Skylar One Global Manager

Skylar One version 12.5.1

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to use a Global Manager system to aggregate data from multiple Skylar One (formerly SL1) systems.

NOTE: Global Manager is available as part of a Skylar One Premium solution. To upgrade, contact ScienceLogic Customer Support. For more information, see https://sciencelogic.com/pricing.

For more information about using the Skylar One Global Manager for multi-stack monitoring, watch the video at https://www.youtube.com/watch?v=NBjuwpbVfPk.

Use the following menu options to navigate the Skylar One user interface:

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

This chapter covers the following topics:

What is Global Manager?

A ***Global Manager*** system is a Skylar One All-In-One Appliance that is configured to aggregate and display data from multiple Skylar One systems. A Global Manager system can aggregate data from either All-In-One Appliances, distributed systems, or both.

a Skylar One system from which data is aggregated by a Global Manager system is referred to as a ***stack***.

For example, suppose your enterprise includes four data centers and that you have installed an All-In-One Appliance in each data center. Each All-In-One Appliance would monitor the devices in its particular data center. You could then install a Global Manager system that aggregates data from all four of those All-In-One Appliance stacks to provide a global view of all four data centers.

A Global Manager system provides the following functions:

- A **Global Manager Stacks** page for viewing a list of the stacks in your Global Manager system
- A global **Dashboards** page for creating and viewing dashboards that display data aggregated from multiple Skylar One systems
- A global **Events** page for viewing events from multiple Skylar One systems
- A global **Devices** page for viewing devices from multiple Skylar One systems
- A global **Business Services** page for viewing business services from multiple Skylar One systems

NOTE: The Global Manager system ***does not*** store any aggregated data on its system; all data aggregation functions of a Global Manager system are performed on-demand, and it merely provides a consolidated view of data being monitored and stored across multiple Skylar One stacks. Similarly, it does not have any configuration or administrative capabilities. All configuration and administrative tasks must be completed on the stacks themselves.

NOTE: Not all Skylar One features are available on a Global Manager system. Only the features described above are available in a Global Manager system.

Chapter 2

Global Manager Configuration

Overview

A Global Manager system is a standard Skylar One (formerly SL1) All-In-One Appliance with additional configuration applied. This chapter describes how to configure a Global Manager system and discover its stacks.

Use the following menu options to navigate the Skylar One user interface:

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

This chapter covers the following topics:

Global Manager Configuration and Discovery Process

When setting up a Global Manager system, you must complete the following steps to properly configure the system and discover its stacks:

1. Ensure that the Global Manager system and its stacks meet all of the necessary *system and technical requirements*.
2. Ensure that the user accounts for the Global Manager system and its stacks meet the necessary *authentication and access requirements*.
3. Optionally, if you want to create external tickets from or align external tickets to events that appear in the Global Manager system, you must configure the Global Manager system and its stacks to *create and align event external tickets*.
4. *Install the ScienceLogic Global Manager PowerPack* on the Global Manager system.
5. On the Global Manager system, edit the NextUI configuration file to *enable Global Manager*. Optionally, you can also update some of the default Global Manager configuration settings in this file.
6. Use SNMP to discover an entry point for each stack that you want to monitor in your Global Manager system. You can then either use *Run Book Actions* or *Dynamic Applications* to add the stacks to the Global Manager system.
7. Verify that your *Global Manager system is successfully configured*.

Each of these steps is described in greater detail in the following sections.

Global Manager System and Technical Requirements

When using a Global Manager system, the Global Manager system and its stacks must meet the following system and technical requirements:

- The Global Manager system must be installed on an All-In-One Appliance built using Skylar One version 10.2 or later on a supported hardware or virtualization platform.
- When deploying or upgrading Global Manager systems, the Global Manager stack and all of its child stacks must run on the same Skylar One build version, as well as the same version of AP2 and Oracle Linux.
- The Global Manager system and each stack from which data is aggregated must be running the same Skylar One platform version and the same AP2 version.

TIP: To locate the version number, launch Skylar One, click your username in the top navigation bar, and select *About*; the Skylar One version appears in the **Platform** section.

NOTE: Only one entry point can be used per stack. Do not discover more than one entry point per stack.

NOTE: When upgrading to a new version of Skylar One, ScienceLogic recommends upgrading all stacks before upgrading your Global Manager All-In-One Appliance.

NOTE: During large-scale upgrades, you might experience minor version mismatches between the Global Manager system and its stacks, but you should work to match these versions as quickly as possible to ensure feature consistency.

- The Global Manager system must be able to communicate with each stack entry point over TCP port 443 (secure HTTP) and UDP port 161 (SNMP).
- The other system requirements for the Global Manager system and each stack are the same as non-Global Manager versions of the same appliances. For more information about system requirements, see the System Requirements page on the ScienceLogic Support site.

The following are the recommended entry points for each architecture type:

Architecture	Recommended Entry Point
Single All-In-One Appliance	All-In-One Appliance
All-In-One Appliances with Disaster Recovery	Primary All-In-One Appliance*
Two Database Servers configured for High Availability	Primary Database Server via the Virtual IP address
Two Database Servers configured for Disaster Recovery	Primary Database Server*
Three Database Servers configured for High Availability and Disaster Recovery	Primary Database Server via the Virtual IP address*

NOTE: If a Skylar One system is configured for high availability or disaster recovery, only one of the Database Servers or All-In-One Appliances can be used as an entry point.

If disaster recovery failover occurs on a system, the devices monitored by that system will not be included in aggregated data on the Global Manager system until you update the discovered entry point to specify the disaster recovery appliance.

For more information about systems configured for high availability or disaster recovery, see the manual ***High Availability & Disaster Recovery Configuration***.

Global Manager User Authentication Requirements

On the Global Manager system and each stack entry point, you must configure appropriate user accounts and permissions for each Global Manager user.

NOTE: Starting in Skylar One version 12.3.0, the requirements for Global Manager user authentication have changed. However, the legacy method is still available for use. For more information, see *Configuring Global Manager to User Authentication Requirements*.

The following authentication rules and access permissions apply:

- Each user of the Global Manager system must have a user account on the Global Manager system, as well as an identical account with the same username and password on each stack they want to monitor.
    - If a user does not have the same credentials on a particular stack, the user will be unable to see that stack on the Global Manager system.
    - To ensure that user accounts are consistent across all Skylar One systems in your environment, ScienceLogic recommends using Active Directory or LDAP for user authentication. For information on how to use Active Directory or LDAP for authentication, see the manual ***Using Active Directory and LDAP***.

NOTE: For information on how to create user accounts, see the chapter on "Creating and Editing User Accounts" in the ***Organizations and Users*** manual.

- If you want to use a custom theme in the Global Manager system, all users must be assigned the same theme in all of the stacks being aggregated.
- The Global Manager system respects user account permissions on a given stack. If a user account for a given stack does not have permission to view events, for example, then that account will not be able to view events for that stack on the Global Manager system.
- In addition to the typical Access Hooks that are required for users to view and perform specific actions with Devices, Events, and Dashboards, there are several Access Hooks that Global Manager users must have included in an Access Key aligned to their user accounts to perform certain actions on the Global Manager system. The following table lists these Access Hooks and their corresponding actions:

Access Hook	Action
GM_STACK_VIEW	View Global Manager stacks on the **Global Manager Stacks** page. With this access hook, you can hide the Global View toggle due to user permission.
GM_STACK_ADD	Add Global Manager stacks
GM_STACK_EDIT	Edit Global Manager stacks
GM_STACK_REMOVE	Delete Global Manager stacks
TKT_CREATE	Create an event ticket. (Must have this Access Hook aligned on both the Global Manager system and the stack on which the event originated.)
TKT_ACCESS_EXTERNAL	Create/align event external tickets. (Must have this Access Hook aligned on both the Global Manager

Access Hook	Action
	system and the stack on which the event originated.)

TIP: If a user with administrator or "Grant All" access is unable to perform the above actions, ScienceLogic recommends creating a new Access Key that includes the above Access Hooks and aligning that new Access Key to the user's account.

NOTE: For more information about Access Hooks, see the ***Access Permissions*** manual.

Example: Global Manager User Account Permissions

As an example of how user account permissions work in a Global Manager system, consider the following scenario:

- A Global Manager system is configured to aggregate data from three stacks, each monitoring 10 devices.
- A user logs in to the Global Manager system using a user account and password that is valid on only two of the stacks.
- Based on the organization memberships of the user account, the user has permission to view only two devices on each of those two stacks.

In this example, the aggregated data provided to the user by the Global Manager system will include only four devices: The two devices on each of the two stacks.

Configuring User Account Authentication Requirements

Starting with Skylar One version 12.2.1, you can configure a Global Manager system to use SSO as its authentication mechanism. ScienceLogic assumes that all of your Skylar One systems have SSO set up properly. While this process currently requires you to perform some manual steps, in a future release most of this work will be automated. To configure your Global Manager system to use SSO as its authentication mechanism, you must perform the following steps:

- *Prepare your Global Manager stack*, and
- *Configure your Global Manager*

Preparing Your Stack

You will first need to create an administrator account. To do this, create a local user on the stack that the Global Manager can use to authenticate. This local user must be an administrator.

IMPORTANT: If you are using SAML SSO accounts, they must exist on the stack before signing into Global Manager. You can accomplish this by having users sign into the stack, or by using an automated process. In a future release, this process will be automated be default.

IMPORTANT: Both the stack and Global Manager must have AP2 Doughnut installed and be on the same Skylar One build version. You must update the stack first, then update the Global Manager, and ensure that AP2 Doughnut is installed on the stack first before authentication.

NOTE: You do not require identical user accounts on the Global Manger and the stack. For the user to have access to the stack from the Global manager using this authentication method, the user must exist on the stack prior. Passwords no longer need to be identical.

Configuring Global Manager

ScienceLogic assumes that the "Skylar One: Global Manager" PowerPack has been installed and the stacks have been discovered.

NOTE: If using SAML SSO authentication on the Global Manager, ScienceLogic assumes that SSO has been set up on the Global Manager.

First, create a Basic Credential for each stack. You will need to create a basic credential for each unique administrator account created on the stacks. If multiple stacks share an administrator username and password, you only need to create one credential. The Global Manager will use this basic credential to log into the stack for all requests.

NOTE: To learn more on how to create a Basic Credential, see the section on "Defining a Basic/Snippet Credential" in the ***Discovery and Credentials*** manual.

Next, enable Global Manager credentials for the **nexui** service. The **nextui** service needs an environmental variable set to enable stacks to have aligned credentials. You will need to add the following variable to the **/opt/em7/nextui/nextui.env** or **/opt/em7/ nextui/nextui.conf** file on the Global Manager:

```
GM_STACKS_CREDENTIAL=enabled
```

NOTE: Skylar One will overwrite the existing `nextui.env` file during an upgrade. For this reason, ScienceLogic strongly recommends using the **/opt/em7/ nextui/nextui.conf** instead.

