less than the search value.	state < 2
>, gt	The field is greater than the search value.	severity > 3
<=, lte	The field is less than or equal to the search value.	state lte 2
>=, gte	The field is greater than or equal to the search value.	severity gte 3
contains	The field includes the specified string.	deviceClass has (description contains 'em7 admin portal')
doesNotContain	The field does not include the specified string.	name contains 'SL1 Classic' or (description contains 'PowerFlow' and description doesNotContain 'Not Deployed') or (description contains 'Extended Architecture' and description doesNotContain 'Not Deployed')
has	The field contains a specific value. The value following "has" must be enclosed in parentheses.	deviceClass has (deviceCategory has (name contains 'Server')) and deviceClass has (description doesNotContain 'vcenter')
in	The field must be part of a specific set of values.	severity in 2,3,4
not	Opposite values; this operator precedes the field name.	not field = abc
isNull	The field is empty.	extTicketRef isNull
isNotNull	The field is not empty.	counter isNotNull

Values

The value you type at the end of a search command depends on the field name and the operator you use. For most searches, you can type the value instead of picking it from the drop-down menu that lists possible search options.

In the following example, the first search value is a string (red text) and the second search value is a numeric value (blue text):



You must use either "quotation marks" or 'apostrophes' for search strings, and strings are not case-sensitive.

Strings

You can create a search command that searches for a specific set of words in a string. You must use either "quotation marks" or 'apostrophes' for your search strings, and strings are not case-sensitive.

The following table lists some of the more common string operators, along with how to use them and examples of search commands that use those string operators:

String operator name	Purpose	Example
`beginsWith`	Search for strings beginning with a specified value	`message beginsWith "Host Resource"`
`endsWith`	Search for strings ending with a specified value	`message endsWith 'shutdown'`
`contains`	Search for strings containing a specified value	`message contains "problem"`
`doesNotBeginWith`	Search for strings that do not begin with a specified value	`message doesNotBeginWith "front"`
`doesNotEndWith`	Search for strings that do not end with a specified value	`message doesNotEndWith 'warning'`
`doesNotContain`	Search for strings that do not contain a specified value	`message doesNotContain "codec"`

Escape characters

In double-quoted strings (strings surrounded by quotation marks), you can include quotation marks in the search by *escaping* the quotation marks. To escape those characters, add a backslash before each quotation mark, such as `\"`.

For example:

```
"Error in \"process x\""
```

In single-quoted strings, you can include the single-quote character by escaping it with a backslash, such as `\'`.

For example:

```
'Eric\'s Laptop'
'Error in "process x"'
```

TIP: You do *not* need to add quotes around strings in your search commands. However, if your string contains only numbers, you might want to add quotes around it to ensure that SL1 interprets it as a string.

If you do not include quotes around strings in your search commands, you must escape the following characters with a backslash:

- all empty spaces or white spaces
- comma
- end parenthesis

Examples:

```
Eric's\ Laptop
Error\ in\ "process\ x"
devices\ \(system\,\ server\)
```

Other than the escape characters mentioned above, you can escape any character. You must escape the backslash character if you want to use it in a string, such as `\\`.

The normal whitespace escape sequences can be used: `\t` (tab), `\n` (new line), `\b` (backspace), `\r` (carriage return), and `\f` (form feed).

You can also use four-digit Unicode hex escape codes in the form `\uXXXX`.

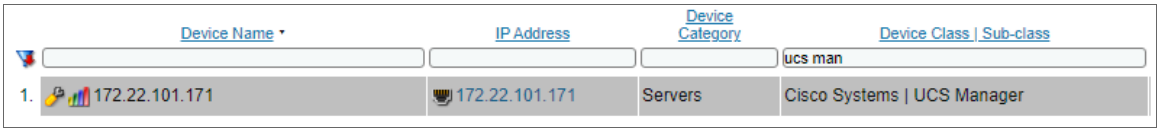
Examples of Advanced Searches

Because the search commands differ for each page in SL1, this section contains a set of search examples based on context.

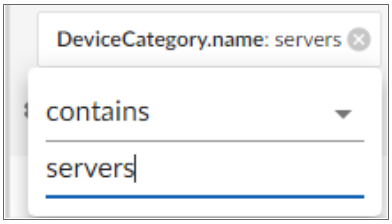
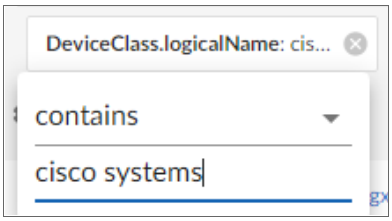
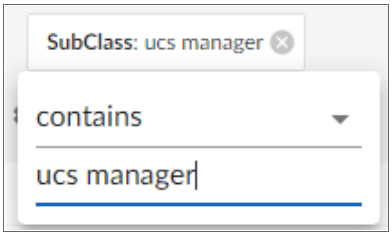
TIP: To view a list of all possible search commands at any point in an Advanced Search, press **[Ctrl+Space]**.

Advanced Search Examples on the Devices Page

When you run a search in the SL1 user interface, SL1 exposes how the data is stored, which is not always obvious in how this translates to Basic and Advanced searches.
For example, if you have the following device on the **Device Manager** page in the classic user interface:



You would use the following Basic and Advanced searches to find the following device data:

Classic User Interface Field	Basic Search Selections	Advanced Search Syntax
Device Category		`deviceClass has (deviceCategory has (name contains 'servers'))`
Device Class		`deviceClass has (logicalName contains 'cisco systems')`
Sub-class		`deviceClass has (description contains 'ucs manager')`

The following table contains additional examples of Advanced Searches for the **Devices** page:

Purpose of Advanced Search on Devices Page	Advanced Search Syntax
Search for all devices with a Device ID of 1, 2, or 3.	`id in 1,2,3`
Search for all devices with "rtp" in the Device Name and an IP Address that starts with 192.168.	`name contains 'rtp' and ip beginsWith '192.168'`
Search for all devices with a custom attribute of "year" and the custom attribute value of "2021".	`attribute has (id = year and value = 2021)`
Search for all devices with a custom attribute of "model" and the custom attribute value of "server" that have "CN" in the Device Name.	`attribute has (id = model and value = server) and name contains "cn"`
Search for all devices that meet the following criteria: • a custom attribute of "SL1ComponentType" and the custom attribute value of "DC"	`attribute has (id eq 'SL1ComponentType' and value eq 'DC') and attribute has (id eq 'SL1Stack' and value eq 'BigBen') and deviceClass has (logicalName contains 'EM7 Data Collector')`

Purpose of Advanced Search on Devices Page	Advanced Search Syntax
• a custom attribute of "SL1Stack" and the custom attribute value of "BigBen" • and a Logical Name of "EM7 Data Collector".	
Search for all devices that meet the following criteria: • aligned with the "Onprem" organization • a Device Class of "Windows Server 2" • and an IP Address that starts with "172".	`organization has (company contains 'Onprem') and deviceClass has (description contains 'windows server 2') and ip beginsWith '172'`
Search for all mail servers based on the organization's naming conventions (all US-based devices start with the prefix of "us-").	`name beginsWith "us-" and name contains "mail" or name contains "smtp"`
Search for all devices aligned with any organization *except* for the System and Smart Tech Business organizations.	`organization has (company doesNotContain System and company doesNotContain 'Smart Tech Business')`
Search for all devices with "01" in the Device Name that belong to the ScienceLogic organization.	`name contains '01' and organization has (company = sciencelogic)`
Search for all devices with a Device Category of "Server" or "System".	`deviceClass has (deviceCategory has (name contains "server")) or deviceClass has (deviceCategory has (name contains "system"))`

Advanced Search Examples on the Events Page

The following table contains a set of sample Advanced Searches for the **Events** page:

Purpose of Advanced Search on Events Page	Advanced Search Syntax
Search for events on devices by Device ID of 1, 2, or 3.	`device has (id in 1,2,3)`
Search for all events that contains the word "error"	`message contains "error"`
Search for all events on devices with a Device Category Name of "xtremio".	`device has (deviceClass has (deviceCategory has (name contains 'xtremio')))`

Advanced Search Examples for Dynamic Component Mapping (DCM) Scenarios

Dynamic Component Mapping (DCM) allows SL1 to collect data from a single management system, such as a VMware ESX server, and then use that data to create multiple device records for the entities managed by that single management system. For example, the managed entities for a VMware ESX server would be the Guest VMs hosted by that ESX server.

The following table contains a set of sample Advanced Searches for DCM devices on the **Devices** page:

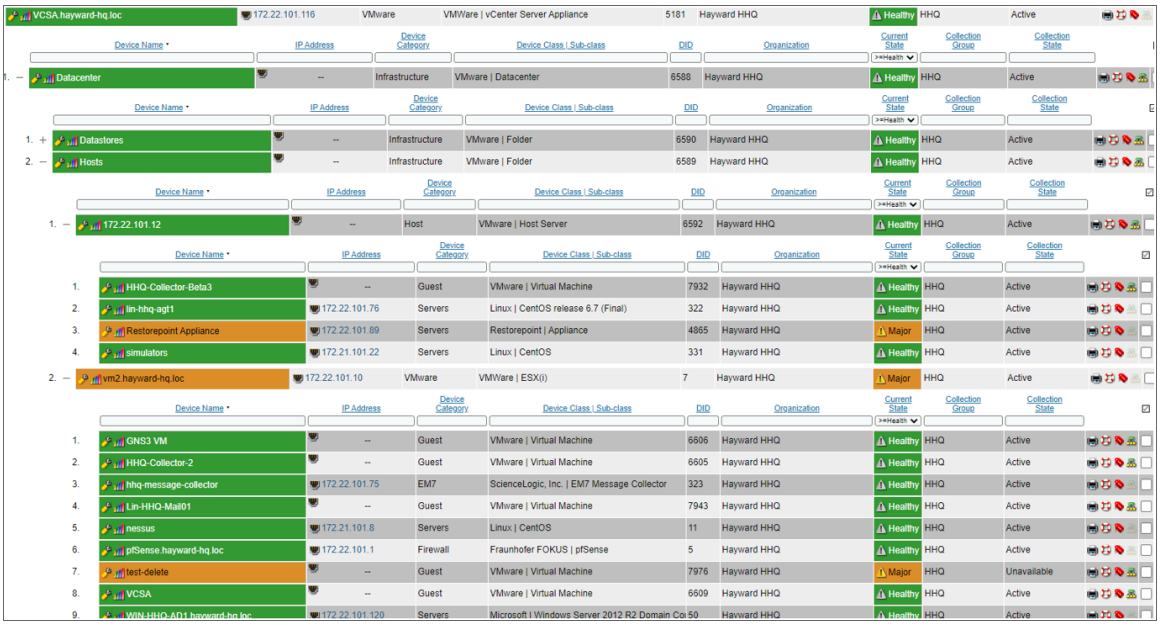
Purpose of Advanced Search	Advanced Search Syntax
Search for all host devices from a specific vCenter and add those devices to a Device Service	`componentRoot has (name contains "VCSA") and (componentParent has (deviceClass has (description contains 'Host Server')) or componentParent has (deviceClass has (description contains 'ESX')))`
Search for SQL servers than run as the master.	`deviceClass has (description contains 'SQL Instance') and componentRoot has (attribute has (id == 'DB_Role'and value contains 'Master'))`

The following sections contain more details about these two Advanced Searches and how they work.

Scenario 1: vCenters

An SL1 system has multiple vCenters, each of which has multiple host servers. You want to include in a Device Service all Virtual Machines (VMs) from just one of the vCenters. This scenario includes the following elements:

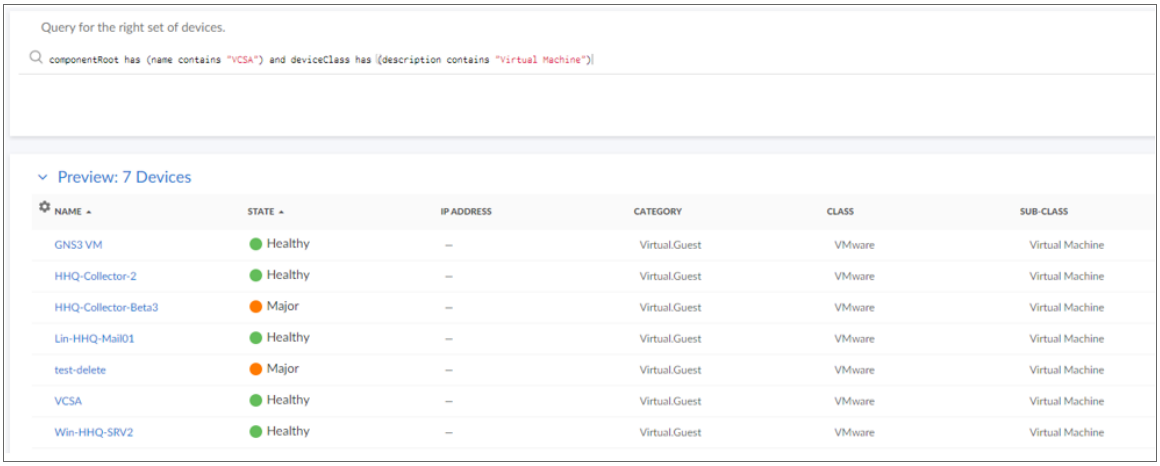
- The vCenter has a host name of **VCSA hayward-hq.loc**
- One of the hosts has a Device Class of **Host Server**, and it contains four VMs
- One of the hosts has a Device Class of **ESX**, and it contains 16 VMs



Search 1a

```
componentRoot has (name contains "VCSA") and deviceClass has (description contains
"Virtual Machine")
```

This search works, but it only returns seven devices instead of the 16 devices you might have expected:



How the query works:

```
componentRoot has (name contains "VCSA")
```

This part of the query returns a list of all devices that have a root with a name that includes VCSA.

```
and deviceClass has (description contains "Virtual Machine")
```

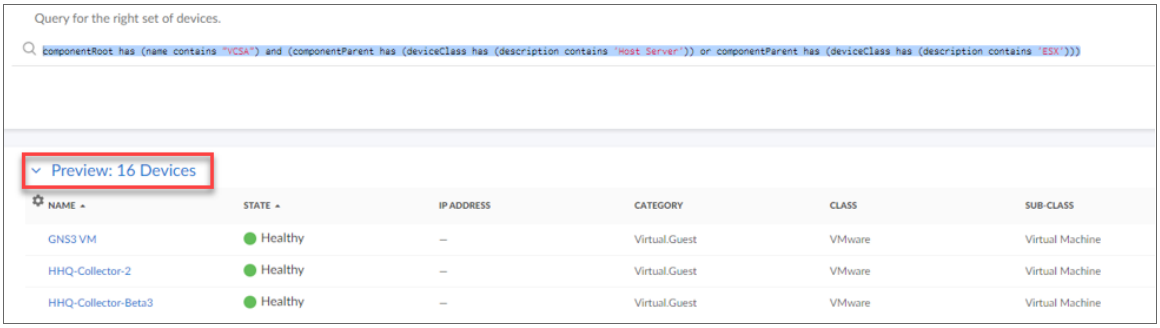
This part of the query filters the results of the first part of the query to isolate the devices with Device Class of **Virtual Machine**

> **NOTE:** The reason why this Advanced Search does not result in the 16 VMs that we can see are hosted by both hosts is that some of the VMs have been *merged*. As a result, their Device Class has been reset to that of the operating system they are running.

Search 1b

```
componentRoot has (name contains "VCSA") and (componentParent has (deviceClass has
(description contains 'Host Server')) or componentParent has (deviceClass has
(description contains 'ESX')))
```

This search successfully returns all 16 VMs:



How the query works:

```
componentRoot has (name contains "VCSA")
```

This part of the query returns a list of all devices that have a root with a name that includes **VCSA**.

```
and (componentParent has (deviceClass has (description contains 'Host Server'))
```

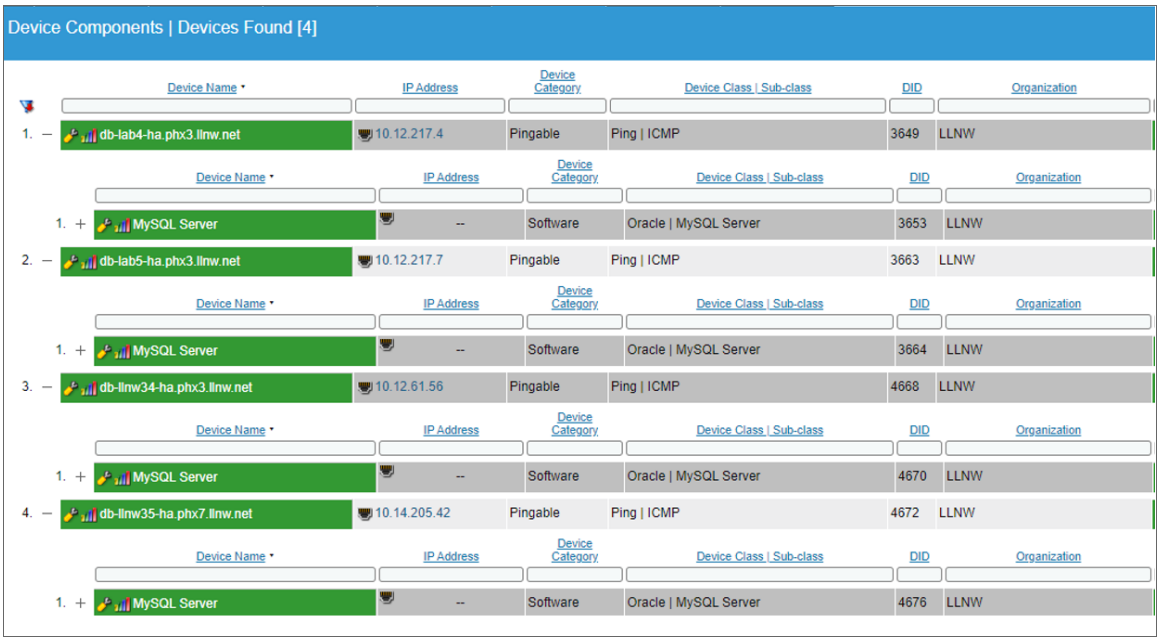
This part of the query filters the results of the first part of the query to isolate the devices that have a parent of the Device Class **Host Server**.

```
or componentParent has (deviceClass has (description contains 'ESX')))
```

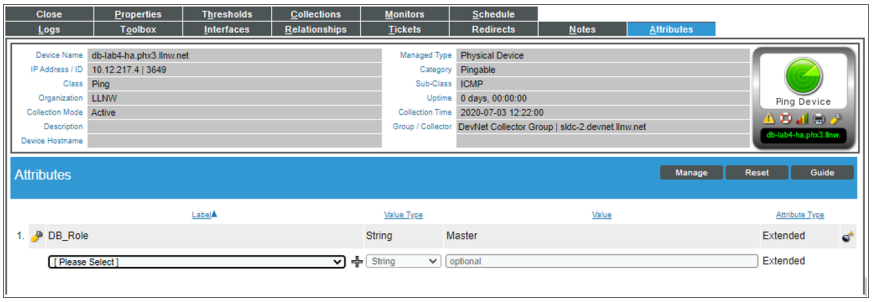
This part of the query then does a second search of the results of the first query, looking for devices with parents that have a Device Class of **ESX**.

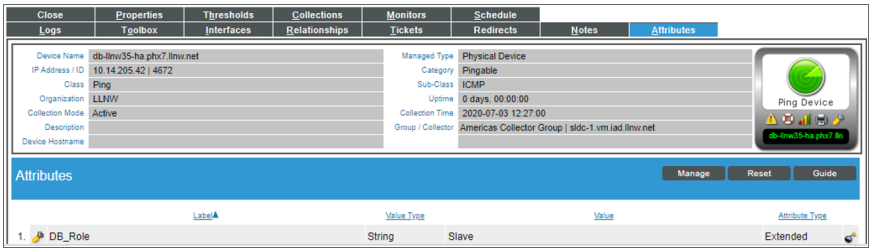
Scenario 2: SQL Servers

A DB Cluster has two SQL Servers than run as the master and two SQL servers that run as the slave:



Four times a year the master and slave is swapped between the two pairs. As this is a planned, infrequent, and manual activity, you can manually swap a custom attribute on the four hosting devices to designate if a device is acting as master or slave:



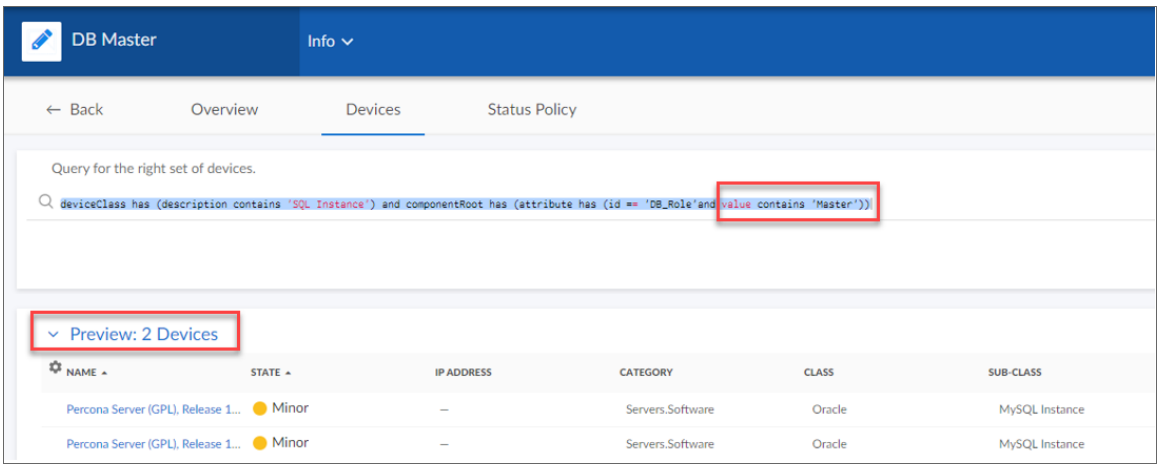


NOTE: For production or higher frequency and automated swapping, making the switch of the custom attributes could be embedded into a switching script and use the API or GQL interfaces to change the value of the custom attributes.

Searches

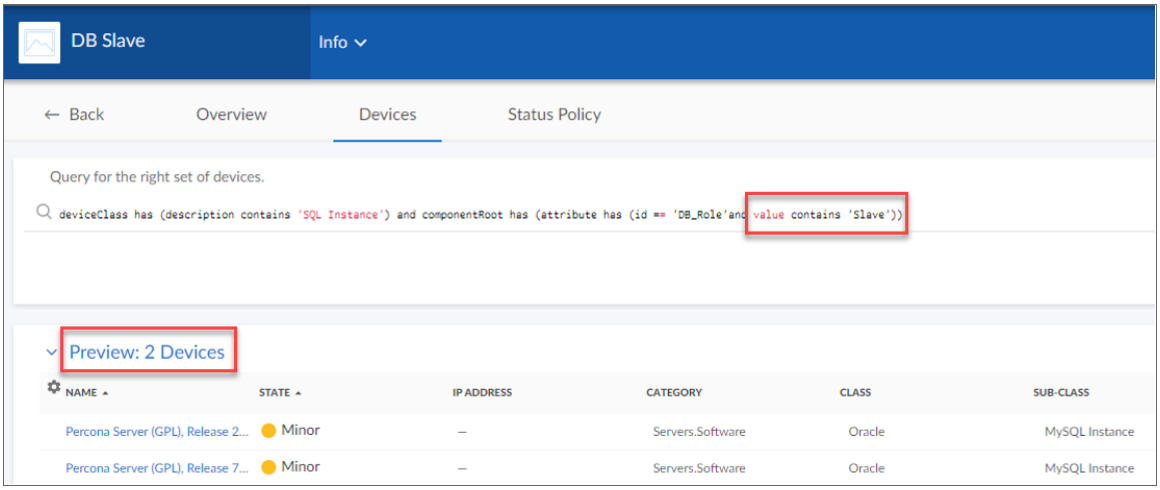
```
deviceClass has (description contains 'SQL Instance') and componentRoot has
(attribute has (id == 'DB_Role'and value contains 'Master'))
```

This search returns the two SQL instances that are running on the two SQL hosts designated as the *master* pair:




```
deviceClass has (description contains 'SQL Instance') and componentRoot has
(attribute has (id == 'DB_Role'and value contains 'Master'))
```

This search returns the two SQL instances that are running on the two SQL hosts designated as the *slave* pair:



How the query works:

```
deviceClass has (description contains 'SQL Instance')
```

This part of the query returns a list of all devices that have a Device Class of **SQL Instance**.

