



Introduction to the New User Interface

SL1 version 8.10.1

Table of Contents

Introduction to the New User Interface	5
Configuring Communication with the ScienceLogic API	6
Logging In and Out of the New User Interface	6
Using Basic Search	7
Filtering Data with SmartViews	9
Using a SmartView	10
Creating a SmartView	11
Editing a SmartView	13
Managing New Features on the Content Management Tab	14
Getting Help and More Information	16
Using Advanced Search	18
Performing an Advanced Search	19
Components of an Advanced Search	20
Fields	21
Operators	23
Values	25
Additional Components of an Advanced Search	25
Strings	25
Escape characters	26
Examples of Advanced Searches	27
Advanced Search Examples on the Devices Tab	27
Advanced Search Examples on the Events Tab	28
Advanced Search Examples on the Services Tab	28
Viewing Dashboards	29
What is a Dashboard?	30
The Leaderboard Widget and Driving Context	30
Widget Legends	32
The Helper Icon	33
Filtering Dashboard Data	33
Using the Time Span Filter	34
Zooming in on a Time Span	34
Using the All Filters Button	35
Focusing on One Device in a Dashboard	37
Creating Dashboards	39
Creating a Dashboard	40
Creating a Widget	41
Editing a Dashboard	56
Resizing and Moving Widgets on a Dashboard	56
Printing a Dashboard	57
Sharing a Dashboard	58
Deleting a Dashboard	59
Managing Events	60
What is an Event?	61
Searching for Events	61
Viewing Events	62
Using the List View	63
Using the Card View	64
Filtering the List of Events	64
Viewing Events by Organization	64
Filtering Events by Severity	66

Filtering for Masked Events	67
Working with Events	68
Acknowledging and Clearing Events	68
Selecting Multiple Events	68
Viewing and Editing Event Notes	69
Using the Event Drawer	70
Working with the Tools Pane	70
Using the Event Investigator	72
Managing Devices	74
What is a Device?	75
What is a Device Record?	75
Searching for Devices	76
Working with Devices	76
Adding Devices	76
Learning More about Devices	77
Using the Device Investigator	77
Adding Metrics to the Overview Tab	78
Comparing Devices	81
Using Device Tools	82
Viewing the Device Information Tab	83
Viewing the Device Interfaces Tab	84
Viewing the Configs Tab	86
Viewing the Events Tab	87
Viewing the Collections Tab	88
Assigning Icons to Device Classes	88
Working with Device Categories	91
Discovery and Credentials	94
What is Discovery?	95
What are Credentials?	95
Prerequisites for Discovering Devices in the New User Interface	96
Discovering Devices	96
Working with Discovery Sessions	104
Monitoring Business Services	105
What is a Business Service?	106
Example: Retail Banking	108
Using the Service Investigator	109
Creating a Business Service	110
Assigning Icons to a Business Service	113
Selecting a Business Service Policy	114
Creating a Business Service Policy	116
Creating a Business Service Template	121
Creating a Business Service From a Template	124
Exporting a Service Template	128
Installing a Template from a PowerPack	131
Default Service Policy Settings	131
Device Service Default Policy	131
IT Service Default Policy	131
Business Service Default Policy	132
Managing Events for Business Services	132
Exporting Service Data with the ScienceLogic API	133
Troubleshooting Services	135
Some services do not generate Health, Availability, or Risk values	135

All services do not generate Health, Availability, and Risk values 140

Error message: "Business service thresholds are missing." 141

503 errors, or Health, Availability, and Risk values that are all the same or inaccurate 141

Introduction to the New User Interface

Overview

This chapter provides an overview of the new user interface for SL1, including how to log in, how to filter data, and how to manage new features.

The following sections describe the various elements of the new user interface:

<i>Configuring Communication with the ScienceLogic API</i>	<i>6</i>
<i>Logging In and Out of the New User Interface</i>	<i>6</i>
<i>Using Basic Search</i>	<i>7</i>
<i>Filtering Data with SmartViews</i>	<i>9</i>
<i>Managing New Features on the Content Management Tab</i>	<i>14</i>
<i>Getting Help and More Information</i>	<i>16</i>

Configuring Communication with the ScienceLogic API

To avoid communication errors between the new user interface and the ScienceLogic API, configure the `em7_limits.conf` file to limit the number of connections per IP on all SL1 appliances that communicate with the ScienceLogic API.

NOTE: Use this configuration if you are using a version of SL1 that is lower than 8.9.0, or if you used the patch to upgrade to 8.9.0 instead of using the ISO version of 8.9.0.

To configure communication on a SL1 appliance:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Open the file `/etc/nginx/conf.d/em7_limits.conf` with vi or another text editor:

```
sudo vi /etc/nginx/conf.d/em7_limits.conf
```
4. To limit the number of connections per IP, add the following line to the file:

```
limit_conn perip 200
```
5. Save your changes and exit the file (`:wq`).
6. Restart the SL1 appliance by executing the following command:

```
sudo systemctl restart nginx
```
7. Run steps 1-6 on all SL1 appliances that communicate with the ScienceLogic API.

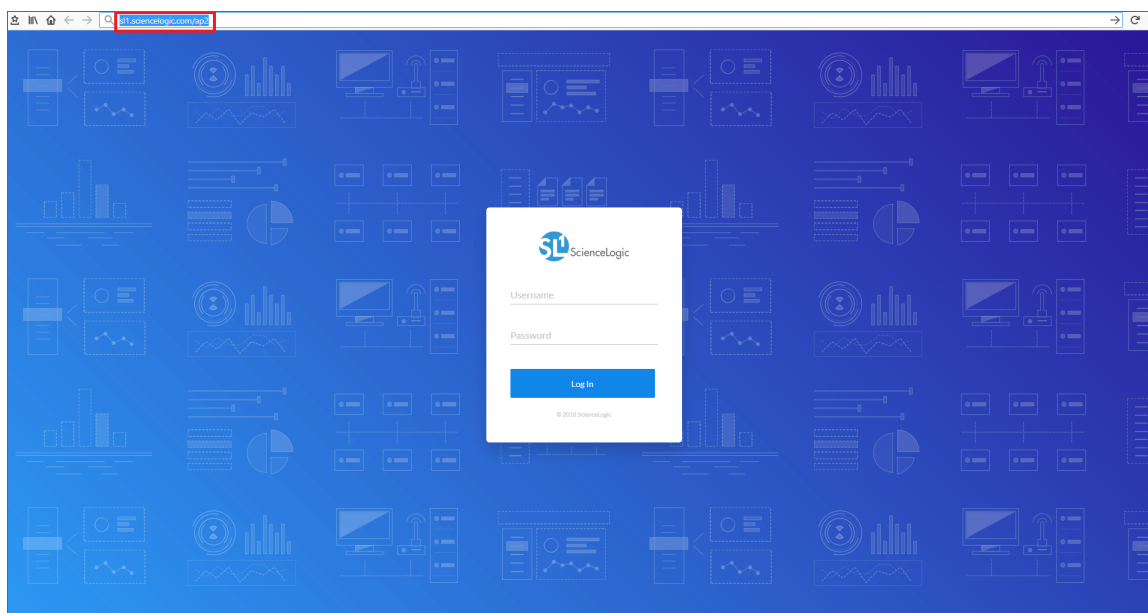
Logging In and Out of the New User Interface

The new user interface for SL1 provides a more intuitive and more efficient way to view and use the data in SL1. The current or "classic" user interface for SL1 still exists. You can toggle between the two user interfaces by adding and removing `/ap2` to the end of the URL for SL1.

NOTE: You can control access to the new user interface by aligning the Admin Portal Access (AP_Access) access hook with an existing Access Key on the **Access Keys** page (System > Manage > Access Keys) in the classic user interface.

To log in to the new user interface:

1. In a browser, type the URL or IP address for SL1.
2. Type **/ap2** at the end of the URL or IP address. For example, you could type **https://sl1.sciencelogic.com/ap2**. The login page for the new user interface appears:



3. Type the current user name and password you use with SL1 and click **Log In**.

NOTE: 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 the new user interface with your SSO credentials. When you log out, the logout screen redirects you to an SSO page instead of the typical login screen.

To log out of the new user interface:

1. Click your user name near the top-right corner of any of the tabs:
2. Click **Log off**. The login page appears.

Using Basic Search

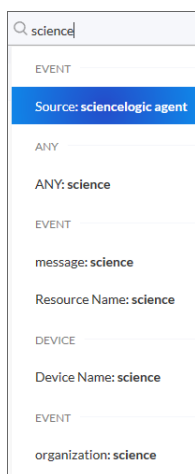
On most tabs and pages in the new user interface, you can use the **Search** field to search for specific elements on that tab or page. The **Search** field contains a magnifying glass icon (🔍) next to the words "Type to search" or "Search". You can access the field above the list of elements on a tab or list.

TIP: To use the Advanced Search, click the **Advanced** link to the right of the **Search** field and use custom search commands to locate elements on a tab or a page. For more information, see [Using Advanced Search](#).

The **Search** field is similar to the Filter-While-You-Type field found in the classic user interface. As you type text in the **Search** field, the new user interface filters the list of elements. However, searches in the new user interface use *all* relevant columns for the search, unlike the Filter-While-You-Type field, which only used the columns that were visible on that tab or page.

To use the **Search** field:

1. Click the **Search** field and start typing search text. As you type, the new user interface provides potential matching values in a drop-down menu and starts filtering the list with your search text. For example, if you start searching for ScienceLogic by typing *science*, a drop-down list appears with a list of columns that might contain that word:



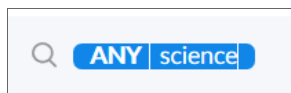
The screenshot shows a search input field with the text "science". Below the input field is a dropdown menu with the following suggestions:

- EVENT
- Source: sciencelogic agent
- ANY
- ANY: science
- EVENT
- message: science
- Resource Name: science
- DEVICE
- Device Name: science
- EVENT
- organization: science

2. You can select a column from the suggestions in the list, or you can type more text. For example, if you are on the **[Devices]** tab and you select *organization: science*, the list displays all devices that belong to organizations that start with "science".

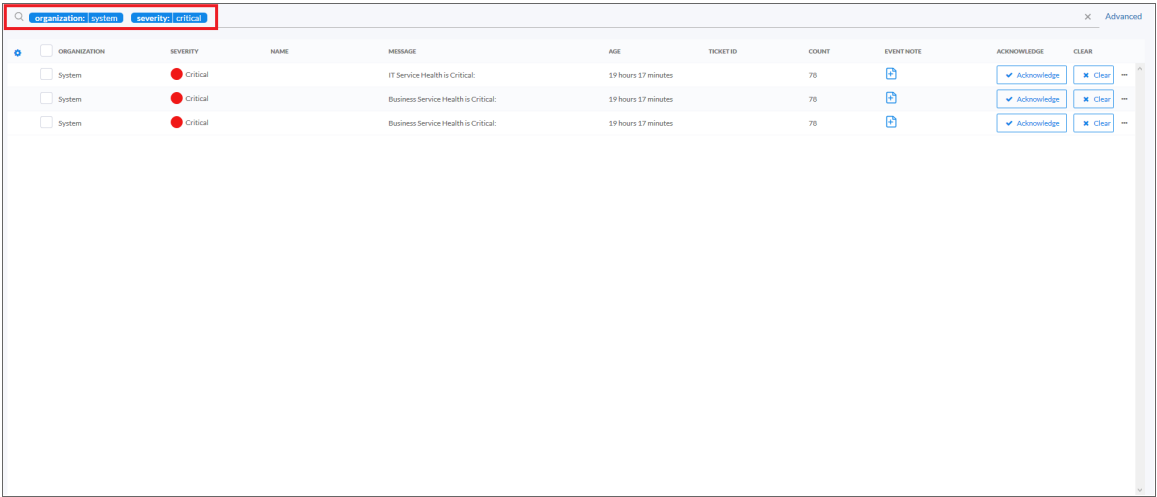
TIP: You could also finish typing "ScienceLogic" to search *only* for devices that are part of the ScienceLogic organization.

3. If you select ANY from the drop-down menu, the search looks through all relevant columns for matches to your search text.



The screenshot shows the search input field with a dropdown menu open. The dropdown menu has a blue bar with the text "ANY" and the search term "science" next to it. The input field contains the text "science".

- You can add more search criteria to an existing search by typing additional text in the **Search** field, and then selecting additional columns from the drop-down list:



- To clear a search, click the **Clear** button () at the end of the **Search** field.

Filtering Data with SmartViews

A **SmartView** defines a global filter based on device category. A **device category** is a label that groups devices by primary function, such as "server" or "storage". The SmartView displays a list of all device categories currently in SL1.

When you select a SmartView, all of the tabs are filtered to display only entries that match the selected device category. For example, if you select *Network* as the SmartView, the **[Events]** tab displays events only for network devices, like routers and switches, and the **[Devices]** tab displays entries only for network devices.

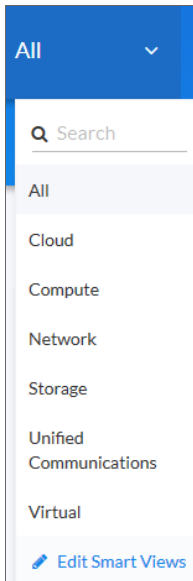
The **All** SmartView displays all of the data currently available in SL1.

NOTE: For additional SmartViews, go to the **[Content Management]** tab (Settings > Content Management) and install the **@sciencelogic/default-smart-views** content package. For more information about content packages, see [Managing New Features on the Content Management Tab](#).

Using a SmartView

To filter all data using a SmartView:

1. On any tab, click the **[SmartView]** button in the top left-hand corner of the tab. A drop-down list appears:



2. Click a filter from the drop-down list. The current tab refreshes and displays only the data that matches that filter. The **[SmartView]** button in the top left-hand corner now displays the name of the filter you clicked.

TIP: To search SmartViews, type search text into the **Search** field at the top of the SmartView drop-down list.

3. To change the filter, click the **[SmartView]** button and select a different filter from the pop-out menu.

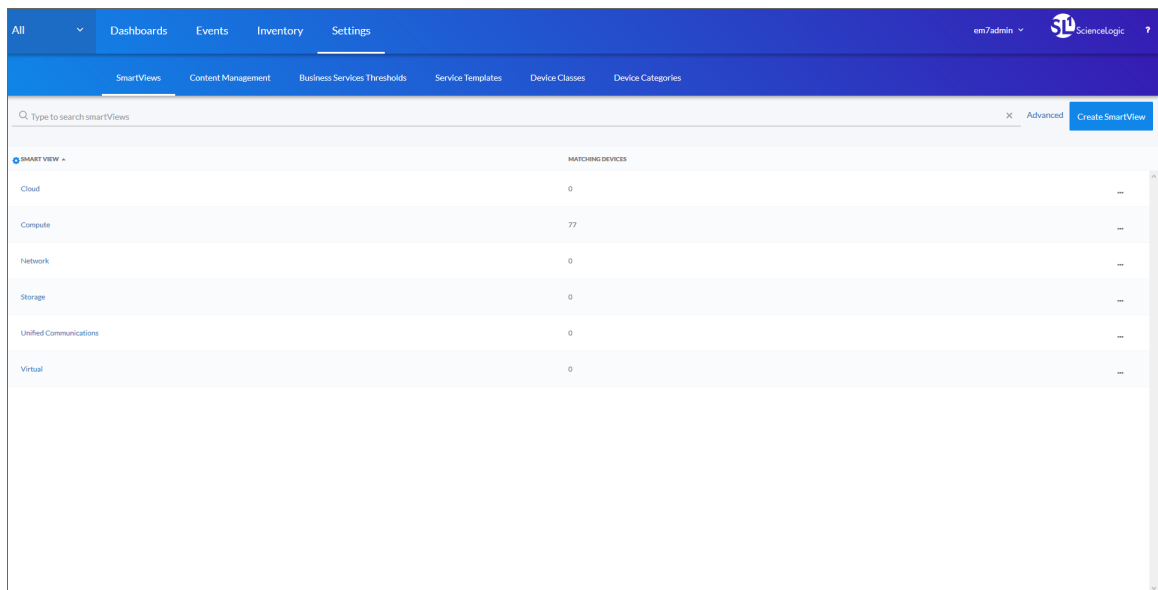
TIP: The SmartView filter is persistent, so the filter that was in use when you logged out of SL1 remains in use when you log in again.

Creating a SmartView

You can create a new SmartView to ensure that SL1 displays data from only the devices you want to monitor.

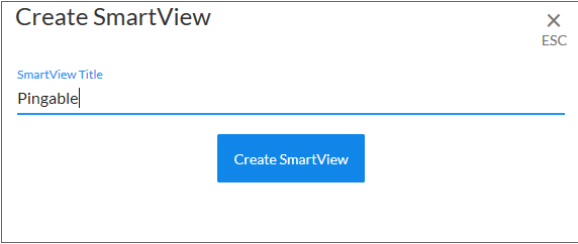
To create a SmartView:

1. Go to the **[SmartViews]** tab (Settings > SmartViews).



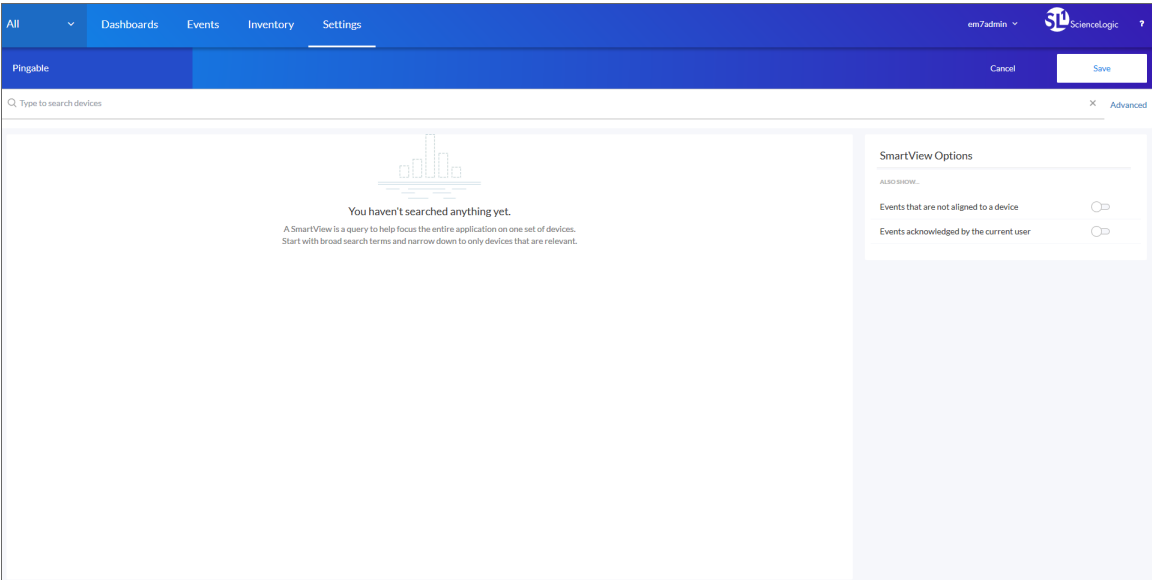
TIP: You can also click the **[Edit SmartViews]** button from the SmartView drop-down list to get to the **[SmartViews]** tab.

2. Click the **[Create SmartView]** button. The Create SmartView modal page appears.



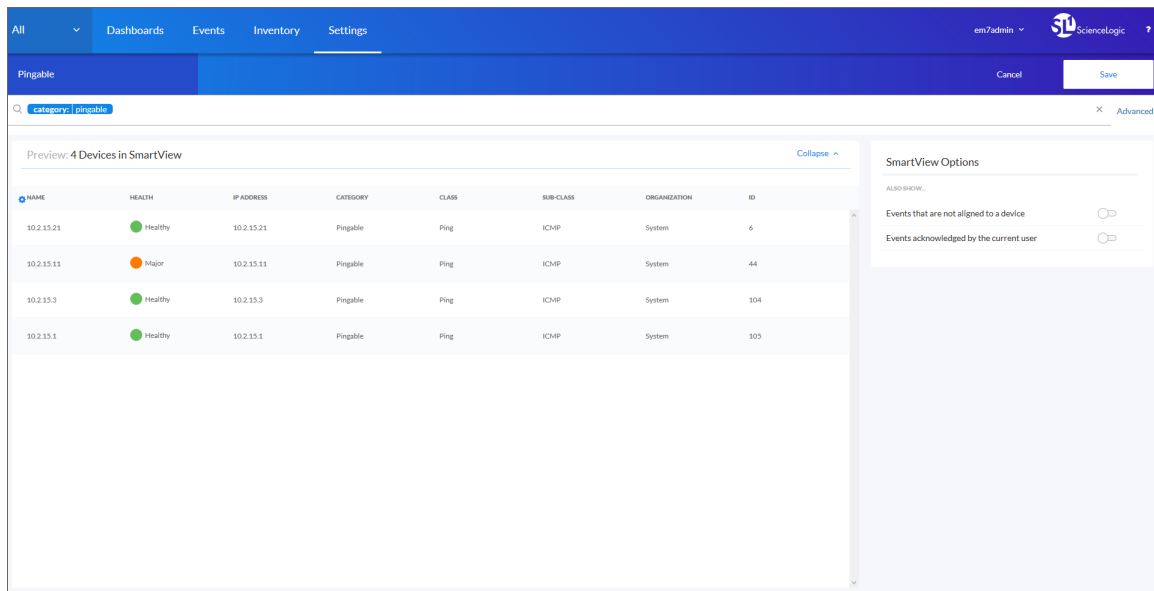
The image shows a modal dialog titled "Create SmartView". It has a close button (X) and "ESC" key indicator in the top right corner. Below the title, there is a label "SmartView Title" and a text input field containing the word "Pingable". At the bottom center of the modal is a blue button labeled "Create SmartView".

3. In the **SmartView Title** field, type a name for the new SmartView and click the **[Create SmartView]** button. A new SmartView page appears:



The image shows the main application interface after creating a SmartView. The top navigation bar is dark blue with tabs for "All", "Dashboards", "Events", "Inventory", and "Settings". The "Pingable" tab is selected. The top right shows the user "em7admin" and the "scienceLogic" logo. Below the navigation bar, there is a search bar with the placeholder "Type to search devices" and a search icon. The main content area is divided into two sections. The left section contains a bar chart icon and the text "You haven't searched anything yet." followed by a brief explanation of SmartView. The right section is titled "SmartView Options" and contains two toggle switches: "Events that are not aligned to a device" and "Events acknowledged by the current user".

- Type search text in the **Search** field for the type of devices you want to include in your SmartView filter. SL1 starts searching while you type:



TIP: Start with broad search terms and narrow down your search to only devices that are relevant. You can use more than one search term. For more information about using the **Search** field, see [Using Basic Search](#).

- To include events that are not associated with devices, click the **Events that are not aligned to a device** toggle.
- To include events that you already acknowledged, click the **Events acknowledged by the current user** toggle.
- Click the **[Save]** button to save your SmartView. The SmartView appears on the SmartViews tab and the SmartView drop-down list.

Editing a SmartView

To edit an existing SmartView:

- Go to the **[SmartViews]** tab (Settings > SmartViews). You can also click the **Edit SmartViews** button from the SmartView drop-down list.
- To search the list of SmartViews, type search text into the **Search** field at the top of the SmartView drop-down list.
- Click the name of the SmartView you want to edit from the list. You can also click the **[Options]** button (⚙️) for that SmartView and select *Edit*.
- Update the search terms for the SmartView and click the **[Save]** button when you are finished.

Managing New Features on the Content Management Tab

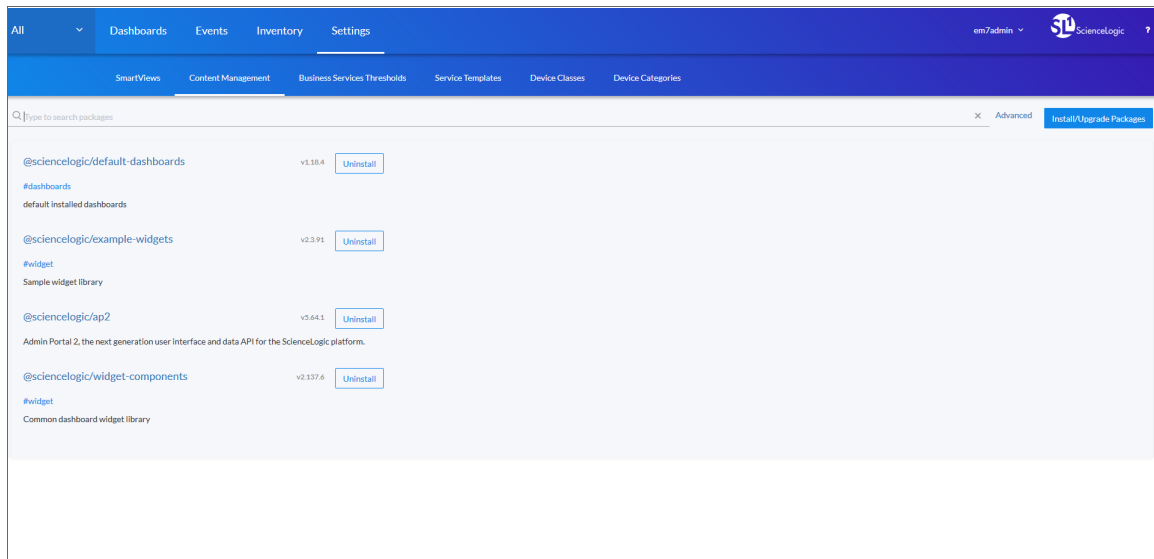
You can use the **[Content Management]** tab to install and upgrade various features of SL1, such as new versions of the user interface (ap2) and new widget components for dashboards. These features are delivered in **content packages**, which you can find on the **[Content Management]** tab under the **[Settings]** tab.

Content package names follow packaging rules for NPM, the package manager for JavaScript. Content packages created by ScienceLogic include **@sciencelogic** in the package name.

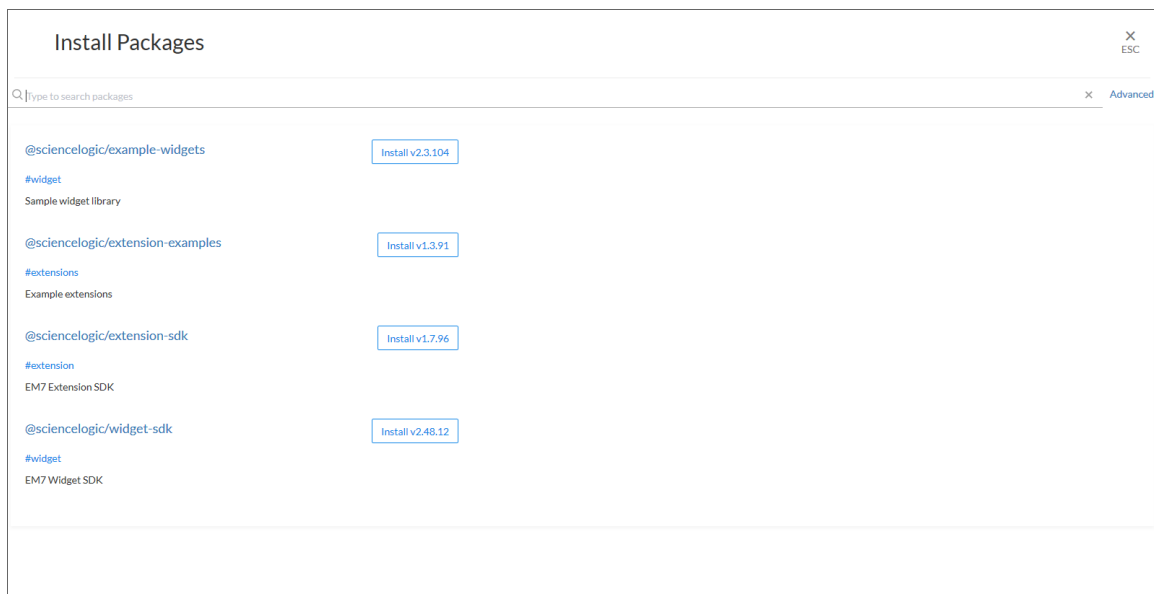
TIP: You can update more than one content package at a time, and you do not need to wait for one package to install before installing another package. Also, you can navigate away from this page and the package or packages will continue to install.

To install or upgrade a content package:

1. Go to the **[Content Management]** tab (Settings > Content Management).



- Click the **[Install/Upgrade Packages]** button. The **Install Packages** page appears.



- Click the **[Install]** button for the content package you want to install. The button changes to **[Installed]** when the package finishes installing. Larger content packages might take longer than usual to install.

NOTE: If you are updating the **@sciencelogic/ap2** content package, allow the package to run for a few minutes, and ignore any "Install Failed" messages.

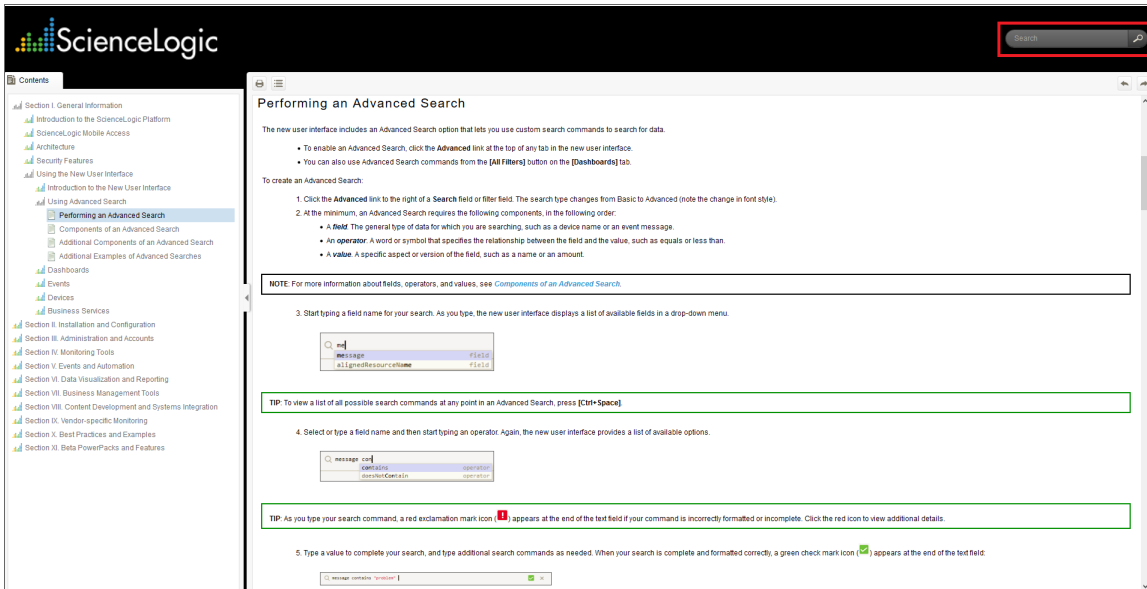
- As a best practice, clear the cache for your browser after the installation, and also clear the cache in the current or "classic" interface by clicking the **[Toolbox]** or "hamburger" button (≡) and selecting *Clear SL1 System Cache*.

TIP: To access the classic SL1 interface, type **/em7** at the end of the URL or IP address, such as **http://sl1.sciencelogic.com/em7**.

- To view more information about a content package, including a short description and a Readme file, where relevant, click the name of the package.
- Click the **[ESC]** button to return to the **[Content Management]** tab. You can leave the **Install Packages** page before a content packages finishes installing.
- To uninstall a content package, click the **[Uninstall]** button for that package.

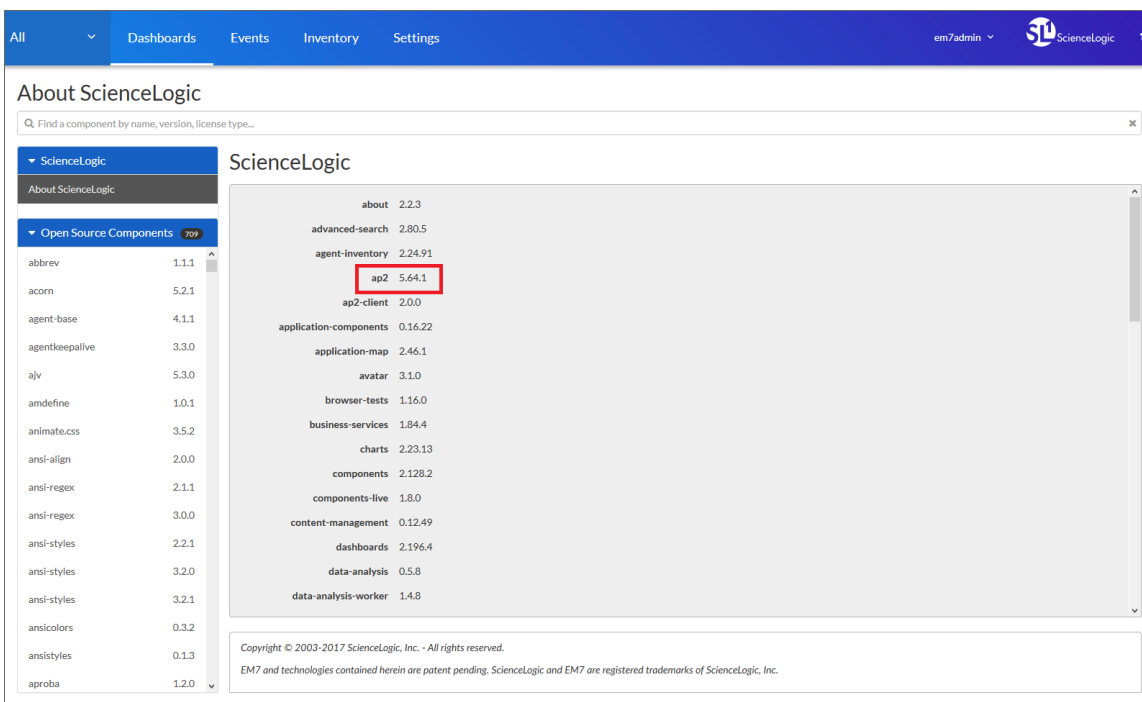
Getting Help and More Information

For documentation about any tab in the new user interface, click the question-mark icon (?) in the top right-hand corner of the tab and select *Help*. A Help topic specific to the current tab appears in a new browser window:



The online Help includes a **Search** field at the top right-hand corner of the window that you can use to find additional topics related to the new user interface and the "classic" user interface.

For more information about the components used by the new user interface, click the question-mark icon (?) in the top right-hand corner of the tab and select *About*. The **About ScienceLogic** page appears:



TIP: To identify the version of the new user interface for SL 1 you have installed, click *About ScienceLogic* in the left-hand pane and locate the **ap2** value in the list of ScienceLogic components in the right-hand pane.

In the left-hand navigation 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.

Chapter

2

2

Using Advanced Search

Overview

This chapter describes how to create advanced searches on the various tabs of the new user interface for SL1.