If you are running a Skylar One system that is on version 12.2.1, 12.1.1 (OL8), AP2 Doughnut version 8.6.30, or higher, you will need to add an additional variable to the **/opt/em7/ nextui/nextui.conf** file on the Global Manager:

```
GM_SESSION_AUTH_CACHE_TTL_MS=0
```

After adding this variable to the file, be sure to restart the **nextui** service by running the following command:

```
sudo systemctl restart nextui
```

Finally, align the Basic Credential to the stack. Each stack needs to have a basic credential aligned using GraphQL. To do so, run the following mutation:

```
mutation alignCreds {
  alignGlobalManagerCredential(credentials: "GUID", id: "INTEGER ID OF
STACK") {
    id
    name
    credential {
      guid
      name
    }
  }
}
```

This mutation requires two parameters: the GUID of the credential you want to align, and the interger id of the Global Manager stack. You can find the GUID of the credentials by using the credentials query using the `guid` field. The following is an example query:

```
query allCredentials {
  credentials {
    edges {
      node {
        guid
        name
      }
    }
  }
}
```

Configuring Global Manager for External Event Ticketing

You can optionally configure your Global Manager system so that users can create new external tickets from the aggregated events that appear in the Global Manager system or align existing external tickets to those events. When you do so, the ticket is aligned to the corresponding event on its native stack.

NOTE: The default ticket setting in Skylar One is to create internal Skylar One tickets. In your Global Manager system, you can create internal Skylar One event tickets on the event's native stack when in non-***Global View*** mode. However, for ***Global View*** mode, you should use only external event ticketing.

To create and align event external tickets, the following configuration settings are required on both the Global Manager system and the event's native stack:

- Users must have the TKT_ACCESS_EXTERNAL Access Hook included in an Access Key that is aligned with their accounts.
- On the **Behavior Settings** page (System > Settings > Behavior), you must set the ***Event Console Ticket Life Ring Button Behavior*** field to *Create/View External Ticket*.
- You must *create run book automation actions* that perform requests to the external ticketing system.

NOTE: For more information about Access Hooks, see the chapter on "Assigning Access Hooks" in the ***Access Permissions*** manual.

For more information about the **Behavior Settings** page, see the section on "Global Settings for User Logins, Discovery, Data Collection, UI Features, and Expiration Warnings" in the ***System Administration*** manual.

For more information about creating or aligning tickets with events in the Global Manager system, see the section on *Creating and Aligning Event Tickets*.

Using Run Book Automation to Populate the Skylar One with Values from External Tickets

The following two fields in the *master_events.events_active* Skylar One database table populate the values for external tickets on the **Events** page:

- ***force_ticket_uri***. This field contains the URI that leads to the external ticket. Selecting the *Create Ticket* option on the **Events** page opens a new window with this URI loaded.
- ***ext_ticket_ref***. This field contains the name or ID number associated with the external ticket. This value is displayed in the ***Ticket External Reference*** column on the **Events** page.

To integrate events with an external ticketing system, you must create run book automation actions that perform requests to the external ticketing system and populate the ***force_ticket_uri*** and ***ext_ticket_ref*** fields in the *master_events.events_active* table.

The following run book automation policies and actions could be used to integrate events with an external ticketing system:

- An automation policy that runs when events are created. Depending on your business needs, this automation policy might run when an event is acknowledged or when a user selects the *Create Ticket* option on the **Events** page. This automation policy would execute the following actions:
    - One or more snippet actions that create a ticket in the external ticketing system. The ticket can be created using one or more of the available variables; for example, %M contains the message text for the event that triggered the automation policy. One of the snippet actions could pass the ticket ID for the ticket to Skylar One.
    - An SQL query action that updates the ***ext_ticket_ref*** and ***force_ticket_uri*** fields for the event. The value of ***ext_ticket_ref*** should be set to the value passed by the previous snippet action (accessed using the %_EM7_RESULT_% variable). The SQL query should use the %e variable (the event ID for the event that triggered the automation policy) to ensure that the query updates the correct event.
- An automation policy that runs when events are cleared. This automation policy would execute a snippet action that:
    - Performs an SQL query to retrieve the ***ext_ticket_ref*** value for the event that triggered the automation policy.
    - Resolves the appropriate ticket in the external ticketing system.

NOTE: For more information about creating run book automation policies, see the chapter on "Automation Policies" in the ***Run Book Automation*** manual.

Installing the ScienceLogic: Global Manager PowerPack

After ensuring that the All-In-One Appliance that you are going to use as your Global Manager system meets the appropriate *system requirements*, you must download and install the *ScienceLogic Global Manager* PowerPack on that All-In-One Appliance.

This PowerPack includes the run book actions and Dynamic Applications that the Global Manager system uses to identify stacks and add them to your Global Manager system.

NOTE: To use run book actions that automatically add newly discovered stacks to your Global Manager system, you must install version 3.0.1 or later of the *ScienceLogic Global Manager* PowerPack.

NOTE: The *ScienceLogic Global Manager* PowerPack is not included in the standard release and is provided separately by ScienceLogic. Contact ScienceLogic Customer Care to obtain the PowerPack.

NOTE: For more information about installing a PowerPack, see the section on "Installing a PowerPack" in the ***PowerPacks*** manual.

Enabling and Configuring Global Manager on an All-in-One Appliance

To configure an All-In-One Appliance as a Global Manager system, you must first edit the NextUI configuration file to enable Global Manager on that appliance.

Optionally, you can also configure the following settings:

- *Stack Timeout*. When the Global Manager system makes a request to a stack, it times out after 4 seconds by default. If the stack does not respond within that time frame, it will issue a "stack timeout" message and will be cached as unavailable, if cache is enabled. This will prevent the Global Manager system from attempting to contact the stack until the cache has expired. You can update this setting to provide the Global Manager system more or less time before stack requests time out.
- *Stack State Cache*. When the Global Manager system makes a request to a stack, it saves the stack's state in cache. The next time the Global Manager system makes a request, it will check the cache and send a request only to stacks that are responsive. This prevents the Global Manager system from having to wait the full stack timeout on stacks that are known to time out. By default, the Global Manager system waits 10 minutes before clearing stale stack cache. You can disable this setting or update the wait time before stale stack cache is cleared.

To enable and configure Global Manager on an All-In-One Appliance:

1. Start an SSH session into the All-In-One Appliance.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

```
sudo vi /opt/em7/nextui/nextui.conf
```

3. In the NextUI configuration file, add the following line at the bottom to enable Global Manager on the All-In-One Appliance:

```
GLOBAL_MANAGER=enabled
```

4. Optionally, to update the stack timeout setting, add the following line to the NextUI configuration file, replacing "[value]" with the desired timeout setting, in milliseconds:

```
GM_STACK_TIMEOUT_MS=[value]
```

5. Optionally, to update the stack state cache setting, add the following line to the NextUI configuration file, replacing "[value]" with "0" (zero) to disable the feature or with the desired timeout setting, in milliseconds:

```
GM_STACKS_CACHE_TTL_MS=[value]
```

6. Restart the NextUI service by running the following command:

```
sudo systemctl restart nextui
```

Discovering Global Manager Stacks

After *installing the ScienceLogic Global Manager PowerPack* on an All-In-One Appliance and then *enabling Global Manager* on that appliance, you must use SNMP to discover a Database Server or All-In-One Appliance entry point for each stack that you want to manage globally.

The *ScienceLogic Global Manager* PowerPack then enables you to add the stacks to your Global Manager system using one of two methods:

- *Add newly discovered stacks automatically using Run Book Actions*, or
- *Add existing stacks by manually aligning a Dynamic Application* and performing some additional configuration to the Global Manager system

Both methods are described in the sections below.

NOTE: ScienceLogic strongly recommends automatically adding newly discovered stacks to the **Global Manager Stacks** page using Run Book Actions (RBAs), as opposed to adding stacks manually using Dynamic Applications. The former method requires fewer license counts for your Global Manager system, and does not require manual Dynamic Application alignment.

Discovery Option 1: Adding Stacks Automatically Using Run Book Actions

The *ScienceLogic Global Manager* PowerPack includes Run Book Actions that automatically detect any newly discovered Skylar One Database Server or All-In-One Appliance entry points and then adds the appliances as stacks in your Global Manager system.

NOTE: This method applies only to newly discovered stacks. To add existing stacks to your Global Manager system, see *Adding Stacks Using Dynamic Applications*.

NOTE: Only one entry point can be used per stack. Do not use SNMP-based discovery to discover more than one entry point per stack.

NOTE: To use run book actions that automatically add newly discovered stacks to your GM system, you must install version 3.0.1 or later of the *ScienceLogic Global Manager* PowerPack.

To add stacks to the Global Manager system using Run Book Actions:

1. Create an SNMP credential for each Database Server or All-In-One Appliance stack entry point that you want to monitor in your Global Manager system.
2. Use the unguided discovery process to discover one Database Server or All-In-One Appliance entry point for each stack that you want to add to your Global Manager system. When doing so, select the SNMP credential that you created in the previous step.
3. Optionally, you can repeat steps 1 and 2 to discover the All-In-One Appliance that you are configuring as a Global Manager system, but this is not required.
4. When you discover a new stack entry point, the Run Book Actions that are included in the *ScienceLogic Global Manager* PowerPack detect the newly discovered Database Server or All-In-One Appliance entry point and then adds the stack to the **Global Manager Stacks** page (◈) in the Global Manager system.

NOTE: For more information about creating an SNMP credential, see the section on "Defining an SNMP Credential" in the ***Discovery and Credentials*** manual.

For more information about using the unguided discovery process, see the section on "Adding Devices Using Unguided Discovery" in the ***Discovery and Credentials*** manual.

Discovery Option 2: Adding Stacks Using Dynamic Applications

The *ScienceLogic Global Manager* PowerPack includes a Dynamic Application that you can manually align to the All-In-One Appliance that you are configuring as a Global Manager system.

This Dynamic Application creates a component device for each Database Server or All-In-One Appliance entry point that you have discovered using SNMP. You can then merge the component device records with the corresponding devices' SNMP records.

NOTE: Only one entry point can be used per stack. Do not use SNMP-based discovery to discover more than one entry point per stack.

To add stacks to the Global Manager system using Dynamic Applications:

1. Create an SNMP credential for each Database Server or All-In-One Appliance stack entry point that you want to monitor in your Global Manager system.
2. Create an SNMP credential for the All-In-One Appliance that you are configuring as a Global Manager system.
3. Use the unguided discovery process or a classic discovery session to discover one Database Server or All-In-One Appliance entry point for each stack that you want to add to your Global Manager system, as well as the All-In-One Appliance that you are configuring as a Global Manager system. When doing so, select the SNMP credentials that you created in steps 1 and 2.
4. Assign the ***ScienceLogic Global Manager*** device class to the All-In-One Appliance that you are configuring as a Global Manager system.
5. Disable ***Auto-Update*** for the All-In-One Appliance that you are configuring as a Global Manager system.
6. Create a SOAP/XML credential for the All-In-One Appliance that you are configuring as a Global Manager system. Use the default settings for all fields except for the following settings:
    - ***Profile Name***. Type a name for the credential.
    - ***URL***. Type "https://%D".
    - ***Username***. Type the username of an account that has access to all API functions on the All-In-One Appliance that you are configuring as a Global Manager system.
    - ***Password***. Type the password for the user you entered in the ***Username*** field
7. Align the ***ScienceLogic: GM Root Stack Inventory*** Dynamic Application to the device record for the All-In-One Appliance that you are configuring as a Global Manager system. Use the credential you created in step 6 with this Dynamic Application.