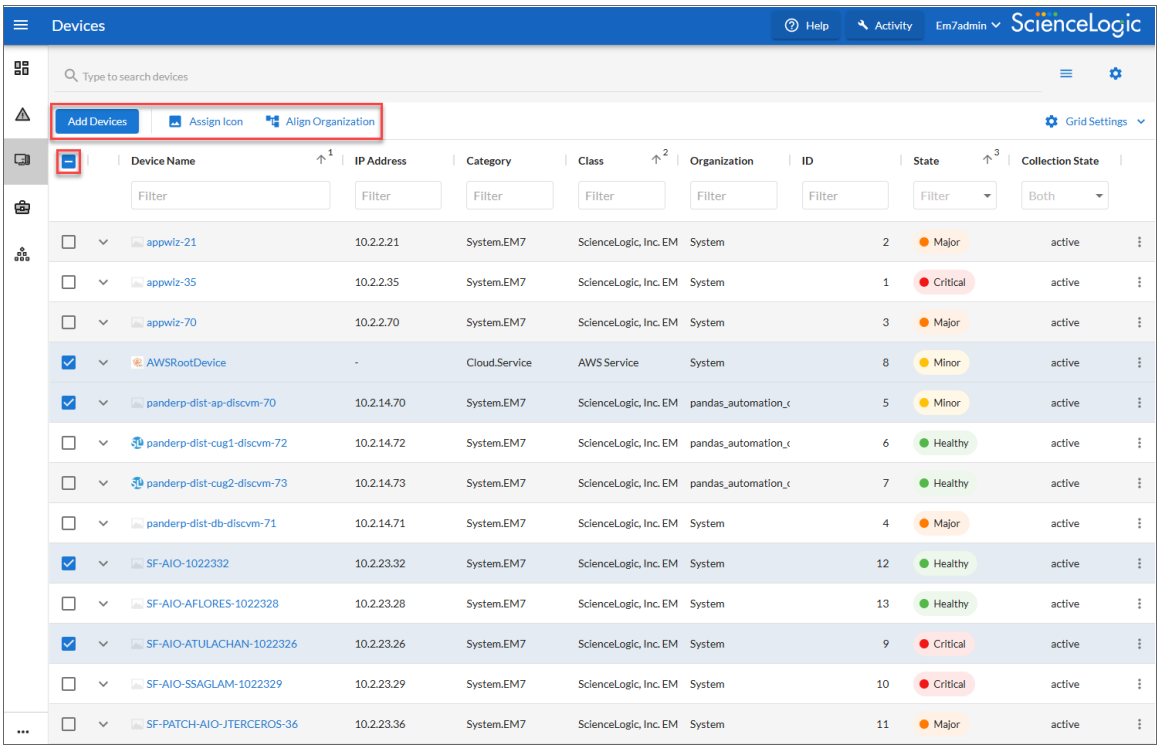
```
and componentRoot has (attribute has (id == 'DB_Role'and value contains 'Slave'))
```

This second part of the query then filters the results of the first query to isolate the devices that have a root device with a custom attribute of **DB_Role** set to *Slave*.

Performing Bulk Actions

If an inventory page in SL1 displays a list of items, and that page contains a checkbox (☐) to the left of each item in the list, you can select two or more items to perform bulk actions on all of the selected items at the same time. For example, on the **Devices** page, you can select two, twenty, or all of the devices on the page, and then you can assign an icon or align an organization with all of the selected devices.

When you use the checkbox to select one or more items in a list, a set of relevant buttons appear at the top of the page. Click a button to run that action on all of the selected devices:



To select all of the items on a page, click the checkbox at the top of the list. To clear all of the selected items, click the checkbox at the top again.

TIP: Pages that contain lists use "infinite scrolling", where the list continues to populate as you scroll toward the bottom of the list. The scrolling stops when you reach the end of the list.

Customizing the SL1 User Interface

A ***theme*** is a graphic template this is applied to the user interface. SL1 includes one System Default theme, but you can completely customize the look and feel of your SL1 system by creating new themes.

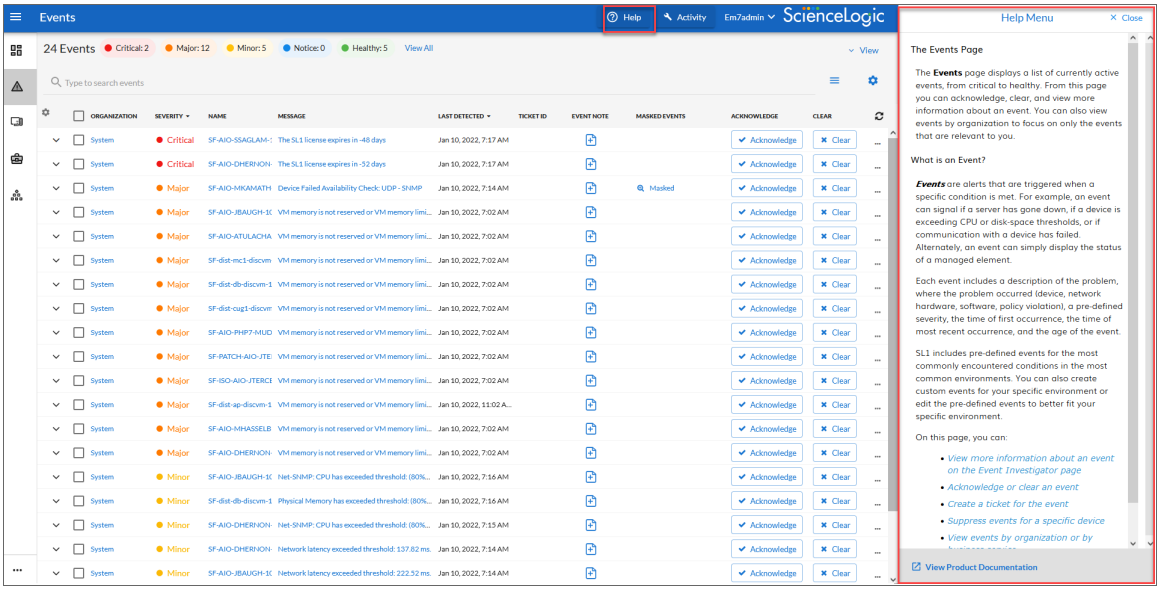
For example, you could create a theme that replaces the SL1 logo with your company's logo and updates the colors used in the user interface to match those used in your company's branding. You can also choose between a light theme or a dark theme for the user interface.

For more information about customizing the user interface using themes, see the manual ***Customizing the User Experience***.

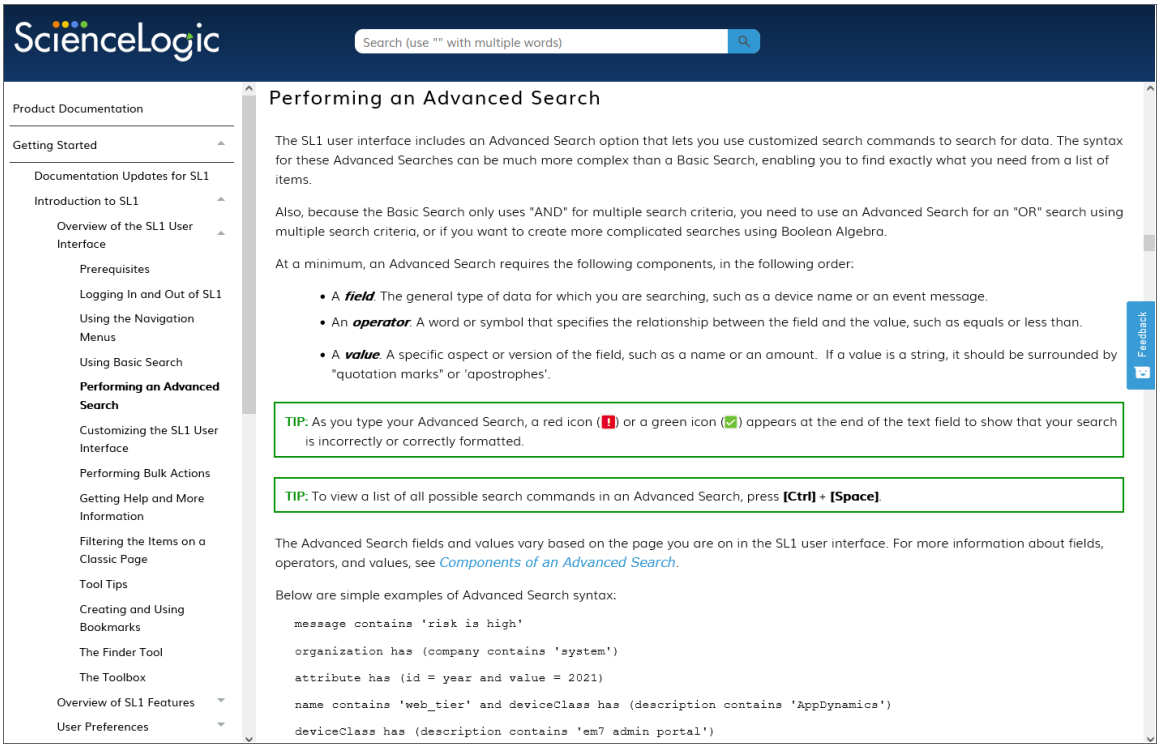
Getting Help and More Information

For product documentation about any page in SL1, click the **[Help]** button at the top right of any page in SL1.

The **Help** menu appears in a new pane on the right side of the SL1 window:



If you click the **View Product Documentation** link at the bottom of the **Help** menu, a product documentation topic specific to the current page appears in a new browser window:



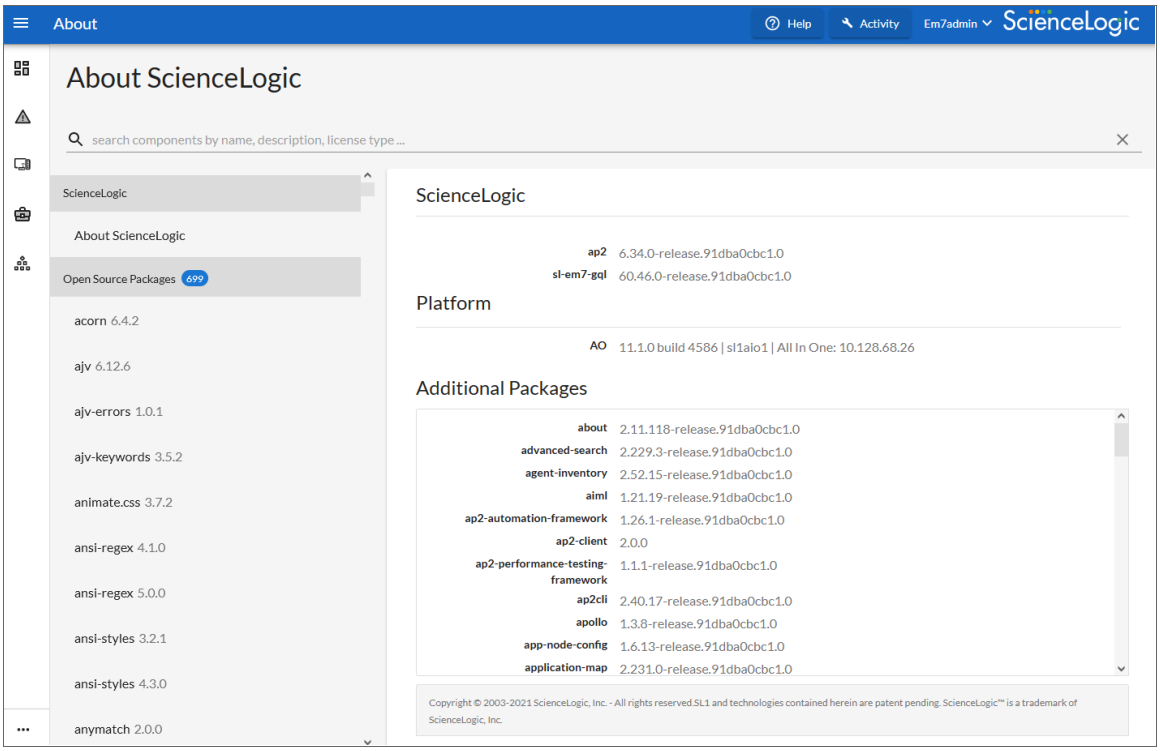
The product documentation includes a ***Search*** field at the top of the page that you can use to find additional topics related to the SL1 user interface. To find a specific topic that is longer than one word, enclose all of the key words in parentheses, such as "business services".

TIP: Click the **[Feedback]** button on the right side of the product documentation window to send comments directly to the ScienceLogic Documentation team, such as reporting typos, inaccuracies, questions, or other comments about that specific page in the Product Documentation.

NOTE: As of version 8.12.2 of SL1, ScienceLogic no longer updates the content that appears when you click the **[Guide]** button in the classic user interface. All help content is maintained in the **Help** menu and the online product documentation, which is located at **https://docs.sciencelogic.com**.

The About Page

For more information about the components used by SL1, click your user name in the navigation bar at the top of any SL1 page and select *About*. The **About ScienceLogic** page appears:



The current version number of the SL1 user interface displays in the ***ap2*** row at the top of the list of components in the right-hand pane, along with the current version of GraphQL used by SL1. The **Platform** section lists SL1 version information for the various components in SL1, including Application Server, Collector Unit, and Database details, and All-In-One configurations (AO) where relevant.

In the left-hand pane, click any of the components in the **Open Source Components** pane to view licensing information about those components, along with links to relevant websites where relevant.

To search for a specific open-source component, type the name of that component in the ***Search*** field at the top of the page. The list of components is filtered by your search terms.

Tips and Best Practices for Using the Product Documentation

Use the following tips and best practices when using the ScienceLogic Help menu and product documentation:

General

- To ensure that you are always using the most recent version of the product documentation, check the URL for this site to make sure you are using either **https://docs.sciencelogic.com/latest/** or **https://docs.sciencelogic.com/<*most-recent-release*>/**.

- The documentation at this site is the same documentation that appears when you click the **[Help]** button at the top of any SL1 page. The Help topic that appears is based on your current page in SL1.

> **NOTE:** If you are using a version of SL1 older than version 11.1.0, you can access the product documentation by clicking your user name and selecting *Help* from the drop-down menu.

- The documentation at this site contains all manuals for the various features of SL1. You can click the *Download manual as PDF* link at the top of each chapter to download the PDF version of the manual.
- If you use the ***Version*** dropdown to navigate to a previous version of the product documentation, the ***Version*** dropdown on the older version might contain links to archived versions that display a 404 error. The ***Version*** dropdown only displays links to currently supported releases of SL1.

Searching the Site

- To search for a specific item in the product documentation, type the relevant information in the ***Search*** bar at the top of the page. After you select a document from the search results page, type the same search into your browser's Search (**Ctrl+F**).
- If you are using a multiple-word search for a specific term, enclose those words in quotation marks (""). For example: **"business services"**.
- To quickly find a video in the product documentation, include the word "video" in your search, along with the topic or feature you want to view. For example: **video maps**.
- Use the following command to search the product documentation via the SL1 API: **https://docs.sciencelogic.com/latest/#search-*<your-query-here>***. For example: **https://docs.sciencelogic.com/latest/#search-business services**.
- After you click a link to a page from the search results, your search term or terms display as one or more highlighted colors. To get rid of the highlights, click the **Remove Highlights** button ( ) on the toolbar at top right of the Help content pane.

Links and Images

- If your browser opens the PDF in a new browser window when you click the *Download manual as PDF* link (instead of downloading the PDF), any text you try to copy and paste from that version will not paste correctly. If you need to copy and paste text from a manual, ScienceLogic recommends that you download the PDF instead and open it in Adobe Reader, as the PDF viewer in a browser produces an image of each page instead of the actual text, and any text you copy and paste from the viewer displays without spaces.
- If a link to an external site does not open properly in a new browser window or tab, right-click the link in the product documentation and select the option to open the link in a new tab or window.
- An image in the product documentation might appear slightly blurry until you click that image to expand it in a pop-up window.
- If you clicked to expand an image in a pop-up window, you will need to click the expanded image in its pop-up window to return it to its regular size before you can click another image or link in the product documentation.
- You can also right-click an image and select *Open Image in New Tab* from the pop-up menu to make the image display at full size in the new browser tab.

Guides from the "Classic" User Interface

- As of version 8.12.2 of SL1, ScienceLogic will no longer update the help content that appears when you click the **[Guide]** button in the user interface. All help content will be updated and maintained here at https://docs.sciencelogic.com.

Chapter 3

Events in the SL1 User Interface

Overview

You can view a list of all events in SL1 or view a list of events for a single device. This section describes how to perform both tasks.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

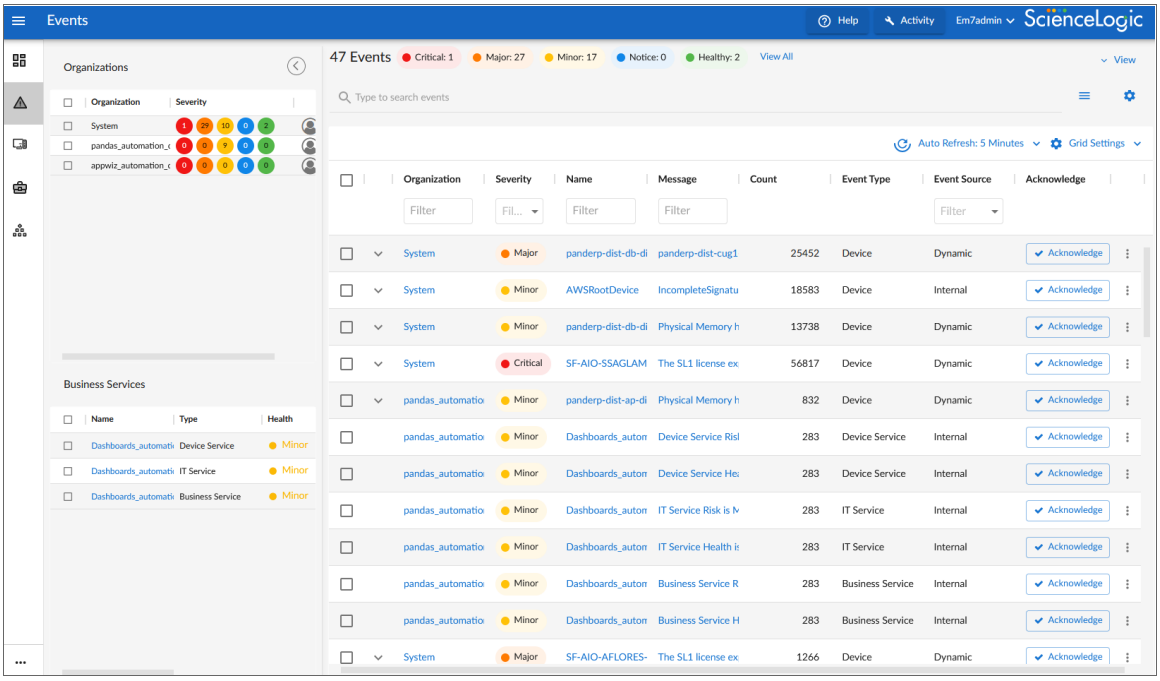
Viewing the List of Events 50
Filtering the List of Events 53
Viewing Additional Data about an Event 59
Using the Event Investigator 61
Acknowledging and Clearing Events 64
Viewing and Editing Event Notes 65
Viewing the Event Policy 66
Suppressing and Unsuppressing an Event for a Device 67
Enabling and Disabling Events 69
Event Throttling 70

Viewing the List of Events

The **Events** page displays a list of currently active events, from critical to healthy. From this page you can acknowledge, clear, and view more information about an event. You can also view events by organization to focus on only the events that are relevant to you.

> **TIP:** By default, the events listed on the **Events** page are sorted by severity, highest to lowest, and then secondarily sorted by the events' last occurrences, most recent to least recent. This ensures that the most severe and most recent events appear at the top of the page. If you prefer, you can change the sorting preferences and SL1 will recall those changes the next time you return to the **Events** page.

To navigate to the **Events** page, click the Events icon (⚠):



For each event, the **Events** page displays the following information:

- ***Organization***. The organization with which the event is associated. Click the organization hyperlink to view more information about the organization. You can optionally filter the list of events so that only events for a specific organization appear on the **Events** page; for more information, see the section *Filtering Events by Organization and Service*.
- ***Severity***. The severity of the event. Possible values are:
  - *Critical*. Indicates a condition that can seriously impair or curtail service and requires immediate attention (for example, service or system outages).

- *Major*. Indicates a condition that impacts service and requires immediate investigation.
- *Minor*. Indicates a condition that does not currently impair service, but the condition needs to be corrected before it becomes more severe.
- *Notice*. Indicates a condition that users should be aware of, but the condition does not affect service.
- *Healthy*. Indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.

> **NOTE:** You can optionally filter the list of events so that only events of a specific severity level appear on the **Events** page; for more information, see the section *Filtering Events by Severity*.

- ***Name***. The name of the entity associated with the event. Click the name hyperlink to view more information about the entity.
- ***Message***. The message generated for the event. Click the message hyperlink to go to *the Event Investigator*, where you can view more information about the event, including a description, its probable cause, and possible resolutions, among other details.

> **NOTE:** You can also view the **Event Investigator** page by clicking the **[Actions]** button (⋮) for the event and selecting *View Event*.

- ***Age***. The number of days, hours, and minutes since the first occurrence of the event. This is also the time since the event occurred without the event having been cleared.
- ***Count***. The number of times the event has occurred or the number of child events associated with the event or the number of masked events associated with the event.
- ***Event Note***. Click the **Note** icon (📝) to view any existing user-defined notes about the event or to create or edit a note about the event. When you do so, the **Edit Event Note** modal page appears, where you can create or edit a note and save your changes. For more information, see the topic "Viewing and Editing Event Notes" in the ***Events*** manual.

> **NOTE:** You can also view, create, or edit event notes by clicking the **[Actions]** button (⋮) for the event and selecting *Edit Event Note*.

- ***Masked Events***. If the event has occurred multiple times on the same device that uses the ***event mask*** setting, click the magnifying glass icon (🔍) or the **Masked** hyperlink to go to the **Event Investigator** page, where you can view details about the masked events. For more information, see the section *Filtering for Masked Events*.

> **NOTE:** You can also view masked events on the **Event Investigator** page by clicking the **[Actions]** button (⋮) for the event and selecting *View Event*.

- ***Automated Actions***. The number of times the event has triggered the execution of an automation policy. If the event has triggered one or more automated actions, click the number hyperlink to go to the **Event Actions Log**, where you can view a log of all automated actions that have occurred for the event. For more information, see the section *Viewing Automated Actions*.

> **NOTE:** You can also view the **Event Actions Log** modal page by clicking the **[Actions]** button (⋮) for the event and selecting *View Automation Actions*.

- ***Event ID***. The unique ID for the event, generated by SL1. Click the ID hyperlink to go to *the Event Investigator*.
- ***Event Source***. The system or application that generated this event. Possible values are:
    - *Syslog*. The event was generated from a system log generated by a device.
    - *Email*. The event was generated by an email from an external agent. For example, Microsoft Operations Manager (MOM).
    - *Internal*. The event was generated by SL1.
    - *Trap*. The event was generated by an SNMP trap.
    - *Dynamic*. The event was generated by a Dynamic Application collecting data from the device.
    - *API*. The event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
    - *SL1 agent*. The event was generated by log file messages collected by the SL1 agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the ***Monitoring Device Infrastructure Health*** manual.

Event Type. The type of entity associated with the event. Possible values are:

- Organizations
- Devices
- Assets
- IP networks
- Interfaces
- Business Service
- IT Services
- Device Services
- Vendors
- User Accounts
- Virtual Interfaces

- ***Last Detected***. The date and time at which the event last occurred on the entity.
- ***Ticket External Reference***. The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in SL1). Click the ticket reference value to view the external ticket in a new window.

> **NOTE:** To link an external ticket to an event, you must create a custom Run Book Automation policy and a custom Run Book Action or use the ScienceLogic APIs. For help with these tasks, contact ScienceLogic Customer Care.

- ***Ticket ID***. The ticket ID of the ticket that has been created for the event, if applicable.
- ***Acknowledge***. If the event has not been acknowledged, this column displays an **[Acknowledge]** button; click the button to acknowledge the event. If the event has been acknowledged, this column displays a check-mark character and specifies the user who acknowledged the event. For more information, see the section "Acknowledging and Clearing Events" in the ***Events*** manual.
- ***Clear***. Click the **[Clear]** button to clear the event. When you do so, the event is removed from the **Events** page.

> **TIP:** You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the ***Introduction to SL1*** manual.

> **TIP:** To rearrange the columns in the list, click and drag the column name to a new location. You can adjust the width of a column by clicking and dragging the right edge of the column. For more information about editing and adding columns, see "Editing the Settings for an Inventory Page" in the ***Introduction to SL1*** manual.

Filtering the List of Events

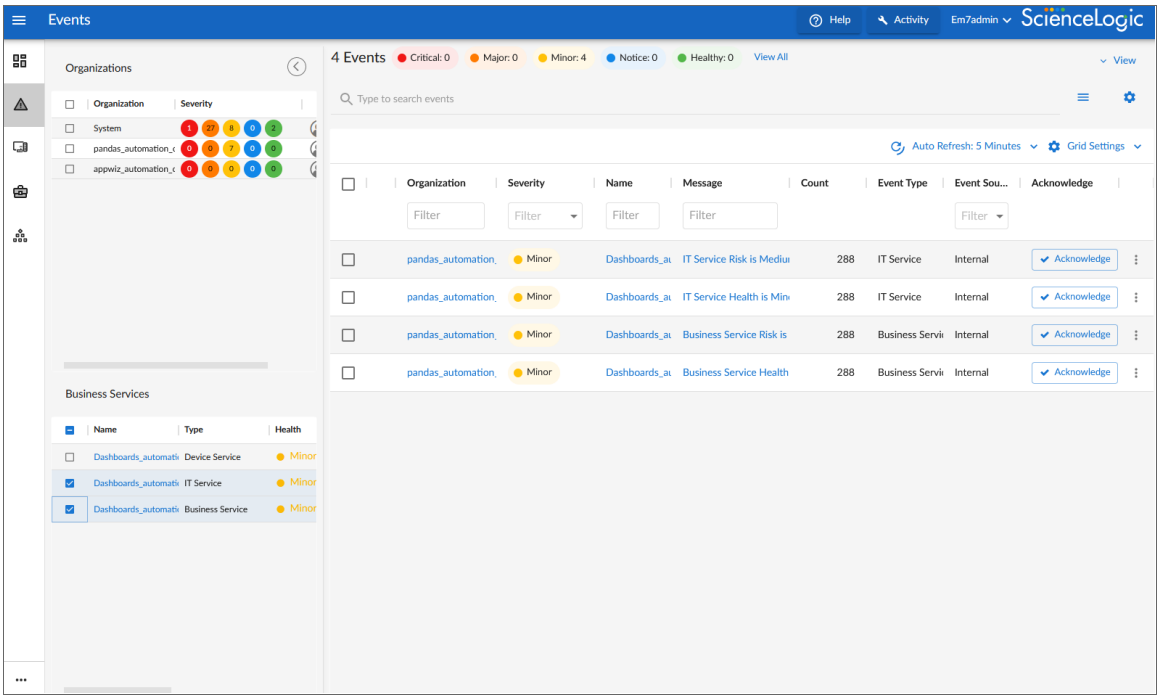
This section explains how to filter the list of events so you can quickly locate and address any potential issues in your environment.