The following sections cover the details of Advanced Search:

<i>Performing an Advanced Search</i>	19
<i>Components of an Advanced Search</i>	20
<i>Fields</i>	21
<i>Operators</i>	23
<i>Values</i>	25
<i>Additional Components of an Advanced Search</i>	25
<i>Strings</i>	25
<i>Escape characters</i>	26
<i>Examples of Advanced Searches</i>	27
<i>Advanced Search Examples on the Devices Tab</i>	27
<i>Advanced Search Examples on the Events Tab</i>	28
<i>Advanced Search Examples on the Services Tab</i>	28

Performing an Advanced Search

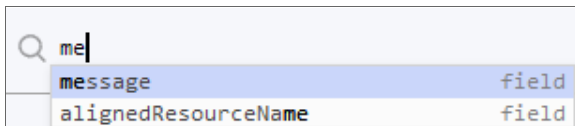
SL1 includes an Advanced Search option that lets you use custom search commands to search for data. To enable an Advanced Search, click the **Advanced** link at the top of any tab or list in the new user interface.

To create an Advanced Search:

1. Click the **Advanced** link to the right of a **Search** field. The search type changes from Basic to Advanced (note the change in font style).
2. 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 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.

NOTE: For more information about fields, operators, and values, see [Components of an Advanced Search](#).


3. Start typing a field name for your search. As you type, the new user interface displays a list of available fields in a drop-down menu.




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

4. Select or type a field name and then start typing an operator. Again, the new user interface provides a list of available options.

A search input field with the text "message con" entered. A dropdown menu is open, showing two options: "contains" and "doesNotContain". Both options are labeled as "operator" on the right side of the dropdown.

TIP: As you type your search command, a red exclamation mark 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.

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

A search input field showing the completed search command "message contains \"problem\"". A green check mark icon is visible at the end of the text field, indicating the command is correctly formatted.

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

TIP: You can type search commands in the Basic Search field, and then click the **Advanced** link to "translate" your basic search into an Advanced 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.

The following table contains examples of Advanced Search commands (the quotation marks signify a string of text):

<i>field</i>	<i>operator</i>	<i>value</i>
name	=	"device-name"
counter	>	10
message	contains	'Error'

In the Advanced Search field, you would type these three searches in the following way:

```
name = "device-name"  
counter > 10  
message contains 'Error'
```

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

NOTE: When the new user interface 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 occurred more than ten times and contain a message with the word "Error" (or "error") :

```
counter > 10 and message contains 'Error'
```

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

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

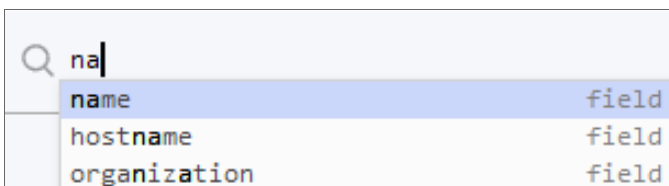
You can use parentheses () to group expressions and to ensure that the expressions are evaluated in the correct order. The following search command looks for either critical events that have only occurred ten times or major events that have occurred more than 50 times:

```
(counter > 10 and status = Critical) or (counter > 50 and status = Major)
```

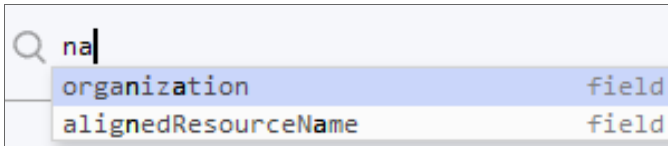
TIP: Searches in the new user interface are *not* case-sensitive, so you can use any combination of upper-case and lower-case letters.

Fields

For most searches, you start your search command with a field name. When you start typing in an Advanced Search field, the new user interface 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 tab you are currently on in the new user interface. The example above is from the Advanced Search field on the **[Devices]** tab. If you typed the same letters in the Advanced Search field on the **[Events]** tab, 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 a device.	<code>alignedResourceName contains "lab"</code>
asset	Search for an asset aligned with a device.	<code>asset has (assetTag contains 1)</code>
dateCreated	Search for the date and time a device was created.	<code>dateCreated isNotNull</code>
deviceClass	Search for devices belonging to a device class.	<code>deviceClass has (class contains 'Cisco')</code>
deviceGroup	Search for devices belonging to a device group.	<code>deviceGroup has (name contains "Network")</code>
hostname	Search for a device hostname	<code>device has (hostname = "srv")</code>
id	Search for the unique numeric ID assigned by SL1.	<code>id contains "10"</code>
isAcknowledged	Search for events that have or have not been acknowledged.	<code>isAcknowledged = true</code>

Field name	Purpose	Example
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")
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.

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	counter > 10 and message contains "error"


Operator name	Purpose	Example
or	Include at least one of multiple search criteria.	name = "server" or message contains "error"
=, ==, eq, EQ, Eq	The field and the value are equal.	name = "server"
contains	The field includes a specific string.	message contains "primary"
has	The field contains a specific value. The value following "has" must be enclosed in parentheses.	organization has (tollfree contains '800')
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
<>, !=, neq	The field and the search value are equal.	field != abc
>, gt	The field is greater than the search value.	severity > 3
<, lt	The field is less than the search value.	state < 2
>=, gte	The field is greater than or equal to the search value.	severity gte 3
<=, lte	The field is less than or equal to the search value.	state lte 2

Operator name	Purpose	Example
<code>isNull</code>	The field is empty.	<code>extTicketRef isNull</code>
<code>isNotNull</code>	The field is not empty.	<code>counter isNotNull</code>

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):

 name contains 'np' and ip beginsWith 192.168|

Additional Components of an Advanced Search

In the new user interface, you can also search for a specific set of words or characters in a string, or search for calculated sets of data.

Strings

You can create a search command that searches for a specific set of words in a string. You can use "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
<code>beginsWith</code>	Search for strings beginning with a specified value	<code>message beginsWith "Host Resource"</code>
<code>endsWith</code>	Search for strings ending with	<code>message endsWith 'shutdown'</code>

String operator name	Purpose	Example
	a specified value	
<code>contains</code>	Search for strings containing a specified value	<code>message contains "problem"</code>
<code>doesNotBeginWith</code>	Search for strings that do not begin with a specified value	<code>message doesNotBeginWith "front"</code>
<code>doesNotEndWith</code>	Search for strings that do not end with a specified value	<code>message doesNotEndWith 'warning'</code>
<code>doesNotContain</code>	Search for strings that do not contain a specified value	<code>message doesNotContain "codec"</code>

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 the new user interface 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 tab in the new user interface, this section contains a set of search examples based on context:

Advanced Search Examples on the Devices Tab

Search for all devices with a Device ID of 1, 2, or 3:

```
id in 1,2,3
```

Search for all devices with an IP Address that starts with 192.168:

```
ip beginsWith '192.168'
```

Search for all devices with "np" in the Device Name or an IP Address that starts with 192.168:

```
name contains 'np' or ip beginsWith 192.168
```

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 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 Tab

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 are errors that have occurred at least 100 times:

```
message beginsWith "Error" and counter >= 100
```

TIP: You can copy a working Advanced Search from one tab and include those search commands in an Advanced Search on another tab. Using this approach, you can now filter events based on any data about a device or any other event-related field.

For example, you created the following Advanced Search on the **[Devices]** tab to search for critical devices within a specific IP address:

```
name contains 'rtp' and ip beginsWith '192'
```

On the **[Events]** tab, you could use that search to find events related to that particular set of devices:

```
device has (name contains 'rtp') and device has (ip beginsWith '192')
```

For another example, you created the following Advanced Search on the **[Devices]** tab:

```
deviceClass has (deviceCategory has (name contains 'xtremio'))
```

The corresponding **[Events]** tab search enables you to see events related to that particular set of devices:

```
device has (deviceClass has (deviceCategory has (name contains 'xtremio')))
```

Advanced Search Examples on the Services Tab

Search for Services related to "Network":

```
( name contains 'network' or description contains 'network') or organization has  
(company contains 'network')
```

Search for devices with a Device Class of "network.router":

```
deviceClass has (deviceCategory has (name contains 'network.router'))
```

Search for devices with a Device Class or Sub-class of "media":

```
deviceClass has (deviceCategory has (name contains 'media')) and deviceClass has  
(description contains 'media')
```

Chapter

3

Viewing Dashboards



Overview

This chapter describes how to view graphs, charts, and tables that display the data collected by the new user interface for SL1.

The following sections explain how to view and manipulate the various elements of dashboards and widgets:

- What is a Dashboard? 30**
 - The Leaderboard Widget and Driving Context 30*
 - Widget Legends 32*
 - The Helper Icon 33*
- Filtering Dashboard Data 33**
 - Using the Time Span Filter 34*
 - Zooming in on a Time Span 34*
 - Using the All Filters Button 35*
 - Focusing on One Device in a Dashboard 37*

What is a Dashboard?

A **dashboard** is a page that displays one or more graphical reports, called **widgets**. In the new user interface, these widgets appear in their own pane, and display charts, tables, and text. 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.

NOTE: If a blue line appears under a widget name, the widget is in the process of updating its data. When the line disappears, the widget is done updating.

NOTE: 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.

The Leaderboard Widget and Driving Context

A **leaderboard widget** lets a dashboard user select specific items in a widget so that data about only those items displays in other widgets in the dashboard:

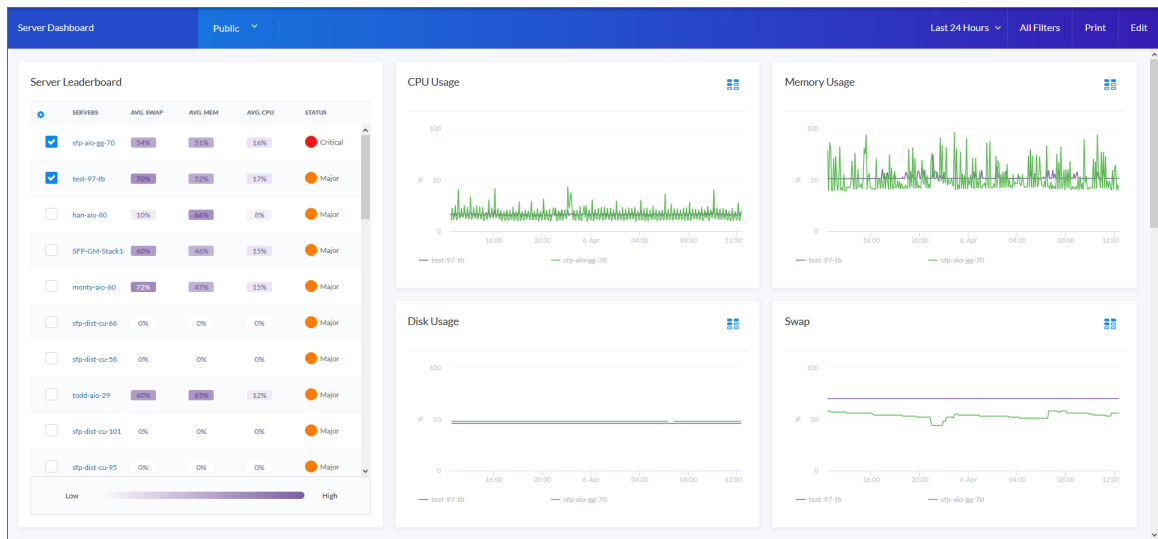
Servers	Avg. Swap	Avg. Mem	Avg. CPU	Status
<input checked="" type="checkbox"/> WIN-4CNHKE2M8J1	18	29	3	Critical
<input checked="" type="checkbox"/> em7ao	10	0	0	Major
<input type="checkbox"/> 192.168.33.147	0	0	0	Major
<input type="checkbox"/> 192.168.33.87	0	0	0	Major

In SL1, this feature is called **driving** data or driving the **context** of a dashboard widget. For example, in the Server leaderboard widget pictured above, if you select one or more servers on the leaderboard widget, the other widgets in the dashboard will display data about just the servers you selected. The other widgets **receive** the context from the "driving" widget, which in this example is the leaderboard widget.

To use a leaderboard widget:

1. On the **[Dashboards]** tab, select an existing dashboard or create a new dashboard with a leaderboard.

2. Select one or more items on the leaderboard widget. The widgets to the right of the leaderboard update with data only for the selected item or items.



3. To automatically select the first few items in the widget that drives "context" to other widgets, click the **[All Filters]** button. The **Default Data** window appears:

The 'Default Data' window is a configuration panel for selecting data sources. It contains four sections: 'By Organization', 'By Device', 'By Service', and 'Auto-Select'. Each section has a search input field and an 'Advanced' link. The 'Auto-Select' section is currently active, showing 'Number of Items' set to 1 and a dropdown menu labeled 'In Driving Widget'. An 'Apply' button is located at the bottom right of the window.

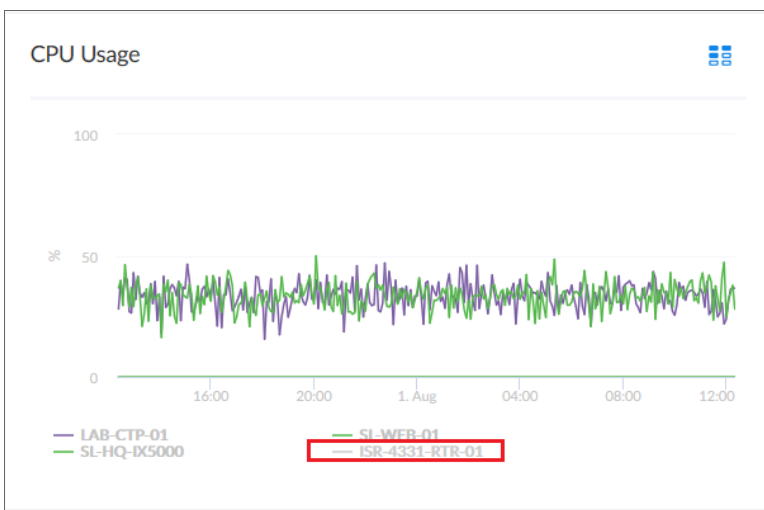
4. In the **Auto-Select** field, specify the number of items in your widget that you want to display as selected.
5. From the **In Driving Widget** drop-down list, select the widget that drives data (or "context") to other widgets in the dashboard.
6. Click the **[Apply]** button to apply your filters and settings.

Widget Legends

The items you selected in the leaderboard also appear at the bottom of each widget that contain line charts and bar charts, arranged by line color and name:



You can click an item name in the legend to toggle the display of data from that item in that widget. The line next to the item name turns gray, and the data remains hidden until you click the item name again.



You can also view more information about a specific point in time for an item by hovering over a line in a graph:



The Helper Icon

After you select one or more items in the Leaderboard widget, the widgets to the right of the Leaderboard display data relevant to your selections. The widgets also contain a small icon at the top right of each widget called a **Helper icon** (☰).

When you click the Helper icon, you can view a list of all of the widgets that drive data or provide **context** to that widget. In the example below, the Capacity Forecast (2 Weeks) widget receives data from both the Storage Leaderboard widget and the Capacity Forecast List widget:



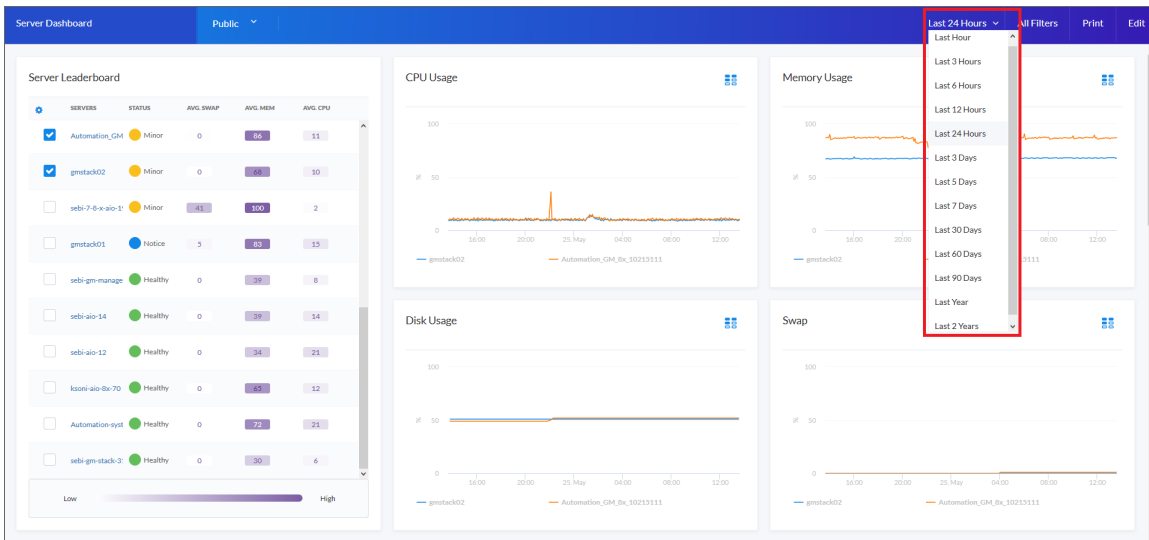
Filtering Dashboard Data

On the **[Dashboards]** tab, you can control the display of a widget, such as changing the time span in all the widgets from one hour to 24 hours, or zooming in or out on widget data.

You can also use the **[All Filters]** button to narrow down the data displayed in all widgets.

Using the Time Span Filter

You can use the **Time span filter** to adjust the time span that appears in all the widgets on a dashboard. The default filter is *Last 24 Hours*, but you can select a timespan of *Last Hour* ranging up to *Last 2 Years*.



TIP: If you see a gap in a line on a graph, that means that no data was collected during that time frame.

Zooming in on a Time Span

You can edit the time span of a line chart widget by clicking and dragging to "zoom in" on a specific time span.

To zoom in on the time span of a widget:

1. If needed, adjust the amount of time showing on *all* widgets by selecting a new value from the Time Span filter. The default time frame is the last 24 hours.

2. On the widget, click the start time you want to view, and then drag the cursor to the left or right to create a gray rectangle.



3. Drag the gray rectangle to the end time you want to view, and then release the mouse button. A more detailed time span displays in the widget.



4. To return to the original graph setting, click the **[Reset zoom]** button.

Using the All Filters Button

The **[All Filters]** button lets you filter the data in a dashboard by Organization, Device, and Service. The search process for the **[All Filters]** button works just like [Search](#) works on other tabs.

To filter dashboard data with the **[All Filters]** button:

1. On any of the dashboards, click the **[All Filters]** button in the top right-hand corner of the **[Dashboards]** tab. The **Default Data** window appears.

Default Data

By Organization

By Device

By Service

Auto-Select

Number of items: 1

In Driving Widget

Apply

2. Click in one of the fields and type your filter text. As you type, SL1 provides potential matching values in a drop-down menu. For example, if you type *switches* in the **By Device** filter field, a drop-down menu appears with a list of columns that might contain that word:

By Device

switches

ANY

DEVICE

name: switches

DEVICE CLASS

Device Class: switches

Device Sub-Class: switches

DEVICE CATEGORY


Device Category: switches

ORGANIZATION

organization: switches

3. You can select a column from the suggestions in the menu, or you can type more filter text.
4. If you do not select a column from the drop-down menu, your search is labeled "ANY". Search looks through all available columns for matches to your search text.

TIP: To use an advanced filter, click the **Advanced** link to the right of the filter field and use custom search commands to filter the data. For more information, see [Using Advanced Search](#).

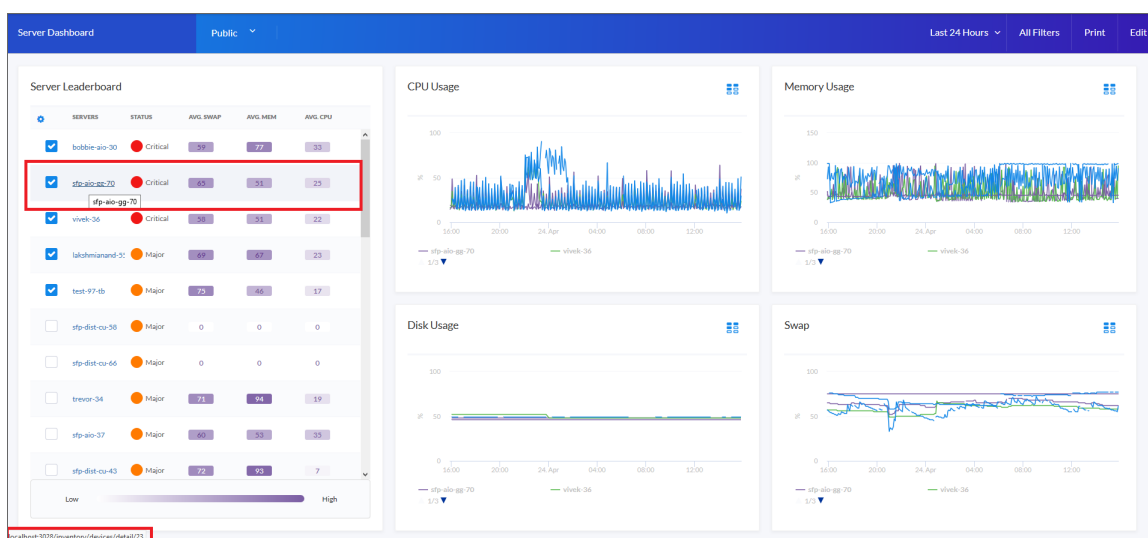
5. To clear a filter, click the **[Clear]** button () at the end of that filter field.
6. To automatically select the first few items in the widget that drives data (also called "context") to other widgets, specify a number in the **Auto-Select** field.
7. To specify the widget that drives data (or "context") to other widgets in the dashboard, select that widget from the **In Driving Widget** drop-down list.
8. Click the **[Apply]** button to apply your filters and settings.

Focusing on One Device in a Dashboard

You can use a leaderboard or table widget to focus on just one device in a dashboard. This feature is useful if you want to view charts and other widgets only for a specific device, or if you want to use the [Print](#) feature to generate a PDF of this dashboard for this device.

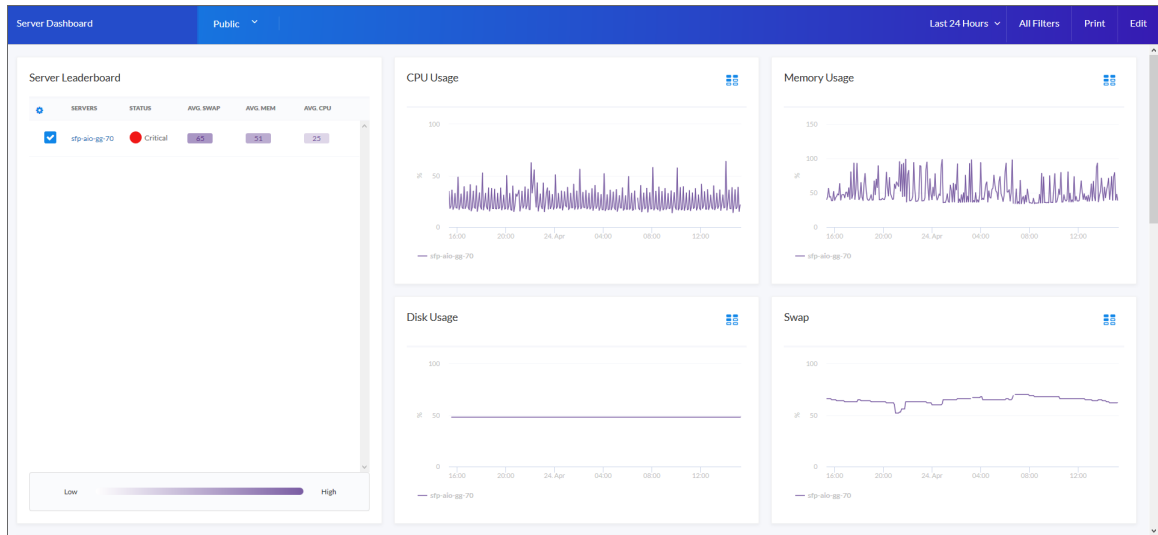
To focus on one device in a dashboard:

1. From the **[Dashboards]** tab, select a dashboard with a device leaderboard, such as **Server Dashboard**:



2. In the leaderboard or table widget, hover over the link for the device you want to view.
3. In the Status Bar of your browser, take note of the number at the end of the URL for that link. For example, <https://em7.scienceologic.com/inventory/devices/detail/23>.

4. Add **?deviceId=<device ID>** to the existing URL for the Server Dashboard, where **<device ID>** is the number you found in step 2. For example, if the original URL for the Server Dashboard is **https://em7.sciencelogic.com/dashboards/server-dashboard**, you would update that URL to the following: **https://em7.sciencelogic.com/dashboards/server-dashboard?deviceId=23** and press **[Enter]**. When the page refreshes, only the specified device appears in the dashboard:



5. To return to the default view for the dashboard, delete the **?deviceId=<device ID>** from the URL.

Chapter 4

Creating Dashboards

Overview

This chapter describes how to view graphs, charts, and tables that display the data collected by the new user interface for SL1.

The following sections explain how to view and manipulate the various elements of dashboards and widgets:

<i>Creating a Dashboard</i>	40
<i>Creating a Widget</i>	41
<i>Editing a Dashboard</i>	56
<i>Resizing and Moving Widgets on a Dashboard</i>	56
<i>Printing a Dashboard</i>	57
<i>Sharing a Dashboard</i>	58
<i>Deleting a Dashboard</i>	59

Creating a Dashboard

Before you can create a new dashboard on the **[Dashboards]** tab, you must first create the widgets that you will use in the new dashboard.


TIP: To ensure that you are using the most recent widget components, download the latest **@sciencelogic/widget-components** content package from the **[Content Management]** tab (Inventory > Content Management. For more information, see [Managing New Features on the Content Management Tab](#).

You can create a **leaderboard widget** that lets a user select specific items in a table widget, so that data about just those items displays in other widgets in the dashboard:

Servers	Avg. Swap	Avg. Mem	Avg. CPU	Status
<input checked="" type="checkbox"/> WIN-4CNHKE2M8J1	18	29	3	Critical
<input checked="" type="checkbox"/> em7ao	10	0	0	Major
<input type="checkbox"/> 192.168.33.147	0	0	0	Major
<input type="checkbox"/> 192.168.33.87	0	0	0	Major

In SL1, this feature is called **driving** data or driving the **context** of a dashboard widget. For example, in the Server leaderboard widget pictured above, if you select one or more servers on the leaderboard widget, the other widgets in the dashboard will display data about just the servers you selected. The other widgets **receive** the context from the "driving" widget, which in this example is the leaderboard widget.

TIP: The typical workflow is to first create the "driving" widget, such as a leaderboard or a table, and then create the "receiving" widget or widgets.

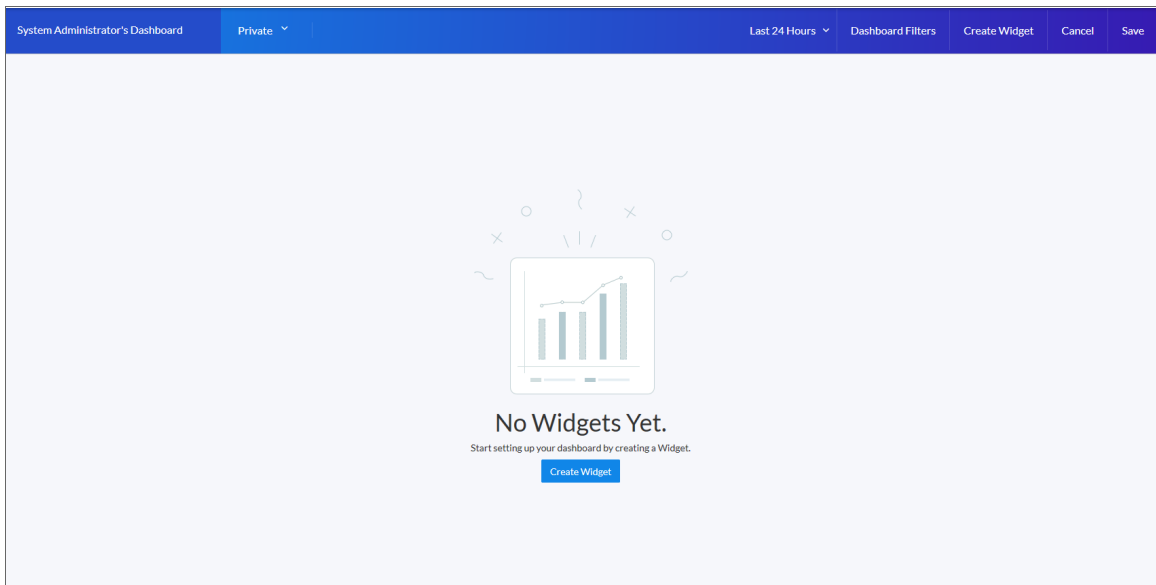
Widgets that receive context from another widget include a **Helper icon** (). When you click the Helper icon, you can view a list of the widget or widgets that drive context to that widget.

TIP: To enable the **Preview** option for a receiving widget, select a row or two in a "driving" widget after you create it, and *then* create the receiving widget.

Creating a Widget

To create a dashboard widget:

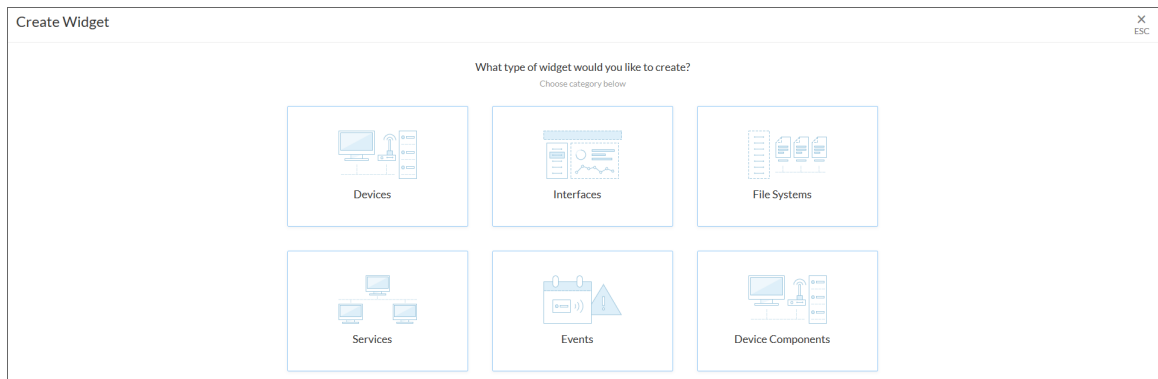
1. On the **[Dashboards]** tab, click the **[Create Dashboard]** button. The **No Widgets Yet** page appears:



TIP: If you are currently viewing a dashboard and want to add a widget to that dashboard, click the **[Edit]** button and then click the **[Create Widget]** button.

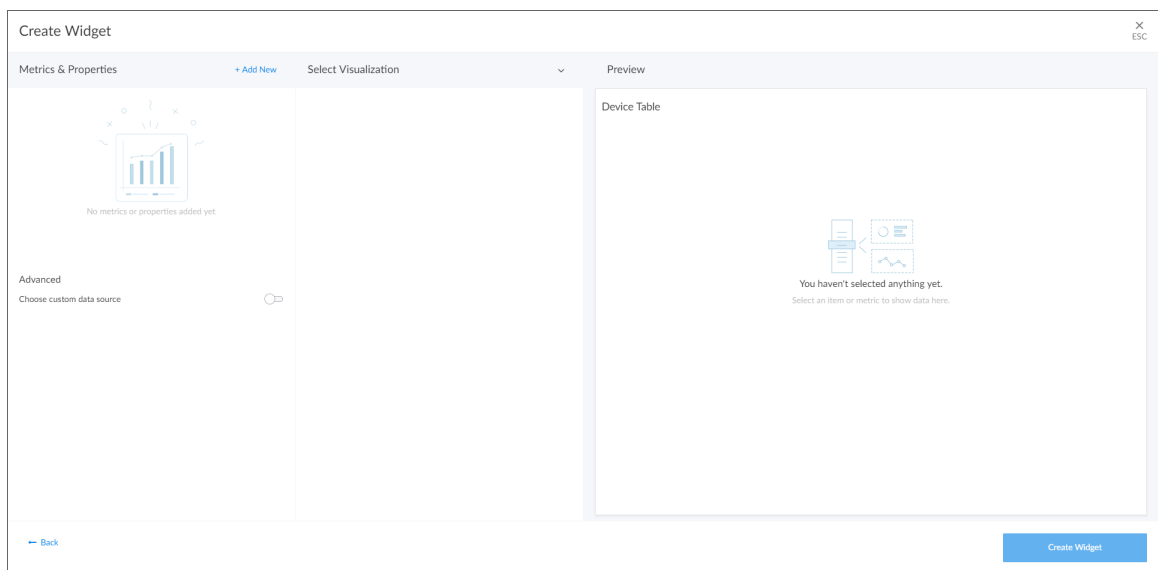
2. If needed, click the **[Edit]** button.
3. If this is a new dashboard, click the **Name** field at the top left of the page and type a name for the new dashboard. By default, the **Name** field displays your username and "Dashboard," such as "Jane Smith's Dashboard". Click the pencil icon (🖋️) to save the name.

4. Click the **[Create Widget]** button. The **Create Widget** page appears:



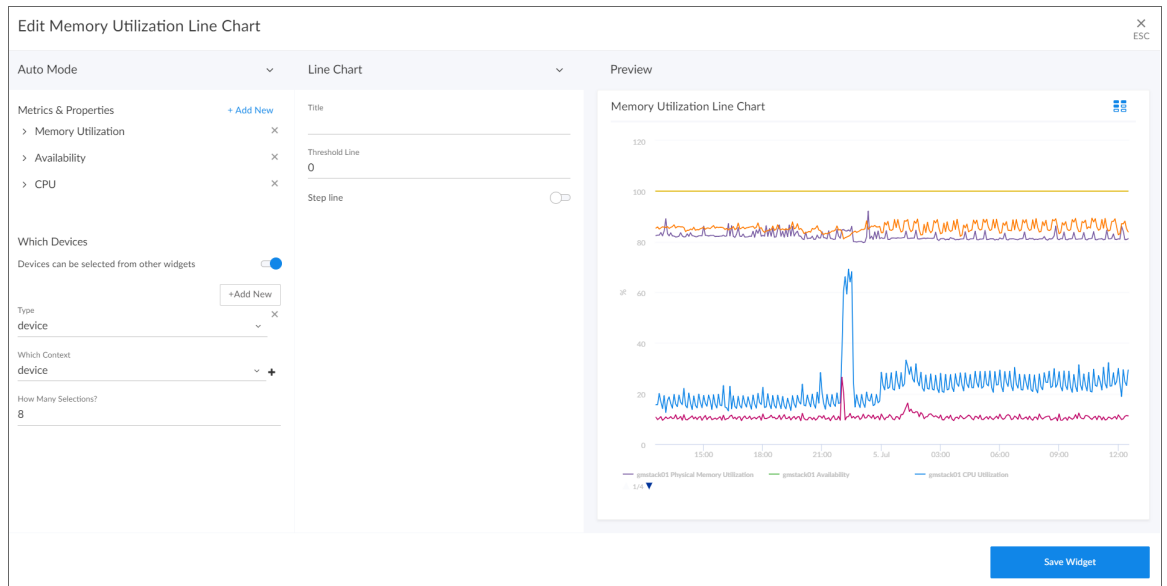
5. Select a widget type by clicking the relevant box. Your options include:
- **Devices**. Displays data based on devices and Dynamic Applications.
 - **Interfaces**. Displays data about network interfaces.
 - **File Systems**. Displays data about disk-space used, in percent, for devices.
 - **Services**. Displays data about business services and the Health, Availability, and Risk data for those services.
 - **Events**. Displays data about the events that exist for devices.
 - **Device Components**. Displays data about entities that run under the control of another device (in a parent-child relationship).