NOTE: If you are using a self-signed certificate, you must edit the snippet in the ***ScienceLogic: GM Root Stack Inventory*** Dynamic Application to set USING_TRUSTED_CERT to False.

8. When collection is performed for the ***ScienceLogic: GM Root Stack Inventory*** Dynamic Application, Skylar One creates a component device for each entry point.
9. In the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), click the **[Actions]** button and then select *Merge Devices*. The **Device Bulk Merge** page displays. Merge the SNMP-based device records for each entry point with the equivalent component device records. To do this:
    - Select the *Names Match* checkbox in the **Device Bulk Merge** page.
    - The page displays a row for each entry point for which the name of the SNMP-based device record matches the name of the component device record. Select the radio button for each pair of entry points.
    - Click the **[Merge]** button.

    The component devices for each entry point are automatically subscribed to the ***ScienceLogic: GM Distributed Appliance Discovery*** Dynamic Application. The ***ScienceLogic: GM Distributed Appliance Discovery*** Dynamic Application will examine each entry point; if the entry point is part of a distributed system, the Dynamic Application will create a component device record for each additional appliance in the distributed Skylar One system.

NOTE: For more information about creating an SNMP credential, see the section on "Defining an SNMP Credential" in the ***Discovery and Credentials*** manual.

For more information about using the unguided discovery process, see the section on "Adding Devices Using Unguided Discovery" in the ***Discovery and Credentials*** manual.

For more information about assigning a device class to a device, see the section on "Manually Assigning an Device Class to a Device" in the ***Device Management*** manual.

For more information about disabling ***Auto-Update***, see the section on "The Settings Tab" of the Device Investigator in the ***Device Management*** manual.

For more information about creating a SOAP/XML credential, see the section on "Defining a SOAP/XML Credential" in the ***Discovery and Credentials*** manual.

For more information about manually aligning a Dynamic Application to a device, see the section on "Manually Aligning a Dynamic Application to a Device" in the ***Device Management*** manual.

For more information about editing snippets in a Dynamic Application, see the ***Snippet Dynamic Application Development*** manual.

For more information about merging device records, see the section on "Merging Devices" in the ***Device Management*** manual.

Verifying Successful Global Manager Configuration

After you have discovered your stacks and added them to your Global Manager system using either of the two possible methods, you can verify that your Global Manager system is configured successfully on the following pages:

- On the **Global Manager Stacks** page (), verify the following:

    - All of the stacks you discovered using SNMP display on the page.
    - All stacks indicate the expected Skylar One version in the ***Version*** column.
    - All stacks indicate the same Skylar One version in the ***Version*** column as the version that appears in the **Platform** section when you click your username in the top navigation bar and select *About*.
- On the **Events** page (⚠), toggle on the **[Global View]** button and verify that events from all operational stacks display on the page and that there are no indications of unresponsive stacks.
- On the **Devices** page (), toggle on the **[Global View]** button and verify that devices from all operational stacks display on the page

Chapter 3

Viewing and Managing Global Stacks

Overview

This chapter describes how to view and manage a list of Skylar One (formerly SL1) stacks from which the Global Manager system can aggregate data.

Use the following menu options to navigate the Skylar One user interface:

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

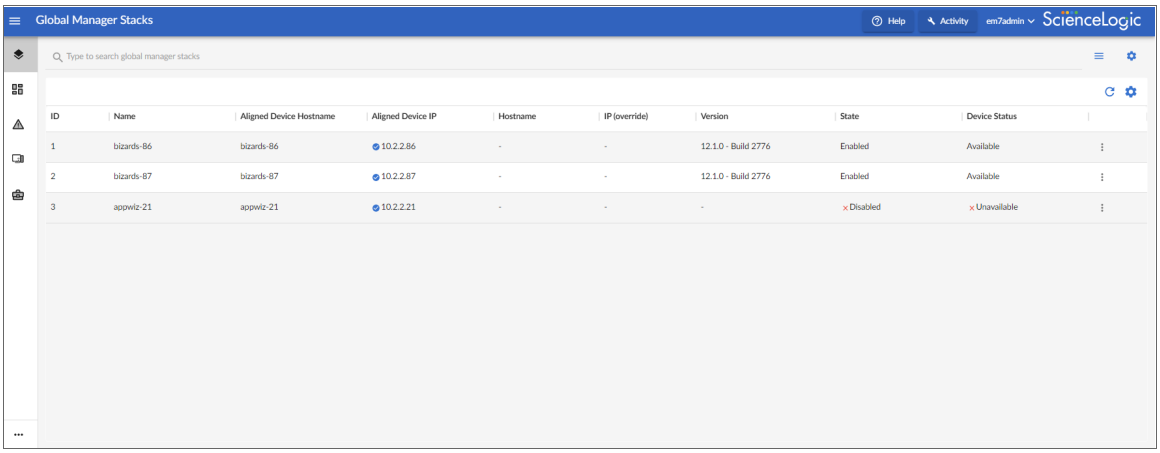
This chapter covers the following topics:

Viewing a List of Global Manager Stacks

The **Global Manager Stacks** page displays a list of all Skylar One stacks from which the Global Manager system is aggregating data.

When you discover the entry points to each stack using SNMP, Skylar One uses the Dynamic Applications and Run Book Actions that are included in the *ScienceLogic Global Manager* PowerPack to automatically add the discovered stacks to the **Global Manager Stacks** page.

To navigate to the **Global Manager Stacks** page, click the Global Manager Stacks icon ( ):



TIP: If you are looking for a very specific set of stacks, click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" operators for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

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

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

For each stack, the **Global Manager Stacks** page displays the following information:

- ***ID***. The numeric ID assigned to the stack by the Global Manager system.
- ***Name***. The name of the stack. This name defaults to the device name of the discovered entry point, but you can edit this name if you have the appropriate user permissions.

- ***Aligned Device Hostname***. The hostname of the discovered entry point.
- ***Aligned Device IP***. The IP address of the discovered entry point.
- ***Hostname (Override)***. The user-entered hostname that the Global Manager system uses to access the stack instead of the discovered entry point hostname listed in the ***Aligned Device Hostname*** field.
- ***IP (Override)***. The user-entered IP address that the Global Manager system uses to access the stack instead of the discovered entry point IP address listed in the ***Aligned Device IP*** field.

NOTE: By default, the Global Manager system will use the hostname or IP address of the discovered entry point, as listed in the ***Aligned Device Hostname*** and ***Aligned Device IP*** columns, to communicate with the stack, with deference given to a hostname over an IP address.

However, if the device name of a discovered entry point is not the fully qualified domain name of that entry point, you can specify that the Global Manager system use a different hostname or IP address to access the entry point instead. To do so, edit the stack information and enter a different hostname or IP address in the ***Hostname (Override)*** or ***IP (Override)*** field.

The Global Manager system will use the following field precedence to determine which hostname or IP address to use for communicating with the stack: ***Hostname (Override)*** > ***IP (Override)*** > ***Aligned Device Hostname*** > ***Aligned Device IP***. On the **Global Manager Stacks** page, a check mark icon (✔) will display next to the hostname or IP address that the Global Manager system is using.

- ***Version***. The version of Skylar One running on the stack.
- ***Device Status***. Indicates whether the discovered entry point is available or unavailable.
- ***State***. Indicates whether the Global Manager will include the stack when executing Global Manager features. Possible values are:
  - *Enabled*. The Global Manager will include the stack when executing Global Manager features. Results from the stack will be included in aggregated views.
  - *Disabled*. The Global Manager will not include the stack when executing Global Manager features. Results from the stack will not be included in aggregated views.

NOTE: When deploying or upgrading Global Manager systems, the Global Manager stack and all of its child stacks must run on the same Skylar One build version, as well as the same versions of AP2 and Oracle Linux.

Editing the Properties of a Stack

If you have the *appropriate user permissions*, you can edit the properties of a particular stack from the **Global Manager Stacks** page, or enable or disable a stack.

To edit the properties of a stack:

1. From the **Global Manager Stacks** page (), click the **[Actions]** button ( ) for the stack you want to edit, and then select *Edit*. The **Edit Stack** modal appears.
2. On the **Edit Stack** modal, change the values in one or more of the following fields:
    - ***Stack Name***. Type a new name for the stack.
    - ***Select Aligned Device***. Select the device record that represents the entry point for the stack.
    - ***Hostname (Override)***. By default, the Global Manager system will use the hostname or IP address of the discovered entry point to communicate with that entry point. If you want the Global Manager system to access the API on the stack entry point using a hostname that is different from the hostname of the device selected in the ***Select Aligned Device*** field, type the preferred hostname in this field.
    - ***IP (Override)***. By default, the Global Manager system will use the hostname or IP address of the discovered entry point to communicate with that entry point. If you want the Global Manager system to access the API on the stack entry point using an IP address that is different from the IP address of the device selected in the ***Select Aligned Device*** field, type the preferred IP address in this field.
    - ***Enabled/Disabled***. Select whether the Global Manager will include the stack when executing Global Manager features. Possible values are:
        - *Enabled*. The Global Manager will include the stack when executing Global Manager features. Results from the stack will be included in aggregated views.
        - *Disabled*. The Global Manager will not include the stack when executing Global Manager features. Results from the stack will not be included in aggregated views.
3. Click **[Save]**.

NOTE: Alternatively, you can enable or disable a stack from the **Global Manager Stacks** page by clicking the **[Actions]** button ( ) for that stack and then selecting *Enable* or *Disable*.

Chapter 4

Viewing Global Devices

Overview

This chapter describes how to view devices in the Skylar One (formerly SL1) Global Manager system. You can view devices on the **Devices** page, which you can access by clicking the Devices icon ( ). From there, you can select a device from the list to view detailed data on the *Device Investigator* page for that device.

For more information about how the Skylar One Global Manager consolidates operations in a single view, view the video at https://youtu.be/uRrkvX9khNs.

Use the following menu options to navigate the Skylar One user interface:

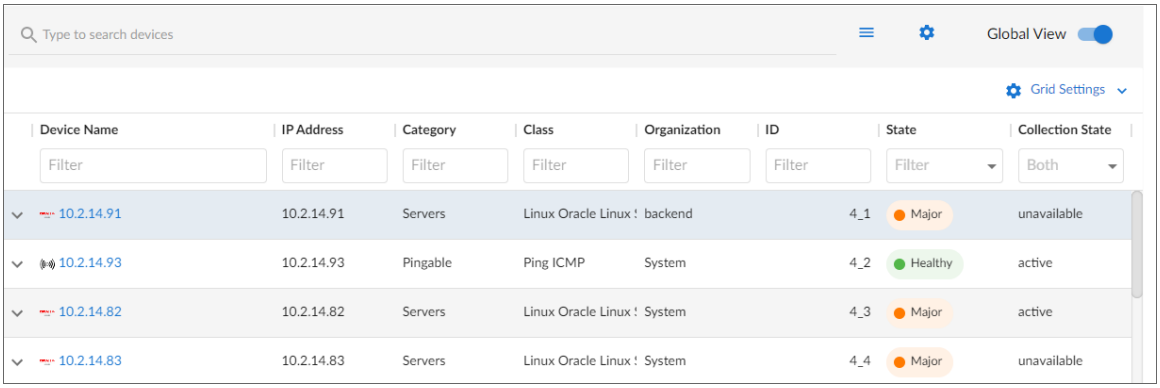
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter covers the following topics:

Viewing the Global List of Devices

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

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



In a Global Manager system:

- When the **[Global View]** button on the **Devices** page is toggled ***on***, you can view a list of all of the devices discovered across all of the stacks in your Global Manager system.
- When the **[Global View]** button on the **Devices** page is toggled ***off***, you can view a list of devices discovered only on the Global Manager system itself.