Filtering Events by Organization and Service

You can view events from all organizations or services, or filter down to just the organizations or services you want to monitor for events.

To view events by organization or service:

1. On the **Events** page, click the **View** menu.
2. Select the **Group by organization** and/or the **Group by business service** toggle. The relevant panel appears on the left with a list of events sorted by severity for each organization and/or service:



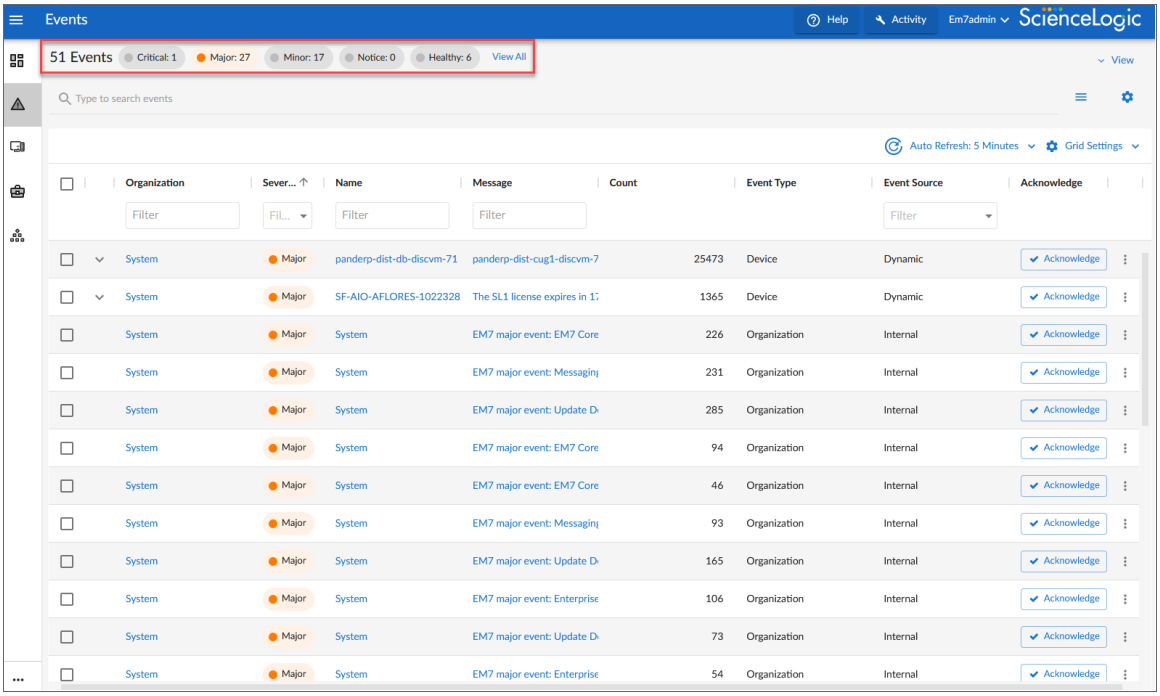
> **TIP:** To hide the **Organizations** and **Business Services** panels, click the left arrow icon ( ). Click the right arrow icon ( ) to expand the panel again.

3. On the left panel, click the check mark icon ( ) to filter the list of events based on the organization or service you selected.

> **TIP:** Click the name of a service to go to the **Service Investigator** page for that service. Click the name of an organization to go the **Organizational Summary Page** for that organization.

Filtering Events by Severity

The **[Events]** page displays a list of currently active events, which can be sorted by any column, such as severity from critical to healthy. You can filter the list of events by severity by clicking one or more of the five colored buttons near the top of the **[Events]** page:



When you click a severity button, the list displays only events with the severity you selected. The severity button you clicked remains in color, while the other buttons turn gray.

TIP: To clear a severity filter, click the **View All** link next to the severity buttons.

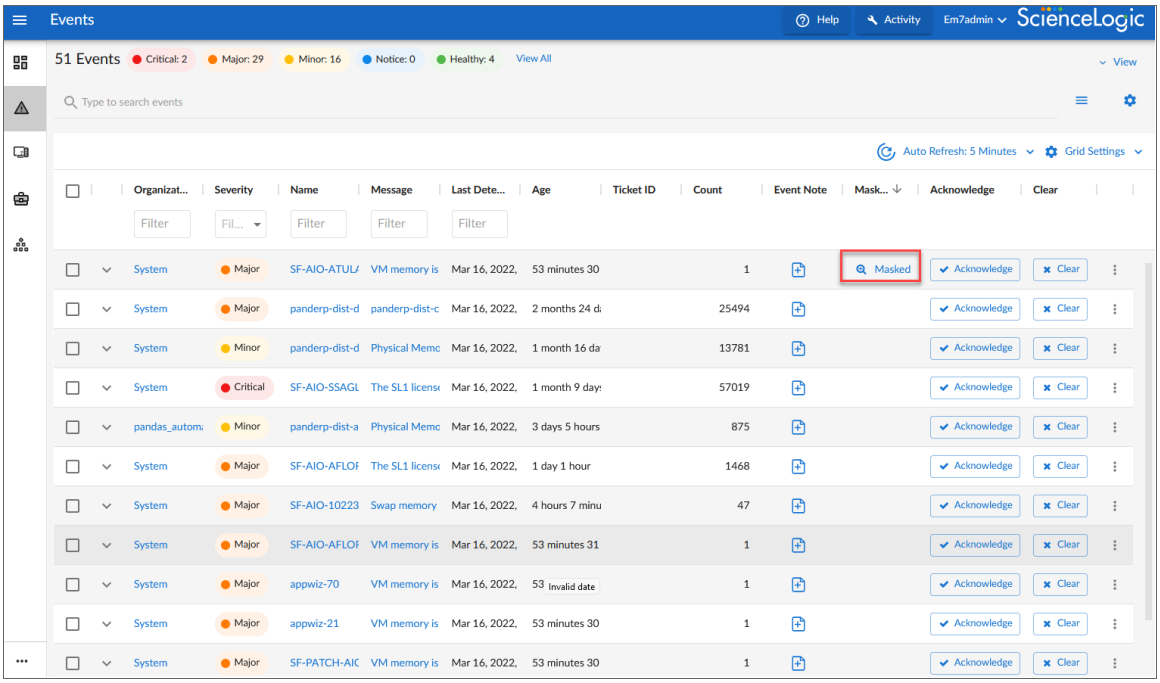
The following color codes are used throughout SL1:

- Red elements have a status of **Critical**. Critical conditions are those that can seriously impair or curtail service and require immediate attention (such as service or system outages).
- Orange elements have a status of **Major**. Major conditions indicate a condition that is service impacting and requires immediate investigation.
- Yellow elements have a status of **Minor**. Minor conditions dictate a condition that does not currently impair service, but needs to be corrected before it becomes more severe.
- Blue elements have a status of **Notice**. Notice conditions indicate a condition that users should be aware of, but the condition does not affect service.
- Green elements have a status of **Healthy**. Healthy conditions indicate that a device or service is operating under normal conditions. Frequently, a healthy condition occurs after a problem has been fixed.

Filtering for Masked Events

When a device uses the ***event mask*** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed on the **Events** page. This allows related events that occur in quick succession on a single device to be rolled-up and posted together under one event description. For example, if a device cannot connect to the network, multiple other services on the device will raise events. SL1 would display the event with the highest severity and roll up all the other events.

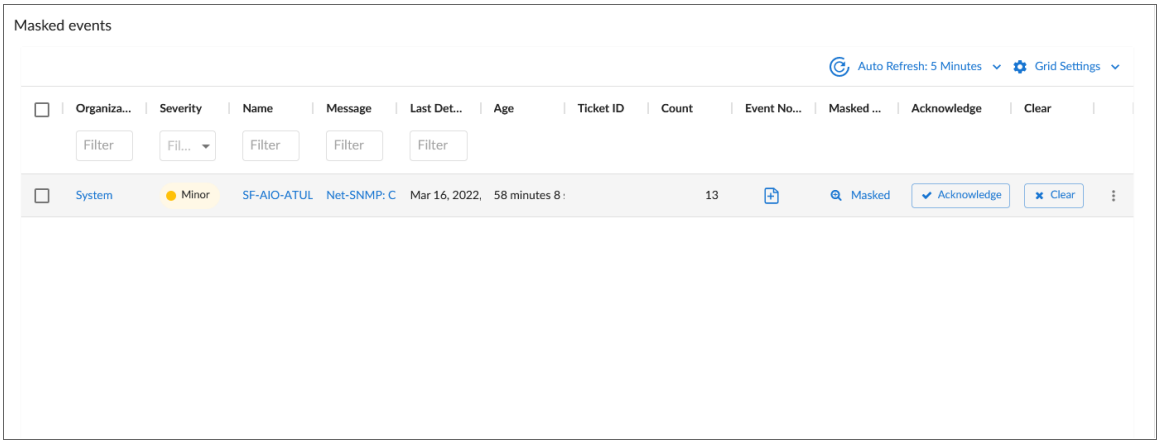
On the **Events** page, any event that contains masked events includes a magnifying glass icon ( ) and the word "Masked" in the **Masked Events** column:



TIP: Click the **[Grid Settings]** button to add the **Masked Events** column, if it is not currently visible.

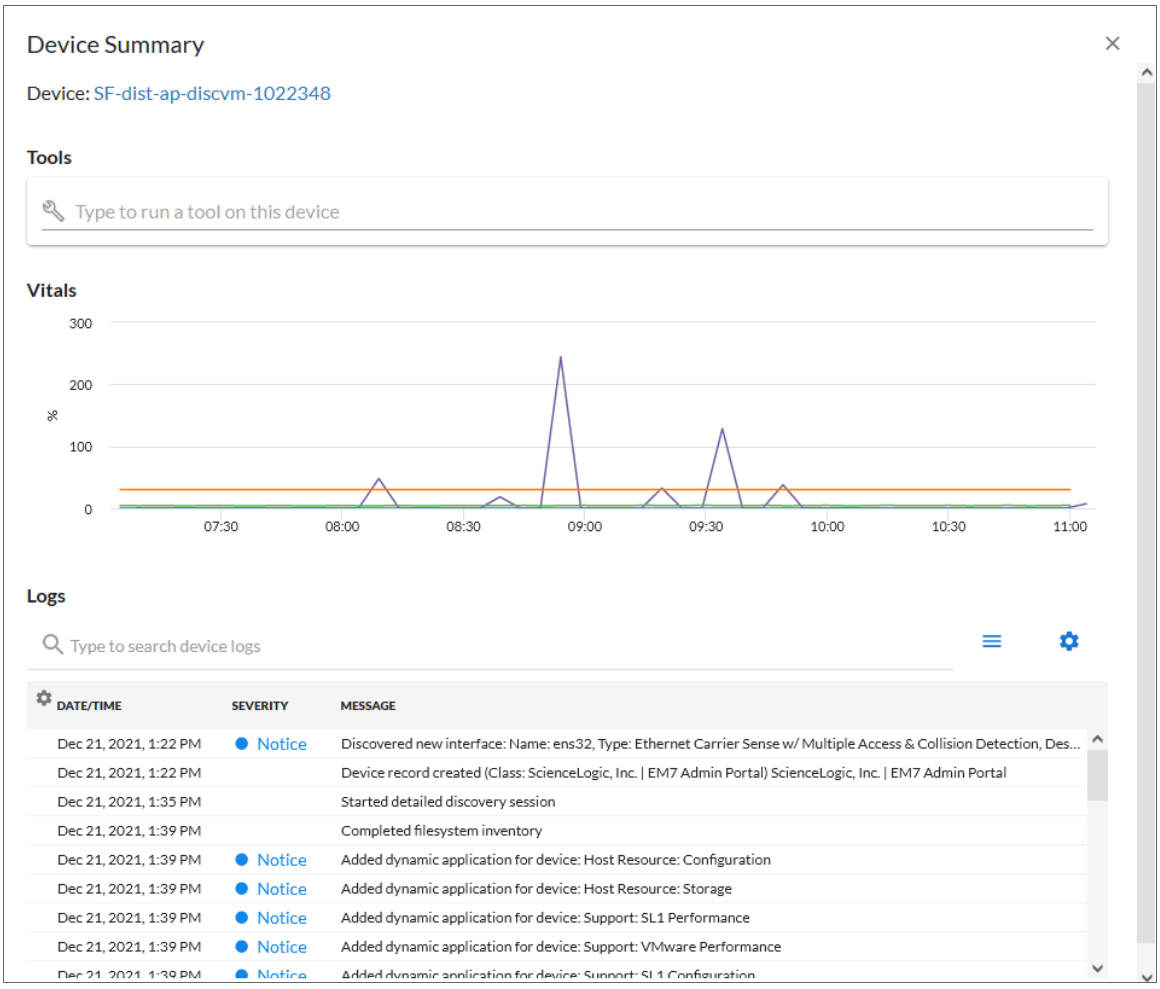
To view more information about masked events:

1. On the **Events** page, click the magnifying glass icon (🔍) or the **Masked** link in the **Masked Events** column for the relevant event. The **Event Investigator** page for that event appears.
2. Scroll down to the **Masked events** section to view the details about the masked events:



Viewing Additional Data about an Event

On the **Events** page and the **Devices** page, you can click the **Expand** icon ( ) next to an event or device to open a new **Device Summary** modal:



NOTE: On the **Events** page, the **Device Summary** modal displays only for events that are aligned with devices.

The detail window for that device contains the **Tools** pane, the **Vitals** graphs, and the **Logs** pane:

- The **Tools** pane enables you to run a set of diagnostic tools or user-initiated actions in the **Activity Center**, or to click on custom links that will open in a separate browser window. Click the search bar to search for tools, actions, or custom links that are available for the device.

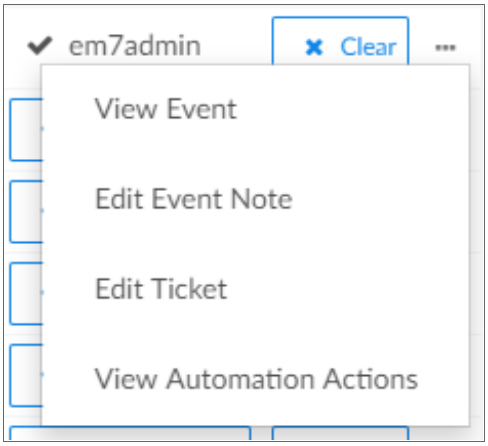
- The **Vitals** pane displays graph data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Logs** pane displays a list of events associated with that device.

TIP: To open the detail or Investigator page for an item, click the link for the item name at the top of the detail window.

Viewing Automation Actions

To view a log of automated actions that have occurred for an event, on the **Events** page, click the **[Actions]** button (⋮) for the event and select *View Automation Actions*. When you do so, the **Event Actions Log** modal page appears.

NOTE: You can also view the **Event Actions Log** modal page by clicking the hyperlink in the ***Automated Actions*** column for a particular event on the **Events** page.



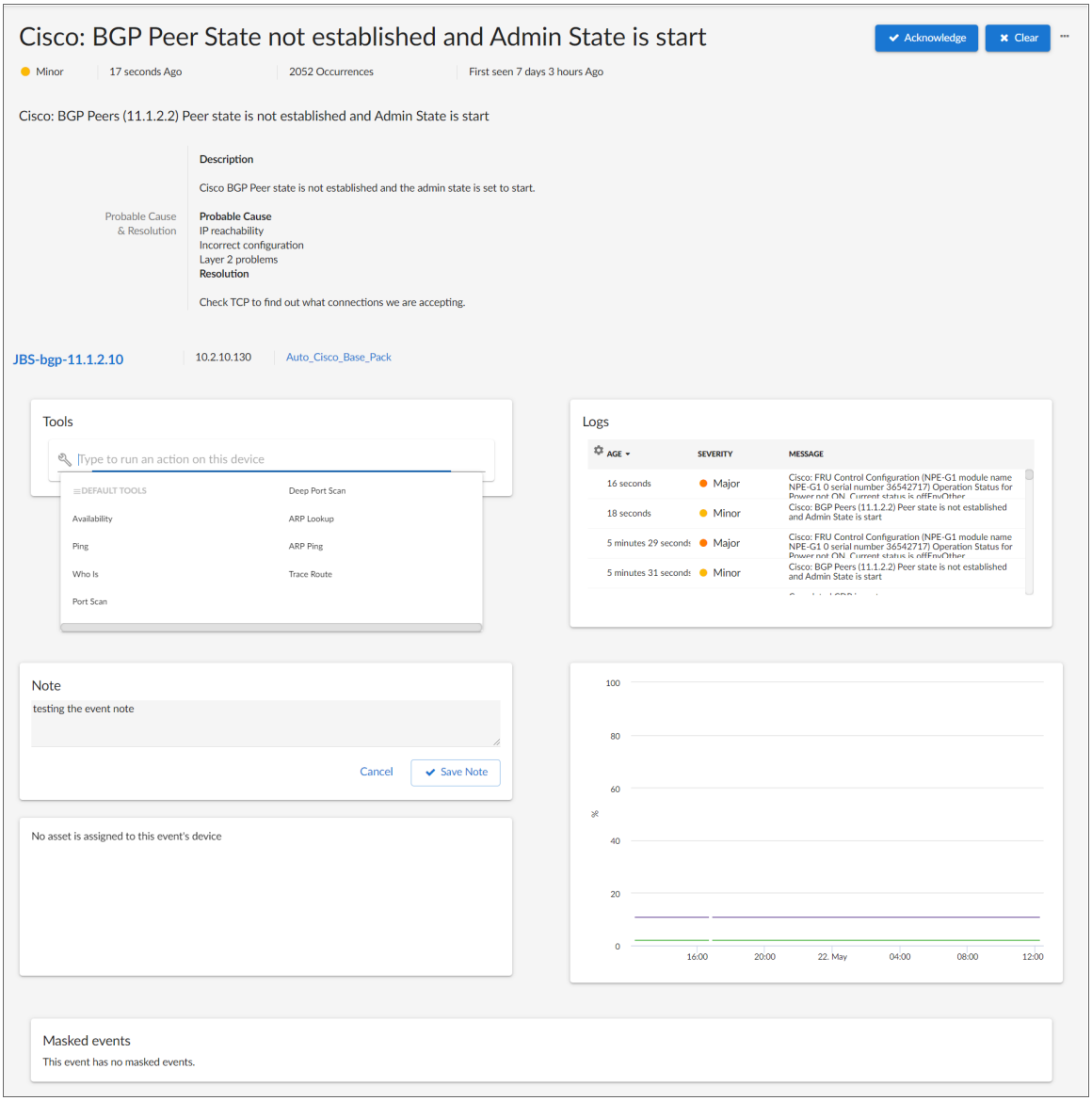
The **Event Actions Log** displays a history of all automation actions that SL1 executed in response to the event.

Each entry in the **Event Actions Log** modal page includes:

- The date and time when the action was executed
- The automation policy that triggered the action
- The name of the action policy
- The result of the action

Using the Event Investigator

The **Event Investigator** page provides details about the event as well as the device associated with the event, where relevant. The **Event Investigator** page includes sections for Probable Cause & Resolution, Tools, Logs, Notes, Assets, a Vitals widget, and a list of masked events:



TIP: To get to the **Event Investigator** page, click the linked text in the **Message** column of the **Events** page, or click the **[Actions]** button (⋮) for the event and select *View Event*.

The top pane of the **Event Investigator** page contains basic event details. From this pane, you can also acknowledge the event, clear the event, or click the **[Actions]** button (⋮) and select *Create Ticket* to create a ticket for that event. If an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.

> TIP: On the **Event Investigator** page, click the name of an aligned device or service to go to the Investigator page for that device or service.

The **Event Investigator** page includes the following sections:

- ***Probable Cause & Resolution***. Displays additional information about the event, based on the event policy.
- ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions. This pane is the same as the **Tools** pane of the Event Drawer. For more information, see the section on *Using the Action Runner*.
- ***Logs***. A list of log entries from the device's log, sorted from newest to oldest by default.
- ***Note***. A text field where you can add new text and edit existing text related to the event and the device associated with the event. For more information, see *Viewing and Editing Event Notes.*
- ***Assets***. One or more asset records associated with the device, such as a piece of equipment owned by an organization. The asset record includes contact information for the technician, administrator, and vendor for that device. You can click the name of an asset to view an **Asset** page for more information.
- ***Vitals***. A widget that displays the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- ***Masked events***. A list of all masked events for the device. When a device uses the ***event mask*** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed in the **Events** page. This allows related events that occur in quick succession on a single device to be rolled-up and posted together under one event description.

Using the Action Runner

You can access the **Action Runner** from either the **Events** page or the **Event Investigator** page. The **Action Runner** enables you to run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open related records in external systems in a separate browser window.

> NOTE: The tools and actions that are available in the **Action Runner** are based on the device type and your user permissions, as determined by your organization assignment and access hooks. For example, if a device does not have an IP address, only the Availability tool will be available.

> NOTE: For more information about user-initiated actions, see the chapter on "Automation Policies" in the ***Run Book Automation*** manual.

To use the **Action Runner**:

1. Access the **Action Runner** for events in one of the following ways:

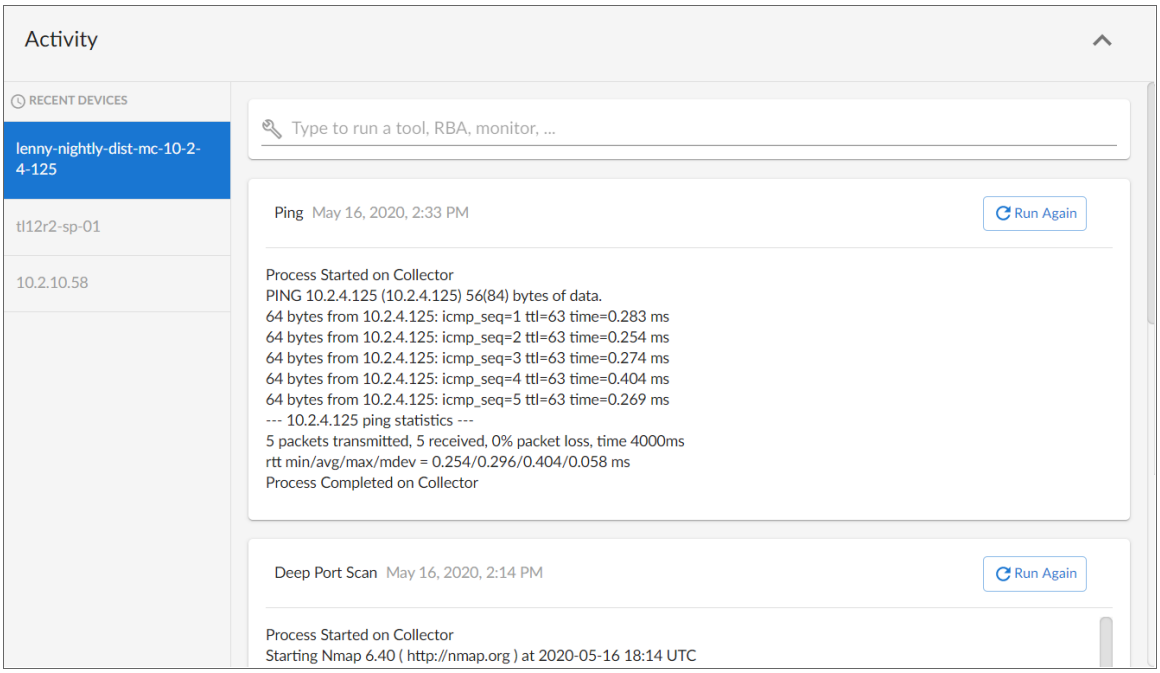
    - On the **Action Runner** page, open the Event Drawer for a particular event. Click the search bar in the **Tools** pane.
    - On the **Action Runner** page, click the search bar in the **Tools** pane.
    - Click the **[Activity]** button in the navigation bar at the top of any page in SL1. Click the search bar.

2. When you click the search bar, a list displays the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:

    - ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
    - ***Ping***. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, SL1 uses the appropriate IPv6 ping command.
    - ***Who Is***. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
    - ***Port Scan***. Displays a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
    - ***ARP Lookup***. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.
    - ***ARP Ping***. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.
    - ***Trace Route***. Displays the network route between SL1 and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, SL1 uses the appropriate IPv6 traceroute command.

    > **TIP:** The tools found in the **Action Runner** can also be found in the Device Toolbox in the classic SL1 user interface.

3. If you clicked a custom link, the link opens in a new browser window or tab. If you clicked on a tool or action, then as it runs, its progress and results appear in a log in the **Activity Center**.
4. After the tool or action has run, if you want to run it again, click the **[Run Again]** button. This button appears only for activities completed during your current session.



NOTE: The left pane of the **Activity Center** displays a list of devices for which you have most recently used the **Action Runner**, with the current device at the top of the list. To use the **Action Runner** for any of the other recently used devices or to view historical logs for the tools or actions that have been run on those devices, click on the device name.

Acknowledging and Clearing Events

When you ***acknowledge*** an event, you let other users know that you are aware of that event, and you are working on a response.

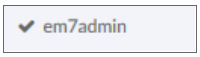
When you ***clear*** an event, you let other users know that this event has been addressed. Clearing an event removes a single instance of the event from the **Events** page. If the event occurs again on the same device, it will reappear in the **Events** page.

NOTE: If the same event occurs again on the same device, it will appear in the **[Events]** tab, even if you have previously cleared that event.

NOTE: When you acknowledge a parent event, all masked events under that parent event are also acknowledged.