After you select the widget type, a new **Create Widget** page appears:

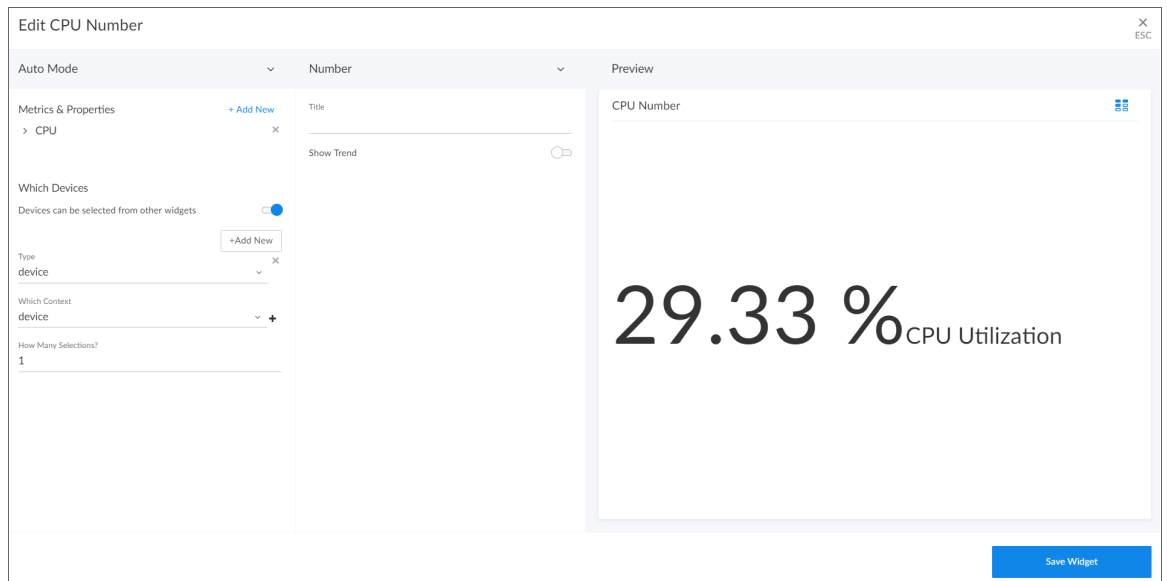


6. Click the **Select Visualization** drop-down list and select how you want this widget to display data. Your options include:

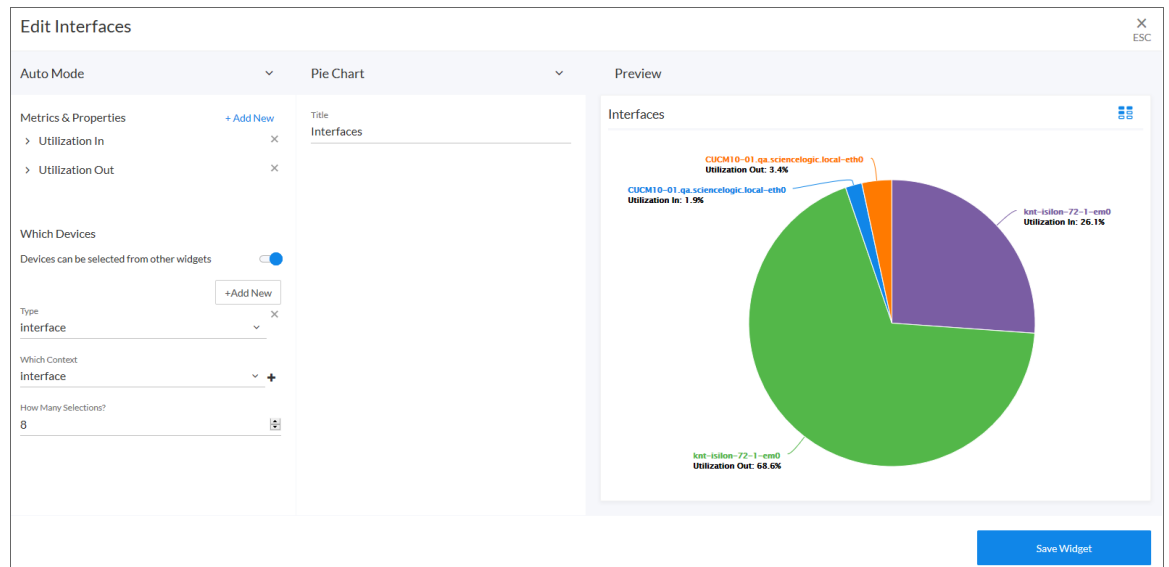
- **Line Chart**. Displays data as a series of data points connected by straight line segments:



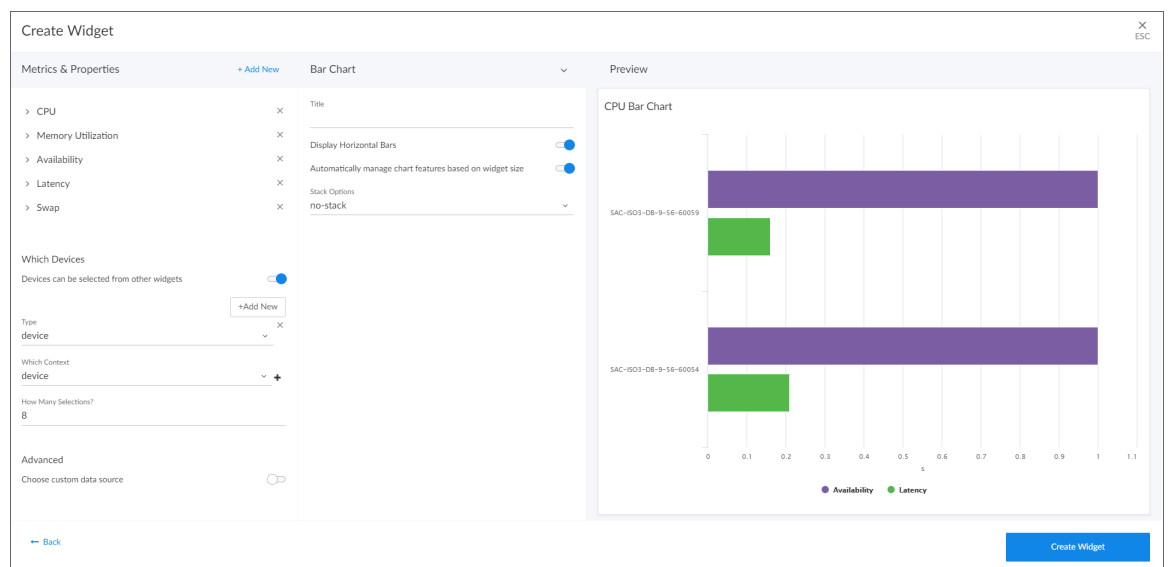
- **Number**. Displays data as a single number to highlight an important metric for a device or event. The size of the number and its related text that displays is based on the size of the widget, so increasing the widget size or screen size results in a larger font size. If multiple devices or events are selected, the number displays the average value for all selected items:



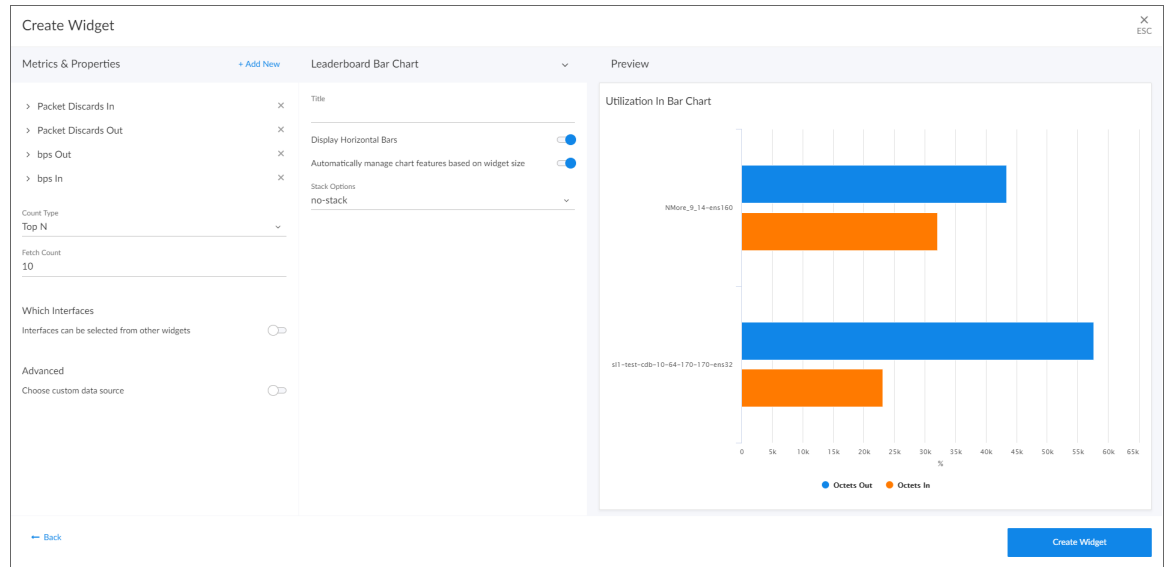
- **Pie Chart.** Displays metrics as a percentage of a whole:



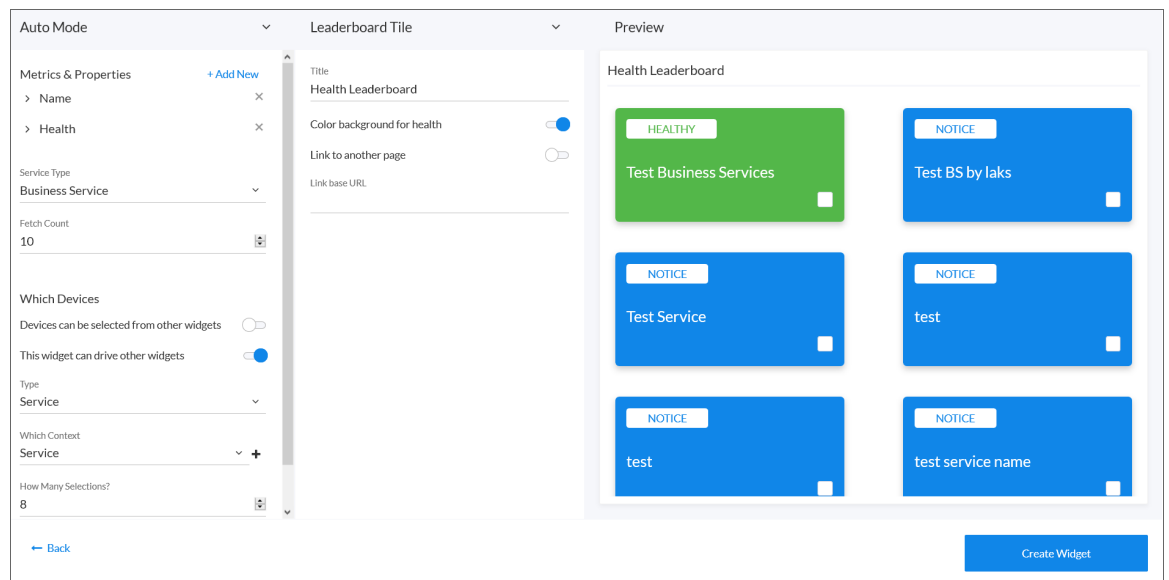
- **Bar Chart.** Displays one or more metrics as a colored vertical or horizontal bar or bars, using absolute values. Selecting a single bar can *drive* data or "context" to other widgets:



- **Leaderboard Bar Chart.** Displays a vertical or horizontal bar chart for the objects with the highest or lowest values for a performance metric. Selecting a single bar can drive data or "context" to other widgets:



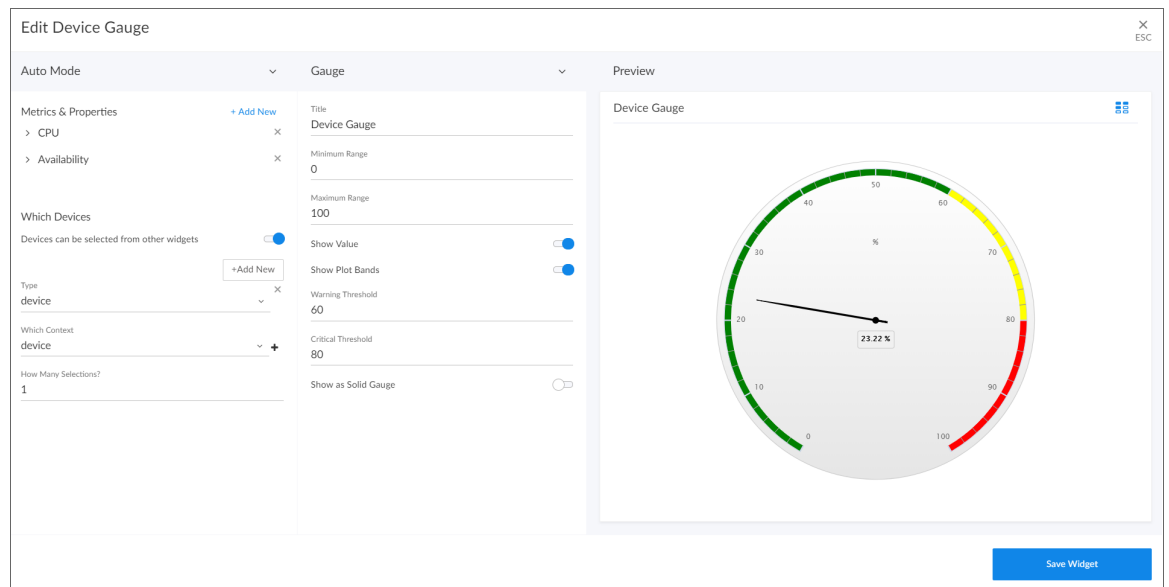
- **Leaderboard Tile.** Displays tiles for the objects with the highest or lowest values for a performance metric. You can use this widget to drive context to another widget, and you can select a service from this widget to go to its **Service Investigator** page (Service widget types only):



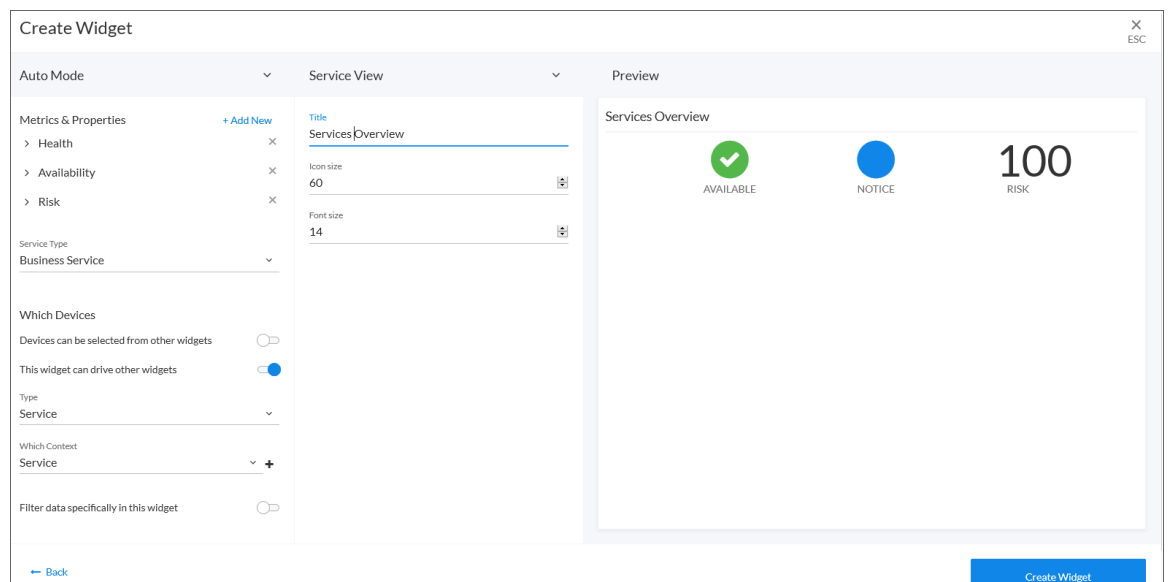
- **Leaderboard**. Displays the objects with the highest or lowest values for a performance metric. A leaderboard widget always *drives* data or "context" to other widgets, instead of *receiving* data or context:

- **Table**. Displays data in a boxed set of rows and columns. A table widget can be used to *drive* data or "context" to other widgets:

- **Gauge.** Displays a value for a single performance metric, using a gauge that looks like a speedometer. You can also select a "solid" gauge, which displays the metric value as a colored section of a half circle:

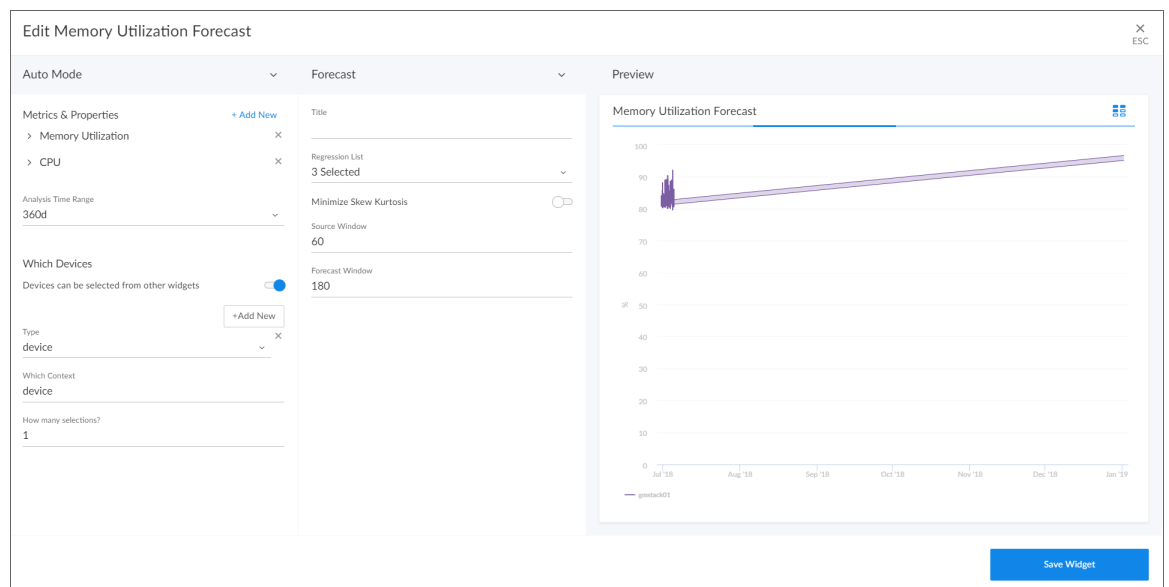


- **Service View.** Displays a quick overview of Health, Availability, or Risk (Service widget types only):



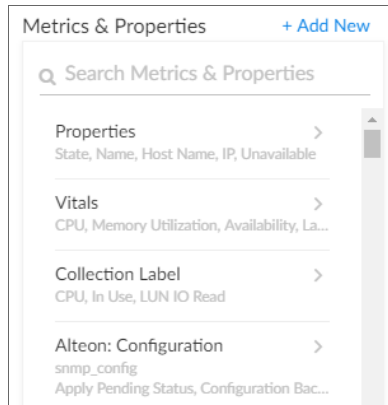
- **Tile.** Displays Health, Availability, or Risk as a colored badge or a solid background depending on the metric (Service widget types only):

- **Forecast.** Displays projected forecast data for a specific object and collection metric using historical data and selected regression methods:

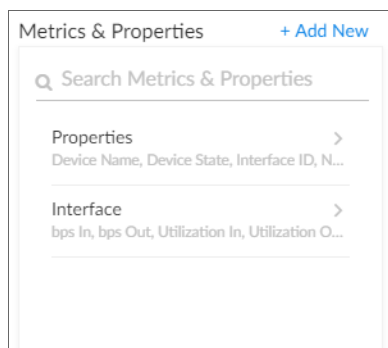


7. Click the **Metrics & Properties** label or click **+ Add New**. A drop-down list displays a set of metric types specific to the widget type you selected:

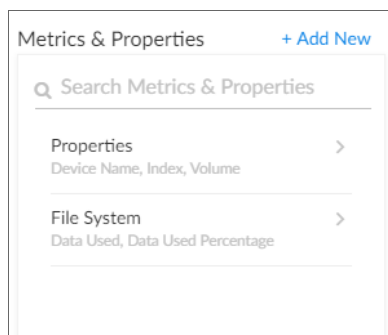
- Devices Widget:



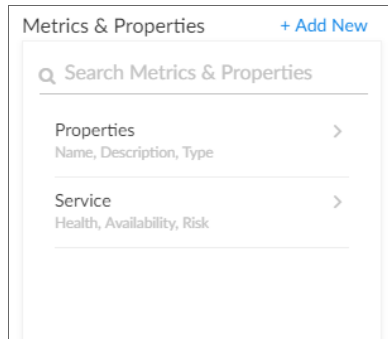
- Interface Widget:



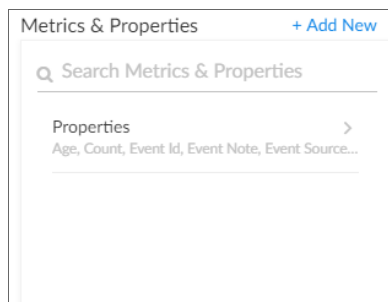
- File Systems Widget:



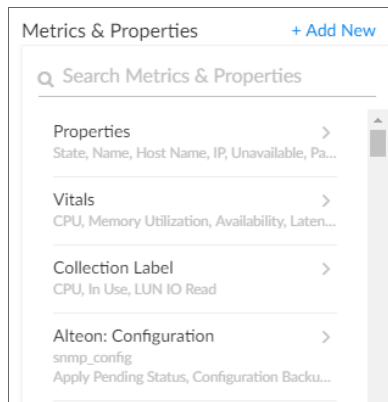
- Services Widgets:




- Events Widgets:



- Device Components Widgets:

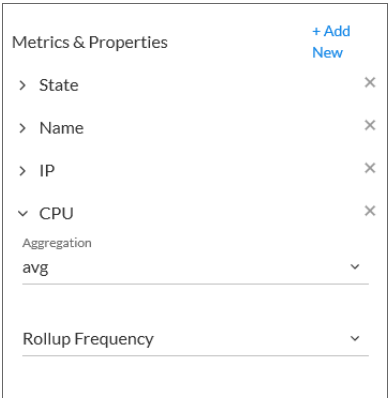



TIP: To locate a specific metric, type a search term in the **Search Metrics & Properties** field.

8. Select a metric type. When you select the name of a metric type, a new metrics menu appears. The options in the list will vary based on the widget type you selected. Your possible options include:
- **Properties.** These metrics contain basic device information, including State, Name, Host Name, IP, Index, Index Label, and Unavailable. Name, Host Name, and State are commonly used for leaderboard widgets.
 - **Vitals.** These metrics contain the key metrics about a device, including CPU, Memory Utilization, Availability, Latency, and Swap.
 - **Collection Label.** These metrics contain the available collection labels that you can use as metrics in the widget. Collection labels allow you to group and view data from multiple performance Dynamic Applications in a single widget.
 - **Dynamic Application metrics.** These metrics contain the available Dynamic Applications that you can use as metrics in the widget, such as "AWS Custom Metrics" or "Cisco: BGP Peer Stats". This menu automatically "expands" with more metrics as you scroll to the bottom of the list.
 - **Interface:** These metrics contain information about discovered network interfaces on the device, including Interface ID, Utilization In or Out, Errors In or Out, and Packet Discards In or Out (for Interface widget types only).
 - **File System.** These metrics contain information about the amount of disk space used, in percent (for File System widget types only).
9. Select one or more metrics from the metrics menu and then click the back-arrow icon () to return to the main **Metrics & Properties** drop-down list.

TIP: To remove a metric from a widget, click the **X** next to the metric name under the **Metrics & Properties** drop-down list.

10. When you are done selecting metrics, click the **Metrics & Properties** drop-down list to minimize it. The list of selected metrics appears under the **Metrics & Properties** field:



11. To edit the options for a specific metric, click the metric name or the forward-arrow icon () to access a menu for that metric. Not all metrics have these additional options. The possible metric settings include:
- **Count Type.** You can choose from *Top N* to display the highest values for the selected metric, or *Bottom N* to display the lowest values for the selected metric (Leaderboard and Table only).
 - **Fetch Count.** Type the number of devices you want to view on the widget (Leaderboard, Table, Tile, and Top N bar chart only).
 - **Aggregation.** Specify the method of aggregation (average, maximum, minimum) to perform on the collected values for this metric.
 - **Analysis Time Range.** Optionally, update the time frame displayed in this widget (Forecast only).
 - **Rollup Frequency.** Specify a type of normalized performance data (hourly, daily, or raw) for this metric. Currently, the Interface BPS metric does not return any data this option is set to raw.
 - **Type.** Select a display type for this metric, such as *heat* for a heat map that displays the percentage of change over time, or *label* for a simple table. If you select heat map, you can also specify the minimum and maximum values for the table. Another example would be for an availability metric, where you can choose between *label* to show availability as a text label or *state* to show availability as a colored icon.
 - **Display Name.** Type a name for this metric.
 - **Minimum Value.** Specify the lowest possible value to be displayed in the widget.
 - **Maximum Value.** Specify the highest possible value to be displayed in the widget.
 - **Unit.** Optionally, specify the unit for this widget, such as a percentage or a unit of time.
 - **Service Type.** Select which kind of services you want to display in the widget. Your options include *Business Services*, *IT Services*, and *Device Services* (Service only).


12. In the **Which <Items>** section, specify if the new widget will *drive* data (or "context") to another widget, or if you want the widget to *receive* data (or "context") from another widget. You can select one of the options, both options, or neither option:

NOTE: Depending on the widget type you selected in step 5, the **<Items>** on this window display as **Devices**, **Interfaces**, **File Systems**, **Services**, **Events**, or **Device Components**.

- **<Items> can be selected from other widgets.** Select this option if you want this widget to *receive* and display data (or "context") based on what a user selects in another widget. This option is selected by default for these visualization types: line chart, number, gauge, and forecast. If you select this option, complete the following fields to define the devices from which you want to receive widget data:
 - **Type.** Select a widget type that will drive data or "context" to this widget. The default type is based on the widget type you selected in step 4 (device, interface, file system, service or event)
 - **Which Context.** Select an existing context label or click the plus icon (**+**) to type a context label for the widget that will drive the data ("context") to this widget. The default context type is based on the widget type, such as device, interface, or service, but you can also select a specific context label from a "driving" widget that you created.
 - **How Many Selections?** Select the number of devices to display by default in the driving widget. For example, if you only want the user to be able to select one device at a time, select 1.

TIP: To add another widget from which this widget can receive data (or "context"), click the **[Add New]** button and complete the **Type**, **Which Context**, and **How Many Selections** fields for that additional widget.


- **This widget can drive other widgets.** Select this option if you want this widget to *drive* data (or "context") to other widgets. This option is selected by default for these visualization types: leaderboard and table. If you select this option, complete the following fields to define the type of devices to which you want to drive data:
 - **Type.** Select the widget type that will receive data or "context" from this widget. The default type is based on the widget type you selected in step 4 (device, interface, file system, service or event).
 - **Which Context.** Select an existing context label or click the plus icon (**+**) to type a context label for this widget if you want this widget to drive data ("context") to other widgets. Also, a File System or Interface widget can publish its content of type "file system or interface" as well as a secondary context of device.
 - **How Many Selections?** Select the number of devices to display by default in this widget. If you only want to show data from one widget at a time, select 1.

TIP: You can see where a receiving widget gets its data by clicking the **Helper icon** () for that widget after you create the receiving widget.

- **Filter data specifically in this widget.** Select this option if you want to view a specific set of data in this widget. For example, you can create multiple leaderboard widgets in a dashboard that contain just the devices you want to view. If you select this option, complete one or both of the following fields to define the type of data you want to display in this widget:
 - **Filter By.** Select the type of widget you want to use as a filter for this widget.
 - **Filter Criteria.** Type a search term to filter this widget.

13. In the **Title** field, type a name for the new widget.

TIP: If you are planning to use this widget to drive context or receive context, take note of the exact name of this widget, as you will need to type it later in the **Which Context** field when you create the new context.


14. Under the **Select Visualization** drop-down list, complete the following fields as needed, depending on the widget type and visualization you selected in steps 5 and 6:
 - **Display Unit Labels.** Select this toggle to display relevant unit labels, such as "KB" or "%" along with the values in the widget.
 - **Threshold Line.** Specify a number that represents the threshold for a line chart (Line Chart only).
 - **Show Trend.** Select this toggle if you want to display trend data (Number only).
 - **Stack Options.** Specify how you want to display data in a bar chart. Your options include *no-stack* (show each value as its own bar), *normal* (show all values in one bar), and *percent* (Bar Chart and Leaderboard Bar Chart only).
 - **Minimum Range.** Specify the upper limit of a gauge. The default is 0 (Gauge only).
 - **Maximum Range.** Specify the upper limit of a gauge. The default is 100 (Gauge only).
 - **Show Value.** Select this toggle to display the current value on a gauge (Gauge only).
 - **Show Plot Bands.** Select this toggle to show the plot bands on a gauge (Gauge only).
 - **Warning Threshold.** Specify where you want the yellow warning portion of a gauge to start. The default is 60 (Gauge only).
 - **Critical Threshold.** Specify where you want the red critical portion of a gauge to start. The default is 80 (Gauge only).
 - **Display Unit Labels.** Select this toggle to display relevant unit labels, such as "KB" or "%" along with the values in the widget.
 - **Link to another page.** Select this toggle to add a link icon () to a Service widget that links to a related Service widget. After selecting the toggle, type a base URL for the related Service widget, using the following format:
`/dashboards/<service type>-service-details?harProviderId=$id`
 where *<service type>* is *business*, *it*, or *device*. *?harProviderId=\$id* is an optional variable that provides access to all widgets related to this widget (Service widgets only).
 - **Regression List.** Select the regression method or methods you want SL1 to try when calculating the forecast data in a forecast widget. You can select multiple types of regression, and SL1 will run all the regressions you selected and display the best two types of regression. ScienceLogic recommends that you select at least three regression methods to produce the most likely forecast. SL1 will then determine which regression method(s) of those you have chosen will best model the forecast data (Forecast only).
 - **Minimize Skew Kurtosis.** Select this toggle button to enable transformation of the source data into a normal distribution by compensating for skew and kurtosis in the data, which makes the data easier to read (Forecast only).
 - **Source Window.** Specify the size of the source window from which the widget will gather data for the forecast. The default is 60 days (Forecast only).
 - **Forecast Window.** Specify the size of the forecast window. The default is 180 days (Forecast only).
15. Click the **[Create Widget]** button to save the new widget. If this button is grayed out, review the settings on the **Create Widget** page for errors or missing data.
16. On the new dashboard page, click the **[Save]** button under the main tab bar.

17. To add additional widgets to the dashboard, click the **[Edit]** button under the main tab bar and repeat this procedure for each new widget.

NOTE: If you created a gauge or number widget and you select more than one item on the widget driving data or "context" to that widget, the gauge or number widget displays data for only the *first* item you selected in the driving widget.

Editing a Dashboard


To edit an existing dashboard:

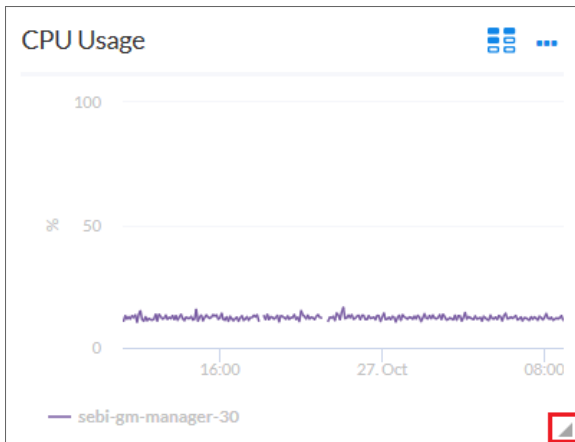
1. Go to the **[Dashboards]** tab and click the name of the dashboard you want to edit. The dashboard page appears.
2. Click the **[Edit]** button under the main tab bar.
3. On the widget you want to edit, click the **[Options]** button () and select *Edit*. The Edit page appears.
4. Make your changes to the widget, and then click the **[Save Widget]** button when you are done.
5. As needed, edit any other widgets on the dashboard.
6. When you are done editing the dashboard:
 - If you want to save the updated dashboard with same name as the existing dashboard, click the **[Save]** button under the main tab bar.
 - If you want to save the updated dashboard as a *new* dashboard, click the dashboard name, type the new name, and then click the **[Save]** button.

Resizing and Moving Widgets on a Dashboard

To resize and move widgets on a dashboard:

1. Go to the **[Dashboards]** tab and click the name of the dashboard you want to edit. The dashboard page appears.
2. Click the **[Edit]** button under the main tab bar.

3. To resize a widget, click the resizing icon () at the bottom right-hand corner of the widget and drag the widget until it is the size you want.



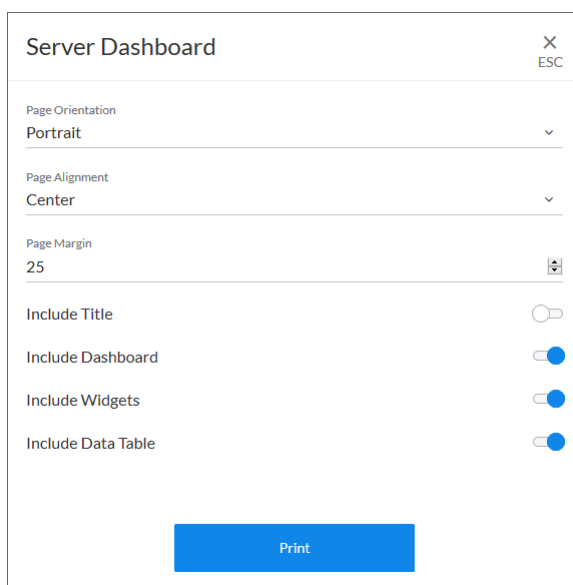
4. To move a widget, click the header for that widget and drag the widget to its new location on the dashboard.
5. Click the **[Save]** button when you are done resizing or moving widgets on the dashboard.