NOTE: You cannot add devices from the **Devices** page while in Global View mode. You can add devices on a particular stack only while on that stack in non-Global View mode.

TIP: If you are looking for a very specific set of devices, click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing and Advanced Search" topic in the ***Introduction to Skylar One*** manual.

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

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

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

For each device, the **Devices** page can display the following information:

- ***ID***. The Device ID. This is a unique number that Skylar One automatically assigns to the device during discovery.
- ***Device Name***. Name of the device. For devices running SNMP or with DNS entries, the name is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The device's IP address.
- ***Class***. The manufacturer and type of device. The device class is automatically assigned during discovery, at the same time as the category.
- ***Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, and printers, among others. The category is automatically assigned during discovery, at the same time as the as device class. For more information about device categories, see the chapter on "Managing Device Classes and Device Categories" in the ***Device Management*** manual.
- ***Organization***. The organization to which the device is assigned.
- ***State***. The current condition of the device, based upon events generated by the device. The device can have one of the following States:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.
    - *Notice*. Device has an informational event associated with it.
    - *Healthy*. Device is running with no problems.
- ***Collection State***. The current condition of data collection for the device. The device can have one or more of the following Collection States:
    - *Active*. Skylar One is collecting data from the device.
    - *Unavailable*. Skylar One cannot connect to the device, and will not collect data from the device until the device becomes available. A physical device falls back to executing the availability ping every five minutes, unless you have critical ping enabled. Component devices get their availability calculated by the component discovery Dynamic Application of the parent device.

- *User-Disabled*. Skylar One is not currently collecting data from the device because the user has disabled collection.
- *System-Disabled*. Skylar One is not currently collecting data from the device because the system has disabled collection.
- *Scheduled Maintenance*. Skylar One is not currently collecting data from the device because it is currently in scheduled maintenance mode.
- *User-Initiated-Maintenance*. Skylar One is not currently collecting data from the device because it has manually been put into maintenance mode by a user.
- *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. Skylar One cannot collect data from the device at this time.

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

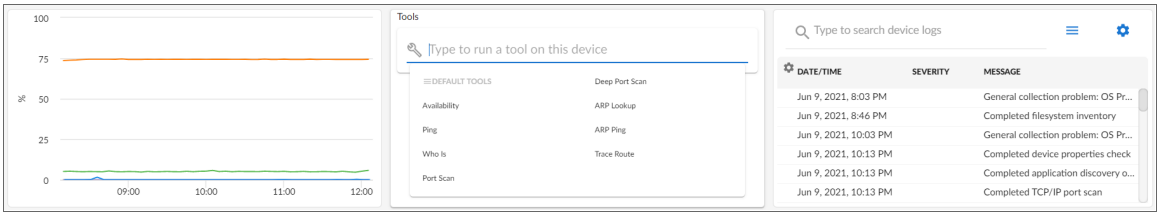
- ***Collector Group***. The collector group to which the device belongs. Collector groups are groups of Skylar One Data Collectors, which are defined on the **Collector Groups** page (Manage > Collector Groups).
- ***SNMP Credential***. The name of the SNMP credential used to monitor the device.
- ***SNMP Version***. The version of SNMP used to monitor the device.
- ***Hostname***. The fully qualified hostname for the device, for devices that are discovered and managed by hostname (instead of IP address). This column does not appear by default, but you can add it by clicking **Grid Settings** > *Column Preferences*.
- ***Date Created***. The date and time on which the device was created.
- ***Organization ID***. The unique numeric identifier of the organization to which the device is assigned.
- ***Class ID***. The unique numeric identifier of the device class.
- ***Category ID***. The unique numeric identifier of the device category assigned to the device.
- ***Type***. The type of device. Options include:
  - *Physical*. A hardware-based device with an IP address.
  - *Component*. An entity that runs under the control of a management device.
  - *Virtual*. A container for collected data.
- ***Collector Group ID***. The unique numeric identifier of the collector group to which the device belongs.
- ***Asset ID***. The ID of any asset associated with the device. The asset ID displays as a hyperlink that you can click to view the asset's properties. For more information about assets, see the ***Asset Management*** manual.
- ***Last Poll***. The date and time at which Skylar One last polled the device.
- ***Uptime***. The amount of time since the device was last initialized.

- ***SL Agent***. Indicates whether an Skylar One agent is installed on the device. If so, you can click the ***Yes*** hyperlink to display a modal where you can update the agent's configuration.
- ***Stack Name***. The name of the stack on which the device was discovered.
- ***Stack ID***. The numeric ID of the stack on which the device was discovered.

NOTE: If you have defined any custom attributes for your devices, you can also add those custom attributes as columns that appear on the **Devices** page.

Viewing Additional Data about a Device

On the **Devices** page, 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:



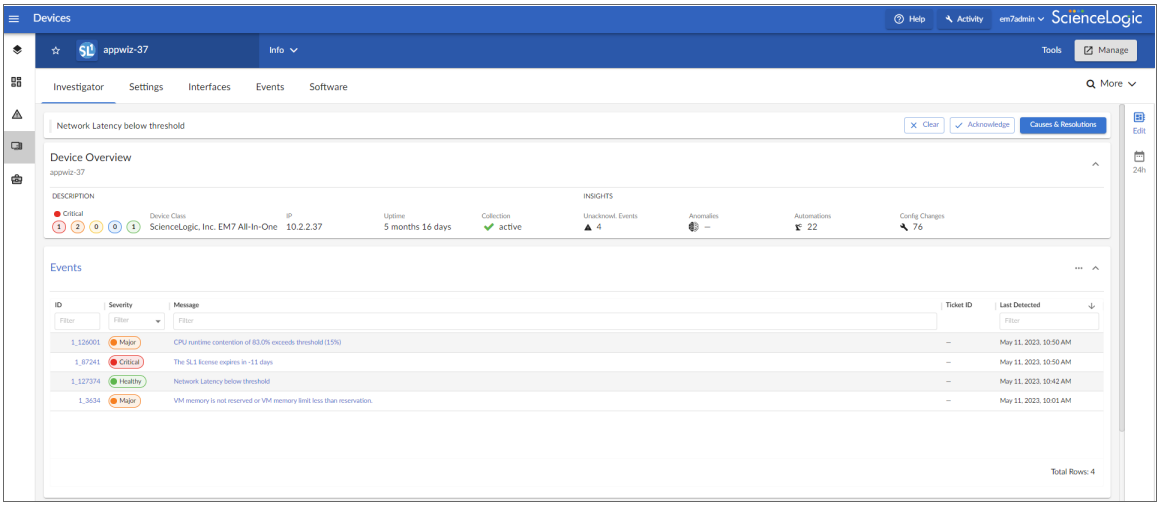
The Device Drawer contains the **Vitals** graph pane and the **Logs** pane.

- The **Vitals** pane displays graph data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging your cursor over a timeframe, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Tools** pane enables you to run a set of diagnostic tools or user-initiated actions in the **Activity Center**, or to click on custom links that will open in a separate browser window. Click the search bar to search for tools, actions, or custom links that are available for the device. For more information, see the section on *Using the Activity Center*.
- The **Logs** pane displays a list of events associated with that device.

TIP: From the list of devices, click the device name to go to the **Device Investigator** page for more details about that device. For more information, see the *Device Investigator* section.

Using the Device Investigator

You can view detailed data about a specific device by clicking the device name on the **Devices** page to open the **Device Investigator** page for that device:



The tabs on the **Device Investigator** page provides access to data associated with a device.

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

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

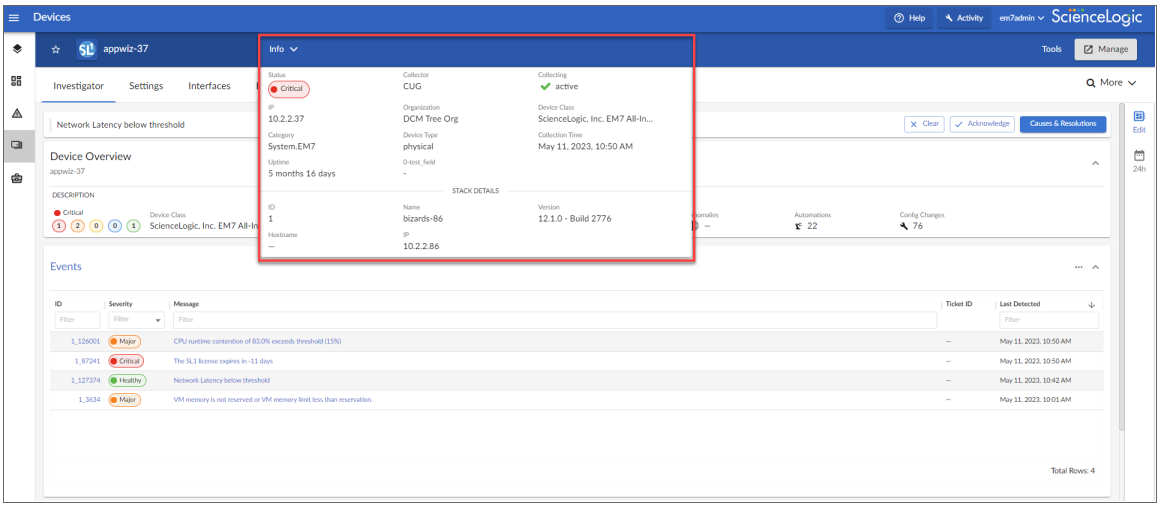
- *Info*. This drawer on the **[Investigator]** tab displays additional information about the device, along with the most recently updated values for uptime and collection time.
- *Tools*. This button opens the **Activity Center**, where you can run a set of diagnostic tools or user-initiated actions, or click on custom links that will open in a separate browser window.
- ***Manage***. In Global View mode, the **Device Investigator** displays only a few of the tabs that appear in the **Device Investigator** in non-Global View mode. The tabs that appear in the **Device Investigator** in Global View mode let you view some device data but not manage the device or change any of its settings. Click the **[Manage]** button to view the full **Device Investigator** and manage the device on its native stack in a separate browser window. After editing the device and saving your changes, you can either close the window to return to Global View mode or keep it open to continue managing the device on its native stack in non-Global View mode.

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

- *Investigator*. 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 under the **Device List** pane on the left side of the screen. You can also compare devices on this tab.
- *Settings*. Enables you to manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more. You can also set user maintenance preferences and disable or enable collection on that device.
- *Configs*. Displays configuration information collected from the device by Dynamic Applications. If the device does not have any configuration data, this tab does not appear.
- *Events*. Displays a list of active and cleared events for the device. You can acknowledge events from this tab or add event notes.
- *Interfaces*. Displays information about the interfaces used by the device. If this device does not use interfaces, this tab does not appear.
- *Software*. Displays a list of all software installed on the device.
- ***More***. This drop-down list lets you select additional tabs to display on the **Device Investigator** page by clicking the star icon next to the tab name. You can search for specific items on a tab and the relevant tab will appear in the search results. You can also remove a tab by clicking the star icon again, turning it from blue to white. Your tab selections are saved and persist until you change them.