To acknowledge and clear events:

1. To acknowledge an event, find the event on the **[Events]** page and click the **[Acknowledge]** button for that event. Your user name replaces the **[Acknowledge]** button for that event:

   You can also click the **[Acknowledge]** button in a specific event's **Investigator** page.

2. To see when an event was acknowledged and who acknowledged it, hover your mouse over an acknowledged field.
3. If an event was acknowledged by another user and you have the relevant permissions, you can click the **[Reacknowledge]** button to acknowledge that event.
4. To clear an event, click the **[Clear]** button. The event is removed from the **Events** page.

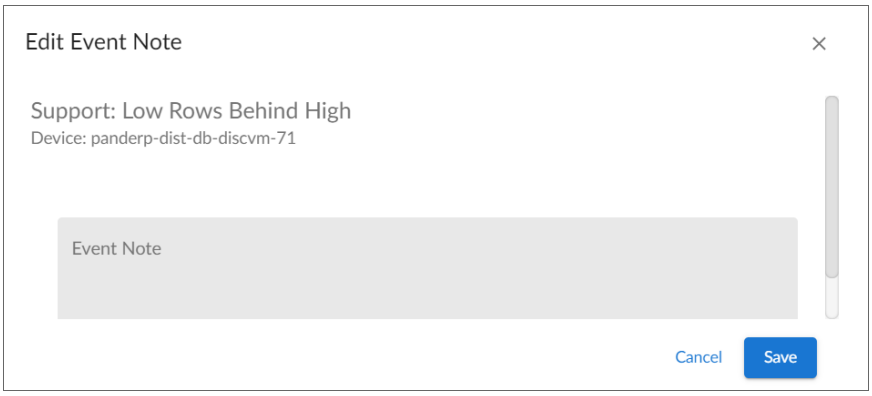
TIP: If you want to hide the **[Acknowledge]** or **[Clear]** buttons on the **Events** page, click the **Select Columns** icon (⚙) and deselect those columns.

Viewing and Editing Event Notes

From the **Events** page, you can access ***event notes***, which contain event definitions, probable causes, and resolutions for the event, along with a text field where you can add more information about the event or the device you are monitoring. If event notes already exist for that event, the opening text of that note appears in the **Event Note** column of the **Events** page.

To view or edit an event note:

1. On the **Events** page, click the **Note** icon ( ) for that event. The **Edit Event Note** window appears:



> **TIP:** You can also edit an event note on the **Events** page by clicking the **[Actions]** button ( ) for that event and selecting *Edit Event Note*. This is helpful if you have hidden the ***Event Note*** column on the **Events** page.

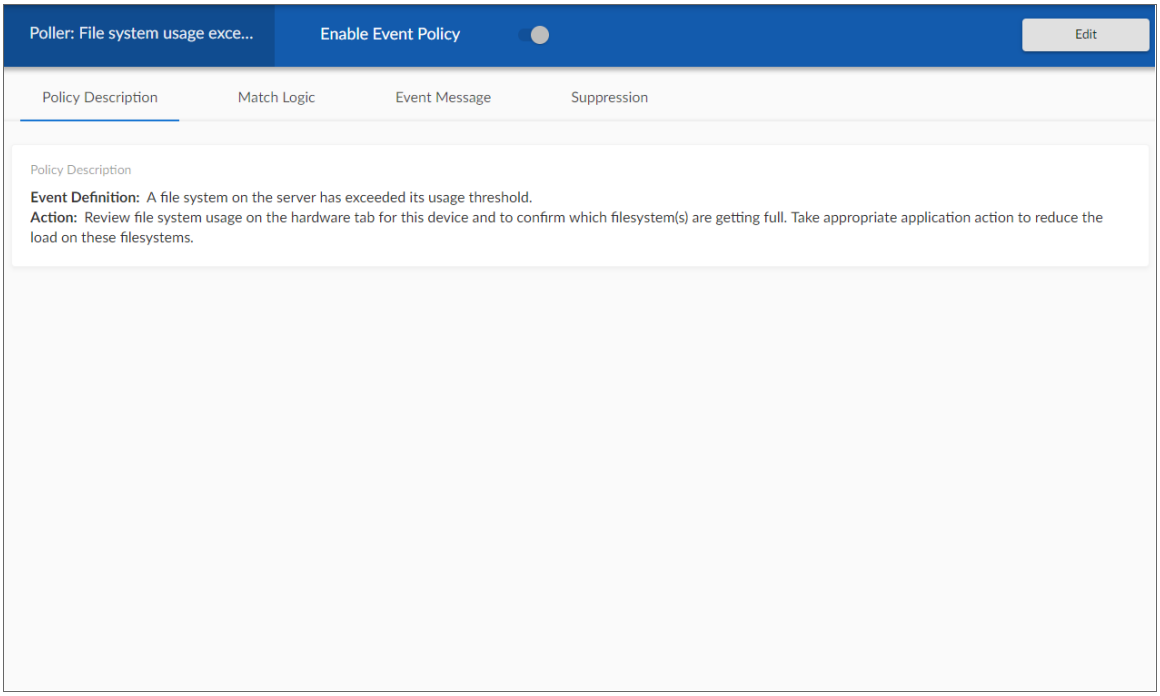
2. Type your additional text for the event note and then click **[Save]**. The event note is updated.

Viewing the Event Policy

From the **Events** page, you can view the Event Policy for an event, which allows you to view a description of the policy, enable or disable the policy, and edit policy details.

To view an Event Policy from the **Events** page:

1. On the **Events** page, click the **Actions** menu (⋮) for that event and select *View Event Policy*. The **Event Policy Editor** page appears for that event:



2. Click the **[Edit]** button to edit the Event Policy. For more information, see the "Defining and Editing Event Policies" chapter of the ***Events*** manual.

Suppressing and Unsuppressing an Event for a Device

When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in the **Events** page or the **Events** tab for a device.

If a suppressed event occurs on a different device, it will appear in the **Events** page and on the **Events** tab for that different device.

When you suppress an event, the current instance of the event still appears in the **Events**. To remove the current instance from the event console, clear the event (see the section *Clearing One or More Events*).

NOTE: To suppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Events/Event:View and Event:Clear. Accounts of type "user" will then be able to view and suppress events that belong to the same organization(s) as the user. For more information on access hooks, see the manuals ***Access Permissions*** and ***Organizations and Users***.

Suppressing an Event

To suppress an event:

1. Go to the **Events** page.
2. Click the **Actions** button (⋮) for the event you want to suppress and select *Suppress Event for this Device*. In the future, if this event occurs again on the same device, the event will not appear in the **Events** page.

NOTE: Users of type "user" can view only suppressed events that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all suppressed events.

Suppressing an Event on Multiple Devices

When you suppress an event on multiple devices, you are specifying that, in the future, if this event occurs again on any of those devices, the event will not appear in the **Events** page or in the **Viewing Events** page for any of those devices.

To suppress an event on multiple devices:

1. Go to **Event Policies** page (Events > Event Policies).
2. In the **Event Policies** page, select the Actions menu (⋮) of the event policy you want to edit and select *Edit*.
3. The selected event policy is displayed in the **Event Policy Editor** page, where you can edit one or more properties of the event policy.
4. Click the **[Suppression]** tab.
5. On the **[Suppression]** tab, you can select the devices or device groups on which to suppress the event. To do so:
    - Click **[Select Devices]** to select one or more devices on which to suppress the event. When you click **[Select Devices]**, the **Available Devices** modal page appears. Select the checkboxes of the devices you want to add to the suppression list, and then click **[Select]**.
    - Click **[Select Device Groups]** to select one or more device groups on which to suppress the event. When you click **[Select Device Groups]**, the **Available Device Groups** modal page appears. Select the checkboxes of the device groups you want to add to the suppression list, and then click **[Select]**.
6. Click **[Save]**.

Unsuppressing an Event

On the **Event Suppression List** page (Events > Suppressions), you can view a list of all suppressed events in SL1 and choose to unsuppress one or more of those events. When you unsuppress an event, if this event occurs again on the same device, the event will appear in the **Events** page.

NOTE: To unsuppress an event, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Suppressions, and Event:Suppressions. Accounts of type "user" will then be able to view a list of suppressed events that belong to the same organization as the user. Accounts of type "user" will also be able to unsuppress one or more of these suppressed events. For more information on access hooks, see the manuals ***Access Permissions*** and ***Organizations and Users***.

To unsuppress an event:

1. Go to the **Event Suppression List** page (Events > Suppressions).
2. Select the checkbox for each event you want to unsuppress.
3. In the ***Select Action*** drop-down menu, in the lower right, select *DELETE Suppression*.
4. Click **[Go]**. In the future, if the unsuppressed event occurs again on the same device, the event will appear in the **Events** page.

Unsuppressing All Instances of an Event

You can simultaneously unsuppress all instances of an event. That is, if a single event has been suppressed for multiple devices, you can unsuppress the event on all devices. In the future, if the unsupressed event occurs again on any device, the event will appear in the **Events** page.

NOTE: To unsuppress an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policies** page and unsuppress one or more events on all devices. For more information on access hooks, see the manuals ***Access Permissions*** and ***Organizations and Users***.

To unsuppress an event on all devices:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkbox for the event you want to unsuppress on all devices.
3. Click **[Clear Suppressions]**. In the future, if the unsuppressed event occurs again on any device, it will appear in the **Events** page or in the **Viewing Events** page for the device.

Enabling and Disabling Events

You can simultaneously disable one or more events on all devices. When an event is disabled, it will no longer appear in the **Events** page for any devices. You can also enable an event that has been disabled.

NOTE: To disable or enable an event on all devices, accounts of type "user" must be granted one or more access keys that include the following access hooks: Registry, Registry>Events>Event Manager, and Event:Add/Rem. Accounts of type "user" will then be able to access the **Event Policies** page and enable one or more events on all devices. For more information on access hooks, see the manuals ***Access Permissions*** and ***Organizations and Users***.

Disabling Events

To disable one or more events:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkboxes for the events you want to disable.
3. Click **[Disable]**. The selected events will no longer appear in SL1 for any device, application, or policy.

Enabling Events

To enable one or more events:

1. Go to the **Event Policies** page (Events > Event Policies).
2. Select the checkboxes for the events you want to enable.
3. Click **[Enable]**. The selected event(s) will once again appear in SL1.

Event Throttling

When SL1 detects syslog messages or traps coming from a single device at a rate greater than 25 messages per second, SL1 throttles the messages.

When SL1 throttles messages from a single IP address, those messages are deleted from the ScienceLogic database. The messages are not passed to the event engine, are not logged, and are not processed as events.

When SL1 throttles messages, SL1 also triggers events:

- ***Event with a Severity of Critical and the message "Inbound Message Flood"***. This event is triggered when a single IP exceeds the threshold of syslog messages or trap messages at least once per minute for the last ten minutes. The default threshold is 25 messages per second.
- ***Event with a Severity of Notice and the message "Inbound Message Spikes".*** This event is triggered when a single IP exceeds the threshold of syslog messages or trap message. The default threshold is 25 messages per second.

Message throttling is enabled by default. To disable message throttling, contact ScienceLogic Customer Support.

To adjust the threshold for message throttling, contact ScienceLogic Customer Support.

To whitelist an IP address so that message throttling does not apply to that IP, contact ScienceLogic Customer Support.

NOTE: SL1 does not support message throttling on IPv6 devices monitored by CentOS5 Data Collectors.

Chapter 4

Devices in the SL1 User Interface

Overview

The **Devices** page allows you to view all of your managed devices in SL1 and also run a discovery to find more devices to monitor. You can select a device from the list on the **Devices** page to view detailed data on the **Device Investigator** page for that device.

> **NOTE:** The list of devices on the **Devices** page matches the list of devices on the **Device Manager** page (Devices > Device Manager).

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

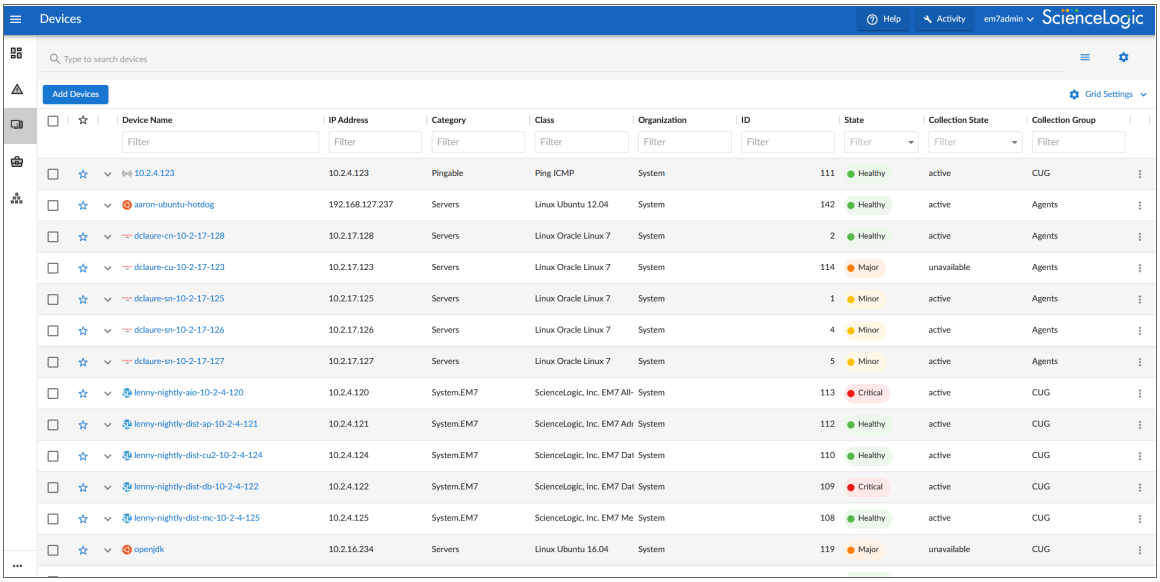
This chapter covers the following topics:

Viewing Devices 73
Adding Devices with Discovery 76
Using the Device Investigator 77
Overview of the Device Investigator Tabs 84
Assigning Icons to Devices 112

Viewing Devices

The **Devices** page allows you to view all of your managed devices in SL1. This section explains how to gather more information about a device from this page.

To navigate to the **Devices** page, click the Devices icon ( ):



TIP: You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the ***Introduction to SL1*** manual.

For each device, the **Devices** page displays the following information:

- ***Device Name***. Name of the device. For devices running SNMP or with DNS entries, the name is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The device's IP address.
- ***Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, and printers, among others. The category is automatically assigned during discovery, at the same time as the as Device Class. For more information about Device Categories, see the chapter on "Managing Device Classes and Device Categories" in the ***Device Management*** manual.
- ***Class***. The manufacturer and type of device. The Device Class is automatically assigned during discovery, at the same time as the Category.
- ***Organization***. The Organization to which the device is assigned.
- ***ID***. The Device ID. This is a unique number that SL1 automatically assigns to the device during discovery.

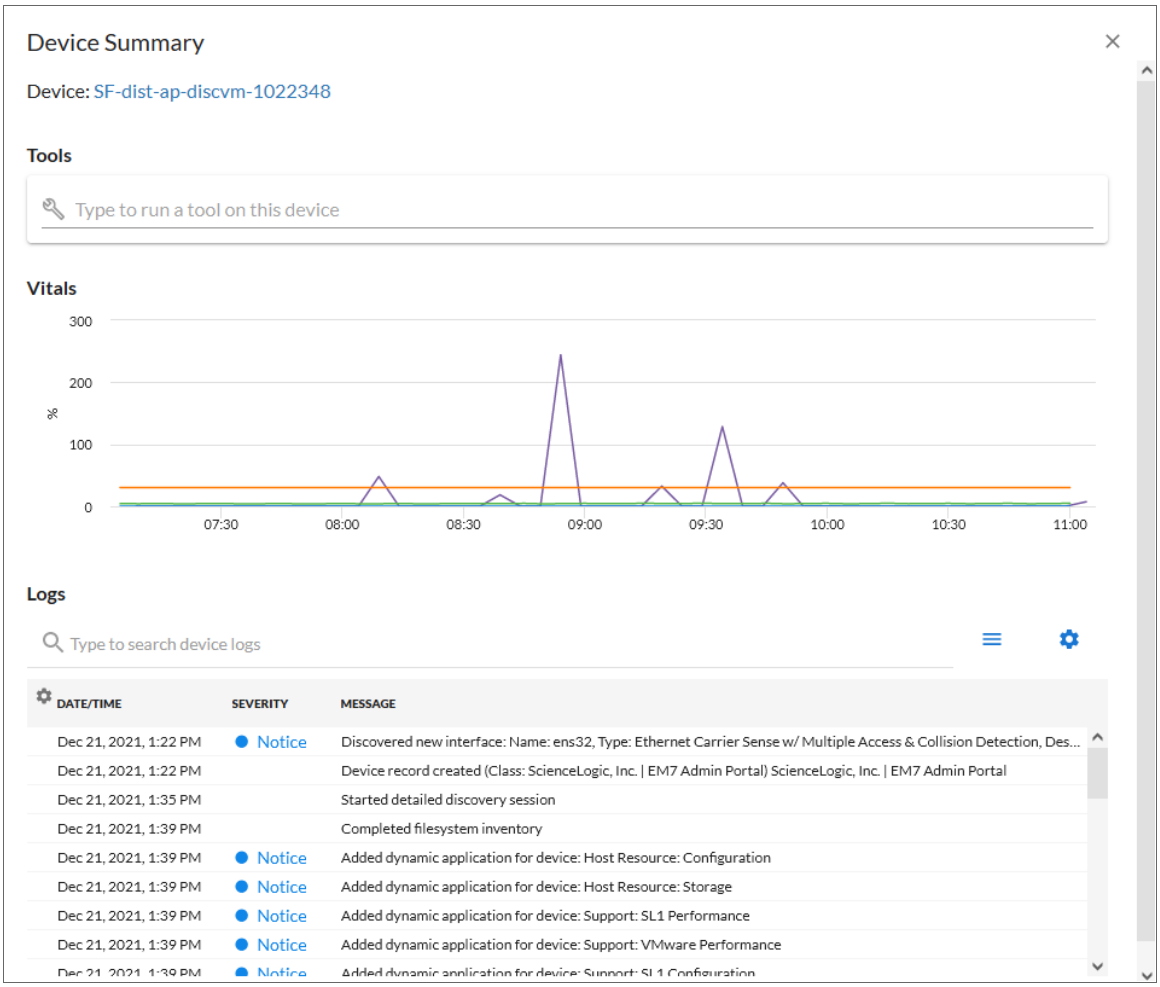
- ***State***. The current condition of the device, based upon events generated by the device. The device can have one of the following States:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.
    - *Notice*. Device has an informational event associated with it.
    - *Healthy*. Device is running with no problems.
- ***Collection State***. The current condition of data collection for the device. The device can have one or more of the following Collection States:
    - *Active*. SL1 is collecting data from the device.
    - *Unavailable*. SL1 cannot connect to the device, and will not collect data from the device until the device becomes available. A physical device falls back to executing the availability ping every five minutes, unless you have critical ping enabled. Component devices get their availability calculated by the component discovery Dynamic Application of the parent device.
    - *User-Disabled*. SL1 is not currently collecting data from the device because the user has disabled collection.
    - *System-Disabled*. SL1 is not currently collecting data from the device because the system has disabled collection.
    - *Maintenance*. SL1 is not currently collecting data from the device because it is currently in scheduled maintenance mode.
    - *User-Initiated-Maintenance*. SL1 is not currently collecting data from the device because it has manually been put into maintenance mode by a user.
    - *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. SL1 cannot collect data from the device at this time.

> **NOTE:** Depending on the circumstances, more than one collection state might appear for a single device. For example, if a device is in a scheduled maintenance mode, the ***Collection State*** might be *Unavailable / Maintenance / System-Disabled*.

- ***Hostname***. The fully qualified hostname for the device, for devices that are discovered and managed by hostname (instead of IP address). This column does not appear by default, but you can add it by clicking **Grid Settings** > *Column Preferences*.

Viewing Additional Data about a Device

On the **Events** page and the **Devices** page, you can click the **Expand** icon ( ) next to an event or device to open a new **Device Summary** modal:



NOTE: On the **Events** page, the **Device Summary** modal displays only for events that are aligned with devices.

The detail window for that device contains the **Tools** pane, the **Vitals** graphs, and the **Logs** pane:

- The **Tools** pane enables you to run a set of diagnostic tools or user-initiated actions in the **Activity Center**, or to click on custom links that will open in a separate browser window. Click the search bar to search for tools, actions, or custom links that are available for the device.

- The **Vitals** pane displays graph data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Logs** pane displays a list of events associated with that device.

> **TIP:** To open the detail or Investigator page for an item, click the link for the item name at the top of the detail window.

Aligning a Device with a Different Organization

To align a device with a different organization:

1. On the **Devices** page, click the **Actions** button (⋯) for the device and select *Align Organization*. The **Align to Organization** window appears.

> **TIP:** To align more than one device to an organization, select the checkboxes to the left of those devices and click ***Align Organization*** in the blue bar at the bottom of the screen.

2. In the **Align to Organization** window, use the ***Organization*** drop-down to search for and select an organization.
3. Click the **[Align Organization]** button. The organization you selected now appears in that ***Info*** drop-down on the **Device Investigator** page for that device.

Adding Devices with Discovery

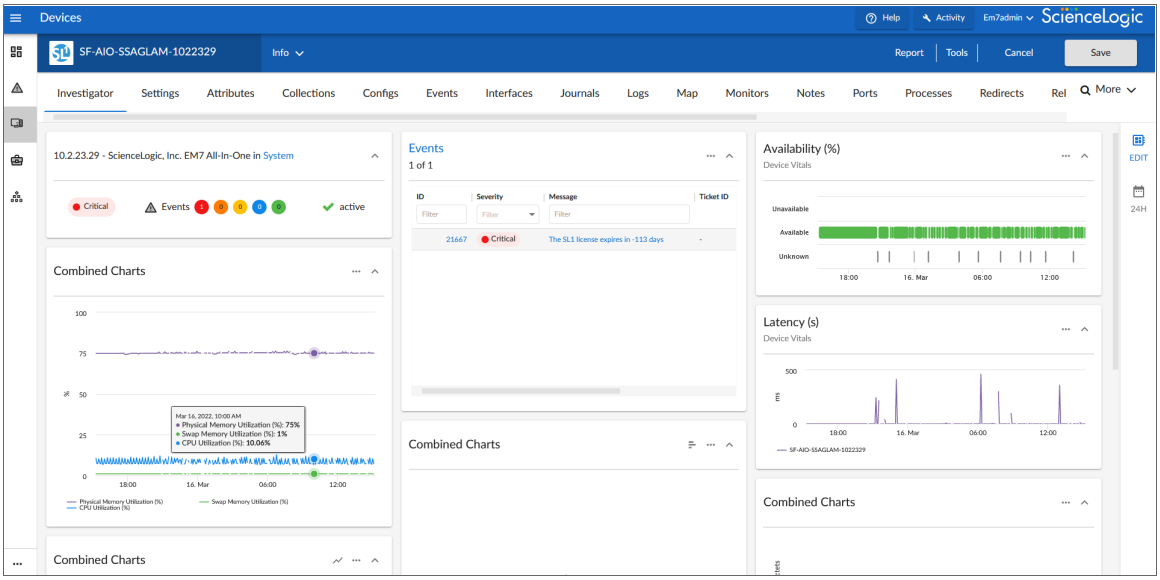
On the **Devices** page, you can click the **[Add Devices]** button to run a guided or unguided ***discovery*** session, a process that searches for and adds more devices to SL1 for monitoring.

For more information about adding devices using guided or unguided discovery, see the ***Discovery and Credentials*** manual.

Using the Device Investigator

The **Device Investigator** displays a customizable, detailed set of data about a specific device.

From the **Devices** page, click the name of a particular device to open the **Device Investigator** page for that device:



The tabs on the **Device Investigator** page provide access to all of the data associated with the device. The tabs are similar to the tabs on the **Device Administration** and **Device Properties** panels in the classic SL1 user interface.

Only tabs relevant to the selected device are available on the **Device Investigator** page. For example, the **[Agent]** and **[Interfaces]** tabs do not display if the selected device does not use agents or interfaces. Also, widgets on the **[Investigator]** tab display as "Empty" where no metrics exist for that widget.

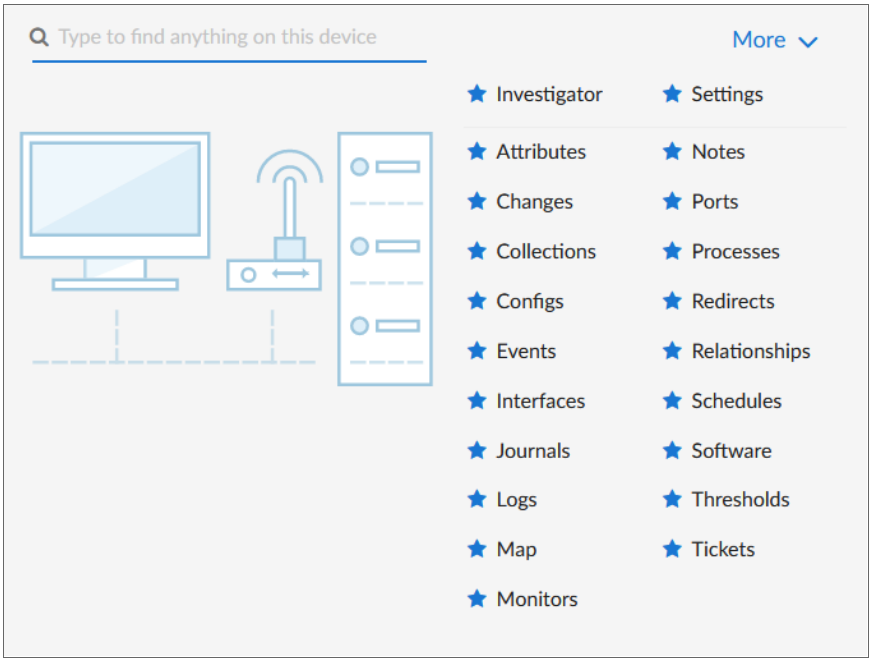
The **Device Investigator** page can include the following menus and buttons:

- *Info*. This drawer on the **[Investigator]** tab displays additional information about the device, along with the most recently updated values for uptime and collection time.
- *Report*. This button lets you generate a detailed report on the device.
- *Tools*. This button opens the **Activity Center**, where you can run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open in a separate browser window.