Printing a Dashboard

You can create a printable version of a dashboard in PDF format.

To create a PDF of a dashboard:

1. Go to the **[Dashboards]** tab and click the name of the dashboard you want to print. The dashboard page appears.
2. Click the **[Print]** button under the main tab bar. A Print dialog appears:



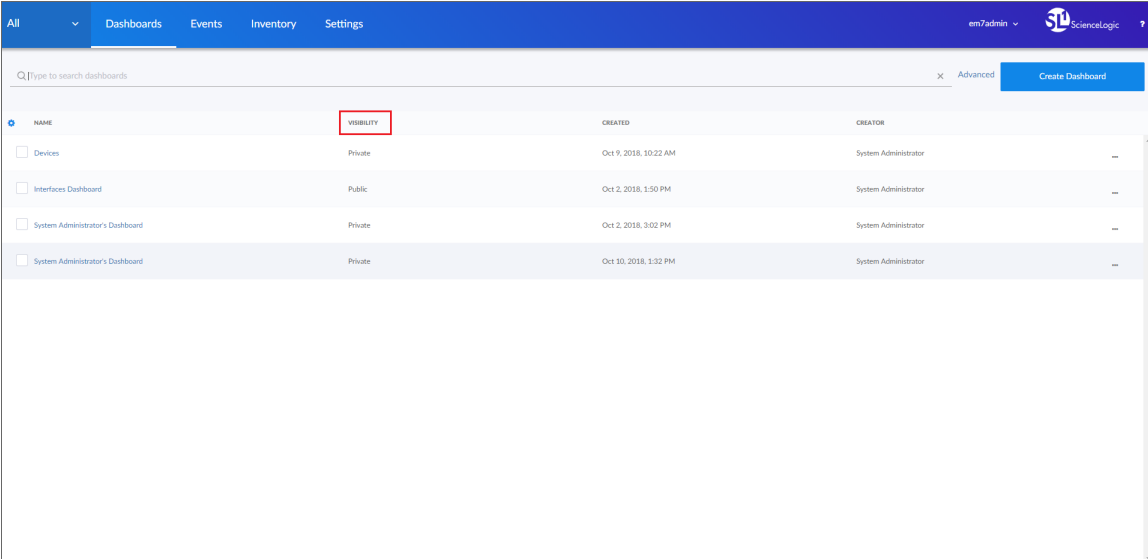
3. Complete the following fields:

- **Page Orientation**. Select from *Portrait* or *Landscape* orientation for the output.
- **Page Alignment**. Select from *Left*, *Centered*, or *Right* justification for the output.
- **Page Margin**. Specify the margins in the output, in pixels. The default is 25 pixels (about .4 inches).
- **Include Title**. Select this toggle if you want to include the title of each widget in the output.
- **Include Dashboard**. Select this toggle if you want to display the current view of the entire dashboard in the output.
- **Include Widgets**. Select this toggle if you want to display all of the individual widgets in the output.
- **Include Data Table**. Select this toggle if you want to display all of the current data in tables in the output.

4. Click the **[Print]** button. SL1 generates a PDF version of the dashboard that you can print.

Sharing a Dashboard

By default a dashboard is private when you create it. You can make a dashboard public, which lets you share it with other users. On the **[Dashboards]** tab, the **Visibility** column lists whether a dashboard is public, private, or shared with only specific organizations.

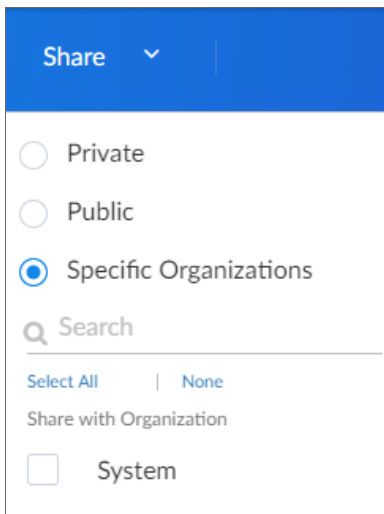


NAME	Visibility	CREATED	CREATOR
<input type="checkbox"/> Devices	Private	Oct 9, 2018, 10:22 AM	System Administrator
<input type="checkbox"/> Interfaces Dashboard	Public	Oct 2, 2018, 1:50 PM	System Administrator
<input type="checkbox"/> System Administrator's Dashboard	Private	Oct 2, 2018, 3:02 PM	System Administrator
<input type="checkbox"/> System Administrator's Dashboard	Private	Oct 10, 2018, 1:32 PM	System Administrator

To change the visibility of a dashboard:

1. Go to the **[Dashboards]** tab and open the dashboard. Click the **[Edit]** button under the main tab bar.
2. Next to the title of the dashboard, click the **Visibility** drop-down list and select one of the following:
 - *Private*. The dashboard is visible to only the creator of the dashboard.
 - *Public*. The dashboard is visible to all users.

- *Specific Organizations*. The dashboard will be shared only with organizations that you select. When you select *Specific Organizations*, a list of organizations appears. You can search for an organization, click *Select All*, or click *None* to deselect all organizations.



Share ▾

☐ Private

☐ Public

☒ Specific Organizations

🔍 Search

Select All | None

Share with Organization

☐ System

3. After you set the visibility of your dashboard, click the **[Save]** button under the main tab bar.

Deleting a Dashboard

You can delete any dashboard that you have created, as well as any other dashboard in the new user interface.

WARNING: If you delete a dashboard, that dashboard is deleted for all users.

To delete a dashboard:

1. On the **[Dashboards]** tab, click the **[Options]** button (⋮) for the dashboard you want to delete and select *Delete*.
2. On the Delete Dashboard dialog, click the **[Delete]** button to permanently remove the dashboard.

Chapter

5

Managing Events

Overview

This chapter describes how to use the new user interface for SL1 to manage events that appear on the **[Events]** tab.

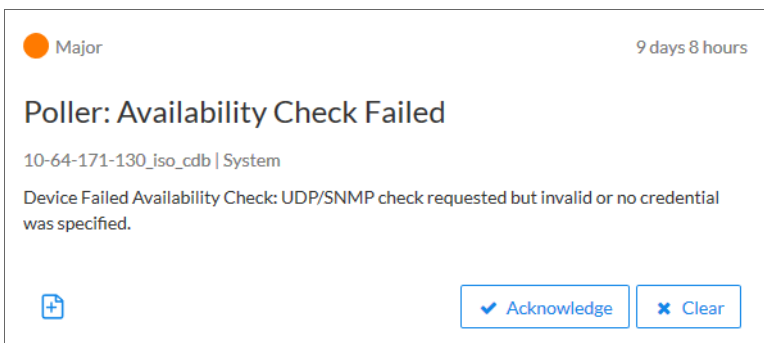
The following sections describe how to use the **[Events]** tab:

<i>What is an Event?</i>	61
<i>Searching for Events</i>	61
<i>Viewing Events</i>	62
<i>Using the List View</i>	63
<i>Using the Card View</i>	64
<i>Filtering the List of Events</i>	64
<i>Viewing Events by Organization</i>	64
<i>Filtering Events by Severity</i>	66
<i>Filtering for Masked Events</i>	67
<i>Working with Events</i>	68
<i>Acknowledging and Clearing Events</i>	68
<i>Selecting Multiple Events</i>	68
<i>Viewing and Editing Event Notes</i>	69
<i>Using the Event Drawer</i>	70
<i>Working with the Tools Pane</i>	70
<i>Using the Event Investigator</i>	72

What is an Event?

One of the quickest ways to monitor the health of your network is to look at events. You can view events on the **[Events]** tab, which is found under the **[Inventory]** tab in the new user interface of SL1.

Events are messages that are triggered when a specific condition is met. For example, an event can signal if a server has gone down, if a device is exceeding CPU or disk-space thresholds, or if communication with a device has failed. Alternately, an event can simply display the status of a managed element:



SL1 generates log messages from incoming trap and syslog data, and also when SL1 executes user-defined policies. SL1 then uses these log messages to generate events. SL1 examines each log message and compares it to each event definition. If a log message matches an event's definition, SL1 generates an event instance and displays the event on the **[Events]** tab.

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.

SL1 includes pre-defined events for the most commonly encountered conditions in the most common environments. You can also create custom events for your specific environment or edit the pre-defined events to better fit your specific environment.

Searching for Events

To locate an event, click the **[Events]** tab and type the name of the event or other search terms into the **Search** field at the top of the list. For more information, see [Using Basic Search](#).

TIP: To use the Advanced Search, click the **Advanced** link to the right of the **Search** field and use custom search commands to locate events. For more information, see [Using Advanced Search](#).

Viewing Events

The **[Events]** tab displays a list of currently active events, from critical to healthy. From this tab 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.


The screenshot shows the ScienceLogic Events tab. The top navigation bar includes 'All', 'Dashboards', 'Events', 'Inventory', and 'Settings'. The 'Events' tab is selected, showing a summary of 406 events with a breakdown by severity: 2 Critical, 346 Major, 10 Minor, 8 Notice, and 20 Healthy. On the left, a sidebar lists organizations: System, Storage Stuff, UCS_Manager.org, backend, and SILO. The main area displays a table of events with columns for Organization, Severity, Name, Message, Age, Ticket ID, Count, Event Note, Name, Ticket External, Acknowledge, and Clear. A detailed view for a specific event (76095-NPE3.cisco.com) is shown, including a Vitals graph, a Tools section with options like Ping, Who Is, Port Scan, Deep Port Scan, ARP Lookup, ARP Ping, and Trace Route, and a Logs section showing event details and timestamps.

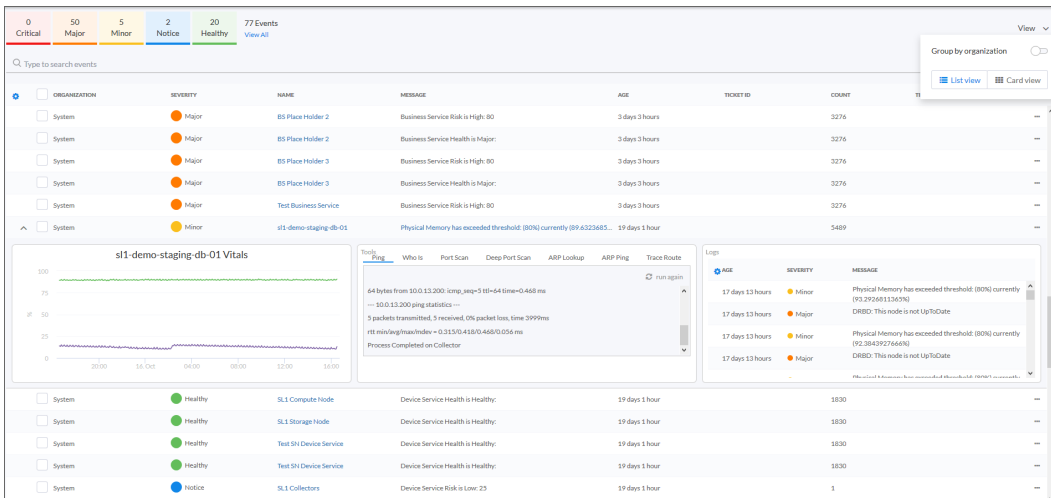
For an event that is **aligned** or associated with a device, you can click the down-arrow icon (▼) for that event in the **List View** (☰) to open the **Event Drawer**. The Event Drawer is a drop-down panel that displays additional data about that event, including a Vitals widget, Tools, and Logs.


In the **Message** column of the List View, you can click the message link to view the **Event Investigator** page for an event aligned with a device. You can also click the **[Options]** button (⚙) for that event and select **View Event**. The **Event Investigator** page includes Tools, Logs, Notes, Assets, and a Vitals widget for an event aligned with a device.

TIP: You can click the device name in the **Name** column to view the **Device Investigator** page for the device aligned with an event. Only events that have a device aligned with them display this link on the **[Events]** tab.


Using the List View

The **List View** () displays event data in a similar way to the **Event Console** in the classic user interface. This view is set up like a table, with one event per row:




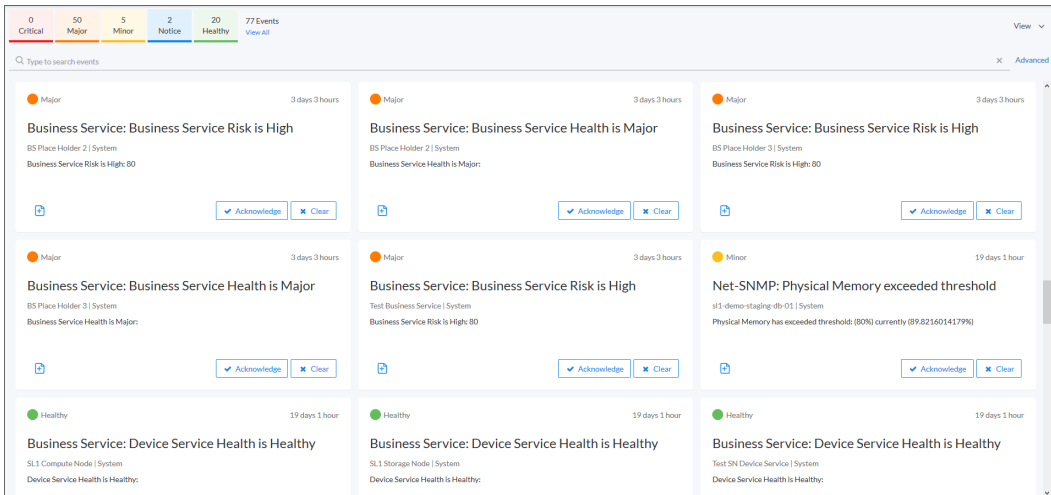
If an event on the **[Events]** tab is associated or "aligned" with a device, you can click the down-arrow icon () next to the name of the event in the List View to open a drop-down panel called a **drawer** that contains additional data about that device.

If you click the name of an event in the List View, you can access an **Event Investigator** page containing additional details about that event.

TIP: To rearrange the columns in the List View, click and drag the column name to a new location. You can adjust the width of a column with by clicking and dragging the right edge of the column. You can click the **Choose Columns** icon () to add or remove columns, or to reset the columns to their default settings.

Using the Card View

The **Card View** () organizes the data for an event in a vertical "card" layout instead of a table layout:



In the Card View, you can acknowledge or clear an event, and you can also edit an event note.

Filtering the List of Events

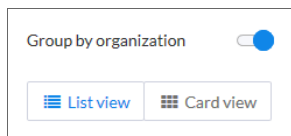
This section explains how to filter the list of events so you can quickly locate and respond to address any potential problems in your environment.

Viewing Events by Organization

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

To view events by organization:

1. On the **[Events]** tab, click the **View** menu.



- Click the **Group by organization** toggle to turn it blue. The **Organizations** panel appears on the **[Events]** tab with a list of events sorted by severity for each organization.

The screenshot shows the Sciencelogic Events dashboard. On the left, the **Organizations** panel is visible, listing organizations like System, Storage Stuff, UCS_Manager.org, backend, and SILO. The main area displays a table of events with columns: ORGANIZATION, SEVERITY, NAME, MARKED, MESSAGE, AGE, TICKET ID, COUNT, EVENT NOTE, ACKNOWLEDGE, and CLEAR. The events are sorted by severity, showing Critical, Major, Minor, Notice, and Healthy categories. A graph titled '76095-NPE3.cisco.com Vitals' is also visible, showing a line chart of system health over time.

TIP: To hide the **Organizations** panel, click the left arrow icon (←). Click the right arrow icon (→) to expand the panel again.

- On the **Organizations** panel, click the check mark icon (✓) for each organization you want to monitor.

Filtering Events by Severity

The **[Events]** tab displays a list of currently active events, ordered 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]** tab:

MAJORITY	ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	COUNT	EVENT NOTE	TICKET EXTERNAL REFERENCE	ACKNOWLEDGE	CLEAR
0	System	Critical	IT Service State Critical: test	IT Service State Critical: test	9 days 13 hours	916			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	Storage Stuff	Critical	RAID Group 1	RAID Group utilization of 99.99% exceeded threshold of 95%.	5 days 4 hours	745			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	10.2.10.155	Cisco (CE Series): The video output (NoneObject NoneObject) is...	3 days 22 hours	1			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	10.2.10.155	Cisco (CE Series): H323 Services H323 Service is ON and there ar...	9 days 13 hours	2750			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	10-64-171-130_iso_cdb	Device Failed Availability Check: UOP/SHMP check requested bu...	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	Storage Stuff	Major	10.2.5.121	Device Failed Availability Check: UOP/SHMP check requested bu...	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	Storage Stuff	Major	3	Device Failed Availability Check: Component device 331 is not av...	9 days 13 hours	2750			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	Storage Stuff	Major	2	Device Failed Availability Check: Component device 332 is not av...	9 days 13 hours	2750			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
2	System	Major	sebi-gm-manager-32	Device Failed Availability Check: UOP - SHMP	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
2	System	Major	sebi-ai-13	Device Failed Availability Check: UOP - SHMP	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	kooni_ais_8k_30215123	Device Failed Availability Check: UOP - SHMP	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
2	System	Major	parker_ais_8k_112	Device Failed Availability Check: UOP - SHMP	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
2	System	Major	sebi-ai-22	Device Failed Availability Check: UOP - SHMP	9 days 13 hours	2748			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	UCS_Manager.org	Major	10.5.100.5	SSL certificate has expired (expires on: 2017-12-28 17:51:41)	8 days 18 hours	17			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	10.2.10.155	SSL certificate has expired (expires on: 2016-12-10 21:55:30)	8 days 18 hours	17			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
2	System	Major	10.2.13.11	Device Failed Availability Check: ICMP Ping	8 days 4 hours	2357			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	CUCM410-01.qa.sciencelogic.local	/ File system usage exceeded major threshold. Limit: 85.0%, Act...	5 days 1 hour	486			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
0	System	Major	gmsta002	SSL certificate has expired (expires on: 2018-05-26 00:43:14)	2 days 18 hours	6			<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear

When you click a severity, 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 does not affect service but about which users should be aware.
- **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

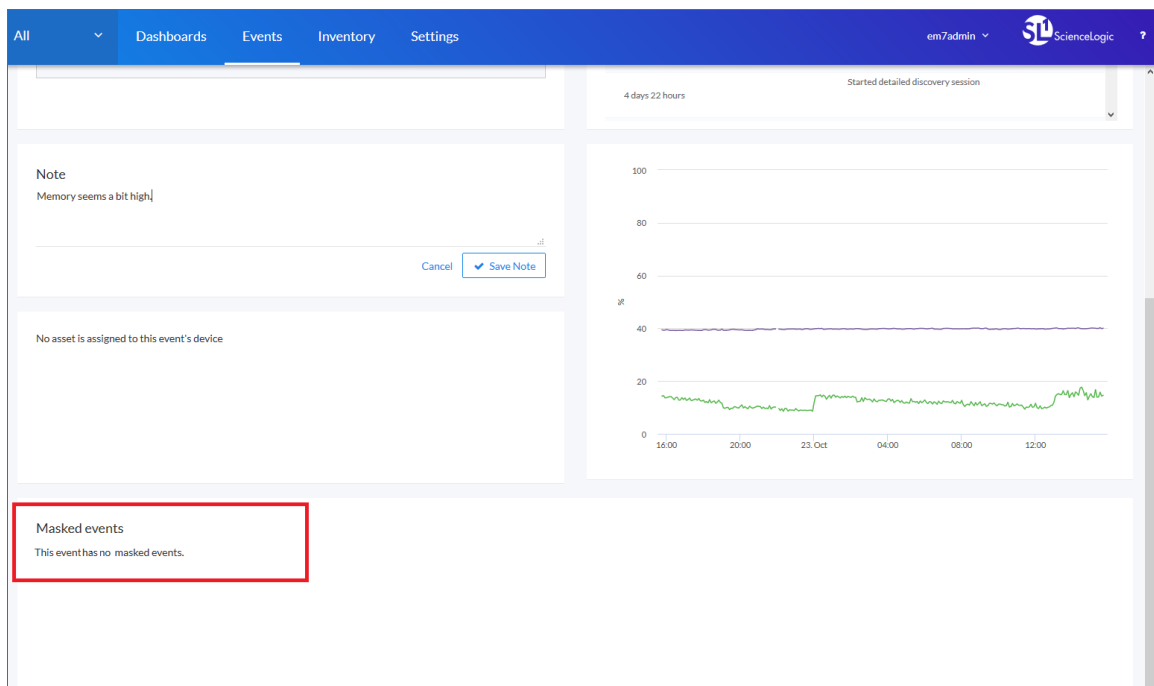
When a device uses the **event mask** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed in the **[Events]** tab. This allows related events that occur in quick succession on a single device to 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.

To view masked events:

1. On the List View of the **[Events]** tab, click the link in the **Message** column for the relevant event. The Event Investigator page for that event appears.

NOTE: Only events aligned to a device display a link in the **Message** column.

2. Scroll down to the **Masked events** section of the **Event Investigator** page to view a list of masked events:



Working with Events

This section describes how to acknowledge and clear events in the new user interface, how to learn more about events, and how to use the Event Tools.

Acknowledging and Clearing Events

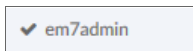
When you **acknowledge** an event, you let other users know that you are aware of that event, and you are working on a response.

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]** tab. If the event occurs again on the same device, it will reappear in the **[Events]** tab.


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.

To acknowledge and clear events:


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



2. To clear an event, click the **[Clear]** button for that event on the **[Events]** tab. The event is removed from the **[Events]** tab.

TIP: If you want to hide the **[Acknowledge]** or **[Clear]** buttons from the List View of the **[Events]** tab, click the **Choose Columns** icon () and deselect the columns you want to hide from the list of columns.

Selecting Multiple Events

In the List View () of the **[Events]** tab, you can use the checkboxes to the left of the event to select more than one event at a time. After you select the events, you can click the **[Acknowledge]** or **[Clear]** button to acknowledge or clear those events simultaneously.

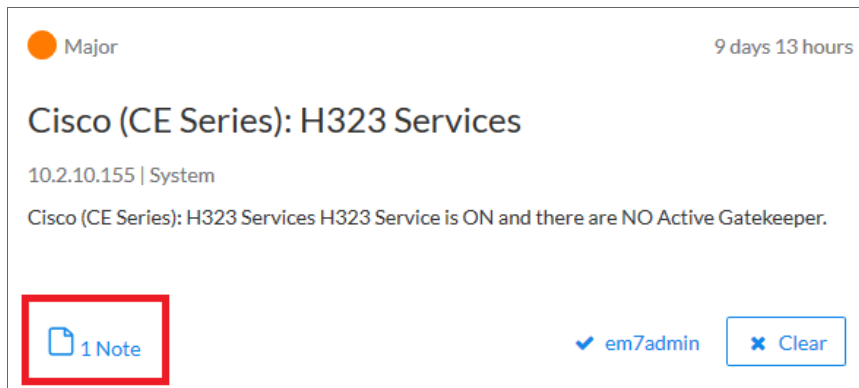
If you do *not* want to acknowledge or clear the selected events, click the **[Clear Selections]** button to deselect the checkboxes.

If you want to select *all* of the events that are currently showing on the tab, click the **[Select All Visible]** button.


Viewing and Editing Event Notes


From the **[Events]** tab, 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 List View, or the text "1 Note" appears in the Card View:





To view or edit an event note:

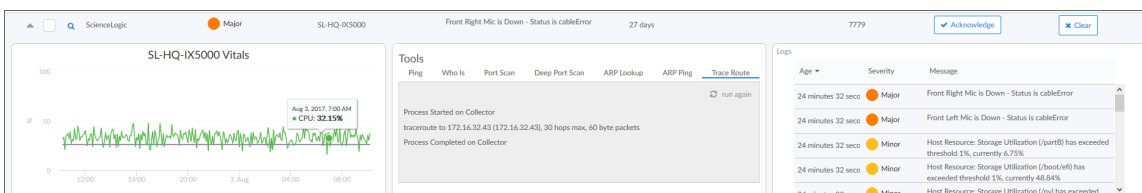
1. On the **[Events]** tab, click the **Note** icon () for that event. The **Edit Event Note** window appears:

TIP: You can also edit an event note from the List View of the **[Events]** tab by clicking the **[Options]** button () for that event and selecting *Edit Event Note*.

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

Using the Event Drawer

In the List View () of the **[Events]** tab, you can click the down-arrow icon () next to the name of an event to open a drop-down panel called the **Event Drawer**. The Event Drawer contains additional data about that event:



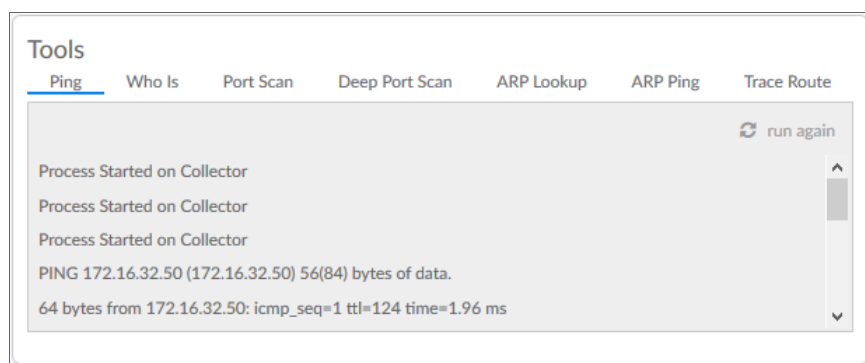
On the Event Drawer, you can access the following panes:

- **Vitals.** A widget displaying 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.
- **Tools.** A set of network tools that you can run on the device associated with the event. These tools can help with troubleshooting and diagnostics. For more information, see [Working with the Tools Pane](#).
- **Logs.** A list of the log entries from the device's log file, sorted from newest to oldest by default.

NOTE: The Event Drawer displays only for events that are aligned with devices.

Working with the Tools Pane

The Tools pane on the Event Drawer in the List View (and also on the **Event Investigator** page) provides access to a set of network tools. The Tools pane lets you to run diagnostics on a device associated with an event without leaving the the new user interface.



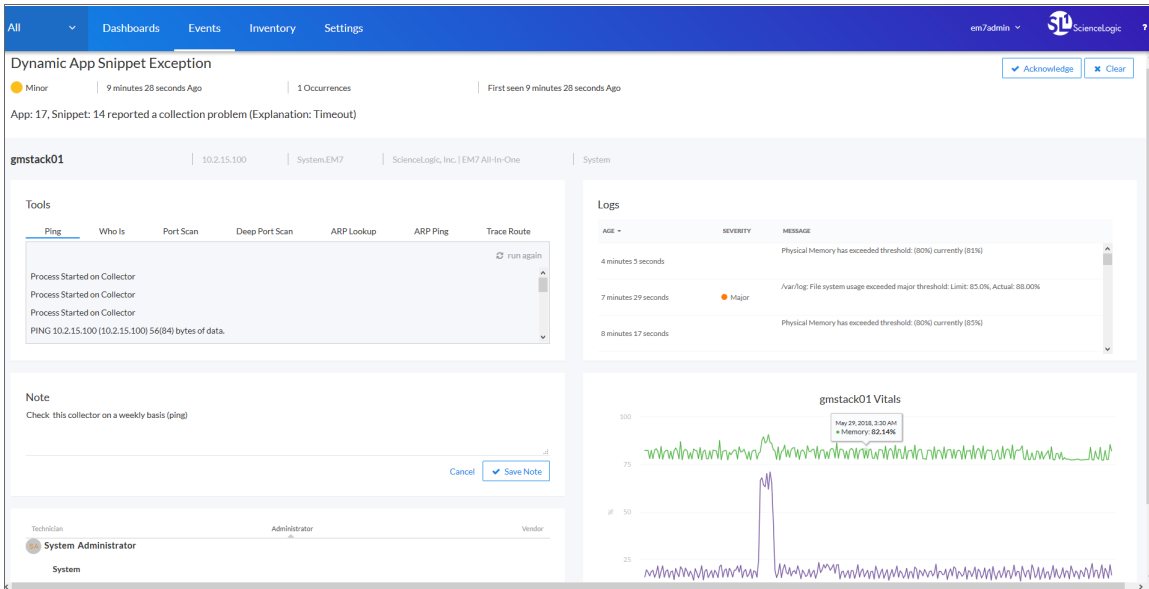
TIP: These tools are the same tools in the Device Toolbox found in the classic user interface.

You can access the following tools from the Event Drawer in the List View of the **[Events]** tab, and also from the **Device Investigator** page for a specific device:

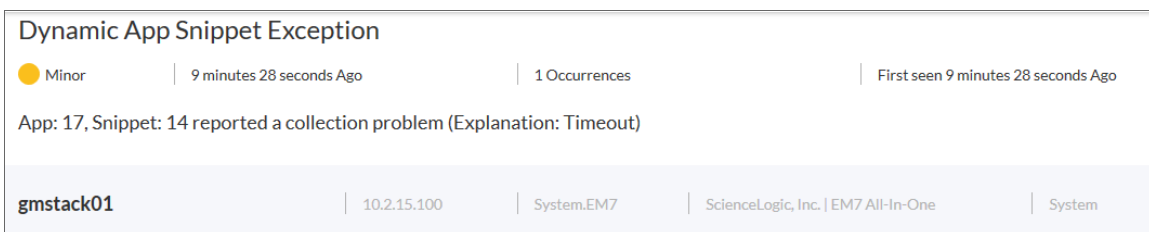
- **Ping**. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, the SL1 uses the appropriate IPv6 ping command.
- **WhoIs**. 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.

Using the Event Investigator

The **Event Investigator** page provides details about the device associated with the event, including Tools, Logs, Notes, Assets, and a Vitals widget.



The top of the **Event Investigator** page provides a quick overview of the event:



The top pane displays:

- name of the event
- event severity
- age of the event
- number of occurrences
- when the event was first seen

From this top pane, you can also acknowledge and clear the event.

The pane below displays the following information about the device associated with the event:

- Device Name
- Device IP
- Device Category
- Device Class
- Organization

The **Event Investigator** page includes the following additional panes:

- **Tools.** A set of network tools that you can run on the device associated with the event. This pane is the same as the Tools pane of the Event Drawer. For more information, see [Working with the Tools Pane](#).
- **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.
- **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]** tab. This allows related events that occur in quick succession on a single device to be rolled-up and posted together under one event description.

Chapter

6

Managing Devices

Overview

This chapter describes how to use the new user interface for SL1 to manage devices and device groups that display on the **[Devices]** tab on the **[Inventory]** tab.

The following sections describe how to use the **[Devices]** tab:

What is a Device?	75
<i>What is a Device Record?</i>	75
Searching for Devices	76
Working with Devices	76
<i>Adding Devices</i>	76
<i>Learning More about Devices</i>	77
Using the Device Investigator	77
<i>Adding Metrics to the Overview Tab</i>	78
<i>Comparing Devices</i>	81
<i>Using Device Tools</i>	82
<i>Viewing the Device Information Tab</i>	83
<i>Viewing the Device Interfaces Tab</i>	84
<i>Viewing the Configs Tab</i>	86
<i>Viewing the Events Tab</i>	87
<i>Viewing the Collections Tab</i>	88
Assigning Icons to Device Classes	88
Working with Device Categories	91

What is a Device?

Devices are all networked hardware in your network. SL1 can monitor any device on your network, even if your organization uses a geographically diverse network. For each managed device, you can monitor status, create policies, define thresholds, and receive notifications (among other features). Some of the devices that SL1 can monitor are:

- Bridges
- Copiers
- Firewalls
- Load Balancers
- Modems
- PDU Systems
- Probes
- Printers
- Routers
- Security Devices
- Servers
- Switches
- Telephony
- Terminals
- Traffic shapers
- UPS Systems
- Workstations

In SL1, devices also include component devices and virtual devices.

What is a Device Record?

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, for example, servers, switches, routers, printers, etc.
- A component of a larger system, for example, a data store in a hypervisor system, a blade server, etc.
- Any other entity about which you want to collect data, but want or need to associate that data with a container that does not correspond directly to a physical device or a component. For example, you might configure a device record that represents a web site or a cloud service.

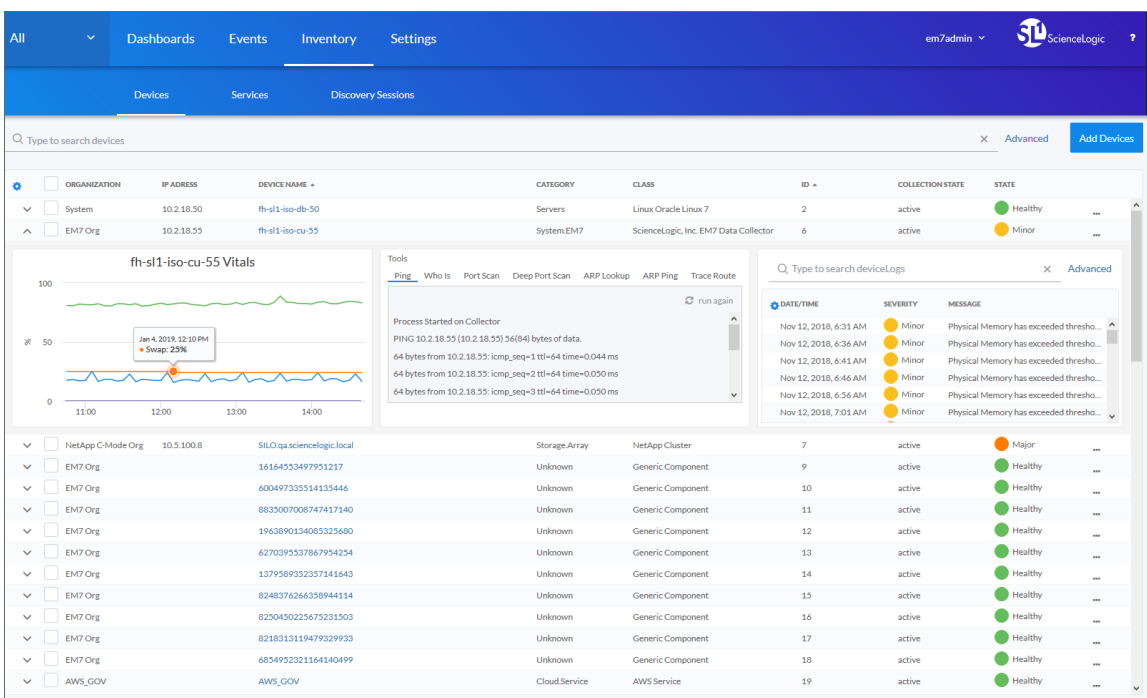
Searching for Devices

To locate a device, click the **[Inventory]** tab and then click the **[Devices]** tab. Type the name of the device or other search terms into the **Search** field at the top of the list. For more information, see [Using Basic Search](#).