Using the Info Drawer on the Device Investigator Page

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



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

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

Additionally, the ***Info*** drawer also displays the following stack information for devices in Global Manager systems:

- ***ID***. The numeric ID of the stack on which the device was discovered.
- ***Name***. The name of the stack on which the device was discovered.
- ***Version***. The Skylar One (SL1) version running on the stack on which the device was discovered.
- ***Hostname***. The hostname of the stack on which the device was discovered.
- ***IP***. The IP address of the stack on which the device was discovered.

Using Device Tools in the Action Runner

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

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

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

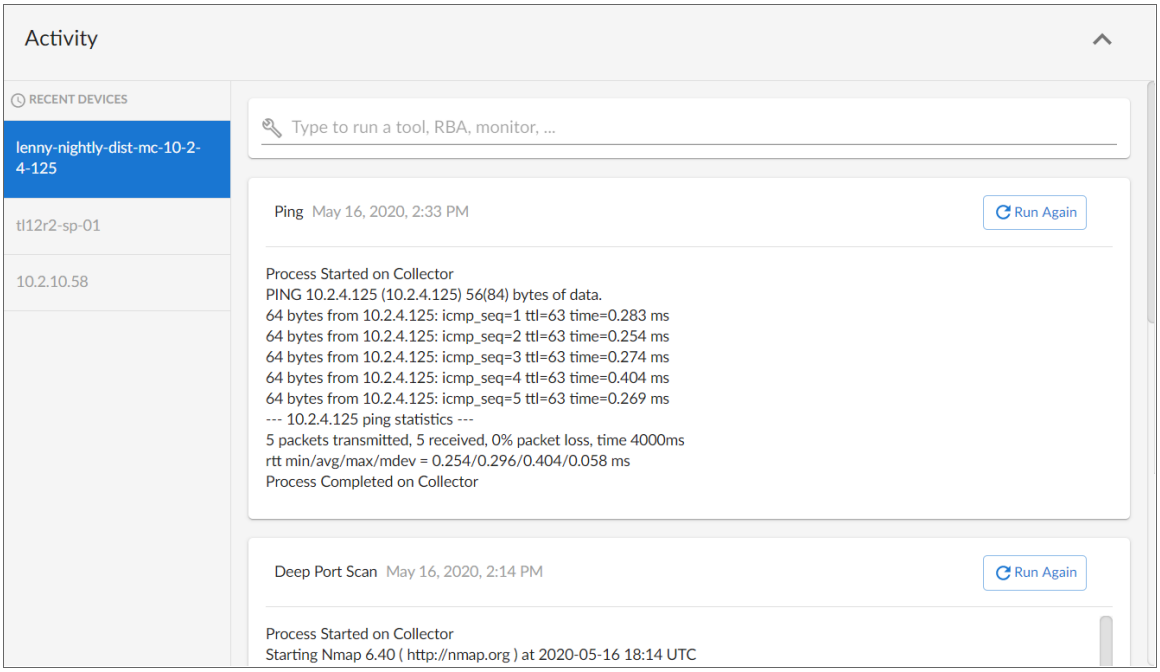
To use the **Action Runner**:

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

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

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

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



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

Managing a Device in a Separate Window

In Global View mode, the **Device Investigator** displays only a few of the tabs that can appear in the **Device Investigator** in non-Global View mode. The tabs that do appear in the **Device Investigator** in Global View mode enable you to *view* some device data but not *manage* the device or change any of its settings.

To manage a device, click the **[Manage]** button in the top-right corner of the **Device Investigator** while in Global View mode. When you do so, Skylar One opens the full **Device Investigator** for that device on its native stack in a separate browser window.

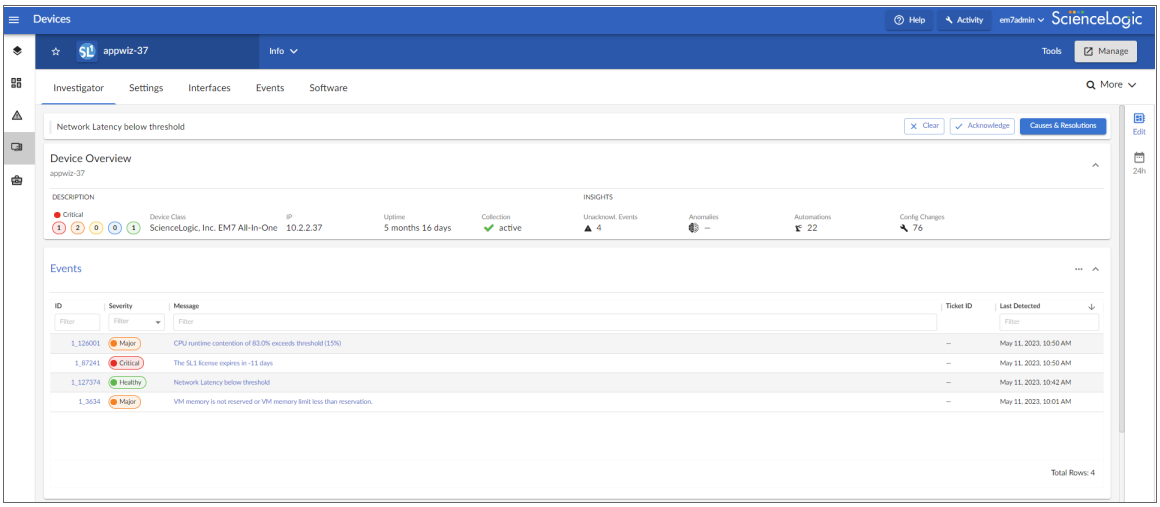
> **NOTE:** For more information about all of the device management options available in non-Global View mode, see the ***Device Management*** manual.

Overview of the Device Investigator Tabs

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

The Investigator Tab

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



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

- ***Device Overview***. Displays a panel that includes basic information about the device, including its current state, device class, IP address, uptime, collection status, unacknowledged event count, machine learning-based anomaly detection status, automated actions count, and configuration changes count.
- ***Events***. Displays a panel with the list of events aligned with this device. In the right-hand pane, you can click the **ID** or **Message** field to view the **Event Investigator** page for that event. You can also click the **Events** panel heading to go to *the **[Events]** tab* for that device.

> **NOTE:** If your device has Skylar Automated RCA suggestions, custom alerts, or accepted alerts, you can click the **[VIEW]** link on the banner that appears at the top of the **Device Investigator** page to go to the **[Events]** tab for that device to review the Skylar Automated RCA content.

> **TIP:** From the **Event Investigator** or **Service Investigator** pages, if you click the name of the device where an event has occurred, you are redirected to the **Device Investigator** page for that device, with an event context panel displaying at the top of the page. From this panel, you can acknowledge, clear, or view causes and resolutions relating to that specific event.

- ***Logs***. Displays a panel with a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting. You can also click on the column headers for ***Date/Time***, ***Source***, ***Event ID***, ***Severity***, and ***Message*** to sort by that column.
- ***Relationships and Membership***. Displays a panel that includes details about the other devices that have relationships to the selected device, as well as the device groups and services to which the device belongs or has membership.
    - The **[Device Relationship]** tab displays the name, relationship type, relationship discovery method, and health for each device that has a relationship with the selected device. You can click the hyperlink in the ***Device Name*** column to go to the **Device Investigator** for the related device.
    - The **[Device Groups]** tab displays the name, device count, and ID for each device group to which the selected device belongs or has membership.
    - The **[Services]** tab displays the name, type, status, description, health, availability, and risk for each service to which the selected device belongs or has membership. You can click the hyperlink in the ***Service Name*** column to go to the **Service Investigator** for the related service.
- ***Map***. Displays a panel with a map of the device and all of the devices with which the device has relationships. You can also click the **Map** panel heading to go to the **[Map]** tab for that device. This panel is disabled by default, but can be enabled by clicking the **[Edit]** button, and then selecting the ***Map*** checkbox.

NOTE: You can customize the appearance of the widgets on the page, including changing their height or width. For more information, see the section on *Customizing the Appearance of Widgets on the Investigator Tab*.

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

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

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

Adding and Removing Metrics on the Investigator Tab

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

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

1. To add a metric panel that is not currently on the **[Investigator]** tab, click the **[Edit]** button on the right sidebar to expand the layout panel, click **[Edit Panels]**, and then click the ***Add a metric*** field. A list of metrics appears:
2. Select a metric from the list, or type the name of a metric and select it from the list. The metric is added to the right pane, and a corresponding widget appears in the left pane.
3. Some metrics might require you to make additional selections, such as the network interfaces associated with a device. Click the field and add one or more additional metrics, as needed.

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

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

NOTE: The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis.

Editing the Metric Panel Order on the Investigator Tab

You can prioritize the order in which information is presented on the **[Investigator]** tab of the **Device Investigator** by changing the order in which the metric panel widgets appear on the page. You can click the **[Edit]** button on the right side of the page and then drag and drop the panels up or down in the right panel to edit the order in which the metric panels appear on the left panel.

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

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel.
2. Hover your mouse over the "Panel" heading of the panel that you want to move until you see an open hand icon appear.
3. Click and hold down the left button on your mouse to grab the panel, and then use your mouse to drag the panel to a different location in the list. When you do so, the open hand icon becomes a closed hand icon, and a blue dotted box appears around the panel.
4. Release the left mouse button to drop the panel in your desired location. The new right-hand panel order will be reflected in the left-hand widget panel.

NOTE: The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis.

Combining Charts on the Investigator Tab

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

To combine charts:

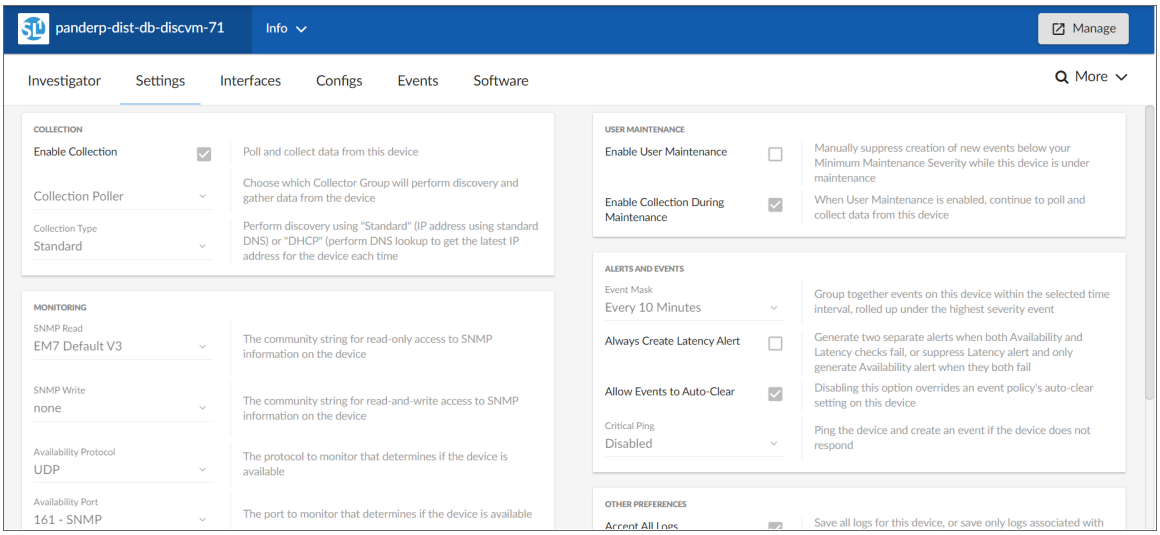
1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel.
2. Hover your mouse over a time-series metric name until you see an open hand icon appear.
3. Click and hold down the left button on your mouse to grab the metric, and then use your mouse to drag the metric into the panel of a different time-series metric in the list. When you do so, the open hand icon becomes a closed hand icon, and the panel containing the combined metrics turns blue.
4. Release the left mouse button to drop the metric into the desired panel. The newly combined metric panel will be reflected in a "Combined Charts" widget in the left-hand widget panel.