The **Device Investigator** page contains the following tabs:

- *Investigator*. Displays panels that provide basic information and metric data about a device. For most devices, the default panels include an Overview panel, Events, Logs, Availability, and combined charts for metrics such as utilization, discards, and errors. You can customize the panel layout on this page to meet your specific business needs, including select additional metrics to display.

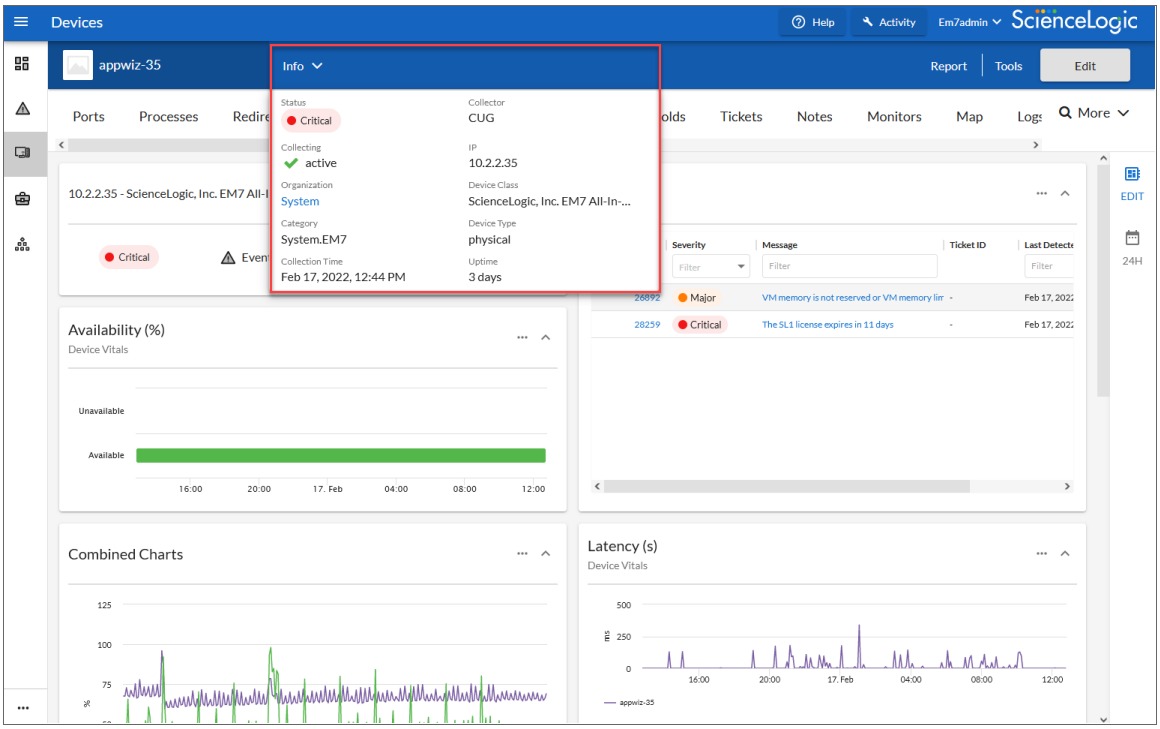
- *Settings*. Lets you manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more. You can also set user maintenance preferences and disable or enable collection on that device.
- *Attributes*. Lists the custom descriptive fields that are currently aligned with this device. On this tab, you can add and remove extended custom attributes to this device.
- *Changes*. Displays active and cleared Change Events for a device.
- *Collections*. Lets you align or un-align Dynamic Applications with this device, enable or disable collection for the Dynamic Applications, and run a Dynamic Application. You can also change credentials and update the poll frequency for a Dynamic Application.
- *Configs*. Displays configuration information collected from the device by Dynamic Applications. If this device does not have any configuration data, this tab does not appear.
- *Events*. Displays a list of active and cleared events for the device. You can acknowledge events from this tab and add event notes.
- *Interfaces*. Displays information about the interfaces used by the device. If this device does not use interfaces, this tab does not appear.
- *Journals*. Displays journal entry information collected from the device by Dynamic Applications.
- *Logs*. Displays all of the messages SL1 and the SL1 Agent, if applicable, have collected from the device.
- *Machine Learning*. Displays a list of machine learning metrics that are enabled for the device.
- *Map*. Opens a map of that device and the devices it is related to (for systems that have the **Maps** page enabled).
- *Monitors*. This tab lets you define monitoring policies for the device.
- *Notes*. Displays notes and attachments associated with the device. You can also edit and create notes.
- *Ports*. Displays a list of all open ports on the device.
- *Processes*. Displays a list of system processes running on the device.
- *Redirects*. Allows you to redirect logs entries from an IP-based device to the current device. This is most useful when the current device is a virtual device, but you can also redirect log entries from one IP-based device to another IP-based device.
- *Relationships*. Displays information about parent-child relationships between devices.
- *Schedules*. Allows you to view and manage all the scheduled processes you have defined in your system.
- *Software*. Displays a list of all the software installed on the device.
- *Thresholds*. Lets you define space and performance thresholds for a device.
- *Tickets*. Displays all open, pending, or working tickets associated with the device.
- **More**. This drop-down lets you select additional tabs to display on the **Device Investigator** page by clicking the star icon next to the tab name. You can search for specific items on a tab, such as Device Class, Uptime, or Category, and the relevant tab will appear in the search results. You can also remove a tab by clicking the star icon again, turning it from blue to white. Your tab selections are saved and remain in place even after you log out:



TIP: Click the forward-slash button (/) to open the **More** drop-down. You can highlight search results using the Up and Down Arrow keys on your keyboard, and select a result by pressing **Enter**. To close the drop-down, click the word ***More***.

Using the Info Drawer on the Device Investigator Page

On the **Device Investigator** page, you can view read-only information about the device in the ***Info*** drawer:



The ***Info*** drawer displays the following information for the device:

- ***Status***. The status of the device.
- ***Collector***. The Collector Group that was last used to collect data from the device. For All-In-One Appliances, this field will contain the name of the default, built-in Collector Group.
- ***Collecting***. Indicates that the device collection is "Collecting" with a green check mark icon ( ), meaning SL1 is periodically collecting data from the device, or "Not Collecting" with a prohibition icon ( ), meaning the SL1 is not currently collecting data from the device.
- ***IP***. IP address of the device.
- ***Organization***. The organization to which this device belongs. Click the organization name to view a detail page for the organization.
- ***Device Class***. Device class for the device. A device class usually describes the manufacturer of the device.
- ***Category***. The device category associated with the device. The device category usually describes the primary function of the device, such as a "server", "switch", or "router".
- ***Device Type***. Specifies whether the device is a physical device or a virtual device.
- ***Collection Time***. Date and time of the most recent collection.
- ***Uptime***. The number of days and hours that the device has been continuously up and communicating with SL1.
- **More Attributes**. This lower section lists any custom attributes that might be aligned with this device.

Running a Device Report

On the **Device Investigator** page for a specific device, you can generate a detailed report on that device. You can specify the information to include in the report and the format that SL1 will use to generate the report, including HTML, PDF, XLS, and more.

1. On the **Device Investigator** page, click the **[Report]** button in the top navigation bar. The **Device Report** modal page appears.
2. In the ***Type*** drop-down, select the type of report you want to generate. Your options include:
    - **[Full Report]**. Includes information about device status, status of all device policies, status of all monitors, status of hardware components, status of all thresholds defined for the device, a list of all active events associated with the device, and information about the last collection time and last entry to the device log.
    - **[Status]**. Includes information about device status, status of all monitors, status of hardware components, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
    - **[Config]**. Includes status of all monitors, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
    - **[Contact]**. Includes contact information for the device's organization and contact information for all vendors and warranty or support accounts.
    - **[Hardware]**. Includes overview of hardware components for the device.
    - **[Notes]**. Includes all notes created in the **Notepad Editor** page.
    - **[Software]**. Displays a list of software installed on the device.
    - **[Processes]**. Displays a list of all processes running on the device.
    - **[Network]**. Includes information about network ports and network configuration.
    - **[Events]**. Includes a list of all active events associated with the device.
    - **[Health]**. Includes information about device status, status of all monitors, status of all Dynamic Applications associated with the device, status of all thresholds defined for the device, and a list of all active events associated with the device.
3. In the ***Format*** drop-down, select the format for the report. Your options include:
    - ***HTML***. Create the report as an HTML document.
    - ***PDF***. Create the report as a PDF document.
    - ***DOC***. Create the report as a Microsoft Word document.
    - ***XLS***. Create the report as Microsoft Excel spreadsheet.
    - ***CSV***. Create the report using comma-separated values.
4. Click **[Create Report]** to generate the report.

Using the Action Runner

On the **Device Investigator** page, you can click the **Tools** menu to display the **Action Runner**. The **Action Runner** enables you to run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open in a separate browser window.

NOTE: The tools and actions that are available in the **Action Runner** are based on the device type and your user permissions, as determined by your organization assignment and access hooks. For example, if a device does not have an IP address, only the Availability tool will be available.

NOTE: For more information about user-initiated actions, see the chapter on "Automation Policies" in the ***Run Book Automation*** manual. For more information about custom links, see the chapter on "Custom Links" in the ***Customizing the User Experience*** manual.

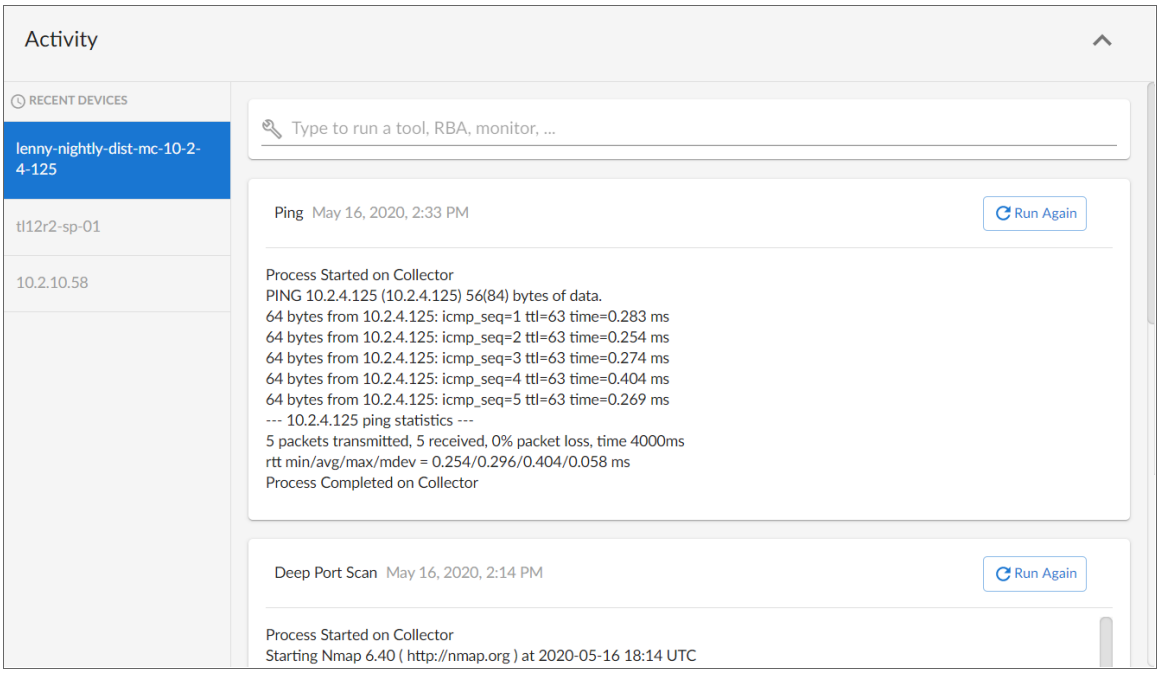
To use the **Action Runner**:

1. Access the **Action Runner** for devices in one of the following ways:
    - On the **Devices** page, open the Device Drawer for a particular device. Click the search bar in the **Tools** pane.
    - On the **Device Investigator** page, click the **[Tools]** button in the top navigation bar.
    - Click **[Activity]** in the navigation bar at the top of any page in SL1. Click the search bar.
2. When you click the search bar, a list appears of the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:
    - ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
    - ***Ping***. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, SL1 uses the appropriate IPv6 ping command.
    - ***Who Is***. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
    - ***Port Scan***. Displays a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
    - ***ARP Lookup***. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.

- ***ARP Ping***. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.
- ***Trace Route***. Displays the network route between SL1 and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, SL1 uses the appropriate IPv6 traceroute command.

TIP: The tools found in the **Action Runner** can also be found in the Device Toolbox in the classic SL1 user interface.

3. If you clicked a custom link, the link opens in a new browser window. If you clicked on a tool or action, then as it runs, its progress and results appear in a log in the **Activity Center**.
4. After the tool or action has run, if you want to run it again, click the **[Run Again]** button. This button appears only for activities completed during your current session.



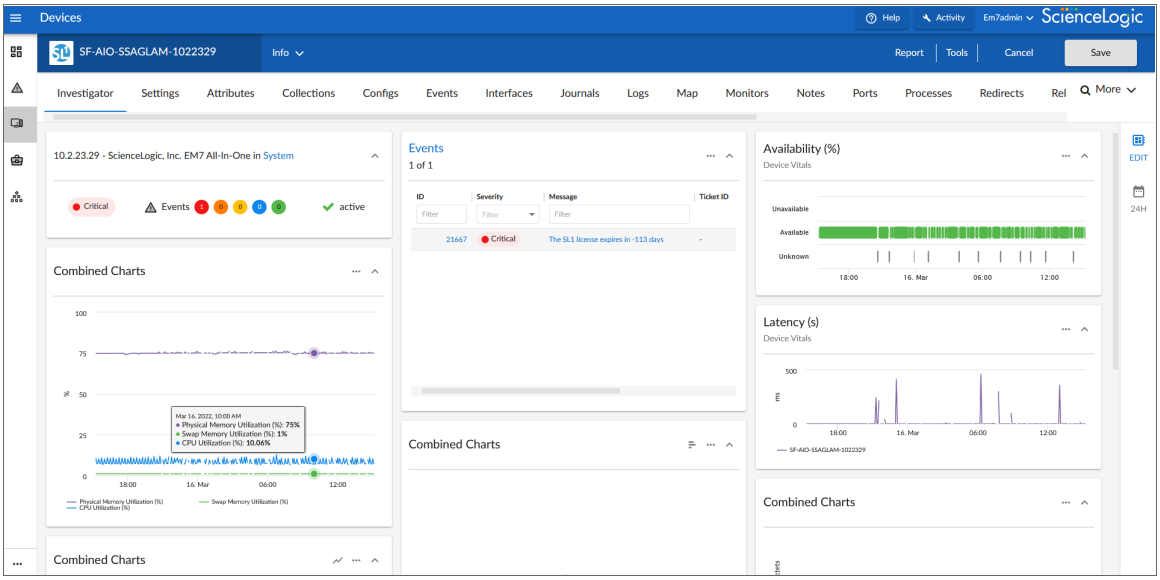
NOTE: The left pane of the **Activity Center** displays a list of devices for which you have most recently used the **Action Runner**, with the current device at the top of the list. To use the **Action Runner** for any of the other recently used devices or to view historical logs for the tools or actions that have been run on those devices, click on the device name.

Overview of the Device Investigator Tabs

The following section provides an overview of how to use the tabs on the **Device Investigator** page for a selected device.

The Investigator Tab

The **[Investigator]** tab of the **Device Investigator** page displays a customizable set of metrics about the selected device.



The device type determines which metrics appear in the **[Investigator]** tab. For most devices, the following panels and metrics appear by default:

- ***Overview***. Displays a panel that includes basic information about the device, including its IP address, Device Class, organization, current state, event count, and collection status.
- ***Events***. Displays a panel with the list of events aligned with this device. In the right-hand pane, you can click the **ID** or **Message** field to view the **Event Investigator** page for that event. You can also click the **Events** panel heading to go to *the [Events] tab* for that device.
- ***Availability***. Displays a panel for the device's availability over time. Availability means a device's ability to accept connections and data from the network.
- ***Latency***. Displays a panel for latency for the device over time, in milliseconds. Latency means the amount of time it takes SL1 to communicate with the device.
- ***Map***. Displays a panel with a map of the device and all of the devices with which the device has relationships. You can also click the **Map** panel heading to go to the **[Map]** tab for that device. This panel is disabled by default, but can be enabled by clicking the **[Edit]** button, and then selecting the ***Map*** checkbox.
- ***CPU Utilization, Physical Memory Utilization, and Swap Memory Utilization***. Displays a combined chart panel with the percentage of CPU, physical memory, and swap memory used by the device over time.
- ***Utilization In and Out***. Displays a combined chart panel with the percentage of utilization in and out for the device's network interfaces.
- ***Discards In and Out***. Displays a combined chart panel with the number of discards in and out for the device's network interfaces over time.
- ***Errors In and Out***. Displays a combined chart panel with the number of errors in and out for the device's network interfaces over time.
- ***Logs***. Displays a panel with a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting. You can also click on the column headers for ***Date/Time***, ***Source***, ***Event ID***, ***Severity***, and ***Message*** to sort by that column.

TIP: You can customize the look and feel of the **[Investigator]** tab by contracting, expanding, and resizing panels as needed. Click the contract icon ( ) in the panel header to display only the header or click the expand icon ( ) to display the panel's full contents. Click the Actions icon ( ) in the panel header and then select *Small*, *Medium*, or *Large* to resize the panel.

TIP: You can customize the appearance of leaderboard panels for interfaces, file systems, and Dynamic Applications in the **[Investigator]** tab. Click the Leaderboard Bar Chart icon ( ) to switch from a bar chart to a line chart, or click the Line Chart icon ( ) to switch from a line chart to a leaderboard bar chart.

TIP: The **[Investigator]** tab panel layout is responsive. Panels are automatically resized or relocated whenever a panel is added or removed, the panels are rearranged on the page, or the browser page increases or decreases in size.

The **Device Investigator** page also includes the following sidebar buttons:

- ***Edit***. Click the **[Edit]** button on the right panel to edit the content that appears on the **[Investigator]** tab and its layout. For example, you can *add or remove metrics*, *edit the metric panel order*, or *combine charts on the [Investigator] tab*.
- ***Timespan***. Click the timespan button on the right panel to adjust the timespan of data that appears in all of the metric panels on the **[Investigator]** tab. The default timespan is *Last 24 Hours*.

NOTE: Select the ***Always display raw data*** checkbox at the top of the timespan selector to ensure that the metric data that appears in the panels on the **[Investigator]** tab always includes the most recent data available. If you do not select that checkbox, SL1 will still display raw data when you select a timespan of less than 2 days, but will automatically display rolled up hourly data for timespan selections of 2-45 days and rolled up daily data for timespan selections of more than 45 days.

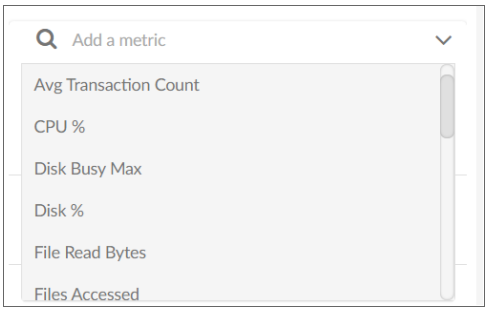
TIP: In the right-hand pane, you can click Expand at the bottom of a panel to make that panel bigger.

Adding and Removing Metrics on the Investigator Tab

Optionally, you can add metrics to the **[Investigator]** tab for Dynamic Applications, interfaces, and the SL1 agent (if applicable), among other things. You can also remove metrics from the **[Investigator]** tab.

To add and remove metrics on the **[Investigator]** tab:

1. To add a metric panel that is not currently on the **[Investigator]** tab, click the **[Edit]** button on the right sidebar to expand the layout panel, and then click the ***Add a metric*** field. A list of metrics appears:



2. Select a metric from the list, or type the name of a metric and select it from the list. The metric is added to the right pane, and a corresponding widget appears in the left pane.

3. Some metrics might require you to make additional selections, such as the network interfaces associated with a device. Click the field and add one or more additional metrics, as needed.

> **NOTE:** You can select up to eight additional metrics per widget.

4. To remove a metric panel from the **[Investigator]** tab, uncheck the corresponding box in the right panel. The metric remains listed in the right panel, but the panel is removed from the **[Investigator]** tab.
5. To completely remove the metric and its corresponding panel from the **[Investigator]** tab, click the **[Remove from Layout]** button (✕) for that metric in the right panel.

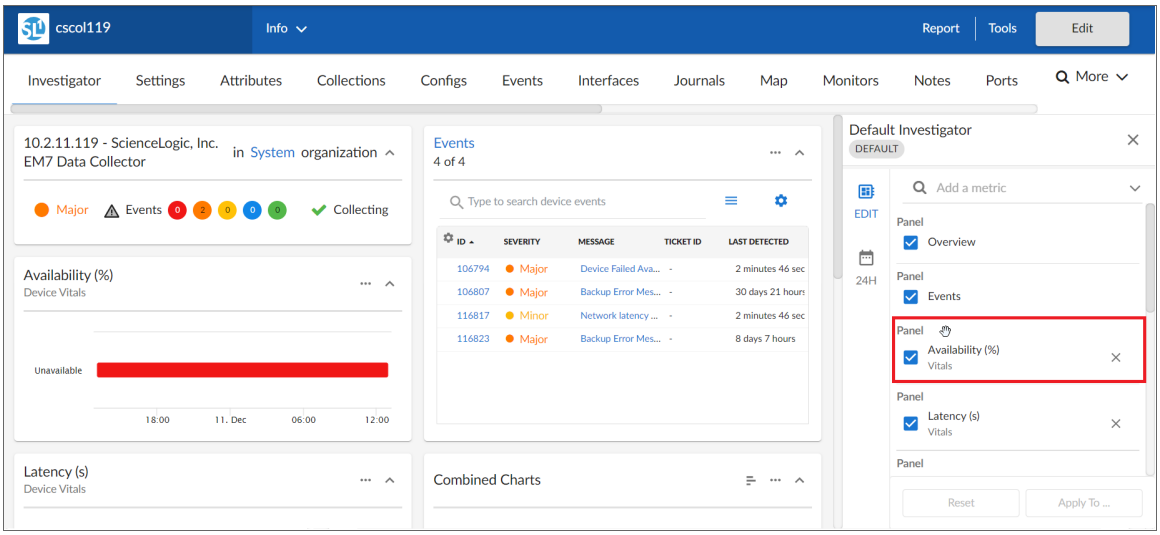
> **NOTE:** The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Editing the Metric Panel Order on the Investigator Tab

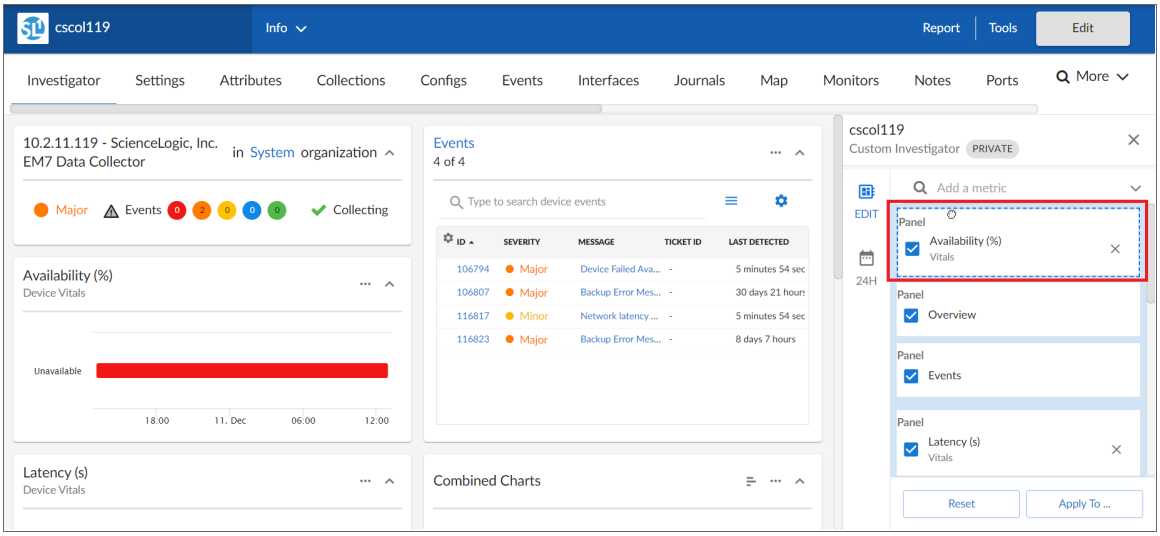
On the **[Investigator]** tab of the **Device Investigator** page, the order in which the metric panels appear in the right panel when you click the **[Edit]** button mirrors the order in which the corresponding metric panel widgets appear in the left panel. You can drag and drop the panels up or down in the right panel to edit the order in which the metric panels appear on the left panel. This enables you to prioritize the information that appears on the page.