TIP: To use the Advanced Search, click the **Advanced** link to the right of the **Search** field and use custom search commands to locate devices. For more information, see [Using Advanced Search](#).

Working with Devices


The **[Devices]** tab (Inventory > Devices) allows you to view all of your managed devices in SL1. This section explains how to gather more information about a device.

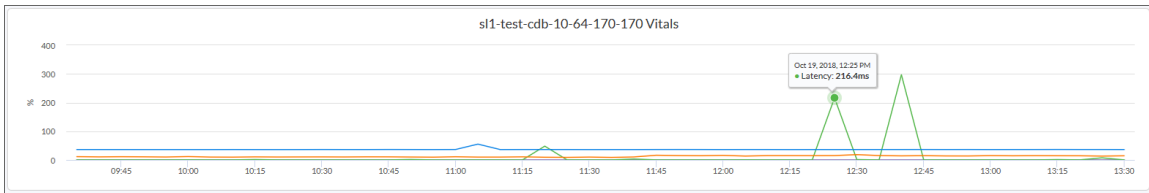


Adding Devices

On the **[Devices]** tab (Inventory > Devices), you can use the process called **discovery** to add more devices to the new user interface for monitoring. For more information, see [Discovery and Credentials](#).

Learning More about Devices

On the **[Devices]** tab, you can click the **Expand** icon () next to a device name to open a drop-down panel called the **Device Drawer**. The **Device Drawer** contains additional data about that device:



The Device Drawer contains the **Vitals** widget, which displays 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 by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.

TIP: From the list of devices, click the device name to go to the [Device Investigator](#) page for more details about that device.

Using the Device Investigator

The **Device Investigator** page (Inventory > Devices, select a device) provides access to all the data associated with a device. The tabs on the **Device Investigator** page are similar to the tabs on the **Device Properties** page in the classic user interface.

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

- **Overview**. This tab displays metrics about a device. For most devices, the default metrics include Logs and the three Vitals: CPU Utilization (percentage), Physical Memory (percentage), and Latency (milliseconds). You can select additional metrics from the **Add a metric** drop-down list. You can also [compare devices](#) on this tab.
- **Device Information**. This tab displays additional information about the device, along with the most recently updated values for uptime and collection time.
- **Device Interfaces**. This tab displays information about the interfaces used by the device. If this device does not use interfaces, this tab does not appear on the **Device Investigator** page.
- **Configs**. This tab displays configuration information collected from the device by Dynamic Applications.
- **Events**. This tab displays a list of events for the device. You can acknowledge events from this tab and add event notes.
- **Collections**. This tab displays a list of all Dynamic Applications aligned with a device.

TIP: You can use the **Time span filter** to adjust the time span that appears in all the metrics on the **Device Investigator** page. The default filter is *Last 24 Hours*, but you can select a time span of Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 3 Days, Last 5 Days, and Last 7 Days.

Adding Metrics to the Overview Tab

The **[Overview]** tab of the **Device Investigator** page displays a customizable set of metrics about the selected device. Each metric controls a list of logs or a widget in the right-hand pane of the page.

The screenshot shows the ScienceLogic Device Investigator interface. The top navigation bar includes 'All', 'Dashboards', 'Events', 'Inventory', and 'Settings'. The user is logged in as 'em7admin'. The selected device is 'sl1-test-cdb-10-64-170-170' with IP '10.64.170.170'. The 'Overview' tab is active, showing a 'Device List' on the left and a main content area with a 'Logs' widget and a 'Vitals: CPU Utilization (%)' widget.

Device List:

- sl1-test-cdb-10-64-170-170

Vitals:

- ☒ Logs
- ☒ CPU Utilization (%)
- ☒ Physical Memory Utilization (%)
- ☒ Latency (s)

Logs (71 logs):

DEVICE NAME	DATE/TIME	SOURCE	EVENT ID	SEVERITY	MESSAGE
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 1:36 P	Dynamic	11757	Major	DRBD: This node is not UpToDate
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 12:45	Internal	11945	Healthy	Network Latency below threshold
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 12:44	Internal	—		Completed filesystem inventory
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 12:41	Dynamic	11757	Major	DRBD: This node is not UpToDate
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 12:40	Internal	11944	Minor	Network latency exceeded threshold: 297.09 ms.
sl1-test-cdb-10-64-170-170	Oct 19, 2018, 12:36	Dynamic	11757	Major	DRBD: This node is not UpToDate

Vitals: CPU Utilization (%)

100

The list of metrics that appears in the **Device List** pane depends on the type of device. For most devices, the following metrics appear by default:

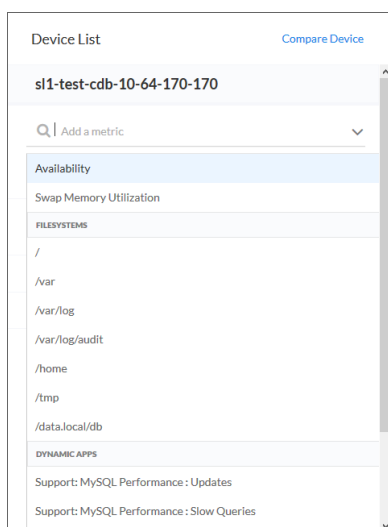
- **Logs**. Displays a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting.

TIP: Click an **Event ID** value in the **Logs** pane to go to the [Event Investigator](#) page for that event.

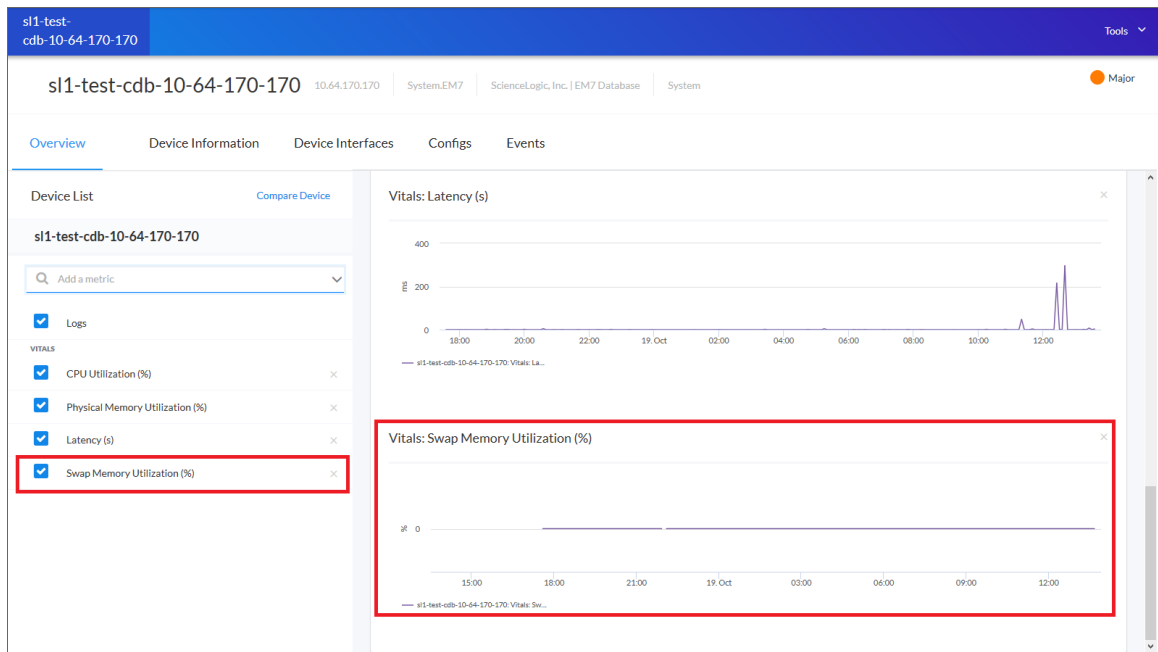
- **CPU Utilization**. Displays a widget for the total amount of CPU used over time, as a percentage of all available CPU.
- **Physical Memory Utilization**. Displays a widget for the physical memory usage over time, in percent.
- **Latency**. Displays a widget for latency for the device over time, in milliseconds. Latency means the amount of time it takes SL1 to communicate with the device.

To add and remove metrics from the **[Overview]** tab :

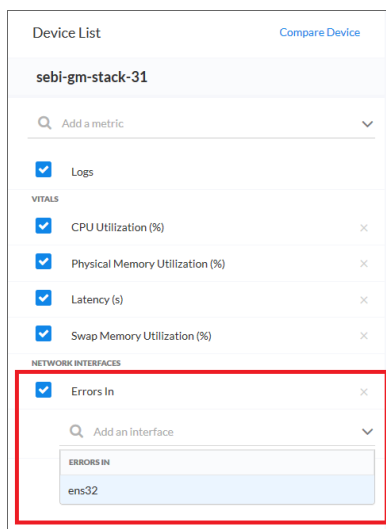
1. To add a metric that is not currently in the **Device List** pane, click the **Add a metric** field. A list of metrics appears:





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 **Device List** pane, and a corresponding widget appears in the right-hand 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.

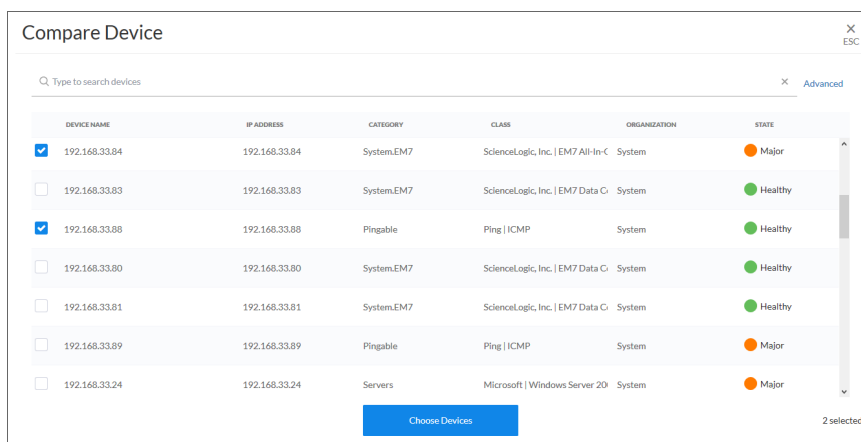
- To remove the widget for a metric from the right-hand pane, click the check mark icon () or the metric name. The metric remains in the **Device List** pane, but the widget is removed from the right-hand pane.
- To completely remove the metric and the widget from the **[Overview]** tab, click the **[Clear]** button () for that metric in the **Device List** pane.

Comparing Devices

On the **[Overview]** tab of the **Device Investigator** page, you can compare the metrics of the current device to the metrics of one or two other devices.

To compare devices:

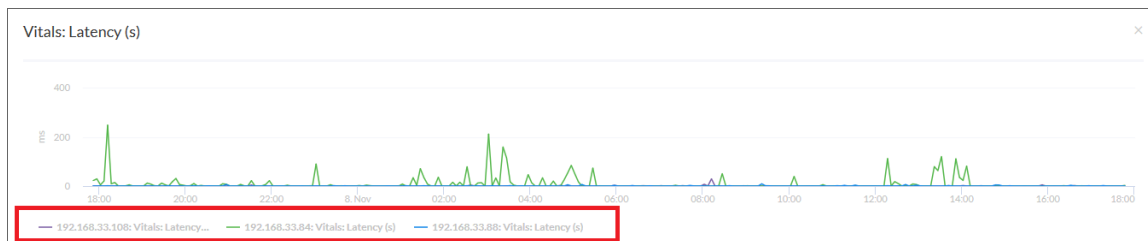
- On the **[Overview]** tab of the **Device Investigator** page, click the **[Compare Device]** button. The **Compare Device** modal page appears:




- Select up to two additional devices from the list and then click the **[Choose Devices]** button.

TIP: You can also search for a device by typing a device name or other search terms in the **Search** field at the top of the list of devices.

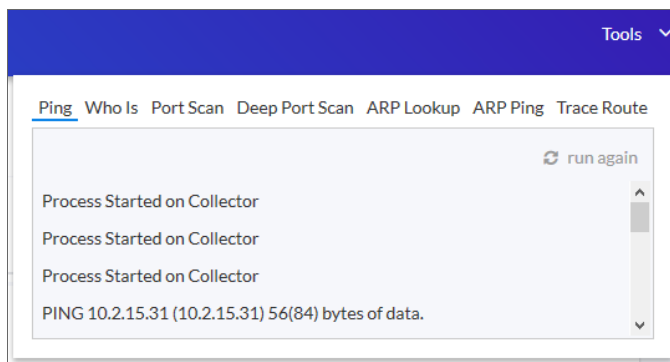
- The selected devices are added to the Device List on the **[Overview]** tab, using the same set of metrics that the current device is using. In the right-hand pane, each widget displays the data from all of the devices:



4. To remove a device from a graph, click the device name in the legend on the x-axis of the graph. You can click the device name again to add the device back to the graph.
5. To add more metrics, click the **Add a metric** field under each device and select the metrics.
6. To remove a device from the Device List, click the **[Clear]** button () at the end of the device name.

Using Device Tools

On the **Device Investigator** page for a device, you can click the **Tools** menu to display the **Tools** panel. The **Tools** panel provides access to a set of network tools. The **Tools** panel lets you to run diagnostics on a device without leaving the the new user interface.



TIP: These tools are the same tools in the Device Toolbox found in the classic user interface.

You can access the following tools from the **Device Investigator** page for a 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.
- **Whols**. 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.

Viewing the Device Information Tab

On the **[Device Information]** tab of the **Device Investigator** page, you can view read-only information about the device.

The screenshot shows the 'Device Information' tab for a device named 'sl1-test-cdb-10-64-170-170'. The interface includes a top navigation bar with the device name and IP address, and a sidebar with tabs for Overview, Device Information (selected), Device Interfaces, Configs, and Events. The main content area displays two sections: 'Basic' and 'Collection'. The 'Basic' section contains a table with device details, and the 'Collection' section contains a table with collection status and time.

sl1-test-cdb-10-64-170-170			
DEVICE NAME	MANAGED TYPE	IP ADDRESS	ID
sl1-test-cdb-10-64-170-170	Physical Device	10.64.170.170	101
CATEGORY	CLASS	SUB-CLASS	ORGANIZATION
System.EM7	ScienceLogic, Inc.	EM7 Database	System

Collection		
UPTIME	COLLECTION STATE	COLLECTION TIME
	Active	—

The **Basic** and **Collection** sections display the following for a device:

- **Device Name.** Name of the device.
- **Managed Type.** Specifies the protocol used to discover the device and whether or not the device is a physical device or a virtual device.
- **IP Address.** IP address of the device.
- **ID.** Unique ID assigned to the device by SL1.
- **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".
- **Class.** Device class for the device. A **device class** usually describes the manufacturer of the device.
- **Organization.** The organization to which this device belongs.
- **Sub-Class.** The sub-class associated with the device, which usually describes the model of a device.
- **Uptime.** The number of days, hours, minutes, and seconds that the device has been continuously up and communicating with SL1.
- **Collection State.** Collection mode. The states include "active", meaning SL1 is periodically collecting data from the device, or "inactive", meaning the SL1 is not currently collecting data from the device.
- **Collection Time.** The date and time that SL1 last collected data from the device.

Viewing the Device Interfaces Tab

On the **[Device Interfaces]** tab of the **Device Investigator** page, 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.

SAC-ISO3-DB-9-56-60061 10.140.234.188 Network Router Cisco Systems 12410 GSR System Tools Minor														
SAC-ISO3-DB-9-56-60061 10.140.234.188 Network Router Cisco Systems 12410 GSR System Tools Minor														
Overview Device Information Device Interfaces Configs Events														
INTERFACE NAME	ALIAS	PORT	HARDWARE DESCRIPTION	MAC ADDRESS	CONNECTION SPEED	COLLECTION STATE	ADMIN STATUS	OPERATIONAL STATE	COLLECTION RATE	COLLECT ERROR	COLLECT DISCARD	ALERTS	ROLLOVER ALERT	INTERFACE INDEX
E10	ID:0000000000...	1	Ethernet0	00:0f:fb:01:ea:9d	10	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	1
E11	ID:0000000000...	2	Ethernet1	00:0f:fb:02:ea:9d	10	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	2
Gi0/0	ID:0000000000...	3	GigabitEthernet...	00:0f:fb:03:ea:9d	1000	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	3
Gi0/1	RLTBCKB; GE...	4	GigabitEthernet...	00:0f:fb:04:ea:9d	1000	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	4
Gi0/2	RLTBCKB; PEE...	5	GigabitEthernet...	00:0f:fb:05:ea:9d	1000	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	5
Gi0/3	ID:0000000000...	6	GigabitEthernet...	00:0f:fb:06:ea:9d	1000	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	6
Se5/0	RLBMFF; CID...	11	Serial5/0		45	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	11
Se5/1	CID:42:HFGN.6...	12	Serial5/1		45	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	12
Se5/2	CID:42:HFGN.6...	13	Serial5/2		45	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	13
Se5/3	CID:42:HFGN.6...	14	Serial5/3		45	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	14
Se5/4	ID:0000000000...	15	Serial5/4		44	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	15
Se5/5	RLBMFF; CID...	16	Serial5/5		45	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	16
CT6/0		17	CT3 6/0		2	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	17
CT6/1		18	CT3 6/1		2	Disabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	18
CT6/2		19	CT3 6/2		2	Disabled	Up	Up	5	Disabled	Disabled	Enabled	Disabled	19

The data displayed on this tab is read-only. Also, if this device does not use interfaces, this tab does not appear on the **Device Investigator** page.

The **Device Interfaces** tab displays the following for every interface used by a device:

- **Interface Name.** The name of the network interface.
- **Alias.** The name assigned by SL1 to the interface.
- **Port.** Port of the interface.
- **Hardware Description.** Description of the network interface. Usually a description of a network-interface card.
- **MAC Address.** Short for Media Access Control Address. A unique number that identifies the interface. MAC Addresses are defined by the hardware manufacturer.
- **Connection Speed.** The amount of data per second that can pass through the network interface.
- **Collection State.** Specifies whether the platform monitors the network interface and collects data from the network interface for reports. Can be either *Disabled* or *Enabled*.

- **Admin Status.** Specifies how the network interface has been configured on the device. Can be one of the following:
 - *Up.* Network interface has been configured to be up and running.
 - *Down.* Network interface has been purposefully disabled.
- **Operational Status.** Specifies current state of the network interface. Can be one of the following:
 - *Up.* Network interface is transmitting and receiving data.
 - *Down.* Network interface cannot transmit and receive data.
- **Collection Rate.** Specifies how often SL1 collects data from the interface, in minutes.
- **Collect Errors.** Specifies whether SL1 will collect data on packet errors on the interface. Packet errors occur when packets are lost due to hardware problems such as breaks in the network or faulty adapter hardware.
- **Collect Discards.** Specifies whether SL1 will collect data on interface discards. Discards occur when an interface receives more traffic than it can handle (either a very large message or many messages simultaneously). Discards can also occur when an interface has been specifically configured to discard. For example, a user might configure a router's interface to discard packets from a non-authorized IP address.
- **Alerts.** Specifies whether SL1 will generate events for the interface. When disabled, the interface is monitored, but events are not generated for the interface.
- **Rollover Alerts.** Specifies whether SL1 will generate an event when the counter for the interface rolls over.
- **Interface Index.** A unique number greater than zero that identifies each interface on a device. These numbers are defined by the device.

Viewing the Configs Tab

On the **[Configs]** tab of the **Device Investigator** page, 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.

The screenshot shows the 'Configs' tab in the Device Investigator interface. The left sidebar lists dynamic applications, with 'Cisco IPSLA Configuration' selected. The main panel displays configuration data for 'Cisco IPSLA Configuration' and 'Cisco IPSLA Supported Configuration'.

Cisco IPSLA Configuration - IPSLA Configuration

PROBE CAPACITY	FREE MEM/LOW WATERMARK	LATEST SET ERROR	MAX PACKET DATABSIZE	MAX ADMIN ENTRY	RESPONDER STATUS	TIME OF LAST SET	APPLICATION VERSION
0	23816559		16384	500	Disabled	0 days, 0:1:9	2.1.1 Round Trip Time



Cisco IPSLA Configuration - IPSLA Supported Configuration



SUPPORTED PROTOCOLS	SUPPORTED PROTOCOLS VALID	SUPPORTED RTT TYPES	SUPPORTED RTT TYPES VALID
	1		1
	1		2
	1		2

The pane on the left displays a list of Dynamic Applications associated with the device. To view the configuration data collected by a Dynamic Application, select it from the **Dynamic Apps** section on the left.



The data displayed on this tab is read-only.

Viewing the Events Tab

On the **[Events]** tab of the **Device Investigator** page, you can view a list of events for the device. You can view the events in the **List View** () or the **Card View** ().

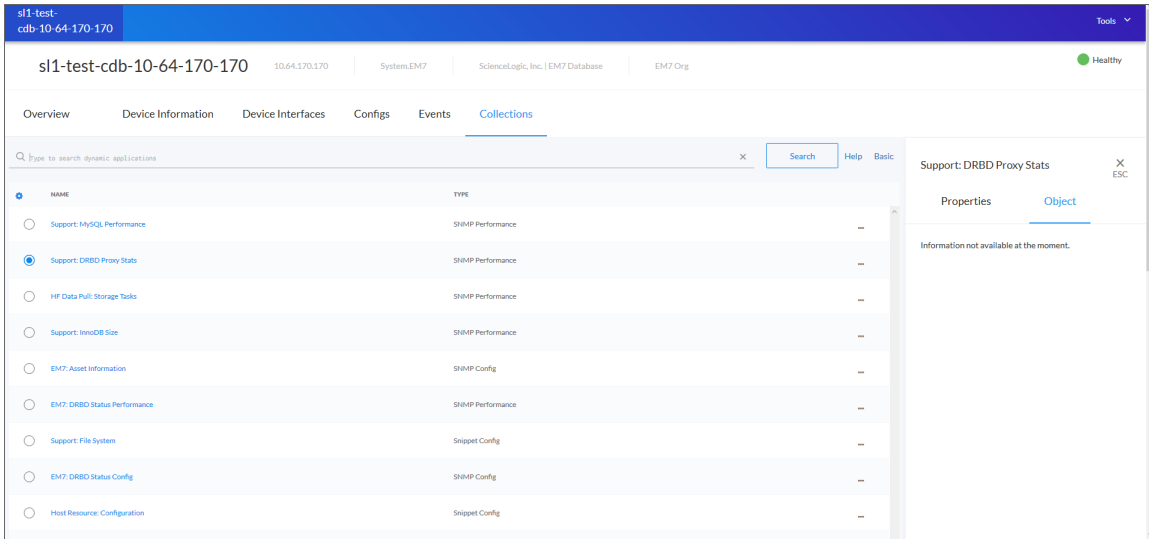
SEVERITY	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	ACKNOWLEDGE	CLEAR
<input type="checkbox"/> Major	DRBD: This node is not UpToDate	20 hours 51 minutes		248		<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear
<input type="checkbox"/> Healthy	Network Latency below threshold	10 minutes 45 seconds		1		<input checked="" type="checkbox"/> Acknowledge	<input checked="" type="checkbox"/> Clear


On this tab you can acknowledge and clear an event. You can also update an event note.

TIP: To view the **Event Investigator** page for an event on this tab, click the **Options** button () for that event and select **View Event**. This option is only available in the **List View** ().

Viewing the Collections Tab

On the **[Collections]** tab of the **Device Investigator** page, you can view a list of all Dynamic Applications aligned with a device. Select a Dynamic Application from the list to view details about that Dynamic Application and what it collects from the device.



Click the **Options** button () to edit, run, or delete a collection on this tab.

Assigning Icons to Device Classes

Each device in SL1 is associated with a **device class**. Typically, device classes map to a make/model pair, such as *Product Name / Model Number*. SL1 includes already-defined device classes for the most popular hardware. When possible, SL1 automatically assigns each discovered device to an existing device class.

Device classes determine:

- How devices are represented in the user interface.
- Whether the device is a physical device or a virtual device.
- How managed devices are discovered with the discovery tool.

On the **[Device Classes]** tab (Settings > Device Classes), you can view a list of existing device classes in the new user interface.

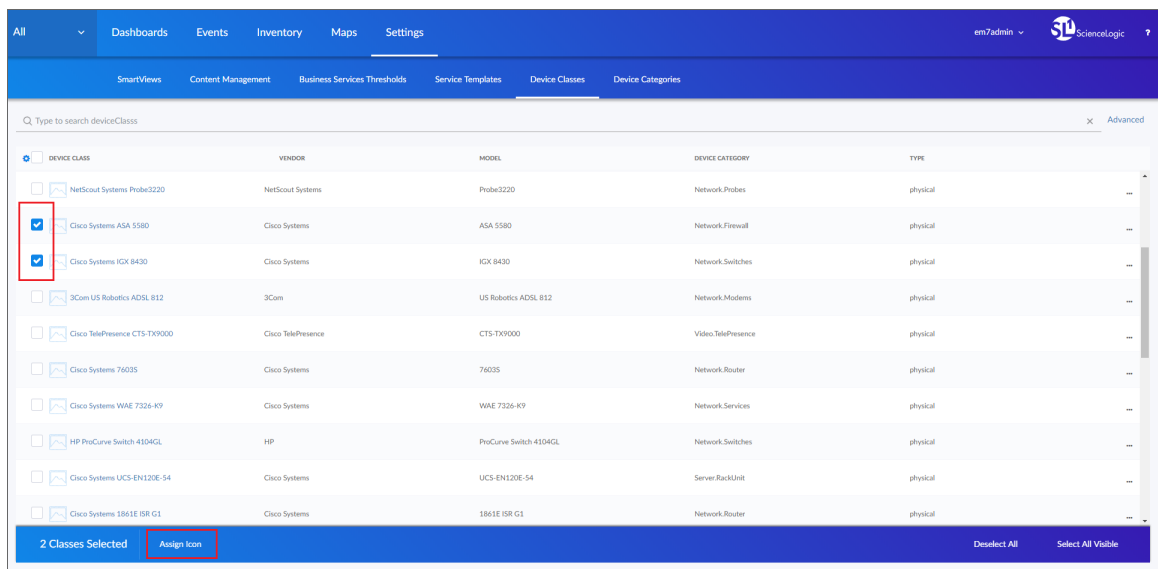
You can also assign an icon to a specific device class. These icons will appear on Device Class and Device Category pages.

DEVICE CLASS	TYPE	DEVICE CATEGORY	MODEL	VENDOR
NetScout Systems Probe3220	physical	Network Probes	Probe3220	NetScout Systems
Cisco Systems ASA 5580	physical	Network Firewall	ASA 5580	Cisco Systems
Cisco Systems IGS 8430	physical	Network Switches	IGS 8430	Cisco Systems
3Com US Robotics ADSL 812	physical	Network Modems	US Robotics ADSL 812	3Com
Cisco TelePresence CTS-TX9000	physical	Video TelePresence	CTS-TX9000	Cisco TelePresence
Cisco Systems 7603S	physical	Network Router	7603S	Cisco Systems
Cisco Systems VME 7326-K9	physical	Network Services	VME 7326-K9	Cisco Systems
HP ProCurve Switch 4104GL	physical	Network Switches	ProCurve Switch 4104GL	HP
Cisco Systems UCS-EH130E-54	physical	Server Rack Unit	UCS-EH130E-54	Cisco Systems
Cisco Systems 1861E ISR G1	physical	Network Router	1861E ISR G1	Cisco Systems
Cisco Systems Probe3704	physical	Network Probes	Probe3704	Cisco Systems
Cisco Systems OH5-13301-DC	physical	Network Repeaters	OH5-13301-DC	Cisco Systems

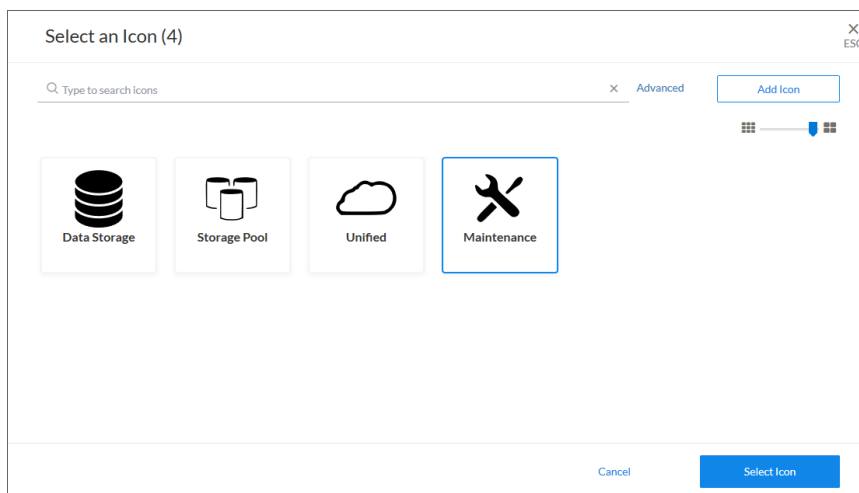
TIP: Click the **Choose Columns** icon () to enable the **Vendor** and **Model** columns.

To assign an icon to a device class:

1. On the **[Device Classes]** tab (Settings > Device Classes), locate the device class for which you want to add an icon.
2. Click the **Options** button (⋮) for that device class and select *Assign Icon*. If you want to assign an icon to more than one device class at once, select the checkboxes next to those device classes and click **Assign Icon** in the blue bar at the bottom of the screen:



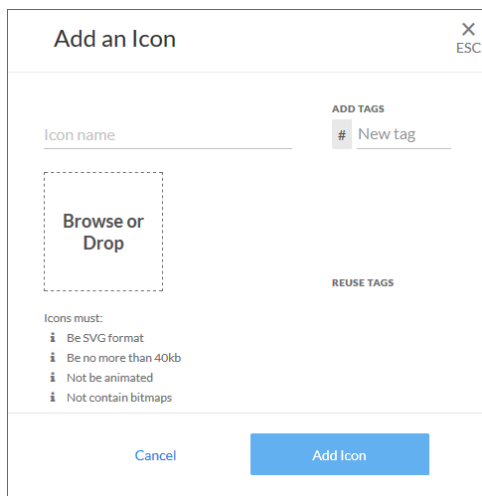
The **Select an Icon** window appears:



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 device class on the **[Device Classes]** tab.

Working with Device Categories

A **device category** is a logical categorization of a device based on the primary function of the device, such as a "server", "switch", or "router". SL1 uses device categories to group related devices in reports and views.

Device categories are paired with device classes to organize and describe discovered devices. The device class usually describes the manufacturer. The device category describes the function of the hardware. Each device class can include a device category.

On the **[Device Categories]** tab (Settings > Device Categories), you can view a list of existing device categories and create new device categories. You can also assign an icon to a specific device category, and those icons will appear on Device Class and Device Category pages.

All			em7admin	SLU Sciencelogic
Dashboards Events Inventory Settings				
SmartViews Content Management Business Services Thresholds Service Templates Device Classes Device Categories				
Type to search deviceCategory X Advanced Create Device Category				
CATEGORY NAME	LAST EDITED BY	LAST EDITED		
Cloud.AppService	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.AvailabilityZone	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.BigData	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Compute	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Database	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.IaaS	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Location	em7admin	Oct 1, 2018, 7:38 PM		
Cloud.Network	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Region	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Service	em7admin	Oct 1, 2018, 7:39 PM		
Cloud.Storage	em7admin	Oct 1, 2018, 7:39 PM		
Environmental.CATV	em7admin	Oct 1, 2018, 7:39 PM		

To create a new device category:

- On the **[Device Categories]** tab (Settings > Device Categories), click the **[Create Device Category]** button. The **Add New Category** window appears:

Add new Category X ESC

Category Name

EDIT USER

ICON

EDIT DATE

Browse


Save Category

2. In the **Category Name** field, type a name for the new device category.
3. To add an icon for the new category, click the **Browse** area to select an existing icon from the **Select an Icon** window.

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. On the **Add New Category** window, click the **[Save Category]** button. The category is added to the **[Device Categories]** tab.

To assign an icon to an existing device category:

1. On the **[Device Categories]** tab (Settings > Device Categories), locate the device category for which you want to add an icon.
2. Click the **Options** button () for that device category and select *Assign Icon*. If you want to assign an icon to more than one device class at once, select the checkboxes next to those device classes and click **Assign Icon** in the blue bar at the bottom of the screen. The **Select an Icon** window appears.
3. To use an existing icon, select that icon from the list of icons and click the **[Select Icon]** button.
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 to search for this icon 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 device class on the **[Device Categories]** tab.

Chapter 7

Discovery and Credentials

Overview

This chapter describes how to use the new user interface for SL1 to discover the devices in your network.

The following topics describe how to discover devices on the **[Devices]** tab and how to manage discoveries on the **[Discovery Sessions]** tab:

<i>What is Discovery?</i>	95
<i>What are Credentials?</i>	95
<i>Prerequisites for Discovering Devices in the New User Interface</i>	96
<i>Discovering Devices</i>	96
<i>Working with Discovery Sessions</i>	104



What is Discovery?

Discovery is the tool that automatically finds all the hardware-based devices, hardware components, and software applications in your network. You must provide the discovery tool with a range or list of IP addresses or a list of fully-qualified domain names (hostnames), and the discovery tool determines if a device, hardware component, or software application exists at each IP address.

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.

The discovery tool also determines which, if any, Dynamic Applications to align with the device. If the discovery tool finds Dynamic Applications to align with the device, the discovery tool triggers collection for each aligned Dynamic Application.

SL1 also uses discovery to update existing information about a device and to add to existing information about a device. This type of discovery is called auto-discovery. For each existing device, SL1 automatically runs auto-discovery every night, to keep device data up-to-date.

You can manually trigger discovery at any time and update the data for one device or multiple devices.

What are Credentials?

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.
- Dynamic Applications use credentials to retrieve SNMP information, database information, SOAP information, XML information, XSLT information, and WMI information.
- Proxied Web Services use SOAP/XML Host credentials to pass authentication information to external web services.
- SL1 includes a type of credential called "Basic/Snippet" that is not bound to a specific authentication protocol. You can use this type of credential for Dynamic Applications of type "WMI", of type "snippet", and when defining system backups. "Basic/Snippet" credentials can also be used for monitoring Windows devices using PowerShell.
- SL1 includes a type of credential that allows SL1 to communicate with an LDAP or Active Directory system. For details on integrating the platform with LDAP or Active Directory, see the manual **Using Active Directory and LDAP**.
- SL1 includes a type of credential that allows Dynamic Applications of type "Snippet" to use SSH to communicate with a remote device. To use these Dynamic Applications, you must define an SSH credential.