NOTE: The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis.

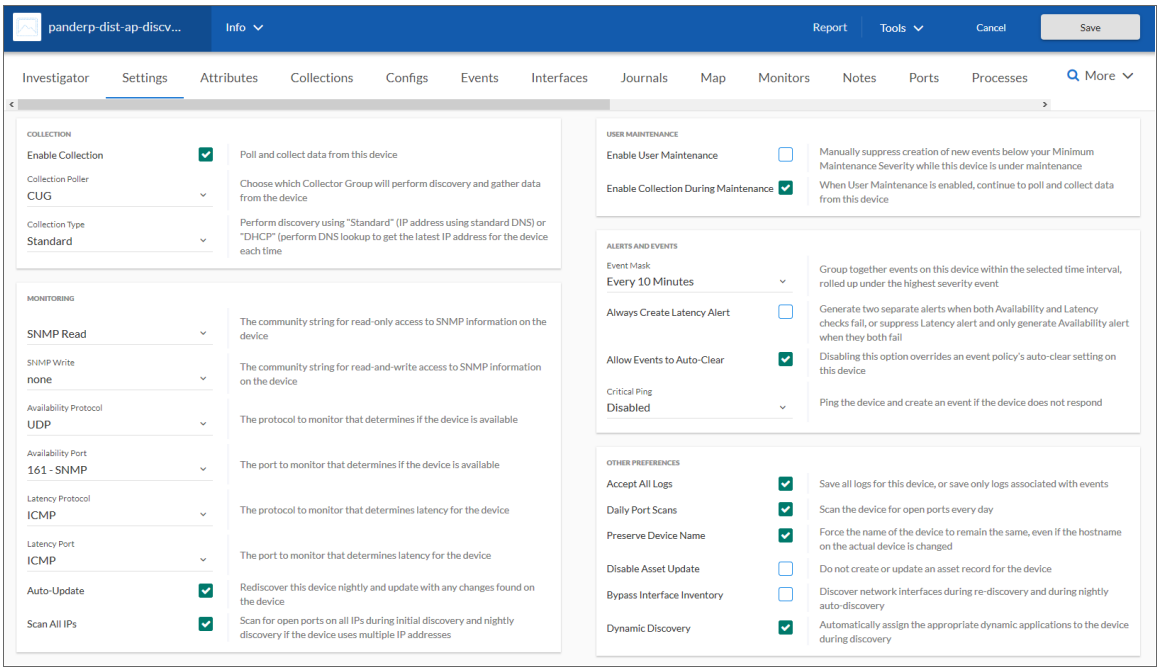
The Settings Tab

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

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



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



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

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

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

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

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

- ***Collect File Information***. Select this option if you want the agent to report the names of files accessed by each monitored process.
- ***Collect Named Pipe Information***. Select this option if you want the agent to collect named pipe information.
- ***Collect Socket Information***. Select this option if you want the agent to collect socket information.
- ***Collect Thread Information***. Select this option if you want the agent to collect thread information.
- ***Collect Non-Intercepted Processes***. Select this option if you want the agent to collect limited information for processes that do not contain the agent library.
- ***Processes Aggregation***. Specify how you want the agent to collect limited information for processes that do not have the agent library in them, and how to aggregate short-lived processes. Your options include the following:
  - *All*: Aggregate every short-lived process into its parent.
  - *None*: Do not aggregate any short-lived process.
  - *Without Sockets*: Aggregate short-lived processes unless those processes have sockets.
- ***Upload Interval***. Specify how often the agent should upload data. Your options include the following:

- *20 Seconds*. Upload a data snapshot every 20 seconds.
- *60 Seconds*. Upload a data summary every 60 seconds. This is the default setting starting with Skylar One version 11.1.0, and version 174 of the Linux agent and version 133 for the Windows agent. This option uses an improved data format that requires fewer Skylar One resources. The Skylar One agent continues to internally collect and poll data every 20 seconds, but the agent summarizes and uploads that data every 60 seconds. There is no data loss even though the data is uploaded less frequently.

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

Set the following **Collection** preferences:

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

Set the following **Monitoring** preferences:

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

Set the following **User Maintenance** preferences:

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

- ***Enable Collection During Maintenance*** . Specifies whether Skylar One will poll the device when user maintenance mode is enabled. If you select *Enabled*, Skylar One will continue to poll and collect data from this device during user maintenance mode.

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

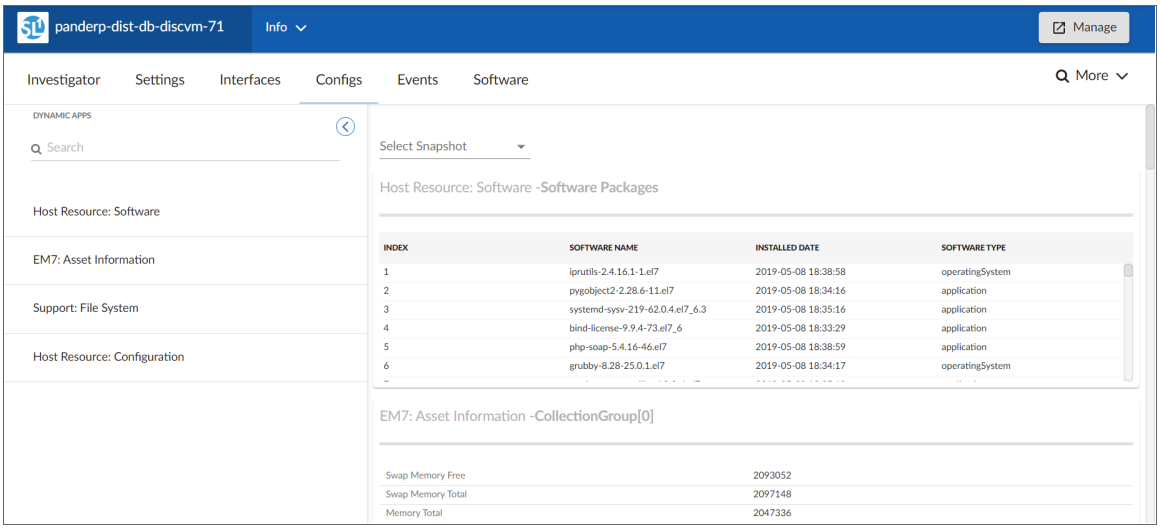
- ***Event Mask***. Specify the time frame for masking events. When a device uses the Event Mask setting, Skylar One groups together events that occur on that device within the specified span of time.
- ***Always Create Latency Alert***. Select this option to generate two alerts when availability and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

Set the following **Other** device preferences:

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

The Configs Tab

On the **[Configs]** tab of the **Device Investigator**, you can view configuration information that has been collected from the device by Dynamic Applications. You can also view a list of all changes that occurred with a Dynamic Application between two specific snapshot reference points.

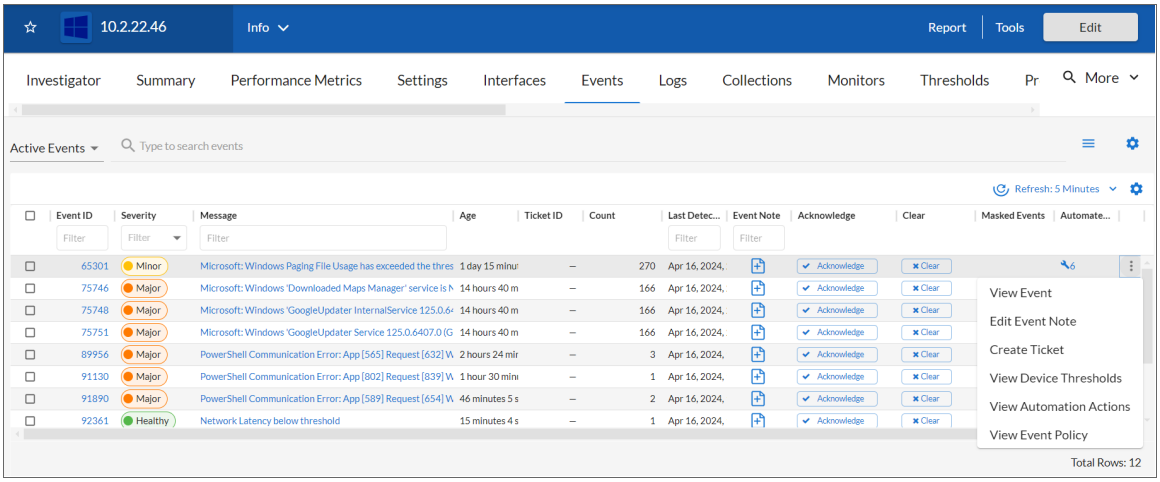


All objects of type "config" are included on the **[Configs]** tab. Usually, "config" objects contain static information about hardware and configuration settings, such as serial numbers, version numbers, and hardware status.

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

The Events Tab

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



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

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

TIP: You can toggle between *Active events* and *Cleared events* by using the drop-down to the left of the ***Search*** field. On this tab, you can also acknowledge and clear an event if you have permission for those actions.

For each event, the **[Events]** tab displays the following information:

- ***Event ID***. The unique ID for the event, generated by Skylar One. The ID appears as a hyperlink. To view the **Event Investigator** page for the event, click the ***ID*** hyperlink. For more information about the **Event Investigator** page, see the ***Events*** manual.
- ***Severity***. The severity of the event. Possible values are:
    - *Critical*
    - *Major*
    - *Minor*
    - *Notice*
    - *Healthy*
- ***Message***. The message generated for the event. The message appears as a hyperlink. To view the **Event Investigator** page for the event, click the ***Message*** hyperlink. For more information about the **Event Investigator** page, see the ***Events*** manual.
- ***Age***. The amount of time (in days, hours, and minutes) since the event first occurred or since its last occurrence without having been cleared.
- ***Ticket ID***. If a ticket has been created for the event, this column displays the ticket ID of that ticket.
- ***Count***. The number of times this event has occurred, the number of child events associated with the event, or the number of masked events associated with the event.
- ***Last Detected***. The date and time at which the event last occurred on the device.

- ***External Ticket***. The numeric ID associated with a ticket from an external ticketing system (that is, a ticket that was not created in Skylar One). If this field displays a value, you can click on that value to spawn a new window and view the external ticket.