To edit the order in which widgets appear on the **[Investigator]** tab:

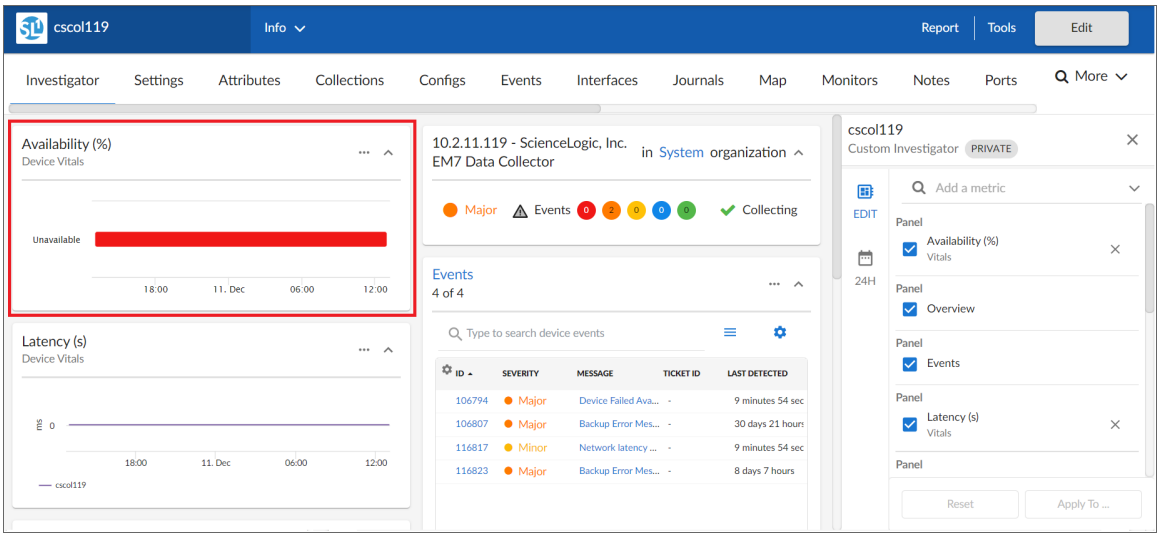
1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel.
2. Hover your mouse over the "Panel" heading of the panel that you want to move until you see an open hand icon appear:



3. Click and hold down the left button on your mouse to grab the panel, and then use your mouse to drag the panel to a different location in the list. When you do so, the open hand icon becomes a closed hand icon, and a blue dotted box appears around the panel.



4. Release the left mouse button to drop the panel in your desired location. The new right-hand panel order will be reflected in the left-hand widget panel.



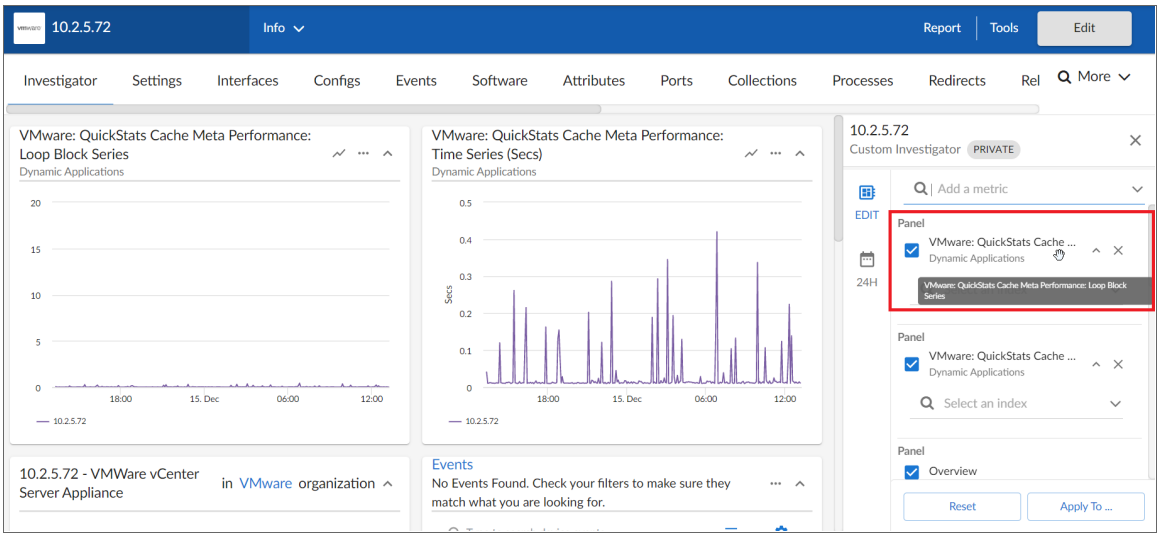
NOTE: The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Combining Charts on the Investigator Tab

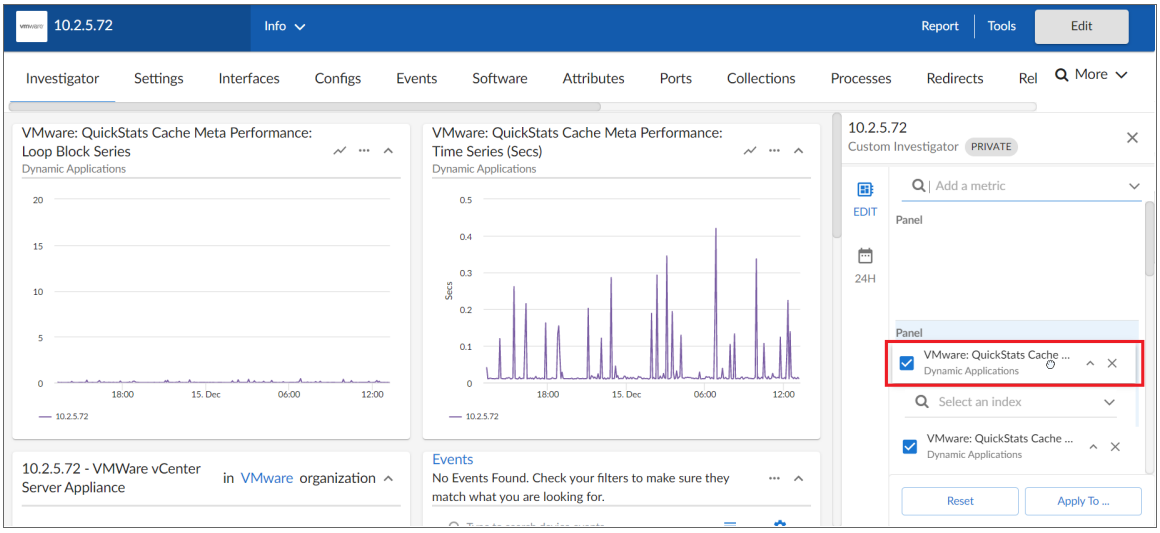
On the **[Investigator]** tab of the **Device Investigator** page, you can combine charts for different time-series metrics to see all of the combined data for those metrics in a single chart.

To combine charts:

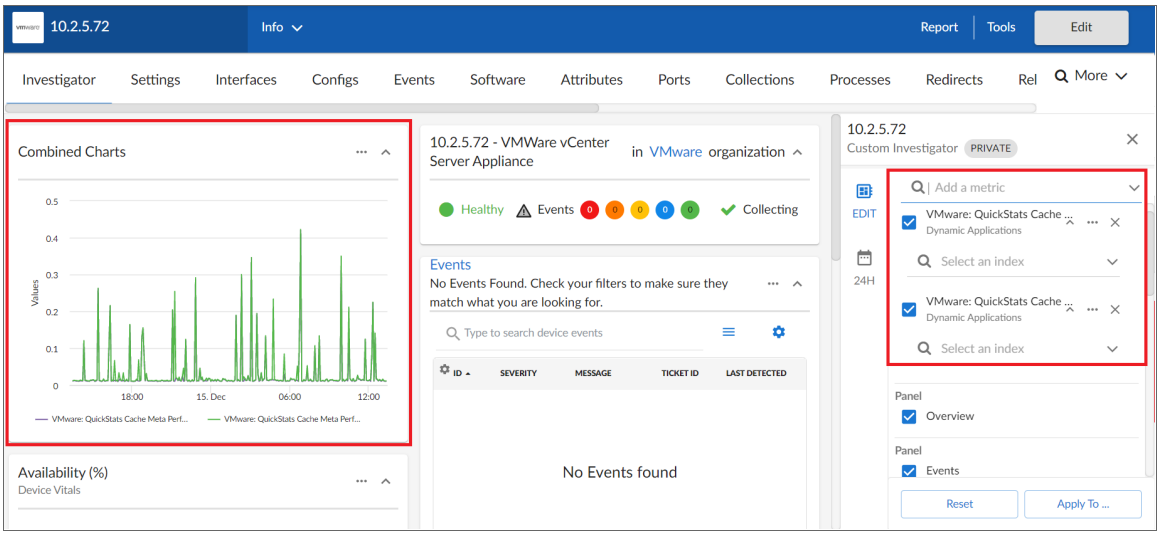
1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel.
2. Hover your mouse over a time-series metric name until you see an open hand icon appear.



3. Click and hold down the left button on your mouse to grab the metric, and then use your mouse to drag the metric into the panel of a different time-series metric in the list. When you do so, the open hand icon becomes a closed hand icon, and the panel containing the combined metrics turns blue.



4. Release the left mouse button to drop the metric into the desired panel. The newly combined metric panel will be reflected in a "Combined Charts" widget in the left-hand widget panel.



NOTE: The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Applying a Custom Device Investigator Layout to Other Devices

The device **[Investigator]** tab has a default layout that includes widgets such as an Overview panel, Events panel, Logs panel, and combined chart panels for utilization, discard, and error metrics. Initially, this layout is assigned to all devices.

You can also create custom **[Investigator]** tab layouts for individual devices or entire Device Classes or Device Categories, and then apply those updates either to only yourself or to all system users.

To apply a custom device **[Investigator]** layout to other devices:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel. When you do so, the **[Investigator]** tab name will appear at the top of the layout panel, along with one of the following labels:
    - ***Default***. Indicates the layout has not been changed from the default settings.
    - ***Private***. Indicates the layout has been changed from the default settings but only applied to the logged in user.
    - ***Public***. Indicates the layout has been changed from the default settings and has been applied to all system users.

2. Make updates to the **[Investigator]** layout as needed, such as by ***adding or removing metrics***, ***editing the metric panel order***, or ***combining one or more charts into a single panel***. When you do so, the label at the top of the layout panel will change to "Private", if it was not already labeled as such.
3. To save the custom **[Investigator]** layout for other devices, Device Classes, or Device Categories, and/or to save the layout for all system users, click the **[Apply To...]** button, and then proceed to step 4. Otherwise, do one of the following:

    - To save the custom **[Investigator]** layout for only the current device and your user account, leave the page. When you do so, SL1 automatically saves the custom layout, and will display the custom layout when you return to the **[Investigator]** for that device.
    - To revert your **[Investigator]** layout changes to the default settings, click the **[Reset]** button.

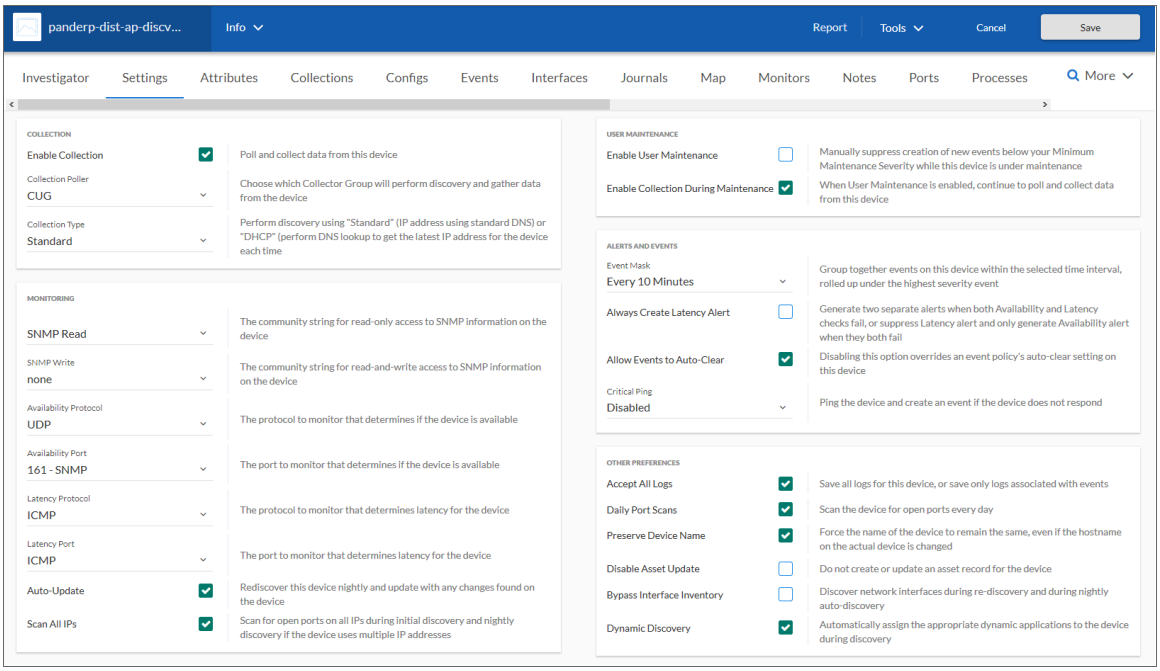
4. On the **Apply "Custom Investigator" to...** modal, use the following tabs and fields to specify the devices and users to which you want to apply the custom **[Investigator]** layout, as well as its name:

    - ***Categories, Classes, and Devices tabs***. Click the appropriate tab(s) at the top of the modal page and then use the search field to locate the specific Device Categories, Device Classes, or individual devices to which you want to apply the custom **[Investigator]** layout. Select the checkbox for each category, class, or device that you want to select.
    - ***Name***. Type a new name for the custom **[Investigator]** layout.
    - ***Apply Investigator for***. Select one of the following options:
        - *Myself*. Applies the custom **[Investigator]** layout to only your user account.
        - *All System Users*. Applies the custom **[Investigator]** layout to all users in your SL1 system.

5. Click **[Review]**. A summary of your selections appears.
6. To confirm your selections, click **[Apply To Selected Types]**.

The Settings Tab

On the **[Settings]** tab of the **Device Investigator** page, you can manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more.



Click the **[Edit]** button to change your settings. When you are done making changes, click **[Save]**.

NOTE: The **Agent** section appears only for agent-type devices.

Set the following **Agent** data collection preferences:

- ***Disk Space***. Specify the amount of disk space in MB that the agent can use to store data. If the agent loses connectivity to SL1, this disk space will be used to store collected data until the connection to SL1 is restored. When connectivity is re-established, the agent uploads all of its stored data.
- ***Excludes***. Type a list of processes and directories, separated by semi-colons, that you do not want the agent to monitor.
- ***Includes***. Type a list of processes and directories, separated by semi-colons, that you want the agent to monitor. This field ensures that specific processes are monitored.

  NOTE: If a process or directory is included in both the ***Excludes*** field and the ***Includes*** field, the item in the ***Includes*** field will override the item in the ***Excludes*** field.

- ***Collect File Information***. Select this option if you want the agent to report the names of files accessed by each monitored process.
- ***Collect Named Pipe Information***. Select this option if you want the agent to collect named pipe information.
- ***Collect Socket Information***. Select this option if you want the agent to collect socket information.

- ***Collect Thread Information***. Select this option if you want the agent to collect thread information.
- ***Collect Non-Intercepted Processes***. Select this option if you want the agent to collect limited information for processes that do not contain the agent library.
- ***Processes Aggregation***. Specify how you want the agent to collect limited information for processes that do not have the agent library in them, and how to aggregate short-lived processes. Your options include the following:
    - *All*: Aggregate every short-lived process into its parent.
    - *None*: Do not aggregate any short-lived process.
    - *Without Sockets*: Aggregate short-lived processes unless those processes have sockets.
- ***Upload Interval***. Specify how often the agent should upload data. Your options include the following:
    - *20 Seconds*. Upload a data snapshot every 20 seconds.
    - *60 Seconds*. Upload a data summary every 60 seconds. This is the default setting starting with SL1 version 11.1.0, and version 174 of the Linux agent and version 133 for the Windows agent. This option uses an improved data format that requires fewer SL1 resources. The SL1 agent continues to internally collect and poll data every 20 seconds, but the agent summarizes and uploads that data every 60 seconds. There is no data loss even though the data is uploaded less frequently.

> **NOTE:** Starting with SL1 version 11.3.0, if you specify 60 seconds for the upload interval, the summary upload now will include "watched" or "monitored" files, just like the snapshot upload does.

Set the following **Collection** preferences:

- ***Enable Collection***. Select this option to enable collection using the collector group specified in the following field.
- ***Collection Poller***. Select the name of collector group you want to use for collection on this device.
- ***Collection Type***. Select the type of collection you want to use on this device. Your options include *Standard* or *DHCP*.

Set the following **Monitoring** preferences:

- ***SNMP Read***. Select the community string for read-only access to SNMP information on the device.
- ***SNMP Write***. Select the community string for read-and-write access to SNMP information on the device.
- ***Availability Protocol***. Select the protocol to monitor that determines if the device is available.
- ***Availability Port***. Select the port to monitor that determines if the device is available.
- ***Latency Protocol***. Select the protocol to monitor that determines latency for the device.
- ***Latency Port***. Select the port to monitor that determines latency for the device.
- ***Auto-Update***. This checkbox specifies whether or not you want SL1 to perform a nightly discovery of the device and update records with changes to the device. If this field is unchecked, SL1 will not perform nightly discovery. Changes to the device, including newly opened ports, will not be recorded by SL1.

- ***Scan All IPs***. If the device uses multiple IP Addresses, SL1 will scan for open ports on all IPs during initial discovery and nightly discovery.

Set the following **User Maintenance** preferences:

- ***Enable User Maintenance***. Specifies whether the device is in user maintenance mode. User maintenance is an option that allows a user to manually put a device in to "maintenance mode". During maintenance mode, for the selected devices, SL1 generate only events with a severity less than the system-wide **Maintenance Minimum Severity** setting. If you select *Enabled*, the device is put in user maintenance mode, and the device will remain in this state until you or another user disables user maintenance mode.
- ***Enable Collection During Maintenance*** . Specifies whether SL1 will poll the device when user maintenance mode is enabled. If you select *Enabled*, SL1 will continue to poll and collect data from this device during user maintenance mode.

Set the following **Alerts and Events** preferences:

- ***Event Mask***. Specify the time frame for masking events. When a device uses the Event Mask setting, SL1 groups together events that occur on that device within the specified span of time.
- ***Always Create Latency Alert***. Select this option to generate two alerts when availability and latency checks fail. Deselect to generate only an availability alert and suppress latency alerts.
- ***Allow Events to Auto-Clear***. Deselect this option to override an event policy's auto-clear setting for this device.
- ***Critical Ping***. Pings the device and creates an event if the device does not respond. When enabled you can select between 5 and 120 seconds.

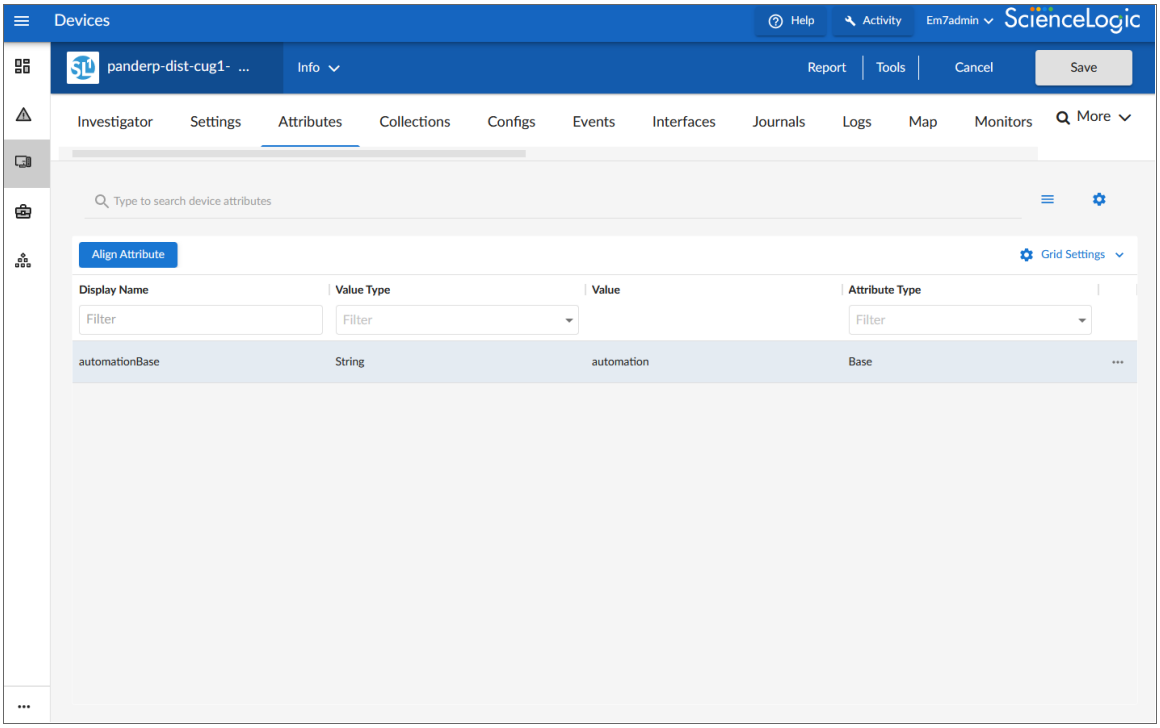
Set the following **Other** device preferences:

- ***Accept All Logs***. This checkbox specifies whether or not you want to keep and save all logs for this device. If you want to retain only logs associated with events, uncheck this field.
- ***Daily Port Scans***. This checkbox specifies whether or not you want SL1 to perform a daily scan of the device for open ports.
- ***Preserve Device Name***. If selected, the name of the device in SL1 will remain the same, even if the name of the actual device is changed. If unselected, the SL1 name for the device will be updated if the name of the actual device is changed.
- ***Disable Asset Update***. If selected, SL1 will not automatically create a new asset record for the device or update the existing asset record for the device. For the single device, this checkbox over-rides any settings defined in the **Asset Automation** page (System > Settings > Assets).
- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces. Your options include:
    - *Selected*. SL1 will not attempt to discover interfaces for this device during re-discovery and nightly auto-discovery.
    - *Not Selected*. SL1 will attempt to discover network interfaces for this device during re-discovery and nightly auto-discovery using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value specified in the **Device Thresholds** page.

- ***Dynamic Discovery***. If selected, SL1 will automatically assign the appropriate dynamic applications to the device during discovery.

The Attributes Tab

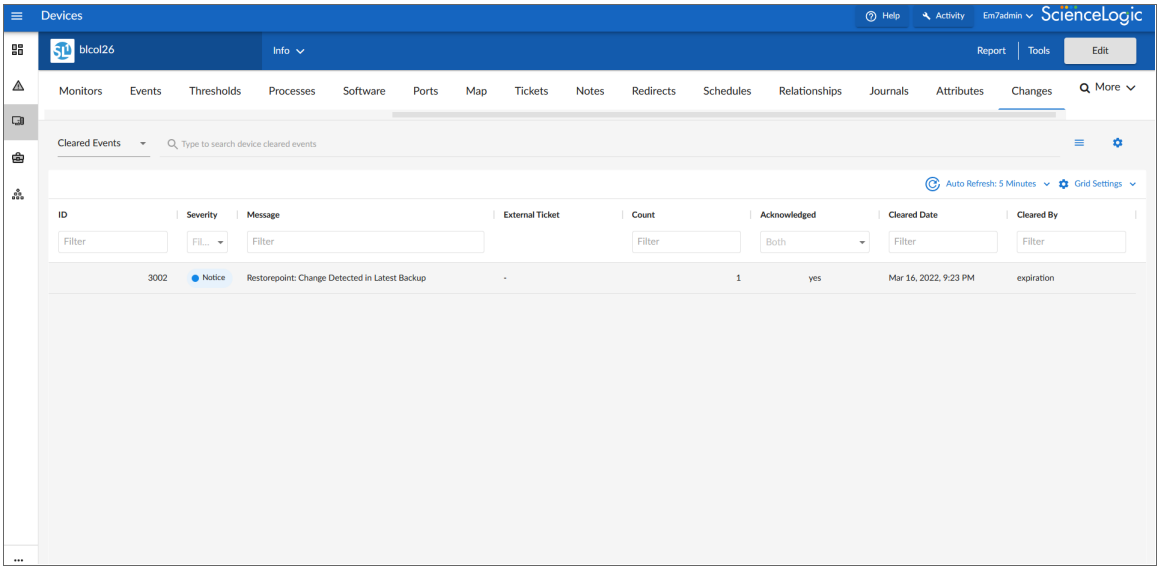
On the **[Attributes]** tab of the **Device Investigator**, you can view a list of list of custom attributes that are already aligned with that device, and you can also add and remove extended custom attributes for the device:



NOTE: For more information about this tab, see the chapter on "Adding Custom Attributes for a Device." in the ***Device Management*** manual.

The Changes Tab

On the **[Changes]** tab of the **Device Investigator**, you can view a list of the active and cleared change events for a device.