- SL1 includes a type of credential that allows Dynamic Applications to retrieve data from Windows devices. If you align a Dynamic Application for PowerShell with a PowerShell credential, SL1 assumes that you want to use its built-in agentless transport to communicate with Windows devices.
- If necessary, a single device can use multiple credentials. If more than one agent or application is running on the device, each agent or application can be associated with its own credential. During discovery, SL1 will use the appropriate credential for each agent.

Prerequisites for Discovering Devices in the New User Interface

To discover all of the devices on your network:

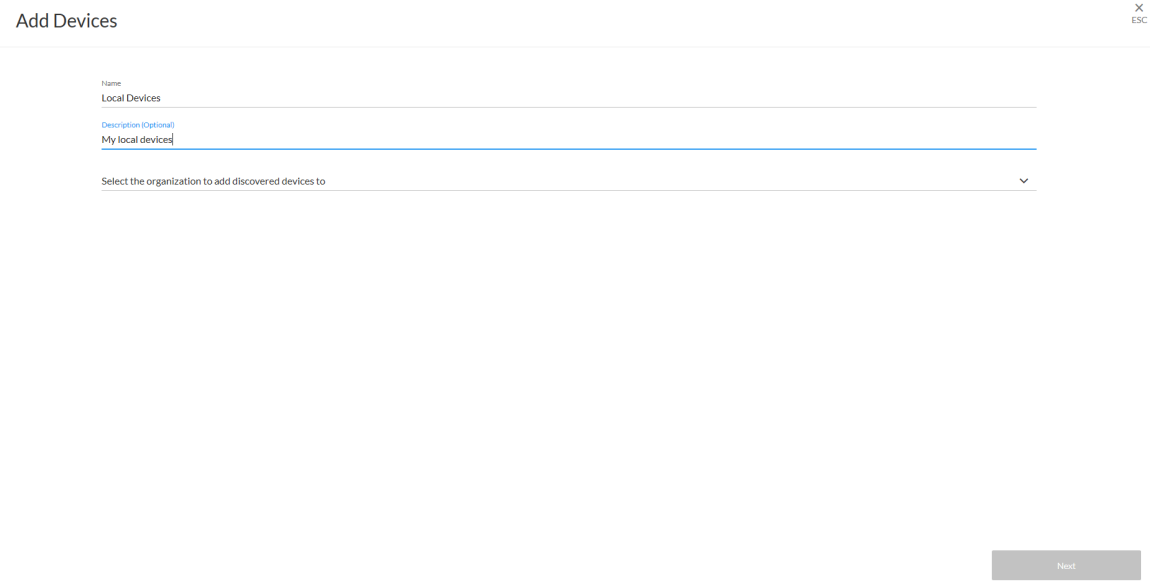
1. Make a note of the range of IP addresses used on your network. If you need help, ask your network administrator.
2. For this release, you must use an existing collector in the classic user interface. You can access collector information on the **Collector Group Management** page (System > Settings > Collector Groups).
3. Also for this release, you must create or use an existing credential in the classic user interface. You can access credential information on the **Credential Management** page (System > Manage > Credentials).
4. Similarly, if you want to use a device template with a discovery session, you must use an existing template in the classic user interface. You can access device templates on the **Configuration Templates** page (Registry > Devices > Templates).
5. In the classic user interface, the Grant All user needs to be used to access new discovery workflow, as the SYS_SETTINGS_LICENSES_PAGE and SYS_SETTINGS_CUGS_PAGE access keys are needed to get collector or collector group information.

Discovering Devices

On the **[Devices]** tab (Inventory > Devices) you can add or "discover" new devices for monitoring in the new user interface. You add devices by creating a **discovery session**, which searches for the devices on the network you specify.

To run discovery to add one or more devices:

1. On the **[Devices]** tab, click the **[Add Devices]** button. The first page of the **Add Devices** wizard appears:



The screenshot shows a web form titled "Add Devices" with a close button (X) and an escape key indicator (ESC) in the top right corner. The form contains three input fields: "Name" with the text "Local Devices", "Description (Optional)" with the text "My local devices", and a dropdown menu labeled "Select the organization to add discovered devices to". A "Next" button is located at the bottom right of the form.

2. Complete the following fields:

- **Name**. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab
- **Description**. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab. Optional.
- **Select the organization to add discovered devices to**. Select the name of the organization to which you want to add the discovered devices.

3. Click **[Next]**. The Credentials page of the **Add Devices** wizard appears:

NAME	CREDENTIAL USER	TYPE	UPDATED BY	LAST EDIT
<input checked="" type="checkbox"/> EM7 Default V3	em7defaultv3	SNMP	em7admin	Jun 8, 2018, 4:21 PM
<input checked="" type="checkbox"/> SNMP Public V1		SNMP	em7admin	Jun 8, 2018, 4:21 PM
<input checked="" type="checkbox"/> SNMP Public V2		SNMP	em7admin	Jun 8, 2018, 4:21 PM
<input type="checkbox"/> Cisco SNMPv3 - Example	[USER_GOES_HERE]	SNMP	em7admin	Jun 8, 2018, 4:20 PM
<input type="checkbox"/> Cisco SNMPv2 - Example		SNMP	em7admin	Jun 8, 2018, 4:20 PM
<input type="checkbox"/> Lifeline: Endpoint SNMP	control	SNMP	em7admin	Jun 8, 2018, 4:13 PM
<input type="checkbox"/> Dell EMC: Isilon SNMPv2 Example		SNMP	em7admin	Jun 8, 2018, 4:18 PM
<input type="checkbox"/> simu_device_200		SNMP	em7admin	Jun 14, 2018, 4:14 PM
<input type="checkbox"/> simu_device_300		SNMP	em7admin	Jun 14, 2018, 4:14 PM
<input type="checkbox"/> IPSLA Example		SNMP	em7admin	Jun 8, 2018, 4:21 PM
<input type="checkbox"/> EM7 Default V2		SNMP	em7admin	Jun 8, 2018, 4:21 PM

4. Select one or more SNMP credentials to allow SL1 to access a device's SNMP data and click **[Next]**. The Discovery Session Details page of the **Add Devices** wizard appears:

Enter basic discovery session details

List of IP's *

192.0.2.0/24

Which collector will monitor these devices?

CUG-Core | SAC-PATCH-CU2-9-28: 10.2.9.28

Run after save

Advanced options

5. Complete the following fields:

- **List of IPs.** Provide a list of IP addresses or fully-qualified domain names for SL1 to scan during discovery. This field is required. In this field, you can enter a combination of one or more of the following:
 - One or more *single IPv4 addresses* separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
 - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
 - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
 - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0:0003".
 - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
 - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.
- **Which collector will monitor these devices?** Select an existing collector to monitor the discovered devices. Required.
- **Run after save.** Select this option to run this discovery session as soon as you click [Save and Close].
- **Advanced options.** Click the down arrow icon (▼) to access additional discovery options.

The screenshot shows a web-based configuration window titled "Add Devices" with a close button (X) and an escape key indicator (ESC) in the top right corner. The window contains a section for "Advanced options" which is currently collapsed, indicated by a right-pointing arrow. Below this section, several configuration fields are visible:

- Initial Scan Level:** A dropdown menu currently set to "6. Deep discovery".
- Scan Throttle:** A dropdown menu currently set to "[System Default (recommended)]".
- Port Scan All IPs:** A dropdown menu currently set to "[System Default (recommended)]".
- Port Scan Timeout:** A dropdown menu currently set to "[System Default (recommended)]".
- Scan Ports:** A text input field containing "21:22:25:80:136".
- Interface Inventory Timeout (ms):** A text input field containing "600000".
- Maximum Allowed Interfaces:** A text input field containing "10000".
- Bypass Interface Inventory:** A toggle switch currently in the "off" position.
- Discover non-SNMP:** A toggle switch currently in the "off" position.

At the bottom left of the window is a "← Back" button, and at the bottom right is a blue "Save and Close" button. A vertical scrollbar is visible on the right side of the configuration area.

In the **Advanced options** section, complete the following fields as needed:

- **Initial Scan Level.** For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
 - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface of SL1.
 - *1. Model Device Only.* Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
 - *2. Initial Population of Apps.* Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform *1. Model Device Only* discovery.
 - *3. Discover SSL Certificates.* Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform *2. Initial Population of Apps* and *1. Model Device Only*.
 - *4. Discover Open Ports.* Discovery will search for open ports. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *4. Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

- *5. Advanced Port Discovery.* Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: If your system includes a firewall and you select *5. Advanced Port Discovery*, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

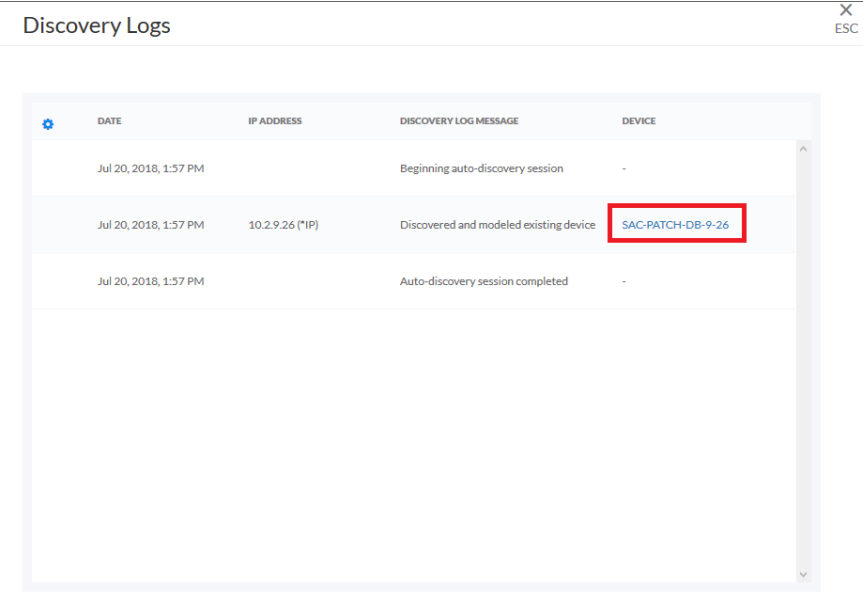
- *6. Deep Discovery.* Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, and *1. Model Device Only*.

NOTE: For devices that don't support SNMP, option *6. Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option *6. Deep Discovery* is compute-intensive.

- **Scan Throttle.** Specifies the amount of time a discovery process should pause between each specified IP address (specified in the **IP Address/Hostname Discovery List** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
 - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
 - *Disabled.* Discovery processes will not pause.
 - *1000 Msec to 10000 Msec.* A discovery process will pause for a random amount of time between half the selected value and the selected value.
- **Port Scan All IPs.** For the initial discovery session only, specifies whether the platform should scan all IP addresses on a device for open ports. The choices are:
 - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
 - *Enabled.* The platform will scan all discovered IP addresses for open ports.
 - *Disabled.* The platform will scan only the primary IP address (the one used to communicate with the platform) for open ports.
- **Port Scan Timeout.** For the initial discovery session only, specifies the length of time, in milliseconds, after which the platform should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
 - *System Default (recommended).* Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
 - Choices between 60 to 1,800 seconds.
- **Scan Ports.** Specify a list of ports to scan, separated by commas. The default is 21,22,25,80,136.
- **Interface Inventory Timeout (ms).** Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, the ScienceLogic platform will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
 - During the execution of this discovery session, the ScienceLogic platform uses the value in this field first. If you delete the default values and do not specify another value in this field, the platform uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).
 - If you specify a value in this field and do not apply a device template to this discovery session, the **Interface Inventory Timeout** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, the ScienceLogic platform uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

- **Maximum Allowed Interfaces.** Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, the ScienceLogic platform will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
 - During the execution of this discovery session, the ScienceLogic platform uses the value in this field first. If you delete the default values and do not specify another value in this field, the platform uses the value in the **Global Threshold Settings** page.
 - If you specify a value in this field and do not apply a device template to this discovery session, the **Maximum Allowed Interfaces** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, the ScienceLogic platform uses the value in the **Global Threshold Settings** page.
- **Bypass Interface Inventory.** Specifies whether or not the discovery session should discover network interfaces.
 - *Selected.* The platform will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the **Bypass Interface Inventory** checkbox in the **Device Properties** page will be selected.
 - *Not Selected.* The platform will attempt to discover network interfaces, using the **Interface Inventory Timeout** value and **Maximum Allowed Interfaces** value.
- **Discover Non-SNMP.** Specifies whether or not the platform should discover devices that don't respond to SNMP requests.
 - *Selected.* The platform will discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** field. These devices will be discovered as "pingable" devices.
 - *Not Selected.* The platform will not discover devices that don't respond to the SNMP credentials selected in the **SNMP Credentials** fields.
- **Model Devices.** Determines whether or not the devices that are discovered with this discovery session can be managed through the platform. Choices are:
 - *Enabled.* When a device is modeled, the platform creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in the platform.
 - *Disabled.* If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in the platform. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with the platform. For the amount of time specified in the **Device Model Cache TTL (h)** field, a user can manually model the device from the **Discovery Session** window.

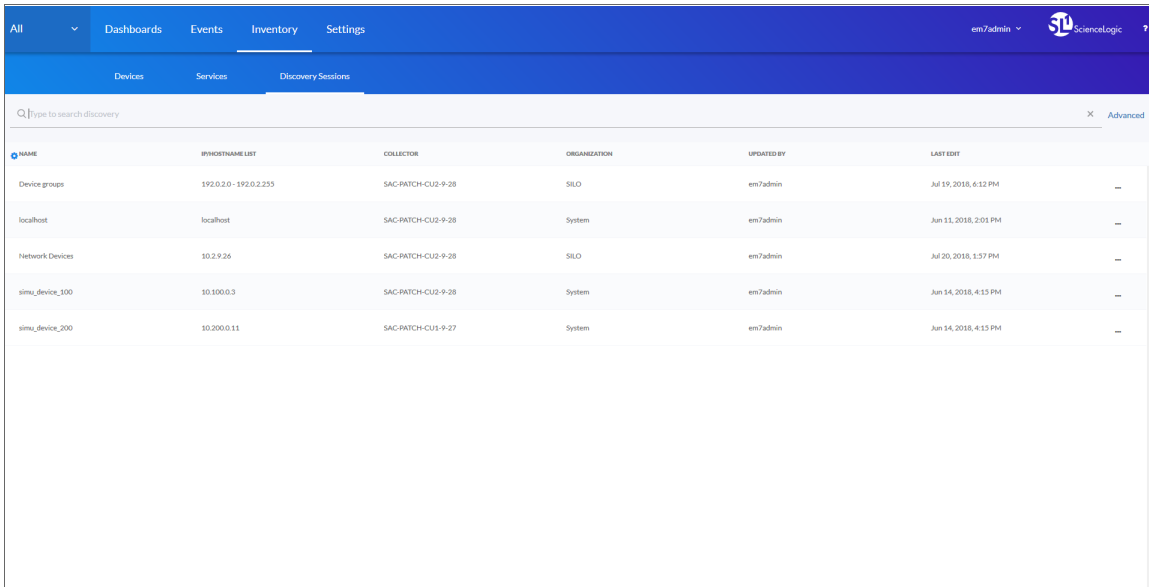
- **Enable DHCP.** Specifies whether or not the specified range of IPs and hostnames use DHCP.
 - **Selected.** The ScienceLogic platform will perform a DNS lookup for the device during discovery and each time the platform retrieves information from the device.
 - **Not Selected.** The ScienceLogic platform will perform normal discovery.
 - **Device Model Cache TTL (h).** Amount of time, in hours, that the platform stores information about devices that are discovered but not modeled, either because the **Model Devices** option is not enabled or because the platform cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
 - **Log All.** Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, the platform logs details about each IP address or hostname specified in the **IP Address/Hostname Discovery List** field, even if the results are "No device found at this address."
 - **Selected.** This discovery session will use verbose logging.
 - **Not Selected.** This discovery session will not use verbose logging.
 - **Apply Device Template.** As the platform discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in the platform. For more information on device templates, see the manual on **Device Groups and Device Templates**.
6. Click **[Save and Close]** to save the discovery session. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device:



DATE	IP ADDRESS	DISCOVERY LOG MESSAGE	DEVICE
Jul 20, 2018, 1:57 PM		Beginning auto-discovery session	-
Jul 20, 2018, 1:57 PM	10.2.9.26 (*IP)	Discovered and modeled existing device	SAC-PATCH-DB-9-26
Jul 20, 2018, 1:57 PM		Auto-discovery session completed	-

Working with Discovery Sessions

The **[Discovery Sessions]** tab (Inventory > Discovery Sessions) displays a list of all the existing **discovery sessions**, which are previous attempts to add devices using discovery:



NAME	IP/hostname LIST	COLLECTOR	ORGANIZATION	UPDATED BY	LAST EDIT
Device groups	192.0.2.0 - 192.0.2.255	SAC-RATCH-CU2-9-28	SILO	em7admin	Jul 19, 2018, 6:12 PM
localhost	localhost	SAC-RATCH-CU2-9-28	System	em7admin	Jun 11, 2018, 2:01 PM
Network Devices	10.2.9.26	SAC-RATCH-CU2-9-28	SILO	em7admin	Jul 20, 2018, 1:57 PM
simu_device_300	10.100.0.3	SAC-RATCH-CU2-9-28	System	em7admin	Jun 14, 2018, 4:15 PM
simu_device_300	10.200.0.11	SAC-RATCH-CU1-9-27	System	em7admin	Jun 14, 2018, 4:15 PM

NOTE: This tab mirrors the list of sessions on the **Discovery Control Panel** page (System > Manage > Discovery) in the classic user interface.

On this tab you can click the **Options** button () for a session and select one of the following actions:

- **Edit.** Run the **Add Device** wizard again so you can make changes to the selected discovery session.
- **Delete.** Delete the selected discovery session. You do not get a confirmation window after you click *Delete*; the session is immediately deleted.
- **Start.** Run the selected discovery session again. The **Discovery Logs** page appears when discovery completes.
- **Show Logs.** The **Discovery Logs** page for the selected discovery session displays data about the most recent run of a discovery session.

Chapter

8

Monitoring Business Services

Overview

This chapter describes how to use the new user interface for SL1 to create and manage business services for your company.

The following sections describe the features of the **[Services]** tab (Inventory > Services):

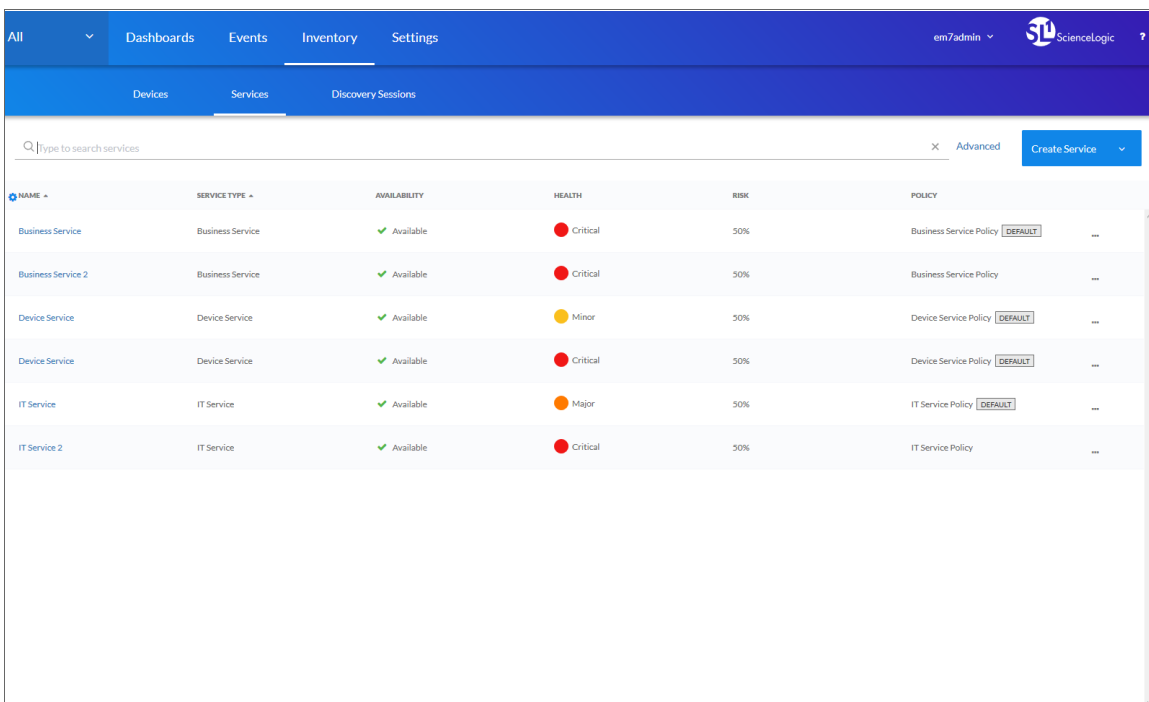
<i>What is a Business Service?</i>	106
<i>Using the Service Investigator</i>	109
<i>Creating a Business Service</i>	110
<i>Assigning Icons to a Business Service</i>	113
<i>Selecting a Business Service Policy</i>	114
<i>Creating a Business Service Policy</i>	116
<i>Creating a Business Service Template</i>	121
<i>Creating a Business Service From a Template</i>	124
<i>Exporting a Service Template</i>	128
<i>Default Service Policy Settings</i>	131
<i>Managing Events for Business Services</i>	132
<i>Exporting Service Data with the ScienceLogic API</i>	133
<i>Troubleshooting Services</i>	135

What is a Business Service?

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.

Create the following types of services on the **[Services]** tab (Inventory > Services), 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.



The screenshot shows the ScienceLogic interface with the 'Inventory' tab selected. The 'Services' sub-tab is active, displaying a table of services. The table has columns for NAME, SERVICE TYPE, AVAILABILITY, HEALTH, RISK, and POLICY. There are six services listed: Business Service, Business Service 2, Device Service, Device Service, IT Service, and IT Service 2. Each service has a corresponding health status icon (green for Available, yellow for Minor, orange for Major, red for Critical) and a risk level of 50%.

NAME	SERVICE TYPE	AVAILABILITY	HEALTH	RISK	POLICY
Business Service	Business Service	Available	Critical	50%	Business Service Policy [DEFAULT]
Business Service 2	Business Service	Available	Critical	50%	Business Service Policy
Device Service	Device Service	Available	Minor	50%	Device Service Policy [DEFAULT]
Device Service	Device Service	Available	Critical	50%	Device Service Policy [DEFAULT]
IT Service	IT Service	Available	Major	50%	IT Service Policy [DEFAULT]
IT Service 2	IT Service	Available	Critical	50%	IT Service Policy

These business services let you gauge the health, availability and risk of your services or the devices that provide those services. On the **[Services]** tab, these values display in the following format and order:

1. **Availability:** Displays whether a device, like a website or a server, is available to be used by customers. A service or device is considered unavailable if SL1 is not able to collect data from the device or service, or if device is usable or not usable. A value of 0 means a device or service is unavailable, and a value of 1 means a device is available. Availability uses the following icons:



2. **Health:** Displays a "severity" icon that represents a numerical value between 0 and 100, which indicates the current status of a device or service to show if its health is worsening or improving. For example, the Health value could indicate when a device is intermittently unavailable because of a power problem and falls below the required level of performance. Health uses the following icons by default:



3. **Risk:** Displays a percentage value between 0 and 100 that indicates how close a service or a device is to being in an undesirable state. The safest possible risk value is 0%, while the worst risk value is 100%. Risk uses the following icons by default:



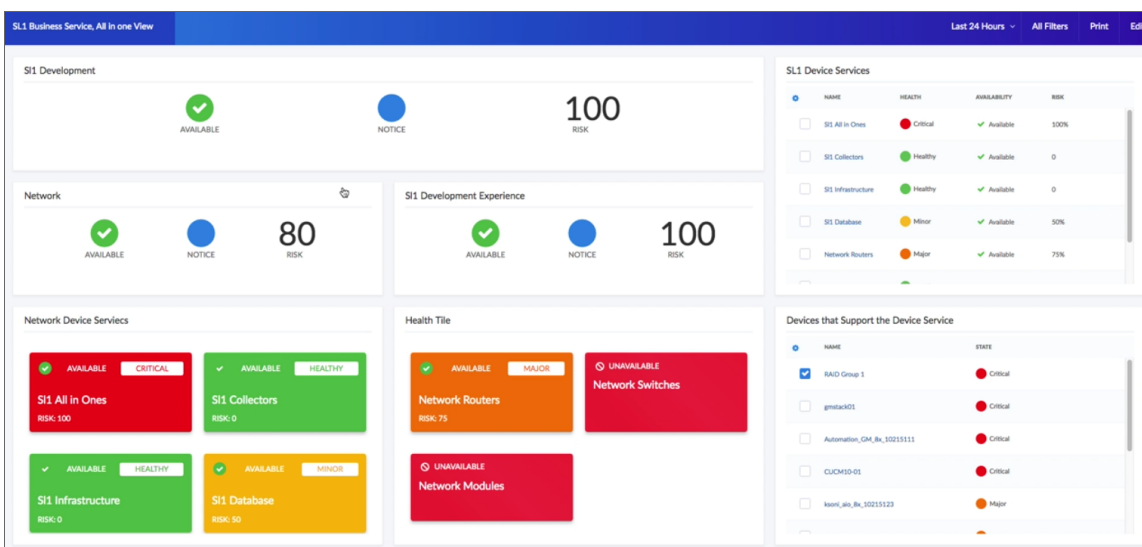
These values are computed in this order because SL1 uses *Availability* values to compute *Health* while SL1 uses both *Availability* and *Health* values to compute *Risk*.

You can define metrics for *device services* based on:

- availability
- latency
- event count
- event severity
- device state
- Dynamic Application data collected by SL1

NOTE: IT services created in the classic user interface are *not* included in the new user interface, and "classic" IT services are not related in any way to the new business services, IT services, and device services.

You can also create dashboards for business services that display information about the state, availability, risk, events, metrics, and other information about a business service. For more information, see the [Creating Dashboards](#) chapter.



Example: Retail Banking

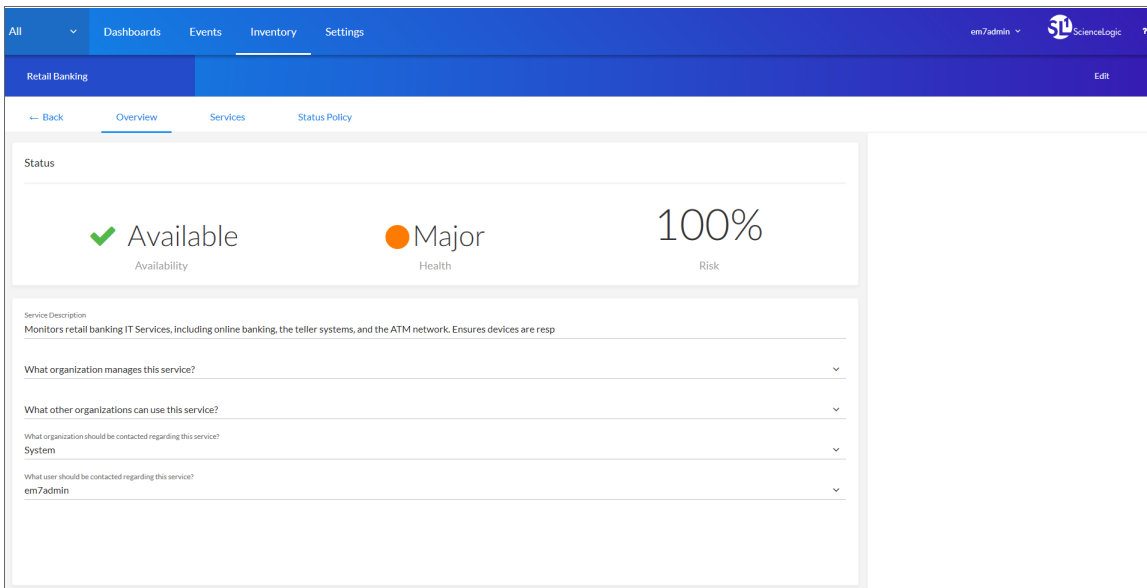
Using SL1 to monitor a business service lets you quickly see whether the service is available and working as expected for a customer or end user. For example, a banking company wants to ensure that their retail banking service is available around the world. They would use the following workflow to set up their services in the new user interface:

1. Because the company has offices around the world, they create multiple **device services** that organize devices based on location or region. The company adds all of its devices to the relevant device services.
2. The company then creates multiple **IT services** to monitor the device services (from step 1), including separate IT services for online banking, teller systems, and ATM networks.
3. Next, the company creates a **business service** for its retail banking business, and this business service includes all of the IT services (from step 2) that deal with retail banking.

NOTE: As needed, the banking company repeats steps 1-3 to create additional business services (made up of IT services and device services) to monitor their commercial banking and investment banking devices and services.

Using the Service Investigator

The **Service Investigator** page appears when you select a service from the **[Services]** tab (Inventory > Services):



The **Service Investigator** page contains three tabs:

- **[Overview]**. Displays a "big-number" dashboard version of the most recent Availability, Health, and Risk values for the service and details about the service description, the managing organization for this service, the organizations that can use this service, the organizations to be contacted about this service, and the user to be contacted about this service.
- **[Services]** or **[Devices]**. Displays the services currently used in a business service or IT service, or the devices included in a device service. You can edit the query for the services or devices in the **Search** field at the top of the tab.
- **[Status Policy]**. Displays a list of all policies of that service type currently in the system and can be chosen to associate with the service being viewed. On this tab, you can change the policy used by a service, and you can also create a new service policy. A **DEFAULT** label appears next to the default policies.


You can click the **[Edit]** button to edit the content on all three tabs to customize your business service.

Creating a Business Service

You can create a new business service to monitor a specific set of IT services and devices for Availability, Health, and Risk values. To create a new business service, you should first determine:

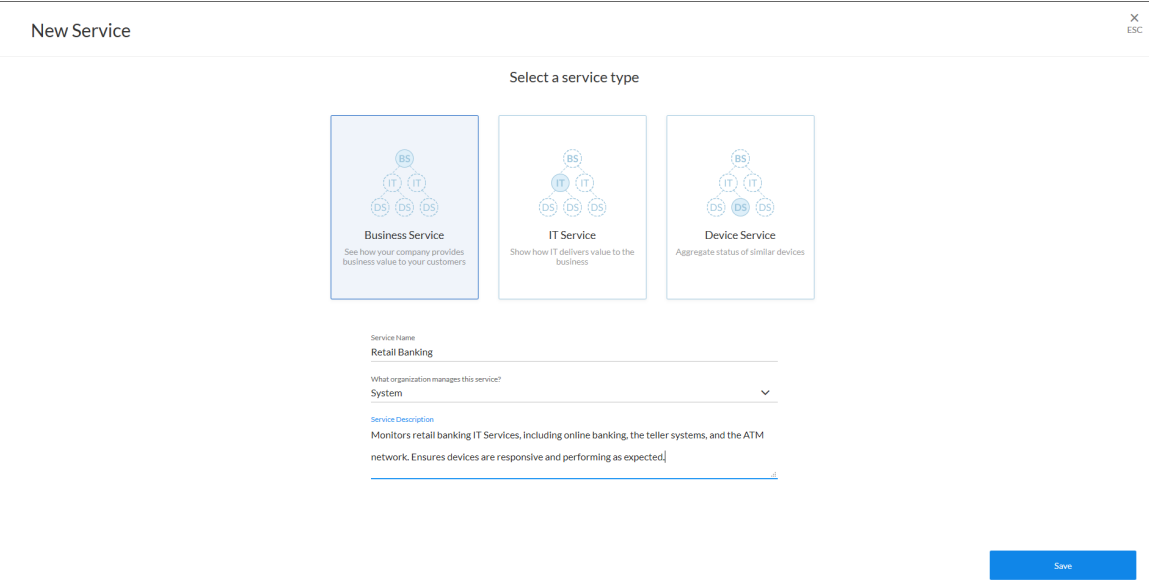
- The devices that impact the business service.
- The IT services that impact the business service.
- The specific conditions that you want to monitor, based on your business processes.

For example, if you provide email service, then a failure of your primary SMTP server and backup SMTP server would constitute a Critical status.

TIP: You can copy an existing service on the **Services** tab by clicking the **[Options]** button () for that service and selecting *Duplicate*.

To create a business service:

1. On the **[Services]** tab (Inventory > Services), click the **[Create Service]** button. The **New Service** page appears:



New Service

Select a service type

Business Service
See how your company provides business value to your customers

IT Service
Show how IT delivers value to the business

Device Service
Aggregate status of similar devices

Service Name
Retail Banking

What organization manages this service?
System

Service Description
Monitors retail banking IT Services, including online banking, the teller systems, and the ATM network. Ensures devices are responsive and performing as expected

Save

2. Select a service type. You should start by creating your device services, then your IT services, and then finally your business service. Your options include:
 - **Device Service.** Monitors a set of related devices.
 - **IT Service.** Monitors a service that IT provides to your to your organization. An IT service includes one or more device services.
 - **Business Service.** Monitors a service your organization provides to your customers. A business service includes one or more IT services.
3. Complete the remaining fields:
 - **Service Name.** Type a unique name for this service.
 - **What organization manages this service?** Select the name of the organization that owns this service.
 - **Service Description.** Type a short description of this service. You can use the text in this description to search for this service on the **[Services]** tab. Optional.
4. Click the **[Save]** button. If you selected *Device Service* in step 2, the **[Devices]** tab appears, with a list of available devices in the **Preview** section. If you selected *Business Service* or *IT Service* in step 2, the **[Services]** tab appears, with a list of available services in the **Preview** section.

Email Business Service						Edit
← Back Overview Services Status Policy						
Query for the right set of services.						
<input type="text" value="Q type to search services"/> × Advanced						
✓ Preview: 3 Services						
SERVICE NAME	SERVICE TYPE	AVAILABILITY	HEALTH	RISK	POLICY	
.testing it service laks for ts dashboards	IT Service	✓ Available	● Healthy	40%	IT Service Policy	DEFAULT
Panda SMTP Relay	IT Service	✓ Available	● Healthy	10%	out of date default IT Service Policy	
Pandas Filter Service	IT Service	✓ Available	● Healthy	30%	out of date default IT Service Policy	

5. Click the **[Edit]** button to start searching for the services or devices you want to monitor.
6. In the **Search** field, type search criteria for the services or devices you want to monitor. A list of services or devices that match your search criteria appears in the **Preview** section:

The screenshot shows the 'Email Business Service' interface. At the top, there's a blue header with 'Email Business Service' on the left and 'Edit' on the right. Below the header, there are tabs: 'Back', 'Overview', 'Services' (which is selected), and 'Status Policy'. A search bar is present with the text 'Query for the right set of services.' and a search icon. The search criteria entered is 'name: smtp'. To the right of the search bar is a link labeled 'Advanced'. Below the search bar, there's a section titled 'Preview: 1 Service'. It contains a table with the following data:

SERVICE NAME	SERVICE TYPE	AVAILABILITY	HEALTH	RISK	POLICY
Panda SMTP Relay	IT Service	Available	Healthy	10%	out of date default IT Service Policy


TIP: If you are looking for a specific set of services or devices, click the **Advanced** link and create a search using AND or OR for multiple search criteria. For example, to search for devices with a Device Class of "network.router", use: `deviceClass has (deviceCategory has (name contains 'network.router'))` For more information, see [Advanced Search](#).