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

- ***Event Note***. A user-defined note to accompany the event. To create or edit a note, click the **Note** icon ( ). The **Edit Event Note** window appears, where you can create or edit a note and save your changes.
- ***Acknowledge***. If the event has been acknowledged, this column displays a check mark and the username of the user who acknowledged the event. If the event has not yet been acknowledged, this column displays an **[Acknowledge]** button; click the **[Acknowledge]** button to acknowledge the event. When you ***acknowledge*** an event, you let other users know that you are aware of that event and are working on a response.
- ***Clear***. Click the **[Clear]** button to clear the event. 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 same event occurs again on the same device, it will reappear in the **[Events]** tab, even if you have previously cleared that event.
- ***Event Source***. The system or application that generated this event. Possible values are:
    - *Syslog*. Event was generated from a system log generated by a device.
    - *Email*. Event was generated by an email from an external agent. For example, Microsoft Operations Manager (MOM).
    - *Internal*. Event was generated by Skylar One.
    - *Trap*. Event was generated by an SNMP trap.
    - *Dynamic*. Event was generated by a Dynamic Application collecting data from the device.
    - *API*. Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
    - *Skylar One agent*. Message is generated by log file messages collected by the Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the ***Monitoring Device Infrastructure Health*** manual .
    - *Skylar Automated RCA*. Event was generated by a Skylar Automated RCA. You can view Skylar Automated RCA events, including suggestions, custom alerts, and accepted alerts. You can also filter the contents of the **[Events]** tab by Skylar Automated RCA events, active events, and cleared events.
- ***Masked Events***. If the event has occurred multiple times on the same device that uses the ***event mask*** setting, click the masked events icon ( ) to open the **Masked Events Overview** modal, where you can view details about the masked events. For more information, see the section *Filtering for Masked Events*.

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

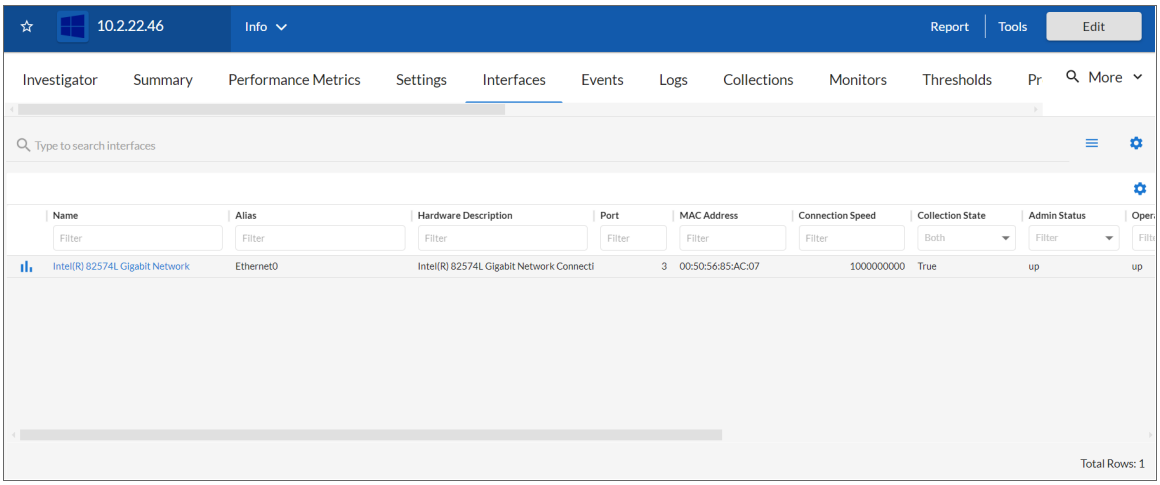
> **NOTE:** You can also view the **Event Actions Log** modal page by clicking the **[Actions]** button ( ) for the event and selecting *View Automation Actions*.

Clicking the **Actions** menu ( ) next to an event gives you the following options, based on your permissions:

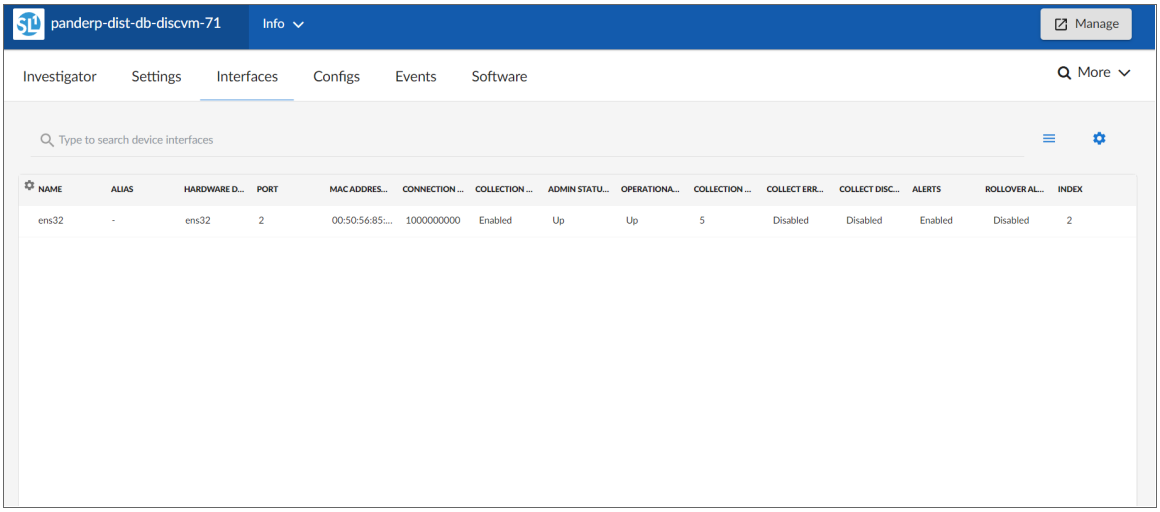
- *View Event*. Navigates to the **Event Investigator** page for that event.
- *Edit Event Note*. Lets you update the Note associated with this event.
- *Create Ticket*. Opens a new ticket in the Skylar One **Ticket Editor**, if you are using Skylar One for your ticketing.
- *Edit Ticket*. Opens an existing ticket in the Skylar One **Ticket Editor**, if you are using Skylar One for your ticketing.
- *Create External Ticket*. Creates a new ticket for the event if you are using an external ticketing system instead of Skylar One.
- *View Event Policy*. Opens the **Event Policy** page for the policy aligned with this event.
- *View Device Thresholds*. Opens the **Device Thresholds** page for the device on which the event occurred.
- *Suppress Event for this Device*. Suppresses the current event on the current device. When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in
- *View Automation Actions*. Displays a log of automations that have occurred for that event. This option is hidden if the event does not have any automation actions aligned to it.

The Interfaces Tab

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



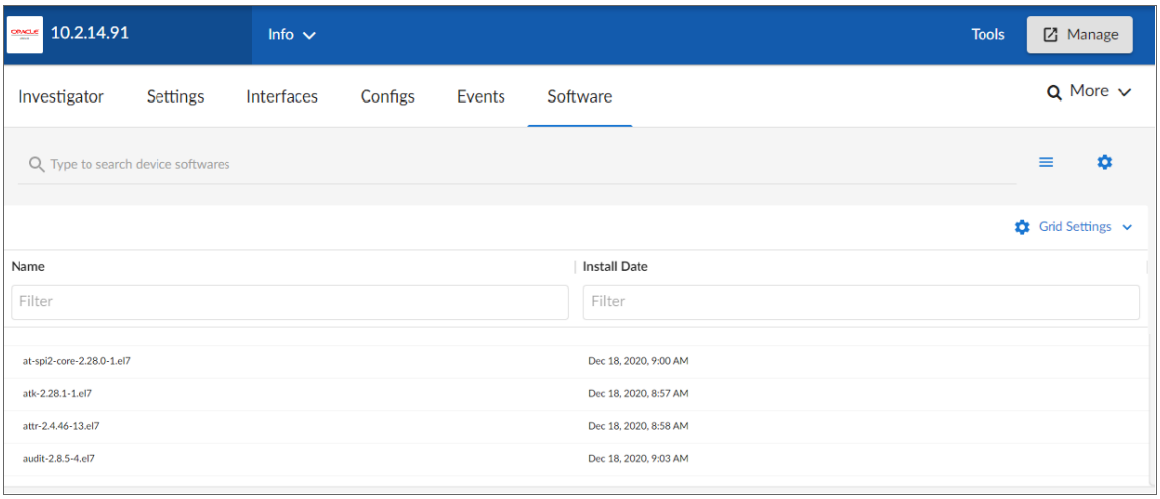
NOTE: For more information about this tab, see the chapter on "Monitoring Network Interfaces" in the ***Monitoring Device Infrastructure Health*** manual.



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

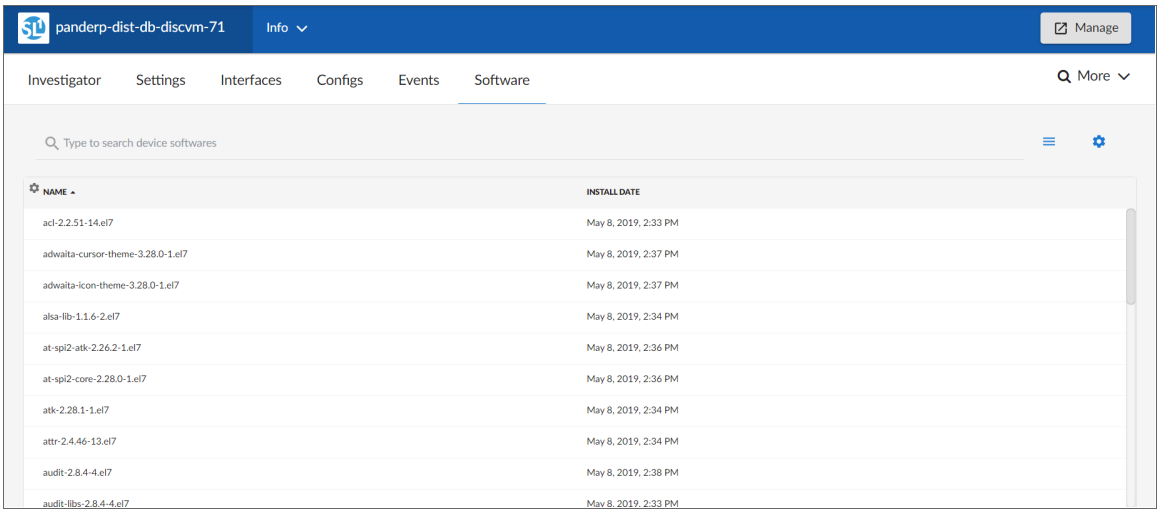
The Software Tab

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



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

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



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

Chapter 5

Viewing Global Events

Overview

This chapter describes how to view events in the Skylar One (formerly SL1) Global Manager system. You can view events on the **Events** page, which you can access by clicking the Events icon (⚠).