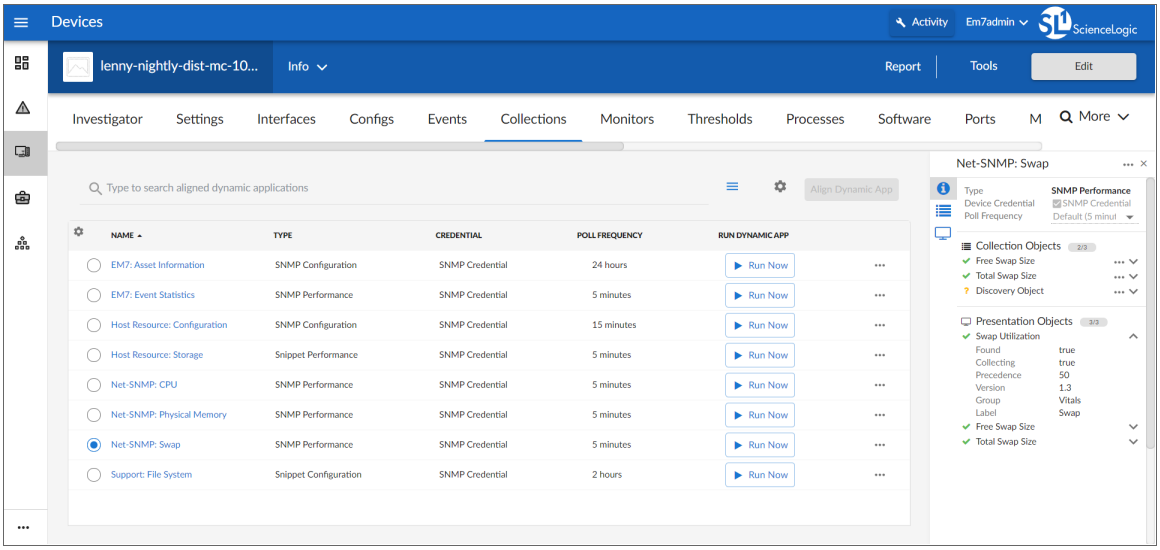
SL1 PowerFlow users can use the **[Changes]** tab to view a list of events that are created when PowerFlow pulls change data from ServiceNow and Restorepoint Synchronization PowerPacks.

Based on your third-party integrations, the tab displays the following information:

- ServiceNow planned change events
- ServiceNow emergency change events
- Restorepoint configuration change events

The Collections Tab

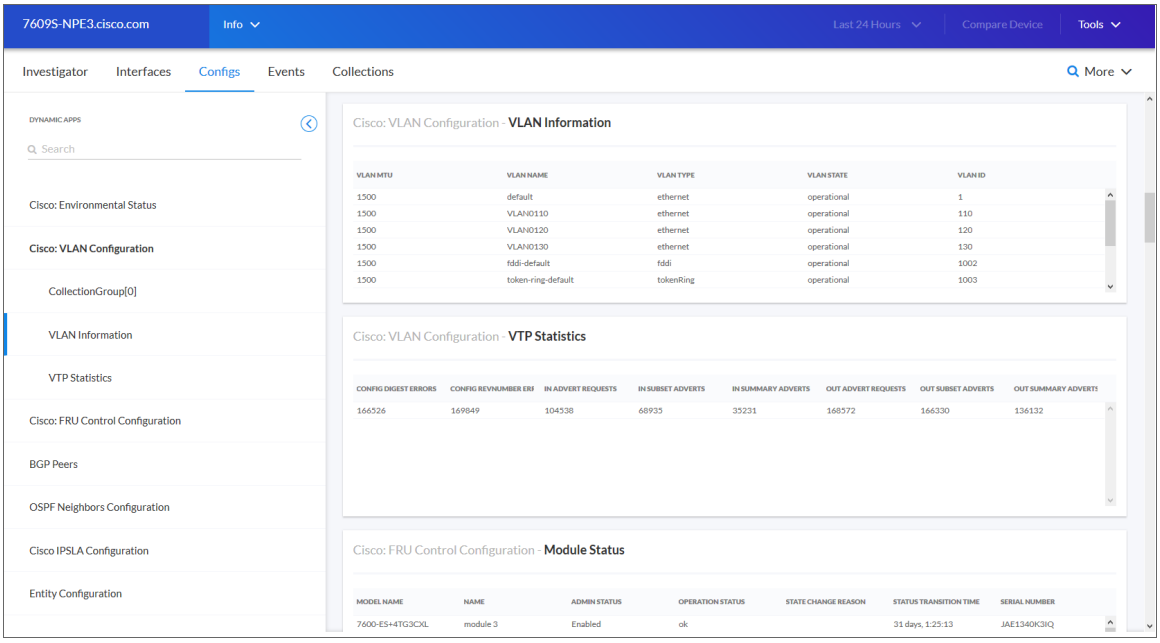
On the **[Collections]** tab of the **Device Investigator**, you can view a list of the Dynamic Applications associated with the device.



NOTE: For more information about this tab, see the chapter on "Managing the Dynamic Applications Associated with a Device" in the ***Device Management*** manual.

The Configs Tab

On the **[Configs]** tab of the **Device Investigator**, you can view configuration information that has been collected from the device by Dynamic Applications.

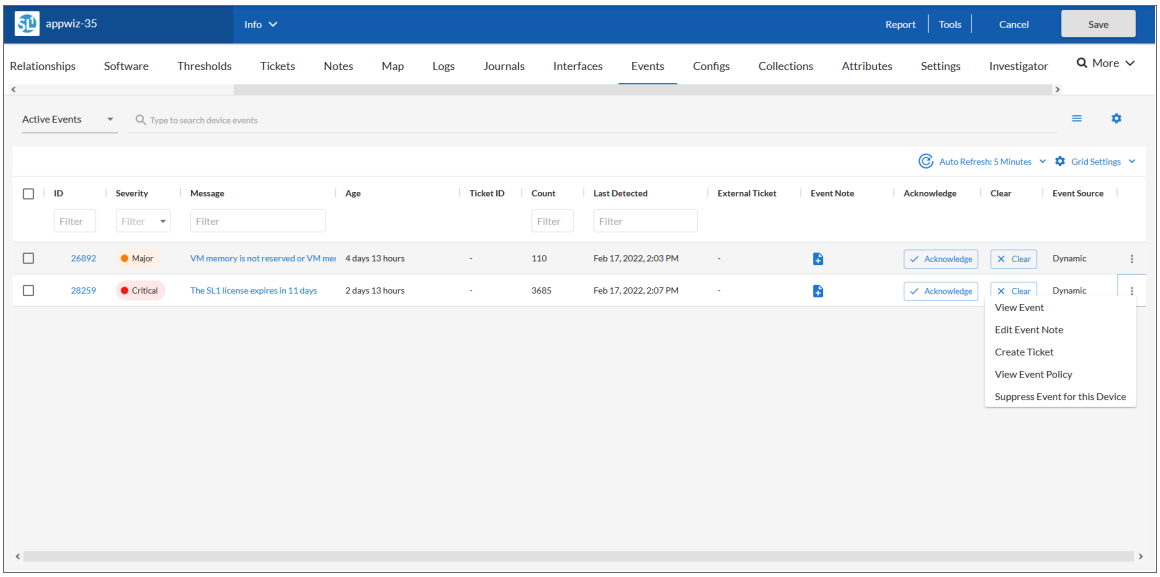


All objects of type "config" are included on the **[Configs]** tab. Usually, "config" objects contain static information about hardware and configuration settings, such as serial numbers, version numbers, and hardware status.

For more information about this tab, see the chapter on "Viewing Configuration & Journal Data" in the ***Monitoring Infrastructure Health*** manual.

The Events Tab

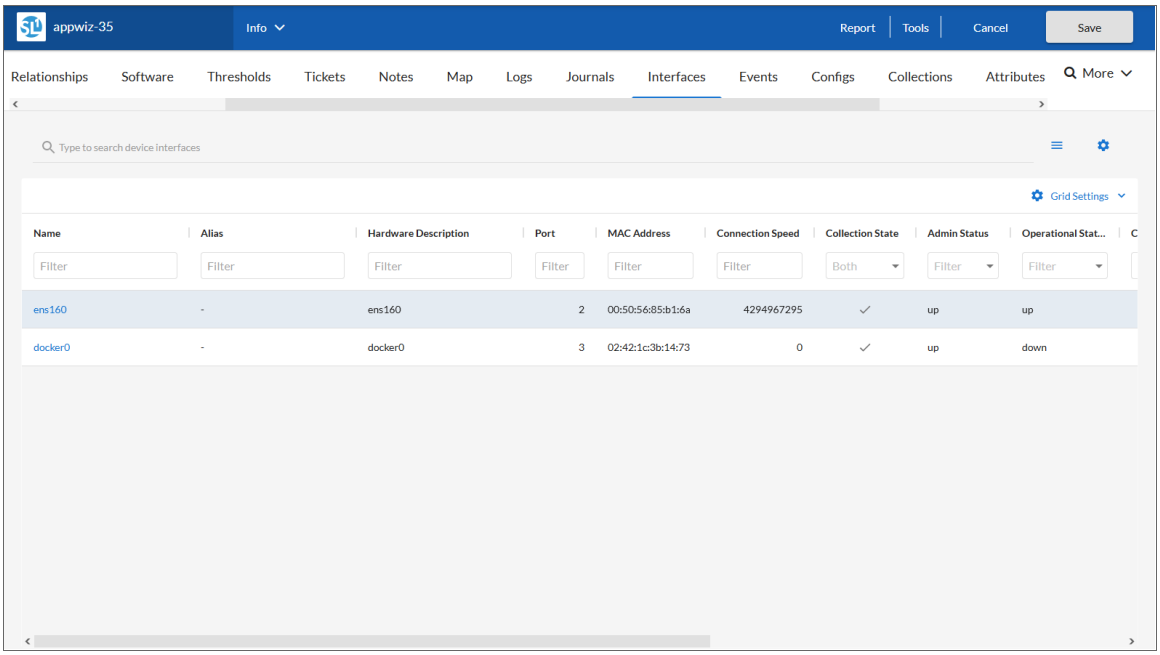
On the **[Events]** tab of the **Device Investigator**, you can view a list of events associated with the device.



NOTE: For more information about this tab, see the chapter on "Viewing Events" in the ***Events*** manual.

The Interfaces Tab

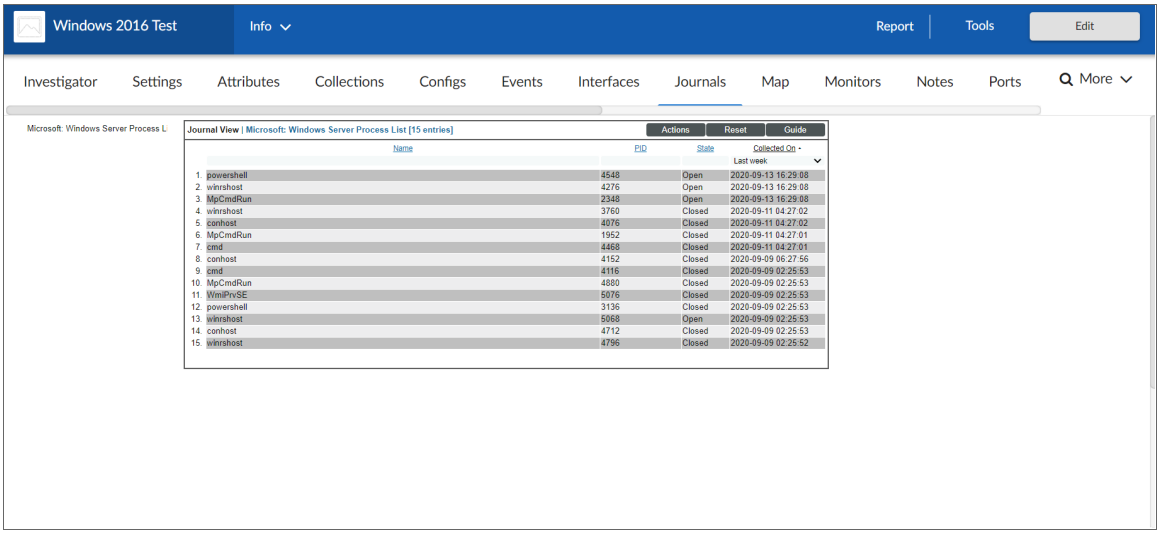
On the **[Interfaces]** tab of the **Device Investigator**, you can view information about the various interfaces used by the device, including Port, Hardware Description, MAC Address, Connection Speed, and other details for each interface.



NOTE: For more information about this tab, see the chapter on "Monitoring Network Interfaces" in the ***Monitoring Device Infrastructure Health*** manual.

The Journals Tab

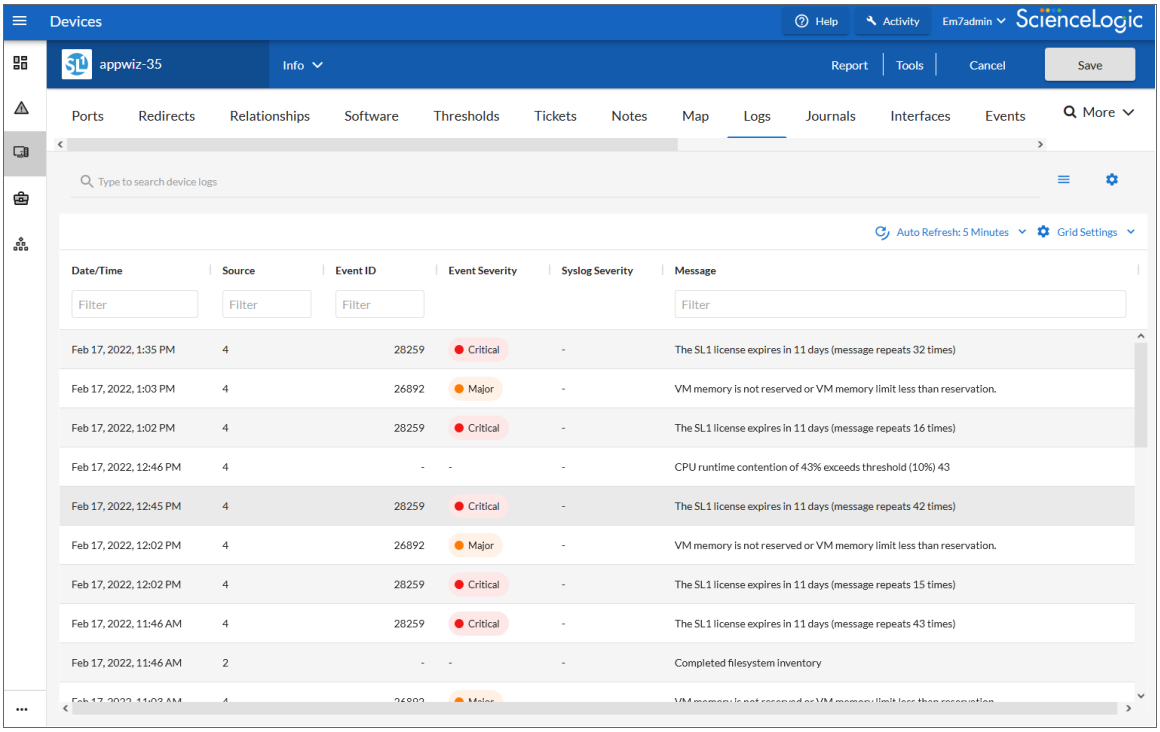
On the **[Journals]** tab of the **Device Investigator**, you can view journal entry information that has been collected from the device by journal Dynamic Applications:



For more information about this tab, see the chapter on "Viewing Configuration & Journal Data" in the ***Monitoring Infrastructure Health*** manual.

The Logs Tab

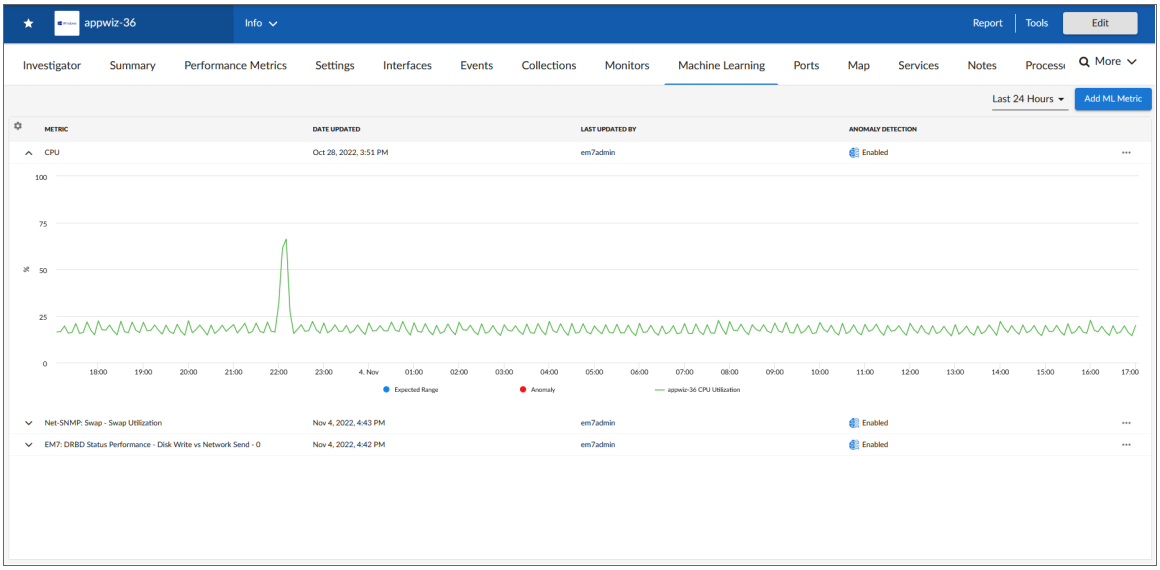
You can view logs and messages for a device in the **[Logs]** tab of the **Device Investigator** page. This is the same set of logs that display on the **[Investigator]** tab for this device.



The **Logs** tab displays all of the messages SL1 and the SL1 agent, if applicable, have collected from the device. You might find it helpful to view these log entries during troubleshooting or to manually check on the status of a device.

The Machine Learning Tab

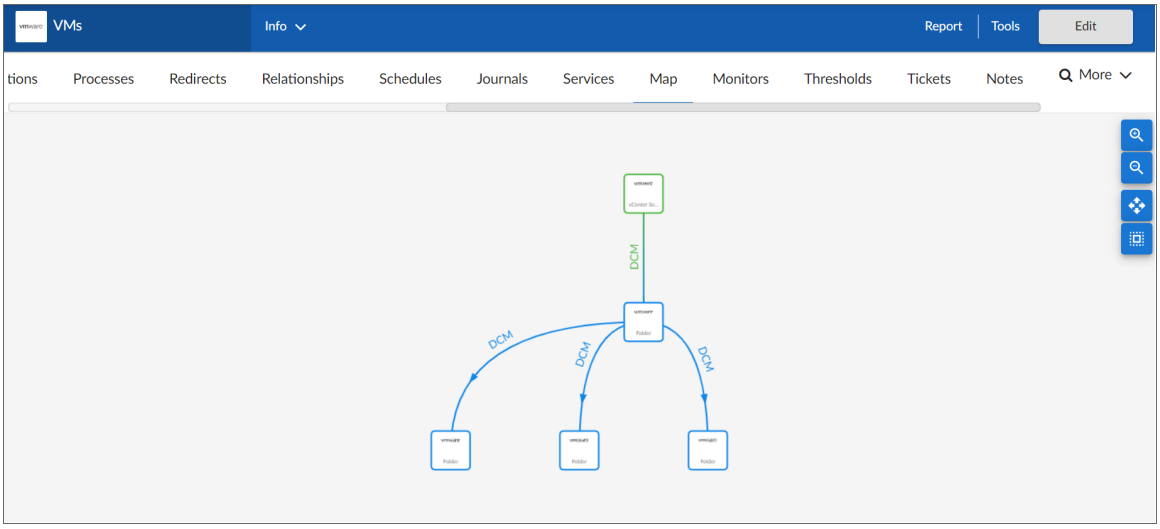
On the **[Machine Learning]** tab of the **Device Investigator**, you can view a list of machine learning metrics that are enabled for the device:



NOTE: For more information about machine learning and anomaly detection, see the ***Anomaly Detection*** manual. For more information about this tab, see the chapter on "Enabling Machine Learning-based Anomaly Detection" in that manual.

The Map Tab

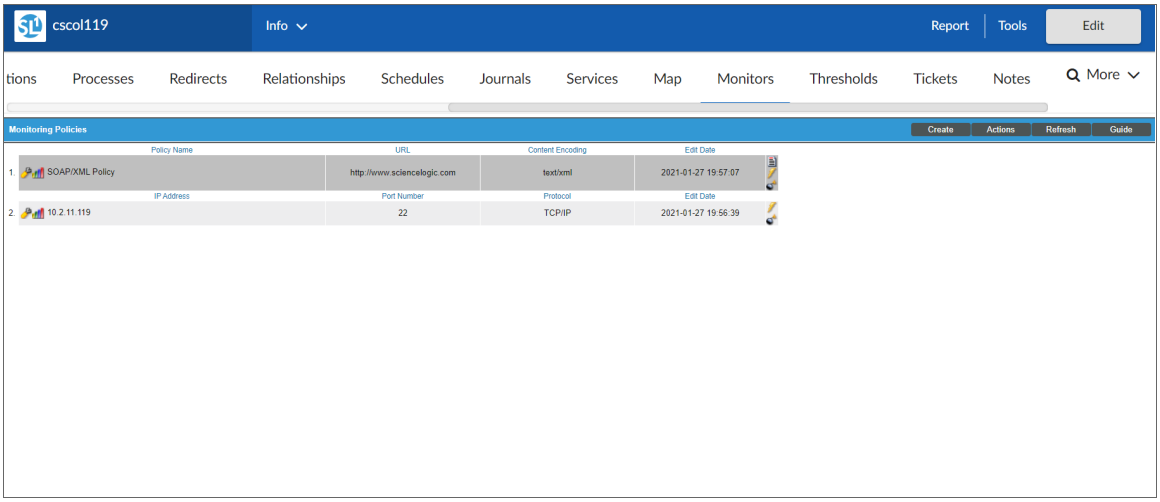
On the **[Map]** tab in the **Device Investigator**, you can view a map of the selected device and all of the devices with which the device has relationships.



NOTE: For more information about maps, see the ***Maps*** manual.

The Monitors Tab

On the **[Monitors]** tab of the **Device Investigator**, you can define monitoring policies for a device.



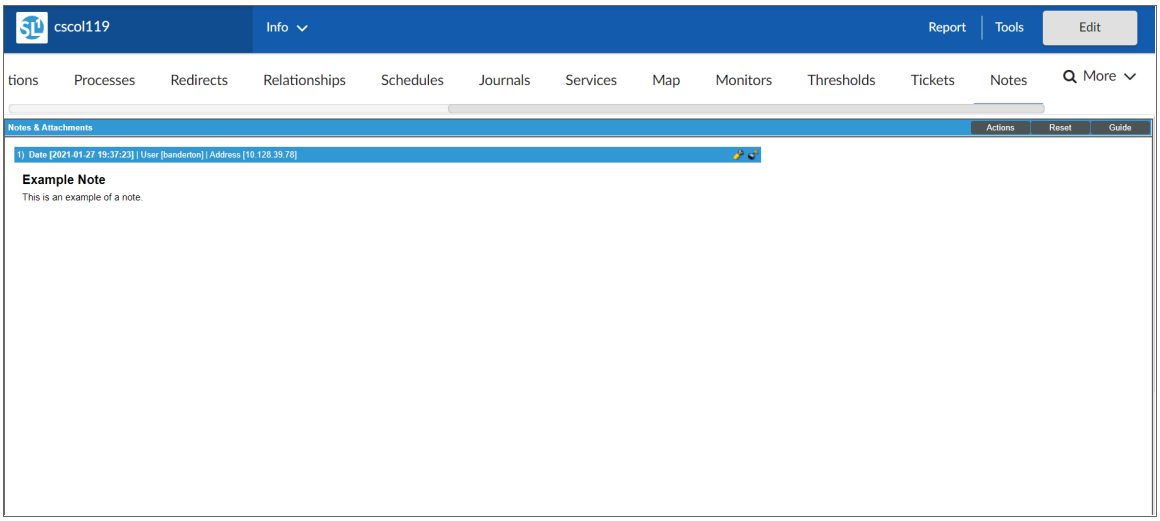
The **[Monitors]** tab allows you to define policies that monitor:

- ***System processes***. Monitors the device and look for the specified system process. For more information, see the chapter on "Monitoring Device Processes" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Domain-name availability and lookup speed***. Monitors the availability and lookup time for a specific domain-name server and a specific record on a domain name server. For more information, see the chapter on "Monitoring Domain Servers and DNS Records" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Email round-trip speed***. Monitor the amount of time it takes to send an email message from SL1 to an external mail server and then back to SL1. For more information, see the chapter on "Monitoring Email Round-Trips" in the ***Monitoring Device Infrastructure Health*** manual.
- ***SOAP and XML transaction speeds***. Monitors any server-to-server transactions that use HTTP and can post files or forms. (for example, SOAP/XML or email). Periodically, SL1 sends a request and some data and then examines the result of the transaction and compares it to a specified expression match. For more information, see the chapter on "Monitoring SOAP and XML Transactions" in the ***Monitoring Device Infrastructure Health*** manual.
- ***TCP/IP port availability***. Monitors ports for availability every 5 minutes. If a port is not available, SL1 creates an event. The data gathered by the port policy is used to create port-availability reports. For more information, see the chapter on "Monitoring Ports" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Web-content availability***. Monitors a website for specific content. SL1 will periodically check the website for specified content. If the content cannot be found on the website, SL1 will generate an event. For more information, see the chapter on "Monitoring Web Content" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Windows services***. Monitors the device and look for the specified service. For more information, see the chapter on "Monitoring Windows Services" in the ***Monitoring Device Infrastructure Health*** manual.

NOTE: All of these monitoring policies can generate events. SL1 uses the data collected by these policies to create performance reports and graphs.

The Notes Tab

On the **[Notes]** tab of the **Device Investigator**, you can add and view notes and other attachments associated with the device.