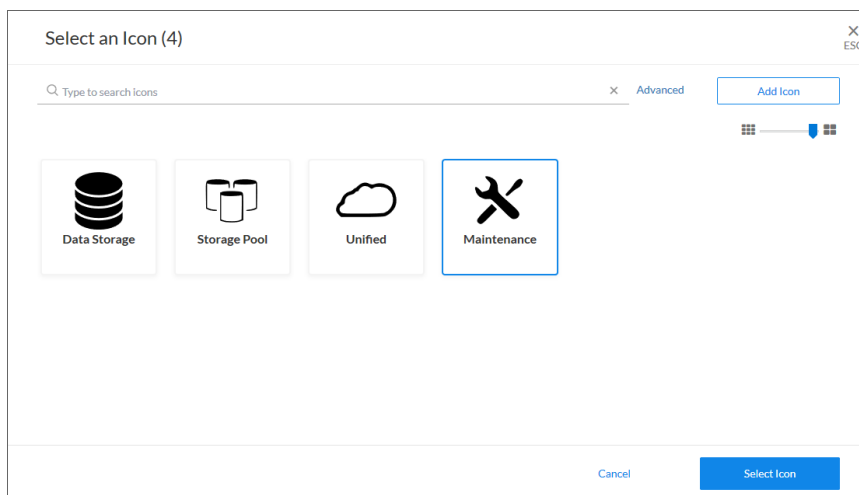
7. When you have the right combination of services or devices, click the **[Save]** button.
8. If needed, click the **[Overview]** tab and then click the **[Edit]** button to update the following fields:
 - **Service Description.** Update the description of this service.
 - **What organization manages this service?** Update the name of the organization that manages this service. The selected organization is also added to the following field.
 - **What other organizations can use this service?** Grant one or more organizations permission to use this service. The organization that manages this service cannot be removed from this drop-down list unless you edit the previous field.
 - **What organization should be contacted regarding this service?** Select the name of the organization that should be contacted with any questions about this service.
 - **What user should be contacted regarding this service?** Select the name of the person who should be contacted with any questions about this service. This person is a member of the organization that manages this service.
9. Click the **[Save]** button. The default policy for the type of service you selected is automatically added to the new service.

10. If you want to use a different business policy with the new service, see [Selecting a Business Service Policy](#).
11. If you want to create a new business policy to use with the new service, see [Creating a Business Service Policy](#).

Assigning Icons to a Business Service

To assign an icon to a service:

1. On the **[Services]** tab (Inventory > Services), locate the service to which you want to add an icon.
2. Click the **Options** button () for that service and select **Assign Icon**. The **Select an Icon** window appears:



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:

The screenshot shows a window titled "Add an Icon" with a close button (X ESC) in the top right corner. The window contains the following elements:

- An "Icon name" text input field.
- An "ADD TAGS" section with a hash icon and a "New tag" text input field.
- A large dashed rectangular box labeled "Browse or Drop".
- A "REUSE TAGS" section.
- A list of requirements under the heading "Icons must:":
 - Be SVG format
 - Be no more than 40kb
 - Not be animated
 - Not contain bitmaps
- At the bottom, there are two buttons: "Cancel" and "Add Icon".


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 device class on the **[Device Classes]** tab.

Selecting a Business Service Policy

Each service type (device service, IT service, and business service) requires a **policy** that determines what it monitors. A business service policy contains a set of rules and conditions that define the Availability, Health, and Risk values for the service, depending on your business needs. Each service requires that one policy be associated with a service at a time.

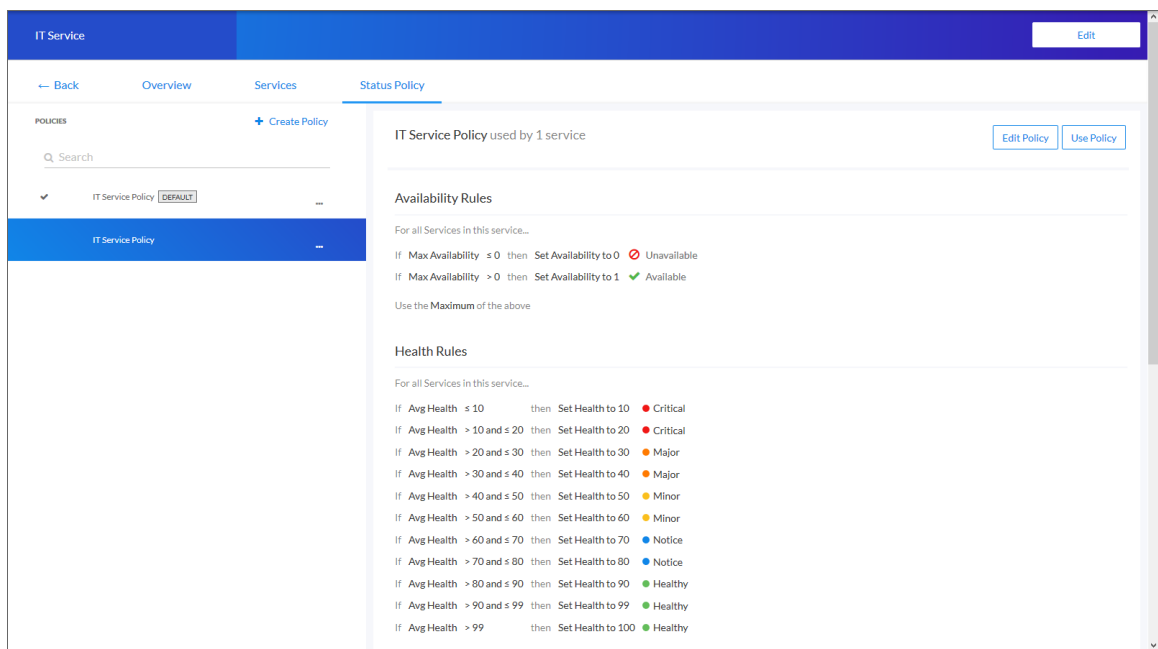
NOTE: The *PowerPack for Business Service Event Policies* contains a set of new business service policies you can use for your services.

When you create a business service of any type, SL1 automatically uses the *default* policy for that particular type of business service. You can remove the default policy after you create a new policy. The default policies cannot be edited.

TIP: If a policy contains errors, an error icon () appears next to the policy name. To view details about what makes the policy invalid, select the policy and hover over the error icon next to the policy name in the right-hand section. A pop-up window lists the problems with the policy.

To select an existing business service policy:

1. On the **[Services]** tab (Inventory > Services, select the service that needs a policy. The **[Overview]** tab for the service appears.
2. Click the **[Status Policy]** tab:



3. In the **Policies** section on the left, select the policy you want to use.

TIP: You can type basic search criteria in the **Search** field to locate a specific policy in the list.

4. To view the details of a selected policy, click the **[Options]** button () for that policy and select *Edit* (or *View* for the default policy). The **Policy Editor** page appears:

Device Services South

Availability Health Risk

Base Availability On

Devices: All Devices in this Service

IF	MAX AVAILABILITY	THEN	SET AVAILABILITY TO
≤ 0		0	Unavailable
> 0		1	Available

+ Add Rule



Available 1 Unavailable 0

Use max of rules

Cancel Save Policy

- Click the **[Cancel]** button when you are done viewing the details for that policy.

TIP: You can copy an existing service policy on the **Services** tab by clicking the **[Options]** button () for that policy and selecting *Duplicate*.


- To add a policy to the service, select the policy in the **Policies** section and click the **[Use Policy]** button in the right-hand section. A check mark icon () appears next to that policy in the **Policies** section, and the words "Current Policy" replace the **[Use Policy]** button in the right-hand section.
- If you want to *delete* a policy you no longer want to use, click the **[Options]** button () for that policy, select *Delete*, and then click **[Delete Policy]**. If that policy is used by any other services, those services are assigned the default policy type. You cannot delete a default policy.

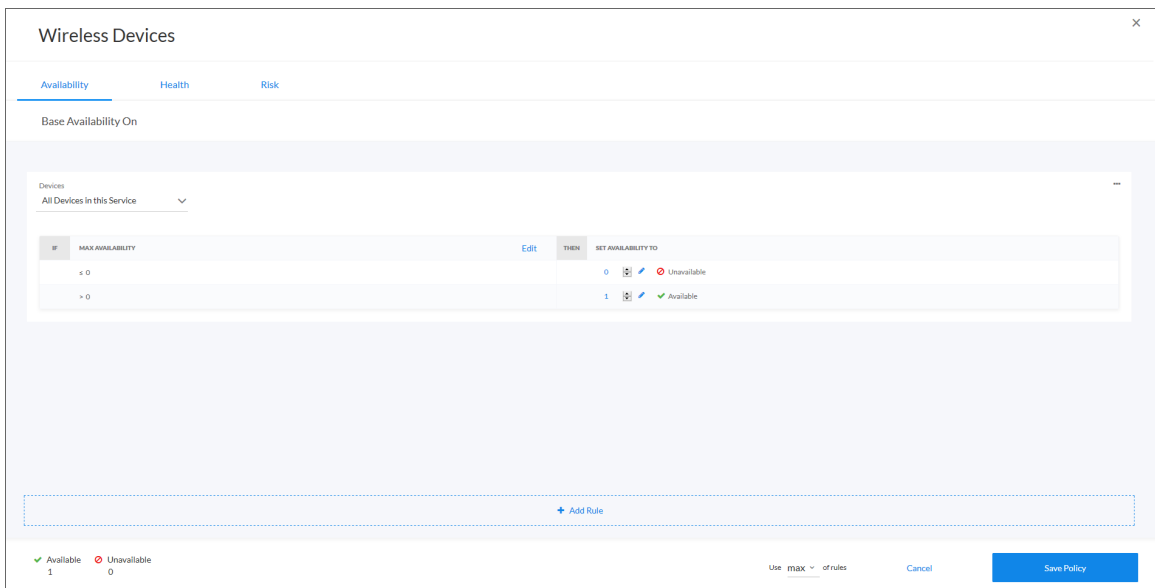
Creating a Business Service Policy

When you create a business service of any type, SL1 automatically uses the *default* policy for that particular type of business service. You can create a new policy to replace the default policy. When you create a new policy, the new policy uses the values from the default policy for that type of service as a starting point.

A policy includes a set of **rules**, and each rule can include one to three **conditions**. If you have multiple rules and conditions, all rules and conditions on a tab must be met to generate the Availability, Health, or Risk value. In other words, if a rule had three conditions, you would set up the conditions for that rule as an IF, AND, AND, THEN statement.









To create a policy:

1. On the **[Services]** tab (Inventory > Services), select the service for which you want to create a policy. The **Service Investigator** page appears.
2. Click the **[Status Policy]** tab, and then click **Create Policy** in the **Policies** section. A **Create Policy** window appears.
3. Type a policy name and click the **[Create Policy]** button. The new policy is added to the **Policies** section on the **[Status Policy]** tab.
4. Click the **[Options]** button () for the new policy and select *Edit*, or click the **[Edit Policy]** button. The **Service Policy Editor** page appears, with a default rule already configured on each tab for Availability, Health, and Risk:



5. On the **[Availability]**, **[Health]**, and **[Risk]** tabs, edit the rules and conditions for each of the three values that make up this policy. Each tab uses the same layout.
6. In the **Services** or **Devices** drop-down list, select one of the following options to filter the services for this policy, as needed:
 - *All Services in this Service* or *All Devices in this Service*. This default setting uses all services or devices that are included in the service.
 - *Queried Services* or *Queried Devices*. This setting uses only the devices or services you specify in the **Search** field that appears when you select this option. This setting lets you filter the list of devices or services for this policy.

7. To update an Availability, Health, or Risk value for a rule, edit the value in the **SET <VALUE> TO** column:

Edit	THEN	SET HEALTH TO
	100	    Healthy
	25	    Major

8. To edit the default conditions for an existing rule, click the **[Edit]** button for that rule. The **Edit Condition** window appears:






9. Complete the following fields:

- **Property.** Select the metric you want to monitor for this condition:
 - If this is a business service or an IT service, your options include *Availability*, *Health*, and *Risk* for the services you want to monitor.
 - If this is a device service, select a device metric, such as Vitals like *Availability* and *Latency* or Dynamic Application metrics.

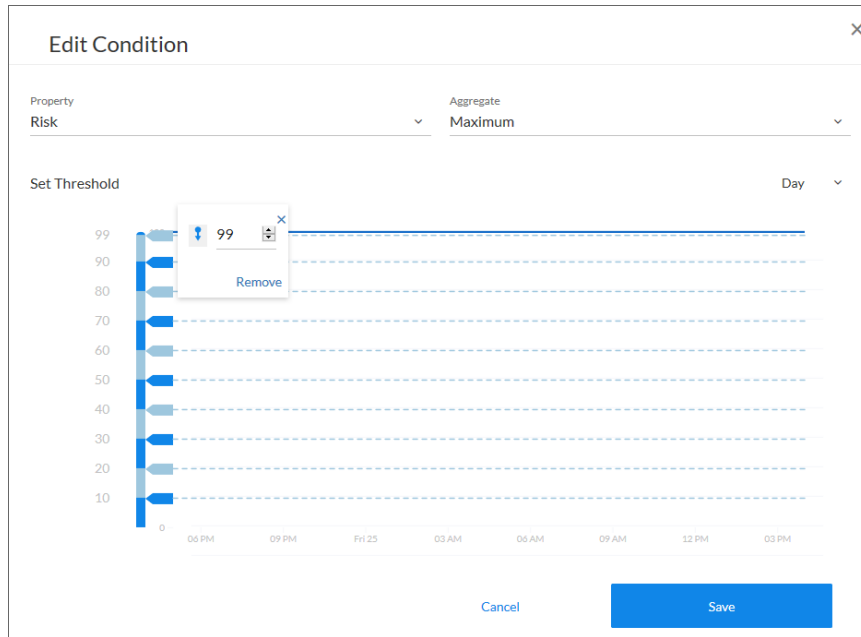
NOTE: If this is a policy for a business service, your options are *Availability*, *Health*, and *Risk*.

- **Aggregation.** Select an aggregation method for the data for this condition. Your options include *Average*, *Minimum*, *Maximum*, *Count*, and *Sum*.
- **Day.** Select a time frame for the data in the graph in the **Set Threshold** section, below. You can use this graph to select reasonable thresholds for your condition. Your options include *Day*, *Week*, and *Month*.

10. In the **Set Threshold** section, click and drag the slider to specify a threshold for this condition. A small **Threshold** window appears, where you can specify the following threshold details:

- The upper threshold icon () lets you set the highest acceptable number for that condition, including any numbers less than that number. For example, $x \leq 80$.
- The lower threshold icon () lets you set the lowest acceptable number for that condition, including any numbers greater than that number. For example, $x \geq 60$.
- The equals icon () in conjunction with a number lets you set a specific number only for this condition. For example, $x = 75$.
- You can specify a range of values by clicking to add a second slider to the **Set Threshold** graph. For example, $40 < x < 60$.
- You can type a number in the **Threshold** window instead of using the slider.

- If needed, you can add a threshold that extends past the existing Y-axis of the table. The scale of the table automatically adjust to the new value.
- The different ranges for your conditions display in alternating shades of dark blue and light blue:



TIP: If the line below the number in the **Threshold** window is red, then your current threshold is invalid. Click the icons or adjust the slider to make sure the line is not red under the threshold value.

11. To save the conditions and threshold settings and close the **Edit Condition** window, click the **[Save]** button.
12. To add more conditions to a rule, click **Edit** on the **Service Policy Editor** page and follow the instructions in steps 8-11.
13. If you have more than one rule, select the type of aggregation you want to use in the **Use <type> of rules** field. You can choose to use the minimum, maximum, or average value for the rules.

NOTE: The Availability value calculates only the minimum and maximum values for rules.

14. Edit any additional conditions or rules on the remaining tabs for this policy, and then click the **[Save Policy]** button.

Creating a Business Service Template

You can create a **service template** from an existing service to simplify the process of replicating an entire service or service hierarchy on another SL1 system. For example, if you want to create the same service hierarchy, but only change the owner of the service hierarchy, creating a service template from an existing service streamlines this process.

To create a service template:

1. On the **[Services]** tab (Inventory > Services), click the **[Options]** button () for the service you want to use as the basis for your template and select **Create Template**. The **Create Template From Service** window appears:

Create Template from Business Service

X
ESC

Please Read Before Continuing

Before creating a Service template, note the following constraints

What can be modified during Service Template creation:

- The name of a Service
- The annotations on a Service
- The annotations on a Status Policy
- The annotations on Rulesets or Rules for a Status Policy
- The query to Identify Devices for a Device Service
- The (optional) query to further restrict Devices for a Rule in a Status Policy

What cannot be modified during Service Template creation:

- The description of a Service
- The query to identify Services for a Business Service or IT Service
- The name of a Status Policy
- Selecting a different Status Policy
- Other details of a Status Policy associated with a Business Service, IT Service or Device Service

The following values are included in a Service but are removed when you use that Service to create a Service Template:

SL1 will request these values when a user uses the Template to create a Service. Users can add stripped values after SL1 creates the Service

- Organization that manages the Service
- Organizations that can use this Service
- Contact Organization or User for the Service

After you create a Service Template, you cannot edit it.

Next

8

Monitoring Business Services

121

- This window contains important information about what you can and cannot do with a service template. After reading this information, click **[Next]**. The next **Create Template From Service** window appears:

Create Template from Business Service

Template Name
Example Template

Description (Optional)

← Back

Next

- Type a name for the template in the **Template Name** field, and type a description of the template in the **Description** field, if needed. Click **[Next]**. The next **Create Template From Service** window appears:

Create Template from Business Service

Business Service
IT Service
Device Service

Services Status Policy

Query for the right set of services.
id in c3b2b65116b4d8314ap=81

Preview: 1 Service

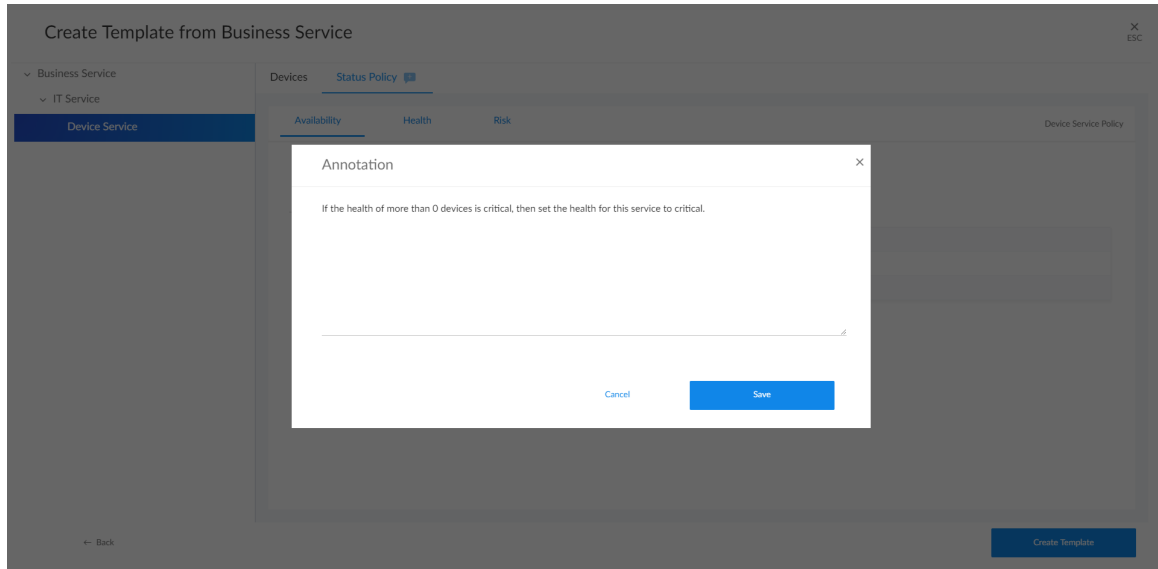
SERVICE NAME	SERVICE TYPE	POLICY
IT Service	IT Service	IT Service Policy


← Back

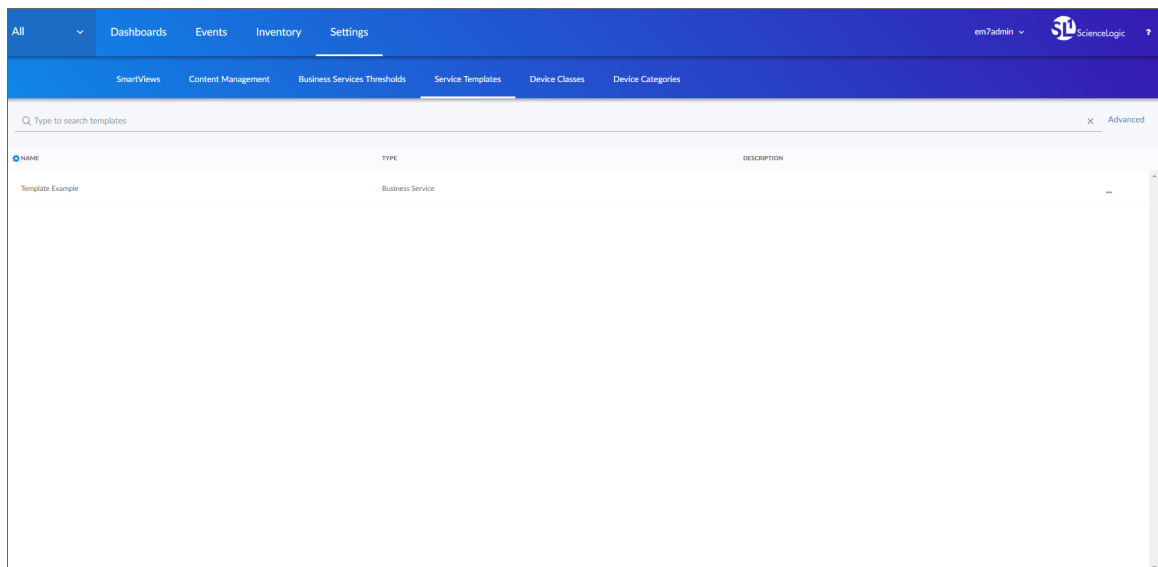
Create Template

- The left side of the window displays the tree for the service hierarchy that is being made into a template. You can select each service in the tree to see information related to that service on the right side of the window. For example, if you select a device service, the **Devices** tab displays the search query used for the devices included in that service. If you select a business service or an IT service, the **Services** tab displays the search query for that service.

- Click the **Status Policy** tab to view the status policy definition for Availability, Health and Risk for that service.
- On the **Status Policy** tab for a device service, you can add annotations for the policies in the template. When a new user uses the template on another system, your annotations can help that user understand the purpose of this status policy.



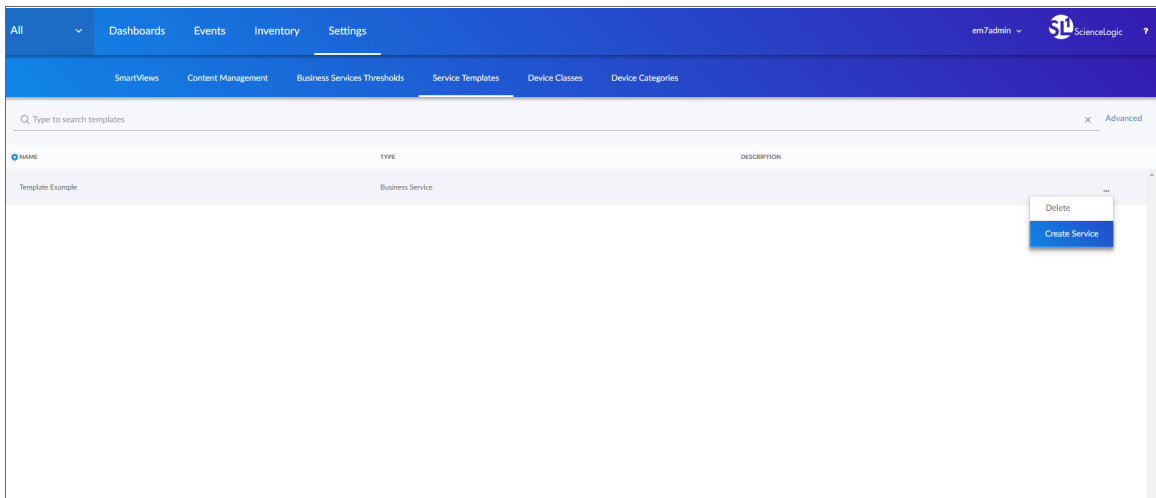
- To leave an annotation for a status policy or rule, click the talk bubble icon () next to the rule or tab. Type your annotation text in the **Annotation** window and click **[Save]**. The talk bubble icon now displays as solid blue, while empty talk bubble icons contain a plus sign.
- Click **[Create Template]**. A confirmation window appears stating that you created the template. Click **[Close]**. The template is now available on the **[Service Templates]** tab (Settings > Service Templates).




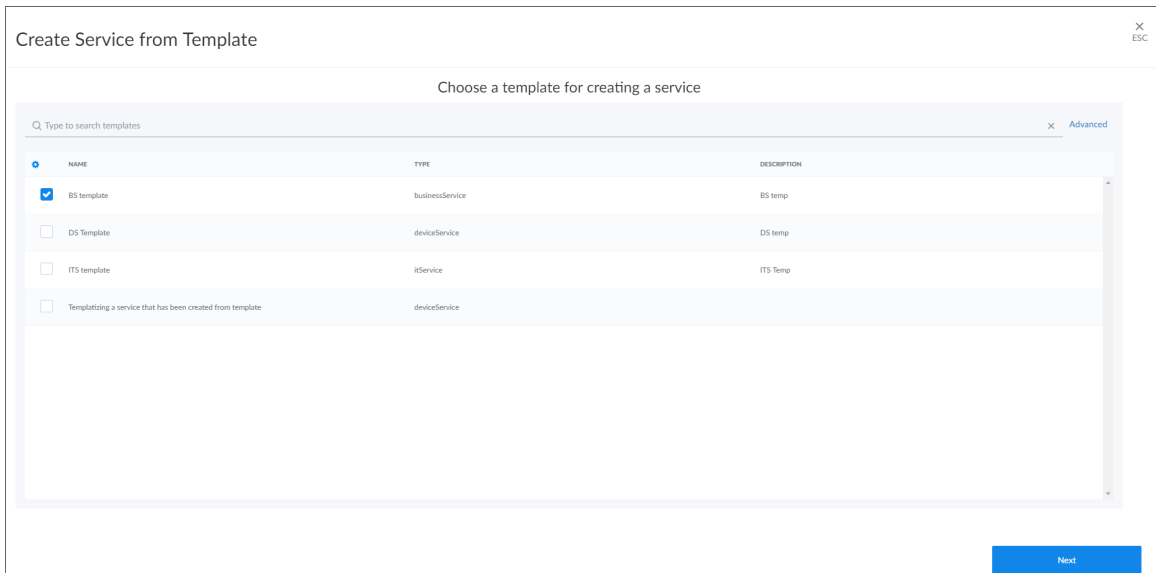
Creating a Business Service From a Template

To create a service from a template:

1. Go to the **[Service Templates]** tab (Settings > Service Templates).



2. Click the **[Options]** button () for the template you want to use and select *Create Service*. The **Create Service from Template** window appears:



TIP: You can also go to the **[Services]** tab (Inventory > Services), click the down arrow on the **[Create Service]** button, and select *Create Service from Template*.

3. Select the template from which you want to create a service and click **[Next]**. The next **Create Service from Template** window appears:

Create Service from Template

Template Name
Template Example

Description (Optional)

What organization manages this service?

Select Organization

System

Next

NOTE: The name and description of the template on this window are read-only.

4. Select an organization from the *What organization manages this service?* drop-down list and click [Next]. The next **Create Service from Template** window appears:

Create Service from Template

test bs by laks

ITS by laks

Test Device Service by laks

Services Status Policy

Query for the right set of services.

id in cjmccou0004ev3er9k3n

Search

Preview: 1 Service

SERVICE NAME	SERVICE TYPE	POLICY
ITS by laks	IT Service	IT Service Policy copy

Back

Create Service from Template

5. To edit the names of the services in the hierarchy at the left, click the service name and update the name. Updating the service names is recommended if you are creating the new service on the same system from which the template was created.
6. Any annotations for a device service that were added when the template was created will be present, and you can edit them and add new annotations.
7. You can edit the rules for Availability, Health, and Risk for a device service in the template.

Create Service from Template

Business Service 2

IT Service 2

Device Service

Devices Status Policy

Availability Health Risk

Base Health On

Devices

Queried Devices

state in 2

IF	COUNT	THEN	SET HEALTH TO
≤ 0		100	Critical
> 0		0	Healthy

Devices

Queried Devices


state in 4

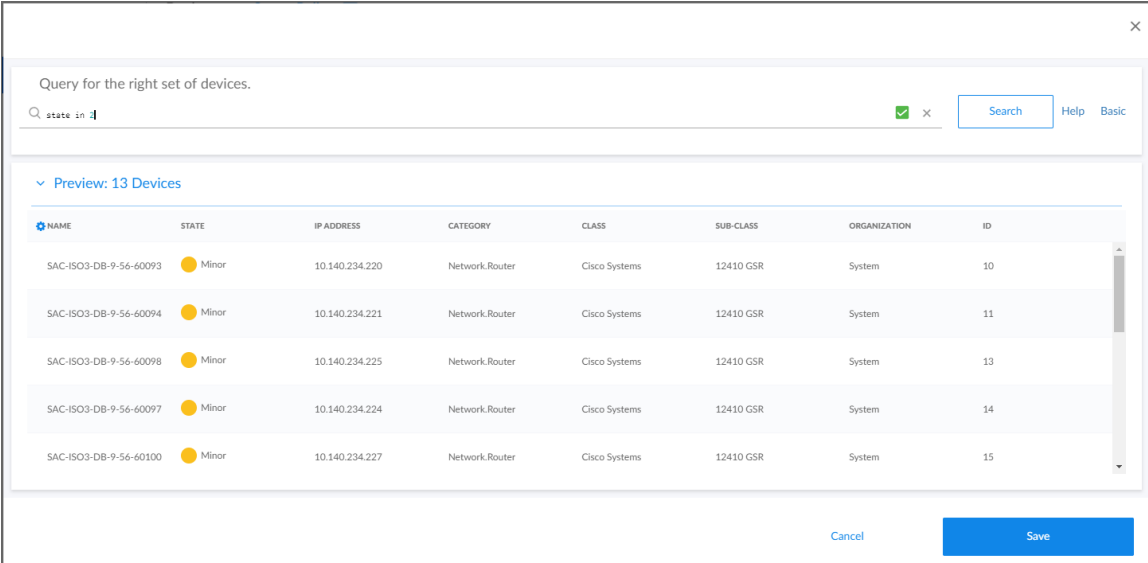
IF	COUNT	THEN	SET HEALTH TO
≤ 0		100	Critical
> 0		25	Notice

Use Min of rules

Back

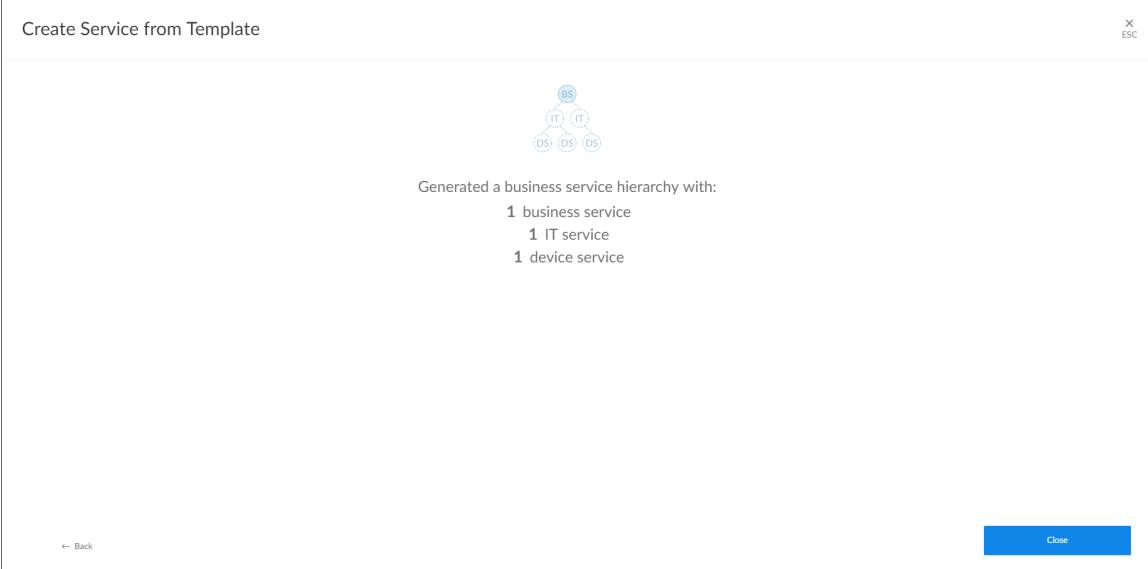
Create Service from Template

8. To edit a rule, click the gray pencil icon () next to the rule, and an edit window appears where you can update the rule:



NAME	STATE	IP ADDRESS	CATEGORY	CLASS	SUB-CLASS	ORGANIZATION	ID
SAC-ISO3-DB-9-56-60093	Minor	10.140.234.220	Network.Router	Cisco Systems	12410 GSR	System	10
SAC-ISO3-DB-9-56-60094	Minor	10.140.234.221	Network.Router	Cisco Systems	12410 GSR	System	11
SAC-ISO3-DB-9-56-60098	Minor	10.140.234.225	Network.Router	Cisco Systems	12410 GSR	System	13
SAC-ISO3-DB-9-56-60097	Minor	10.140.234.224	Network.Router	Cisco Systems	12410 GSR	System	14
SAC-ISO3-DB-9-56-60100	Minor	10.140.234.227	Network.Router	Cisco Systems	12410 GSR	System	15

9. Click the **[Save]** button to close the edit window.
10. Click the **[Create Service from Template]** button to save your service. A confirmation window appears:



Generated a business service hierarchy with:

- 1 business service
- 1 IT service
- 1 device service

11. Click the **[Close]** button. In the Inventory > Services page, you will see your new services listed.

Exporting a Service Template

If you want to use a business service template on another SL1 system, you can package that template into a PowerPack and export it to the other system.

To package and export a service template:

1. After creating your template, log in to the classic user interface.
2. Go to **The PowerPack Manager** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and select *Create a New PowerPack*.
4. On the **PowerPack Properties** page, type a name for the PowerPack in the **Name** field and click **[Save]**.