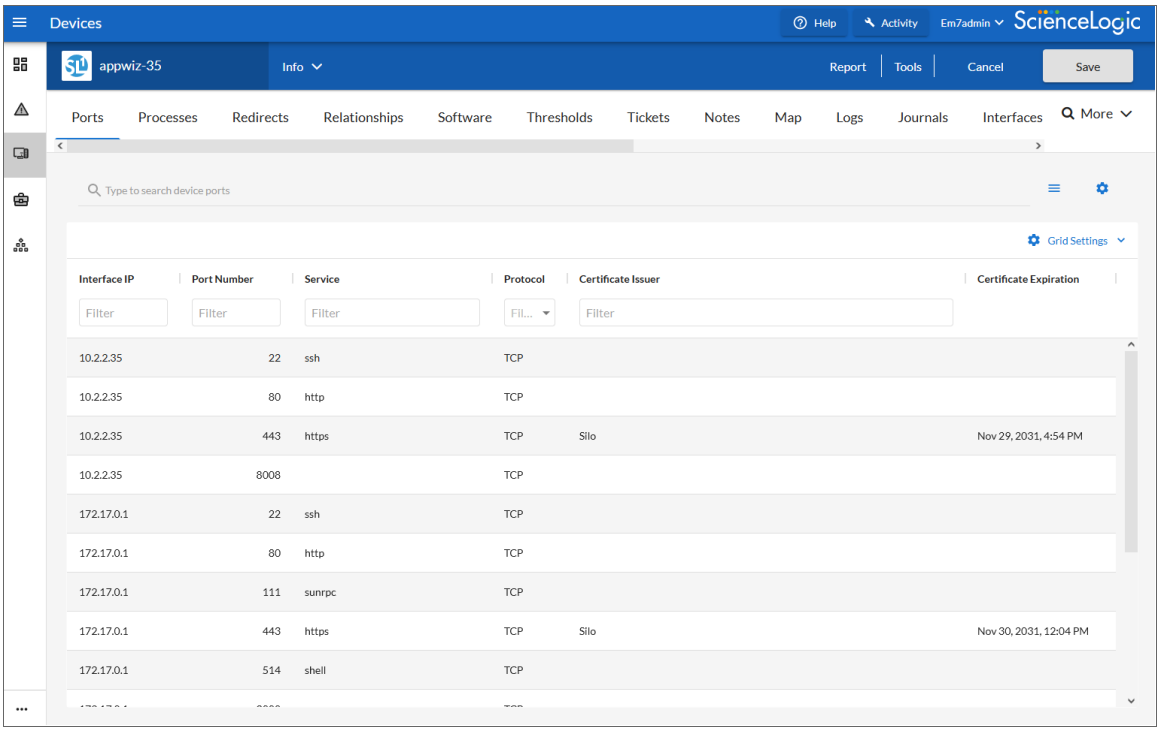


To add a note to a device:

1. Go to the **[Notes]** tab of the **Device Investigator**.
2. Click the **[Actions]** button and then select *Notepad Editor*. The **Notepad Editor** modal page appears.
3. In the **Notepad Editor** modal page , you can enter notes or comments about the device.
    - You can format the text and include links, images, and videos in the note.
    - You can also include a document template (System > Customize > Document Templates) in the field.
4. When you are finished adding content to the note, click **[Save]**. The note will appear in the **[Notes]** tab, along with any other notes about the device. Each note includes the username, date and time, and text of the comment. You can perform the following on each note entry:
    - ***To view a note's attachment***, click the paperclip icon ( ).
    - ***To edit the content of a note***, click the wrench icon ( ). The **Notepad Editor** modal page appears. You can update the note; format the text; insert content from a saved template; and add an attachment, image, or video to the note. Click the **[Save]**button to save your changes.
    - ***To delete a note***, click its bomb icon ( ).

The Ports Tab

On the **[Ports]** tab of the **Device Investigator**, you can view a list of all open ports on a device:



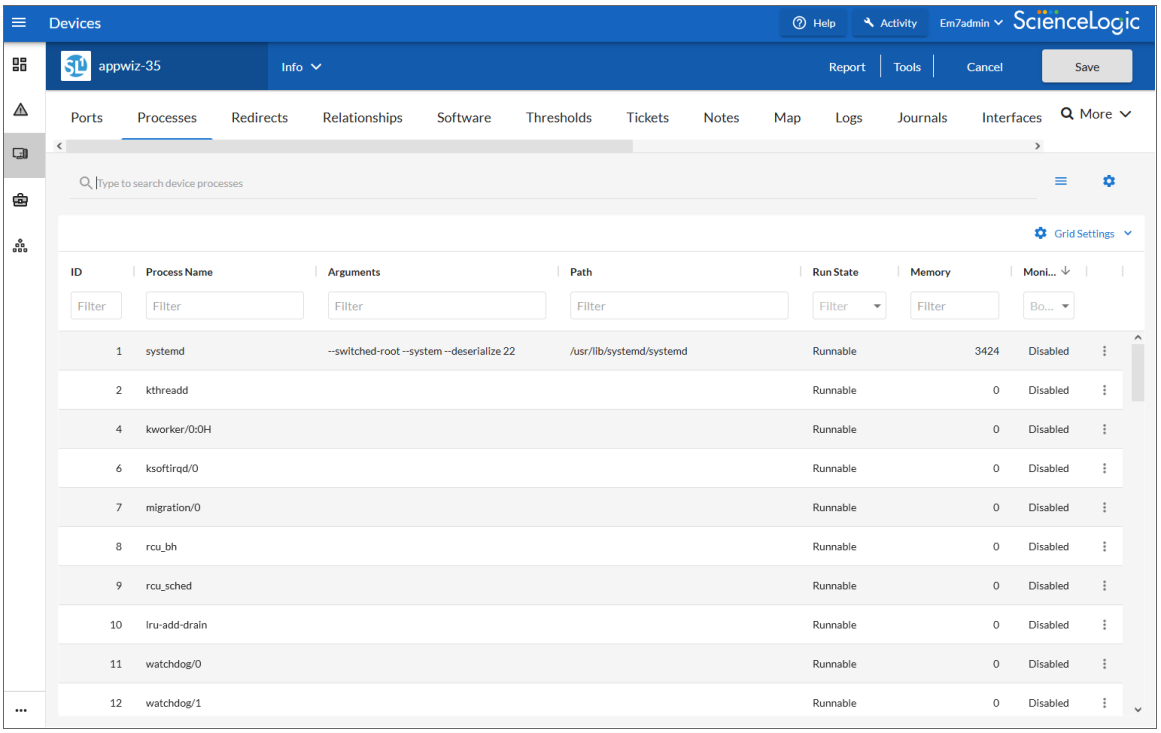
Every night, SL1 scans all the ports of each managed device. If any new ports are opened, SL1 adds the port to the list on the **[Ports]** tab.

NOTE: For more information about this tab, see the chapter on "Monitoring Ports" in the ***Monitoring Device Infrastructure Health*** manual.

The Processes Tab

A ***process*** is a program that is currently running on a monitored device or has been run in the past and is currently idle. Sometimes a process is called a task.

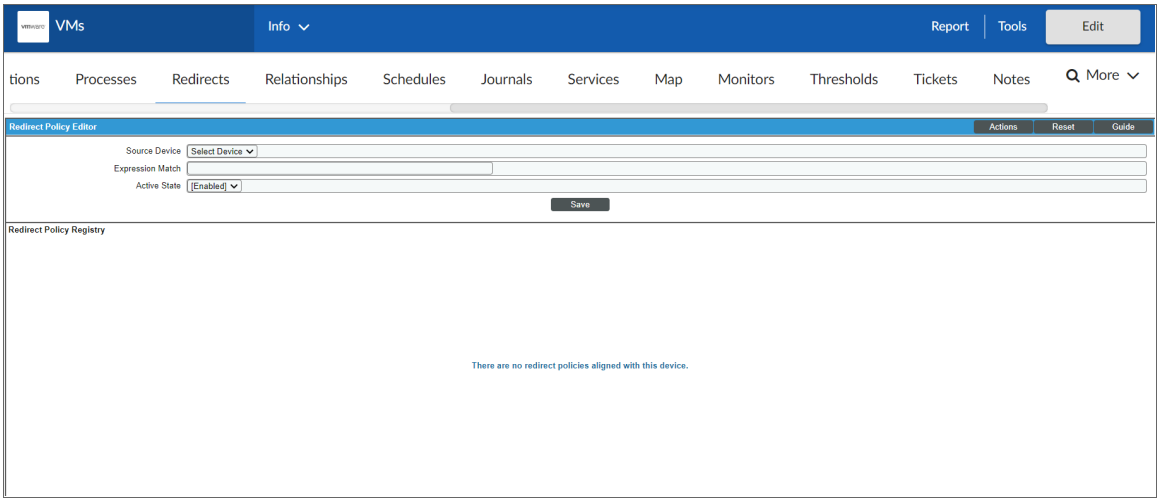
On the **[Processes]** tab of the **Device Investigator**, you can view information about the processes running on the device. The **[Processes]** tab displays a combined list of processes collected via SNMP and the agent, where applicable.



NOTE: For more information about this tab, see the chapter on "Monitoring Device Processes" in the ***Monitoring Device Infrastructure Health*** manual.

The Redirects Tab

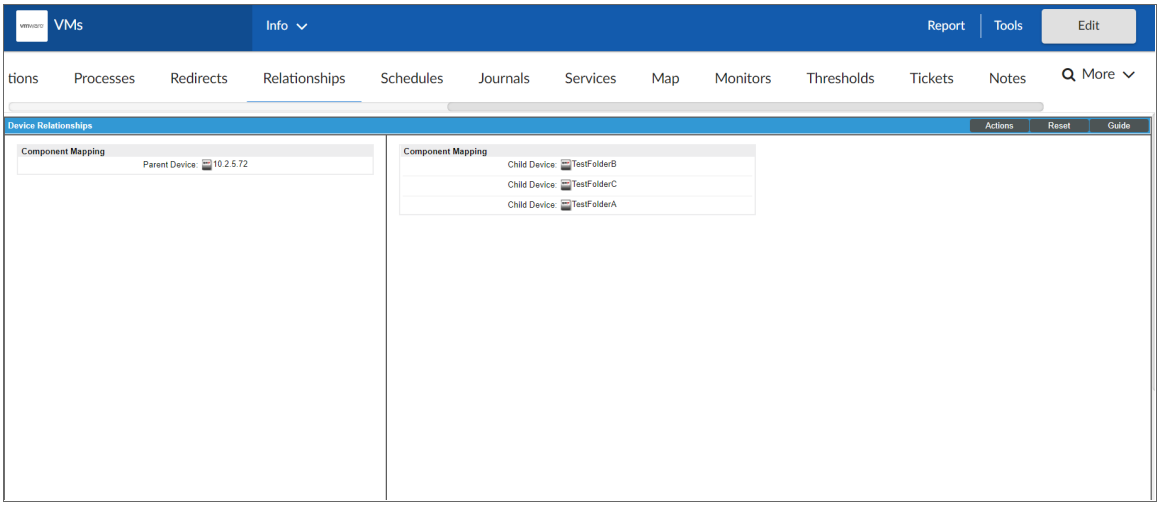
On the **[Redirects]** tab of the **Device Investigator**, you can redirect log entries from one IP-based device to another IP-based device, or from an IP-based device to a virtual device.



NOTE: For more information about this tab, see the chapter on "Viewing Device Logs" in the ***Monitoring Device Infrastructure Health*** manual.

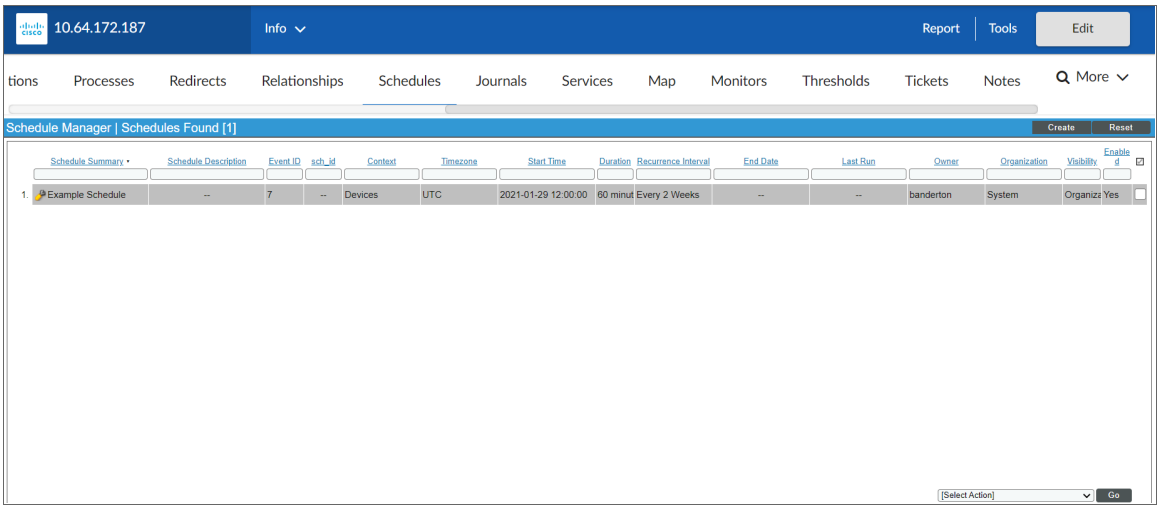
The Relationships Tab

On the **[Relationships]** tab of the **Device Investigator**, you can view information about parent-child relationships between the selected device and other devices.



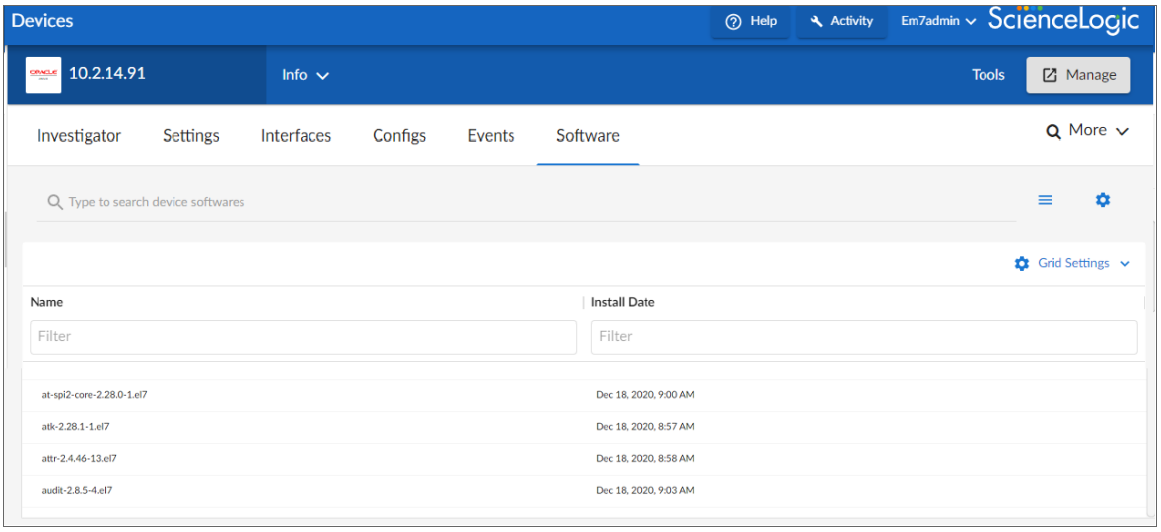
The Schedules Tab

On the **[Schedules]** tab of the **Device Investigator**, you can manage all the scheduled process you have defined in your system. You can define scheduled tasks for a number of things, such as backup management, dashboards, devices, and Run Book Automation policies.



The Software Tab

On the **[Software]** tab of the **Device Investigator**, you can view a list of all the software installed on the device.



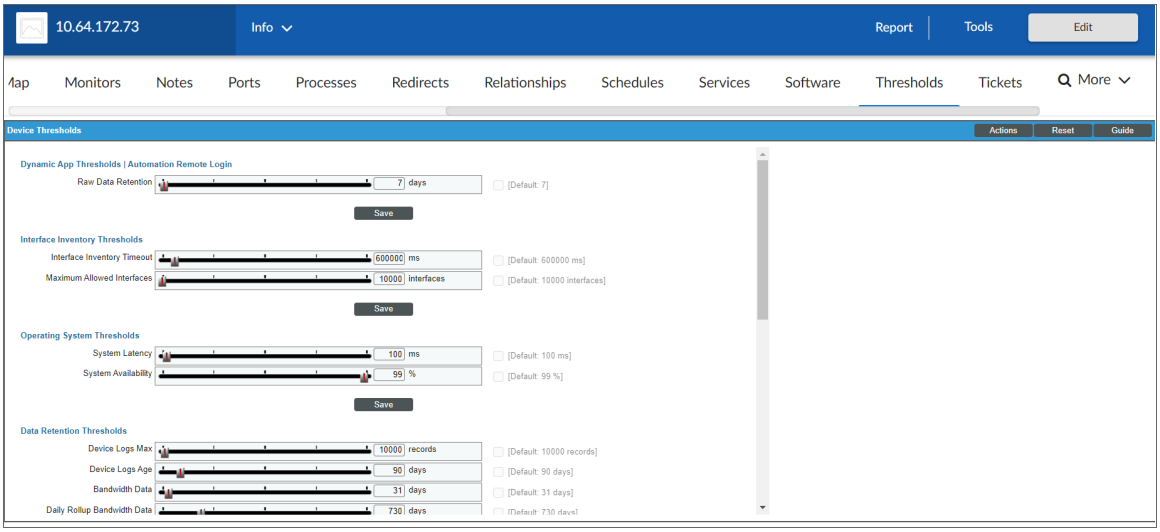
For each installed software title, the **[Software]** tab displays the following information:

- ***Name***. Name of the software.
- ***Install Date***. Date and time the software was installed on the device.

NOTE: For more information about this tab, see the chapter on "Monitoring Hardware and Software" in the ***Monitoring Device Infrastructure Health*** manual.

The Thresholds Tab

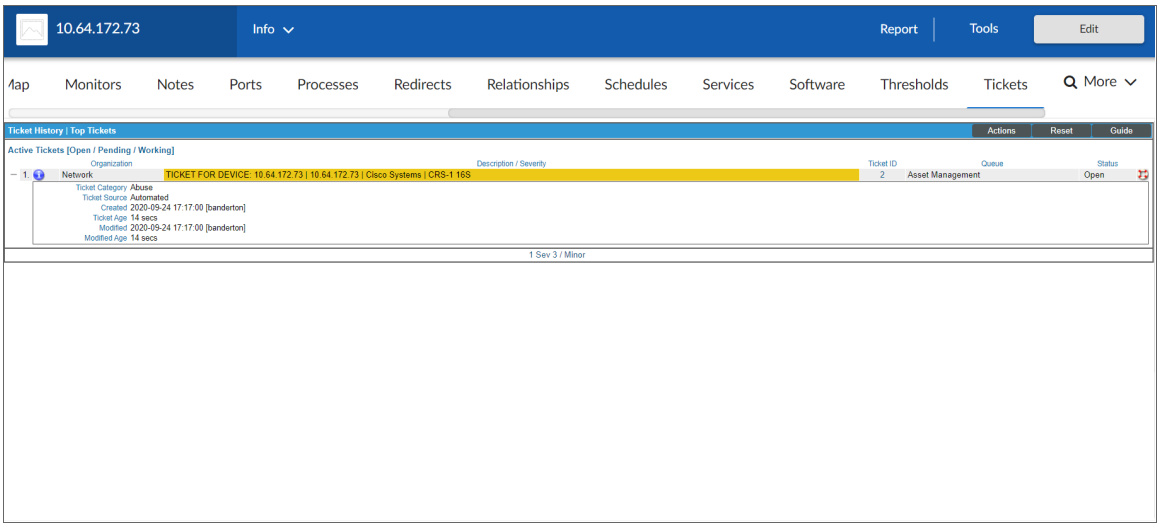
On the **[Thresholds]** tab of the **Device Investigator**, you can define usage and performance thresholds and data retention thresholds for a device:



When performance thresholds are exceeded, SL1 will generate an event for the device. When space thresholds are exceeded, SL1 will remove the oldest data from the database. For each of these thresholds, SL1 defines a default value. You can edit the thresholds to meet your needs.

The Tickets Tab

On the **[Tickets]** tab of the **Device Investigator**, you can view all tickets associated with the device and create new tickets to associate with the device:



The **[Tickets]** tab displays critical information about each ticket. If you require more detail, you can access the **Ticket Editor** from this page by clicking on the ticketing icon ( ) for that ticket.

You can also create a new ticket from this page.

To create a new ticket for a device:

1. Go to the **[Tickets]** tab of the **Device Investigator**.
2. Click the **[Actions]** button and then select *Create a Ticket*. The **Ticket Editor** page appears.
3. On the **Ticket Editor** page that appears, define the basic parameters for the ticket. For information about the fields on this page, see the chapter on "Creating and Editing Tickets" in the ***Ticketing*** manual.

   > **NOTE:** The ***Description*** and ***Element*** fields are automatically populated with information about the device.

4. When you are finished, click **[Save]**.

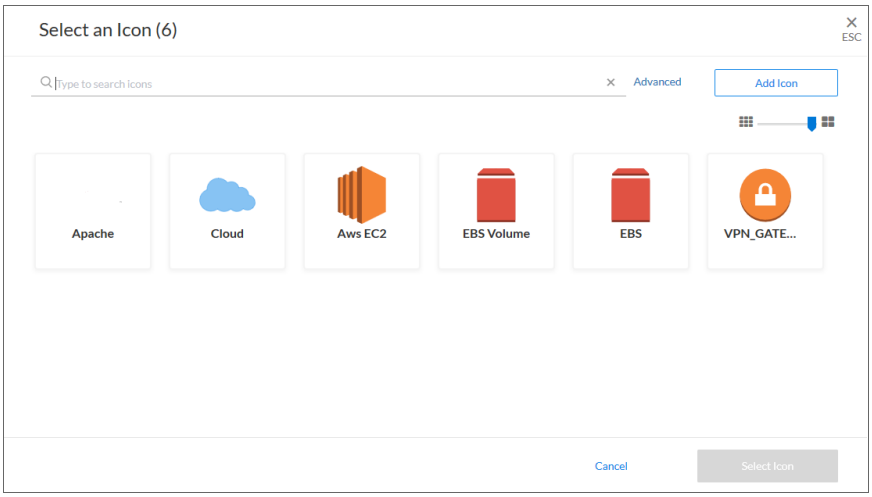
Assigning Icons to Devices

You can customize the look and feel of the devices that appear on the **Devices** page by assigning an icon a device, device class, or device category.

To assign an icon to a device, device class, or device category:

1. On the **Devices** page, **Device Classes** page (Devices > Device Classes), or **Device Categories** page (Devices > Device Categories), locate the device, class, or category for which you want to add an icon.

2. Click the ***Actions*** button (⋮) for that item and select *Assign Icon*. The **Select an Icon** window appears:



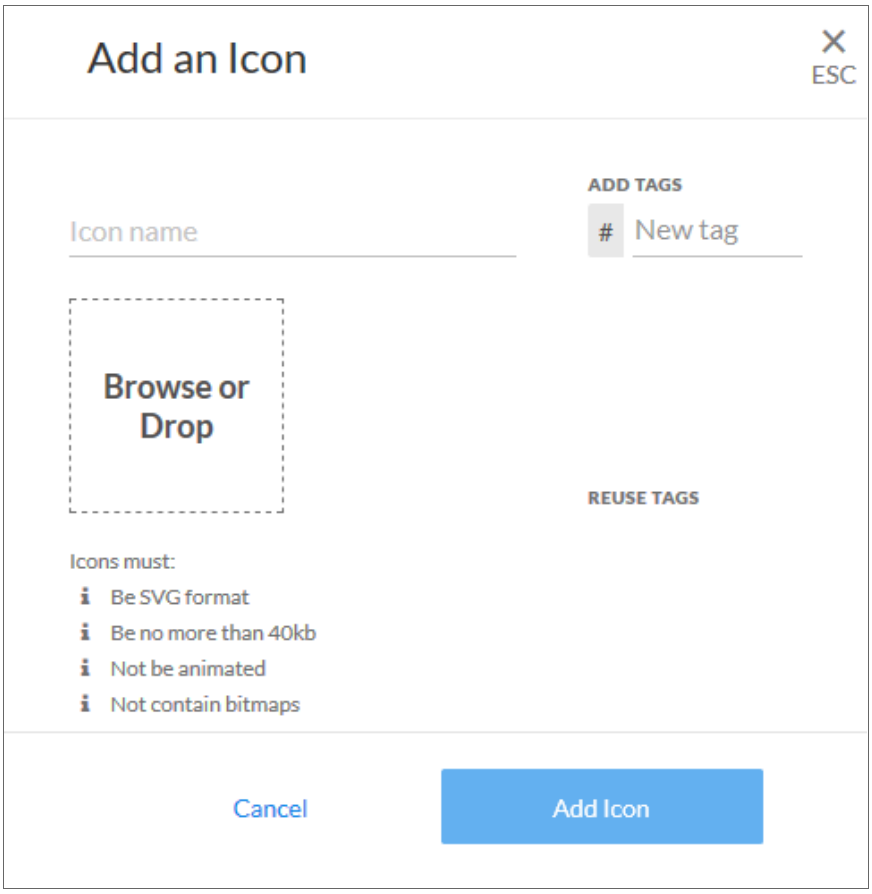
> **TIP:** To assign an icon to more than one device, device class, or device category, select the checkboxes to the left of those items and click the **[Assign Icon]** button.

3. To use an existing icon, select that icon from the list of icons and click the **[Select Icon]** button.

> **TIP:** If an icon includes a tag, you can search for that icon by typing some or all of the tag text in the ***Search*** field.

4. To upload an icon from your local drive, make sure that the image file meets the following criteria:
    - The image file should be in .SVG format.
    - The file should not be larger than 40 KB.
    - The file should not be animated.
    - The file should not contain bitmaps.

5. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears:



6. In the ***Icon name*** field, type a name for the icon you want to upload.
7. In the ***Add Tags*** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
8. You can click the ***Browse or Drop*** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
9. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
10. Click the **[Select Icon]** button to add the icon to the selected item.

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010