ScienceLogic, Inc. - Google Chrome
Not secure | 10.100.100.180/em7/index.em7?exec=powerpack_editor&sub=props

Create New PowerPack™

- ▼ Manage PowerPack™
 - Properties
 - Build / Export
 - Features / Benefits
 - Technical Notes
 - Documentation
- ▼ Contents
 - Dynamic Applications
 - Event Policies
 - Device Categories
 - Device Classes
 - Device Templates
 - Device Groups
 - Reports
 - Dashboard Widgets
 - Dashboards
 - Run Book Policies
 - Run Book Actions
 - Run Book Action Types
 - Ticket Templates
 - Credentials
 - Credential Tests
 - Proxy XSL
 - Transformations
 - UI Themes
 - IT Services
 - Log File Monitoring
 - Policies
 - AP Content Objects

Properties

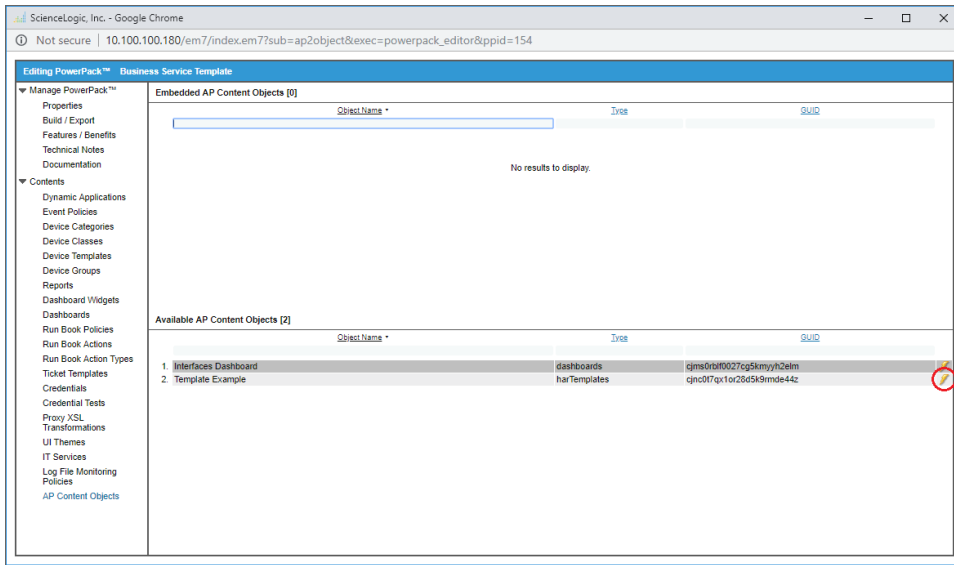
Name	Business Service Template	Creation	em7admin [2018-10-16 15:19:44]
Version	1	Modification	em7admin [2018-10-16 15:19:44]
Publisher		Revision	0
License Key		ID	
Description			
Vendor(s) Supported			
Model(s) Supported			
Version(s) Supported			
Minimum EM7 Version			

Release Notes and Change Log

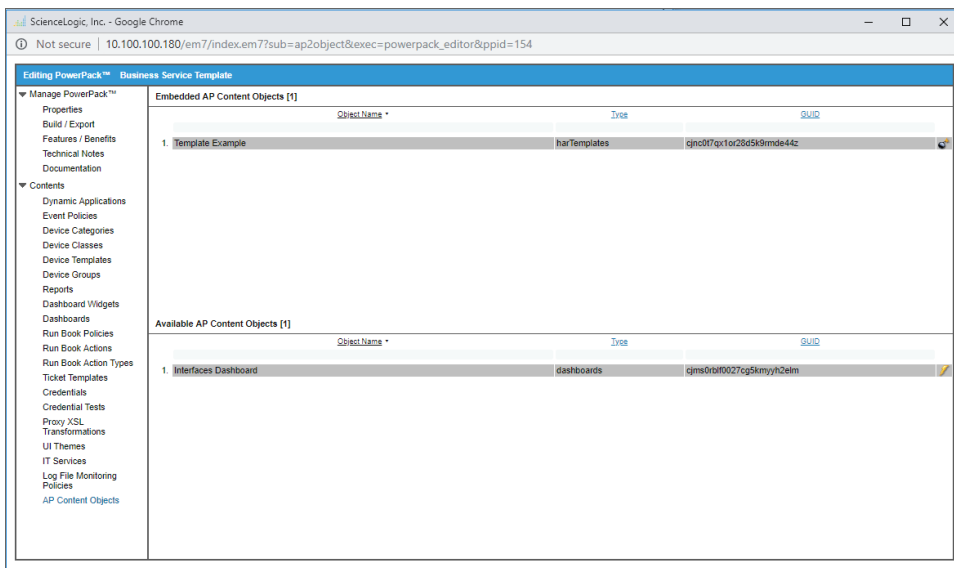
Start typing or drop image here ...

Save

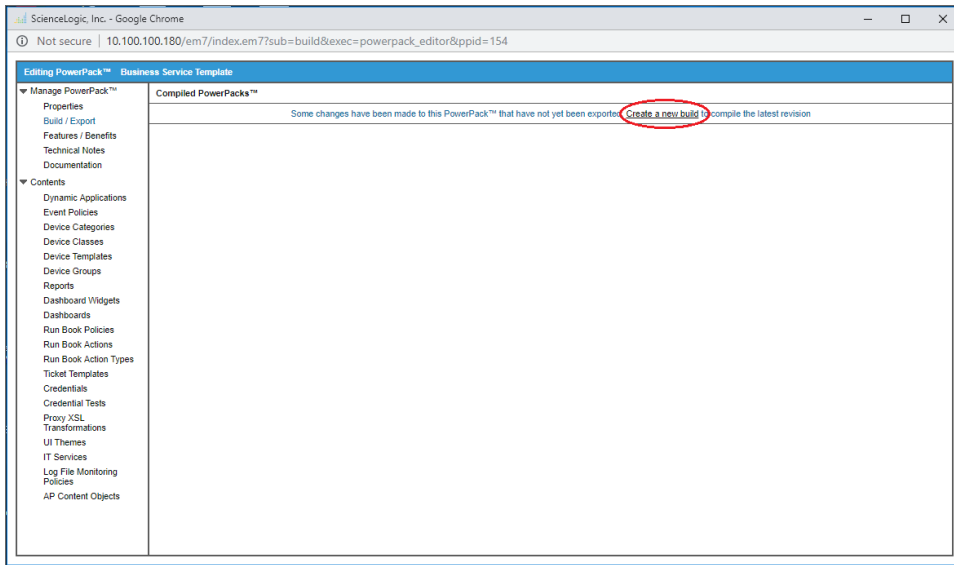
5. Select *AP Content Objects* from the left-nav on the **PowerPack Properties** page. Your template appears in the **Available AP Content Objects** pane:



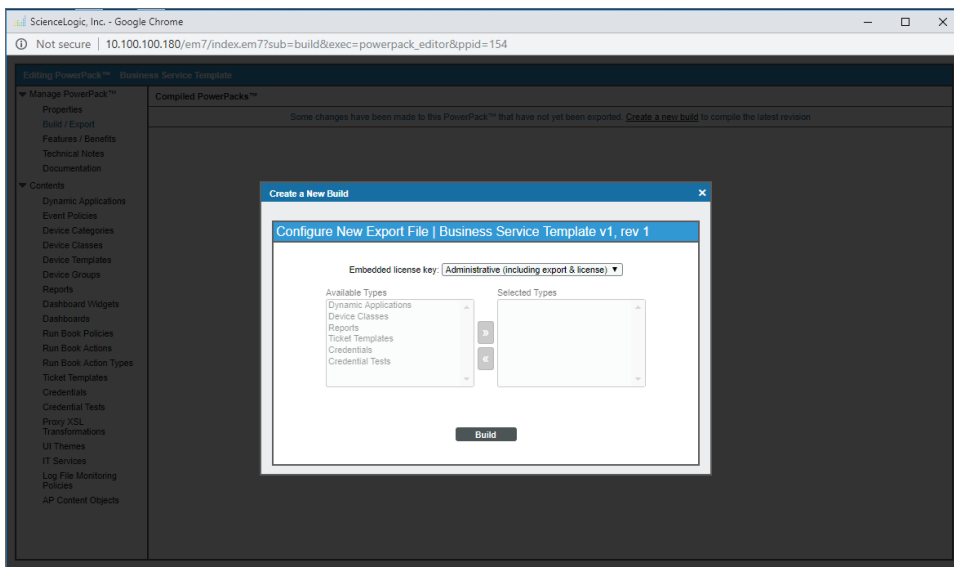
6. Click the lightning bolt icon () next to the template to add it to the PowerPack. The template moves up to the **Embedded AP Content Objects** pane:




7. Select *Build/Export* from the left-nav to open the **Compiled PowerPacks** window, and then click the *Create a new build* link:




8. In the **Configure New Export File** window, select *Administrative (including export & license)* from the **Embedded license key** drop-down list. Click **[Build]**.



9. When the PowerPack finishes building, you can download the build with the download icon () and use that file to upload the template to a new SL1 system.

Installing a Template from a PowerPack

1. On the system on which you want to install the template, import the PowerPack on the classic ScienceLogic user interface in the **PowerPack Manager** page.
2. Once you have imported the PowerPack, click the **[Actions]** button and select *Install PowerPack*.
3. Find the PowerPack you created in the **Imported PowerPacks** window and click its lightning bolt icon ().
4. When the **Install PowerPack** window appears, click the **[Install]** button.
5. When it has finished installing, the template will appear in the Settings > Service Templates page of the SL1 user interface.

Default Service Policy Settings

The following sections describe how the three default service policies calculate Availability, Health, and Risk:

Device Service Default Policy

Availability: Maximum available: if one device is available, then all are available

Health: Based upon the worst device severity, then uses the following settings:

- Critical = 0-20
- Major = 21-40
- Minor = 41-60
- Notice = 61-80
- Healthy = 81-100

Risk: Based upon the worst device severity, then uses the following settings:

- Healthy= 0-20
- Notice = 21-40
- Minor = 41-60
- Major = 61-80
- Critical = 81-100

IT Service Default Policy

Availability: Maximum available: if one service is available, then all are available

Health: Average Health value of all services

Risk: Maximum Risk value of any service

Business Service Default Policy

Availability: Maximum available : if one service is available, then all are available

Health: Average Health value of all services

Risk: Maximum Risk value of any service

Managing Events for Business Services

When SL1 evaluates the state of a service, it reviews the Health, Availability, and Risk values produced by your business services, IT services, and devices services. SL1 then compares those values against the alert thresholds that are defined on the **[Business Service Thresholds]** tab (Settings > Business Services Thresholds):

The screenshot shows the 'Business Services Thresholds' configuration page. The page has a top navigation bar with 'All', 'Dashboards', 'Events', 'Inventory', and 'Settings'. Below this is a sub-navigation bar with 'SmartViews', 'Content Management', 'Business Services Thresholds', 'Service Templates', 'Device Classes', and 'Device Categories'. The 'Business Services Thresholds' tab is selected, and an 'Edit' button is visible. The main content area has a heading 'Enable alerts and set thresholds for all Business Services, IT Services, and Device Services.' and three columns for configuration:

Business Services	IT Services	Device Services
AVAILABILITY		
<input checked="" type="checkbox"/> Unavailable	<input checked="" type="checkbox"/> Unavailable	<input checked="" type="checkbox"/> Unavailable
<input checked="" type="checkbox"/> Available	<input checked="" type="checkbox"/> Available	<input checked="" type="checkbox"/> Available
HEALTH		
<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Critical
<input checked="" type="checkbox"/> Major	<input checked="" type="checkbox"/> Major	<input checked="" type="checkbox"/> Major
<input checked="" type="checkbox"/> Minor	<input checked="" type="checkbox"/> Minor	<input checked="" type="checkbox"/> Minor
<input checked="" type="checkbox"/> Notice	<input checked="" type="checkbox"/> Notice	<input checked="" type="checkbox"/> Notice
<input checked="" type="checkbox"/> Healthy	<input checked="" type="checkbox"/> Healthy	<input checked="" type="checkbox"/> Healthy
RISK		
<input checked="" type="checkbox"/> Very High greater than 80	<input checked="" type="checkbox"/> Very High greater than 80	<input checked="" type="checkbox"/> Very High greater than 80
<input checked="" type="checkbox"/> High greater than 60	<input checked="" type="checkbox"/> High greater than 60	<input checked="" type="checkbox"/> High greater than 60
<input checked="" type="checkbox"/> Medium greater than 40	<input checked="" type="checkbox"/> Medium greater than 40	<input checked="" type="checkbox"/> Medium greater than 40

If any of the thresholds on the **[Business Service Thresholds]** tab are crossed, SL1 generates an alert message. For an event to be produced, you need to create or install an event policy that watches for that alert message and produces an event when it sees that alert message.

TIP: To update the thresholds on this tab, click the **[Edit]** button, select which thresholds should generate an alert message, and then click **[Save]**.

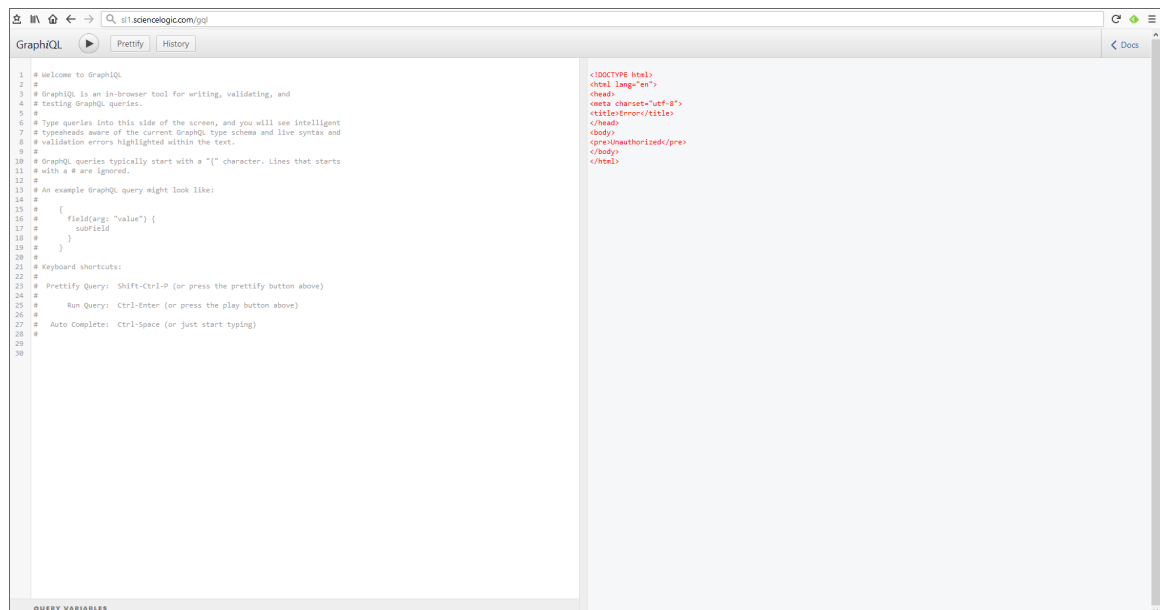
By monitoring the events tied to your business services, you can act quickly if one of your services is unavailable, unhealthy, or potentially at risk.

Exporting Service Data with the ScienceLogic API

By navigating to the GraphiQL interface, you can export business service data with the ScienceLogic API. GraphiQL is a user interface for interactively exploring the capabilities of, and executing queries against, a GraphQL API.

To access the GraphiQL interface:

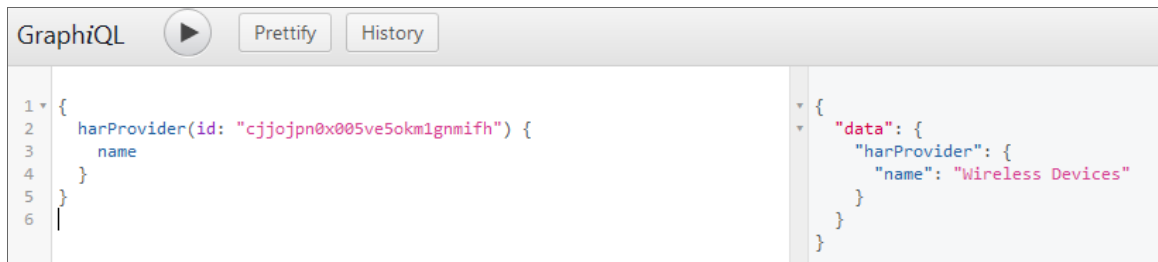
1. In a browser, type the URL or IP address for the new user interface.
2. Type `/gql` at the end of the URL or IP address. For example, you could type <https://sl1.sciencelogic.com/gql>. The GraphiQL interface appears:



3. In the new user interface, make a note of the URL that displays for the service you want to export. For example, if you have a service named "Wireless Devices," and its URL in the new user interface is <http://sl1.sciencelogic.com/inventory/services/cjjoipn0x005ve5okm1gnmifh/overview>. Make a note of the value between `/services` and `/overview`. In this example, the value you need is `cjjoipn0x005ve5okm1gnmifh`.
4. In the GraphiQL interface, create a *harProvider* query for the service you want to export, using the following format:

```
query {harProvider (id:"<Service_URI>") { name} }
```

- Click the **[Execute Query]** (Play) button to tell GraphQL to send the query to the GraphQL server and get the results. Using the example service from step 3, the query and its data appear in the following format:



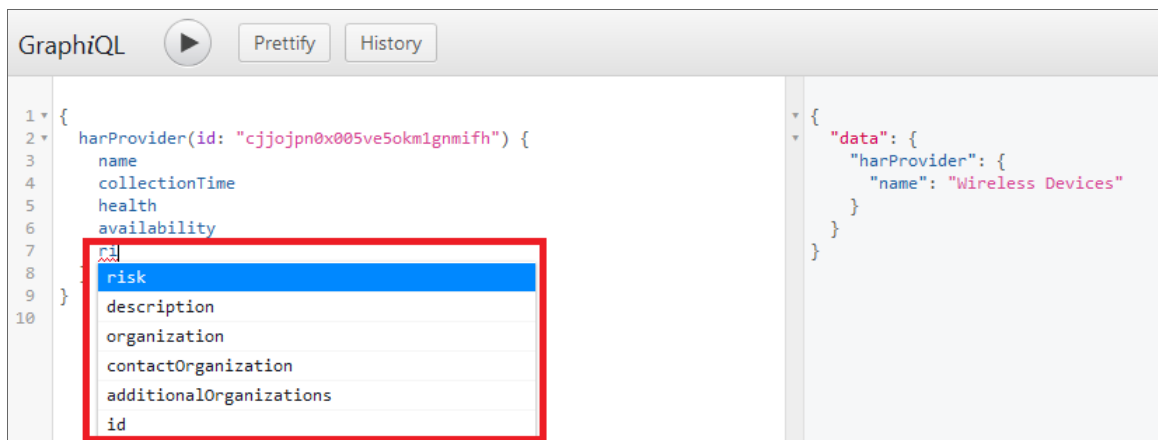
The screenshot shows the GraphQL IDE interface. On the left, the query editor contains the following query:

```
1 {
2   harProvider(id: "cjjojp0x005ve5okm1gnmifh") {
3     name
4   }
5 }
6
```

On the right, the JSON response is displayed:

```
{
  "data": {
    "harProvider": {
      "name": "Wireless Devices"
    }
  }
}
```

- To export additional data, use the filter-while-you-type capabilities of the GraphQL interface to gather other information, such as the collection timestamp, health, availability, and risk:



The screenshot shows the GraphQL IDE interface. The query editor on the left contains the following query:

```
1 {
2   harProvider(id: "cjjojp0x005ve5okm1gnmifh") {
3     name
4     collectionTime
5     health
6     availability
7     risk
8   }
9 }
10
```

A dropdown menu is open below the 'risk' field, showing a list of available fields: 'risk', 'description', 'organization', 'contactOrganization', 'additionalOrganizations', and 'id'. The 'risk' field is currently selected and highlighted in blue. The JSON response on the right is the same as in the previous screenshot.

- After you finish updating your query, click the **[Execute Query]** button.



The screenshot shows the GraphQL IDE interface. The query editor on the left contains the following query:

```
1 {
2   harProvider(id: "cjjojp0x005ve5okm1gnmifh") {
3     name
4     collectionTime
5     health
6     availability
7     risk
8   }
9 }
10
```

The JSON response on the right is updated to include the new fields:

```
{
  "data": {
    "harProvider": {
      "name": "Wireless Devices",
      "collectionTime": 1531773000,
      "health": 100,
      "availability": null,
      "risk": 0
    }
  }
}
```

Troubleshooting Services

This section covers some of the issues you might encounter while working with services and policies on the **[Services]** tab, and how to resolve those issues.

Some services do not generate Health, Availability, or Risk values

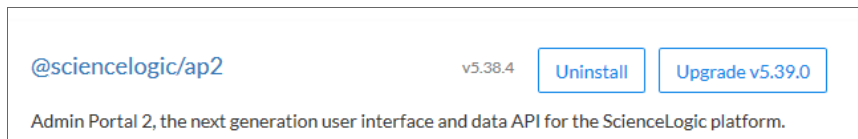
In this situation, some services in SL1 do not generate any values for Health, Availability, or Risk. For example, a dash might appear instead of a value in the **Status** table on the **Service Investigator** page:

Status		
-	● Healthy	10%
Availability	Health	Risk

To address this issue, review the following settings and suggestions:

Step 1: Confirm you have the latest code for the new user interface:

1. Navigate to the **[Content Management]** tab (Settings > Content Management).
2. Click the **[Install/Upgrade Packages]** button. The Install Packages page appears.
3. If needed, upgrade to the latest version of **@sciencelogic/ap2** to potentially resolve any issues that might have caused this issue.
4. For example, in the following image, the *installed* version of **@sciencelogic/ap2** is 5.38.4, while the *latest* version is 5.39.0:



Step 2: Turn up the log level to trace:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Open the file `/usr/local/silo/nextui/nextui.env` with `vi` or another text editor:

```
sudo vi /usr/local/silo/nextui/nextui.env
```
4. Change the log setting to the following: **NEXT_UI_LOG_LEVEL=all:trace**
5. Restart the new user interface and GraphQL with the following command:

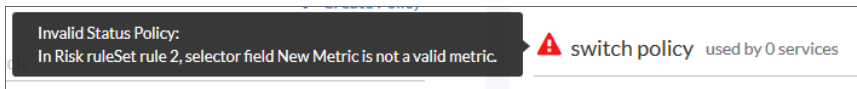
```
sudo systemctl restart nextui
```

6. Tail the log with the following command:

```
sudo journalctl -u nextui -f
```

Step 3: Ensure that your service policy is valid:

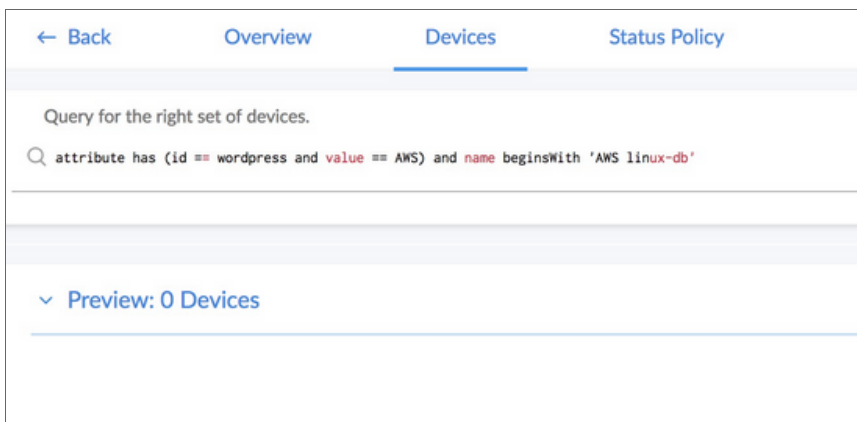
1. In the new user interface, navigate to your service on the **[Services]** tab (Inventory > Services).
2. Review the policy used by that service for any validation errors, as in the following example:



3. Address any errors in the service policy.

Step 4: Ensure that your service contains at least one service or device:

1. Navigate to the **[Services]** tab (Inventory > Services).
2. Navigate to the **[Devices]** or **[Services]** tab for the service or services that are not displaying values.



3. Ensure that at least one device or service appears in the **Preview** section. If not, create a new search for devices or services.

Step 5: Ensure that your service policy *rules* contain at least one service or device:

1. Rule filters select a subset of the devices or services defined by the service filter. If a device service filter results in five devices, the rule filter selects some subset of those five devices. You might create rule filters that exclude all devices or services in the service, resulting in no metric values.
2. The following rule filter only selects the devices with a state of 4, or Critical. If no devices have a state of 4, the resulting list of devices for that filter will be empty, and you cannot get any device metric values:

Base Availability On

Devices
Queried Devices

state in 4

Search

IF	COUNT DEVICES	THEN	SET AVAILABILITY TO
	≤ 0		1 ✓ Available
	> 0		0 ✗ Unavailable

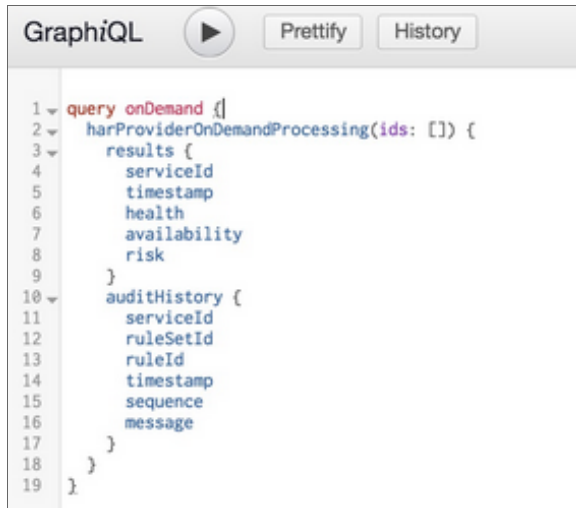
3. In this case, we are counting devices, so the count is zero and produces a value based in the condition table.
4. If the metric had been a normal device metric like latency, the result would have been "null," because getting the average latency from zero devices results in null.

Step 6: Generate audit data by running onDemandProcessing with the GraphQL interface:

1. In a browser, type the URL or IP address for the new user interface, and then type **/gql** at the end of the URL or IP address. The GraphQL interface appears.
2. On the left side of the GraphQL editor, type the following query:

```
query onDemand {  
  harProviderOnDemandProcessing(ids: []) {  
    results { serviceId timestamp health availability risk }  
    auditHistory { serviceId ruleSetId ruleId timestamp sequence message }  
  }  
}
```

3. Click the **[Execute Query]** (Play) button to tell GraphiQL to send the query to the GraphQL server and get the results:



4. Review the resulting audit information on the right side of the GraphiQL editor:
5. If you know the service ID you are looking for, search for it by clicking inside the right pane and typing **cmd+f**. The GraphiQL interface highlights the services that match the ID you looked for:



6. Scroll down to see the audit information for this service (look for the highlighted information):

```

    "auditHistory": [
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyh40m00a31byxi5chr1u5",
        "ruleId": "cjfcyh48300a41byxqcw5tqx4",
        "timestamp": 1524698040,
        "sequence": 1,
        "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: availability Rule: 1"
      },
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyh40m00a31byxi5chr1u5",
        "ruleId": "cjfcyh48300a41byxqcw5tqx4",
        "timestamp": 1524698040,
        "sequence": 2,
        "message": "No matching row found in condition table Result: null Service: Web DS Cloud Policy: Device Service Policy RuleSet: availability Rule #: 1 Matching Row #: none Constituents: 0 Values: {max availability: null}"
      },
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyh40m00a31byxi5chr1u5",
        "ruleId": null,
        "timestamp": 1524698040,
        "sequence": 3,
        "message": "RuleSet Result: null Service: Web DS Cloud Policy: Device Service Policy RuleSet: availability Aggregation: max Values: []"
      },
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyglb00931byxmyu8zdm",
        "ruleId": "cjfcygyxos00941byxg2o5k3hu",
        "timestamp": 1524698040,
        "sequence": 4,
        "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: health Rule: 1"
      },
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyglb00931byxmyu8zdm",
        "ruleId": "cjfcygyxos00941byxg2o5k3hu",
        "timestamp": 1524698040,
        "sequence": 5,
        "message": "Rule Result: 100 Service: Web DS Cloud Policy: Device Service Policy RuleSet: health Rule: 1 Matching Row #: 1 Matching Row: [IF (-Infinity <= count <= 0) THEN 100] Constituents: 0 Values: {count : 0}"
      },
      {
        "serviceId": "cjk9k2fcw0022r2qim00m52vq",
        "ruleSetId": "cjfcyglb00931byxmyu8zdm",
        "ruleId": "cjfcygyxtf00981byxam86mbiv",
        "timestamp": 1524698040,
        "sequence": 6,
        "message": "Service has no constituents for rule. Service: Web DS Cloud Policy: Device Service Policy RuleSet: health Rule: 5"
      }
    ]
  }

```

7. After running onDemandProcessing with the GraphiQL interface and updating the log settings on the server to do *all:trace*, you can now see trace-level log messages in the terminal where you ran `sudo journalctl -u nextui -f`.

- Review the log messages for errors and warnings:

```
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: 00:22:03.169 <-- dao.js:327 (Object.getMetricValuesForConstituents) [ { GraphQLError: Variable "$metricSearch" got invalid value {"first":{"guid":{"eq":"d_check"}}}; Field "guid" is not defined by type MetricSearch at value.first; did you mean id?
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coercionError (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:179:10)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:148:36)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:132:30)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at coerceValue (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/utilities/coerceValue.js:55:12)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at getVariableValues (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/values.js:74:53)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at buildExecutionContext (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.js:246:63)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at executeImpl (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.js:148:17)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at execute (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/execution/execute.js:131:229)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at graphqlImpl (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:112:31)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at /var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:66:223
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at new Promise (<anonymous>)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at graphql (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/graphql/graphql.js:63:10)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at Object.gqlLocal [as graphql] (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/@sciencelogic/sl-em7-gql/build/middleware/gql.js:116:33)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at Object.getMetricValuesForConstituents (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/@sciencelogic/sl-em7-gql/build/lib/businessServices/dao.js:321:26)
Apr 26 00:22:03 dc2-sl1-db01 node[25004]: at Object.getMetricValuesForConstituents (/var/opt/em7/gui/nextui/lib/node_modules/@sciencelogic/ap2/node_modules/@sciencelogic/sl-em7-gql/build/lib/businessServices/dao.js:321:26)
```

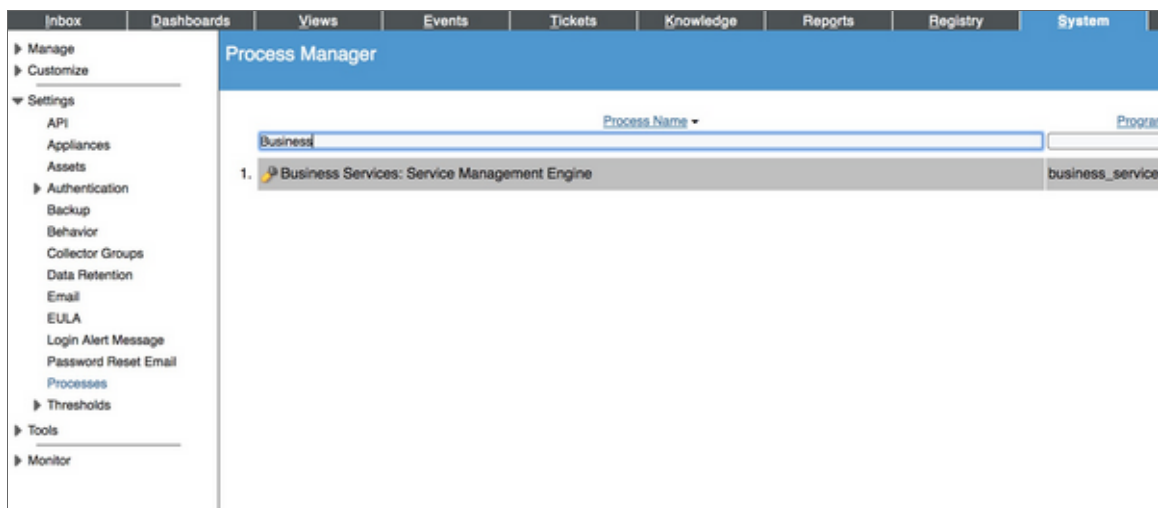
All services do not generate Health, Availability, and Risk values

In this situation, *all* of your services in SL1 fail to generate any values for Health, Availability, or Risk.

To address this issue, review the following settings and suggestions.

Step 1: Confirm that the Business Services process exists in your "classic" SL1 system:

- In the classic user interface, navigate to the **Process Manager** page (System > Settings > Processes) and start typing "Business" in the **Process Name** filter:



Step 2: Follow the steps in [Generate audit data using the GraphiQL user interface](#), above. If the process times out, then the processing has taken more than two minutes to complete, and no computed results are stored.

Step 3: Look for logs from the python process:

1. The python process calls the onDemandProcessing GraphQL query. If python is having trouble connecting to GraphQL, it could be an authentication problem or some other code-related issue.
2. Look in `/var/log/em7` for newly created logs, and `ls -lrt` to see if any new error logs were created with "business" in the file name.
3. Also check the ***silos.log*** for messages related to the `business_service_management` process:

```
grep service /var/log/em7/silo.log
```

Error message: "Business service thresholds are missing."

In this situation, you receive the following error message: "Business service thresholds are missing. Your administrator or support must fix the database to continue editing thresholds."

This situation occurs if a user deleted threshold data from SL1, either with GQL or with the database.

To address this issue, contact your SL1 administrator or ScienceLogic Support.

503 errors, or Health, Availability, and Risk values that are all the same or inaccurate

In this situation, you might see 503 errors in logs or in the user interface. You might also see Health, Availability, and Risk values that are all the same or inaccurate.

To avoid communication errors between the new user interface and the ScienceLogic API, configure the `em7_limits.conf` file to limit the number of connections per IP on all SL1 appliances that communicate with the ScienceLogic API.

NOTE: Use this configuration if you are using a version of SL1 that is lower than 8.9.0, or if you used the patch to upgrade to 8.9.0 instead of using the ISO version of 8.9.0.

To configure communication on a SL1 appliance:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. Open the file `/etc/nginx/conf.d/em7_limits.conf` with vi or another text editor:

```
sudo vi /etc/nginx/conf.d/em7_limits.conf
```

4. To limit the number of connections per IP, add the following line to the file:

```
limit_conn perip 200
```

5. Save your changes and exit the file (`:wq`).
6. Restart the SL1 appliance by executing the following command:

```
sudo systemctl restart nginx
```

7. Run steps 1-6 on all SL1 appliances that communicate with the ScienceLogic API.

© 2003 - 2019, 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



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

International: +1-703-354-1010