Use the following menu options to navigate the Skylar One user interface:

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

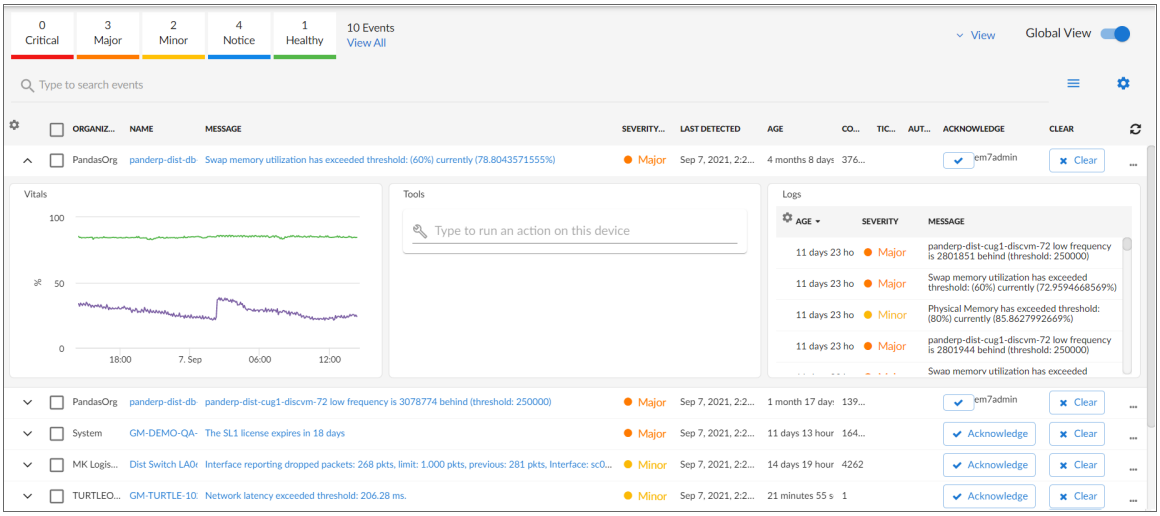
This chapter covers the following topics:

Viewing the Global List of Events

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

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

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



In a Global Manager system:

- When the **[Global View]** button on the **Events** page is toggled ***on***, you can view a list of events that have occurred across all of the stacks in your Global Manager system.
- When the **[Global View]** button on the **Events** page is toggled ***off***, you can view a list of events that have occurred only on the Global Manager system itself.

TIP: If you are looking for a specific set of events, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode, you can create an advanced search using "AND" or "OR" operators for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

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

- ***Organization***. The organization with which the event is associated. Click the organization hyperlink to view more information about the organization.
- ***Severity***. The severity of the event. Possible values are:
    - *Critical*. Indicates a condition that can seriously impair or curtail service and requires immediate attention (for example, service or system outages).
    - *Major*. Indicates a condition that impacts service and requires immediate investigation.
    - *Minor*. Indicates a condition that does not currently impair service but needs to be corrected before it becomes more severe.
    - *Notice*. Indicates a condition that does not affect service but about which users should be aware.
    - *Healthy*. Indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.

  Optionally, you can filter the list of events so that only events of a specific severity level appear on the **Events** page. For more information, see the section *Filtering Events by Severity*.
- ***Name***. The name of the entity associated with the event. Click the name hyperlink to view more information about the entity.
- ***Message***. The message generated for the event. Click the message hyperlink to go to *the Event Investigator*, where you can view more information about the event, including a description, the probable cause for the event, and possible resolutions, among other things.

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

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

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

- ***Masked Events***. If the event has occurred multiple times on the same device that uses the ***event mask*** setting, click the masked events icon ( ) in the **Masked Events** column for the relevant event open the **Masked Events Overview** modal, where you can view details about the masked events. For more information, see the section *Filtering for Masked Events*.

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

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

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

- ***Event ID***. The unique ID for the event, generated by Skylar One. Click the ID hyperlink to go to *the Event Investigator*. In a Global Manager system, when the **[Global View]** button is toggled on, the event ID will be preceded by a number and an underscore, where the number preceding the underscore represents the stack on which the event occurred.
- ***Event Source***. The system or application that generated this event. Possible values are:
    - *Syslog*. The event was generated from a system log generated by a device.
    - *Email*. The event was generated by an email from an external agent. For example, Microsoft Operations Manager (MOM).
    - *Internal*. The event was generated by Skylar One.
    - *Trap*. The event was generated by an SNMP trap.
    - *Dynamic*. The event was generated by a Dynamic Application collecting data from the device.
    - *API*. The event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
    - *Skylar One agent*. The event was generated by log file messages collected by the Skylar One agent. For more information about creating Log File Monitoring Policies to monitor log file messages collected by the agent, see the ***Monitoring Device Infrastructure Health*** manual.

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

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

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

NOTE: To link an external ticket to an event, you must create a custom Run Book Automation policy and a custom Run Book Action or use the ScienceLogic APIs. For more information, see the *Configuring Global Manager for Event Ticketing* section. For help with these tasks, contact ScienceLogic Customer Care.

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

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

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

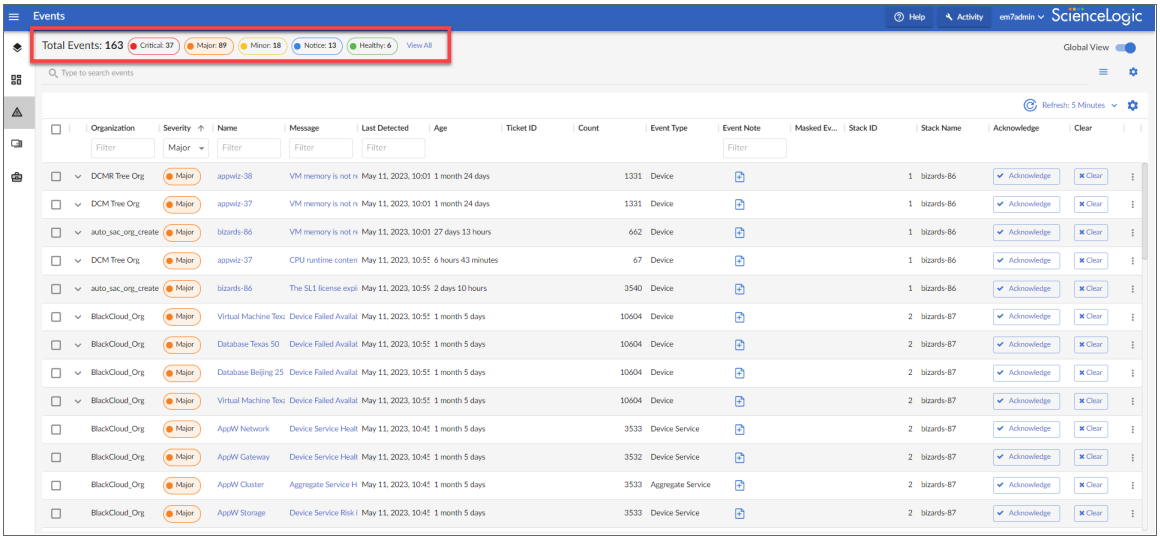
TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

Searching and Filtering the List of Events

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

Filtering Events by Severity

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



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

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

The following color codes are used throughout Skylar One:

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

Filtering for Masked Events

When a device uses the ***event mask*** setting, events that occur on a single device within a specified span of time are grouped together, and only the event with the highest severity is displayed on the **Events**

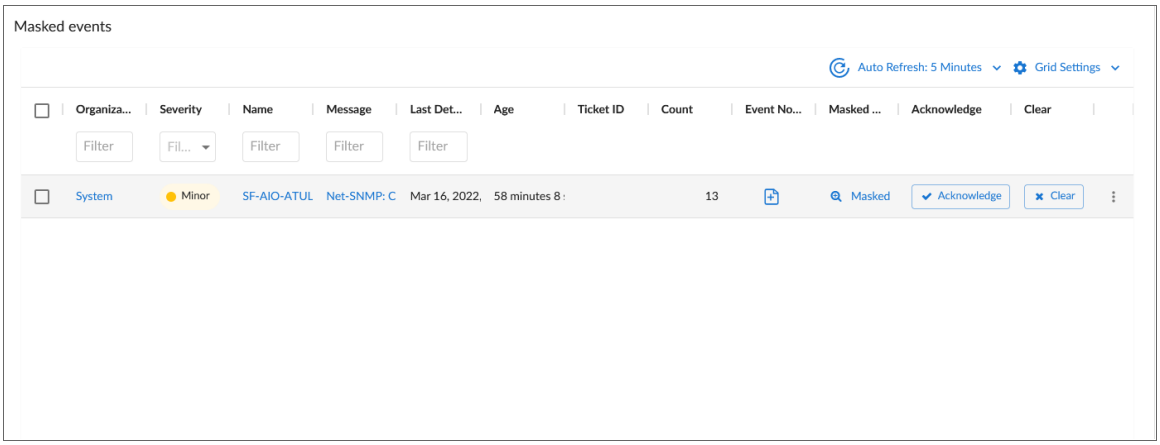
page. This allows related events that occur in quick succession on a single device to be rolled-up and posted together under one event description. For example, if a device cannot connect to the network, multiple other services on the device will raise events. Skylar One would display the event with the highest severity and roll up all the other events.

On the **Events** page, any event that contains masked events includes the masked events icon ( ) in the **Masked Events** column.

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

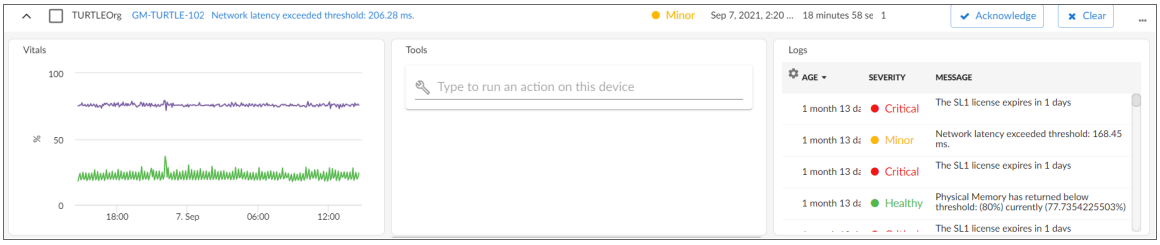
To view more information about masked events, click the masked events icon ( ) in the **Masked Events** column on the **Events** page. The **Masked Events Overview** modal appears, where you can view details about the masked events.

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



Viewing Additional Data about an Event

On the **Events** page, 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:



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

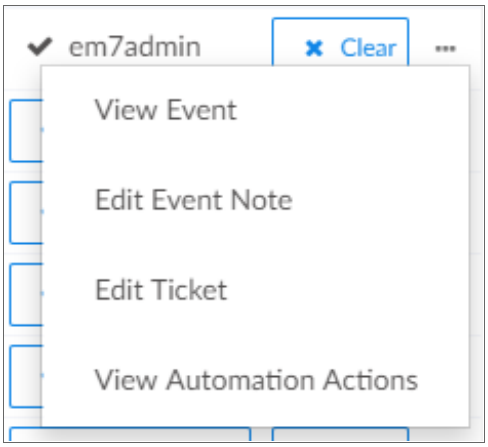
On the Event Drawer, you can access the following panes:

- The **Vitals** pane displays graph data for 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 your cursor over a timeframe, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Tools** pane enables you to run a set of network diagnostic tools or user-initiated actions in the **Activity Center**. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions. For more information, see the section on *Using the Action Runner*.
- The **Logs** pane displays a list of the log entries from the device's log file, sorted from newest to oldest by default.

Viewing Automation Actions

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

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



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

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

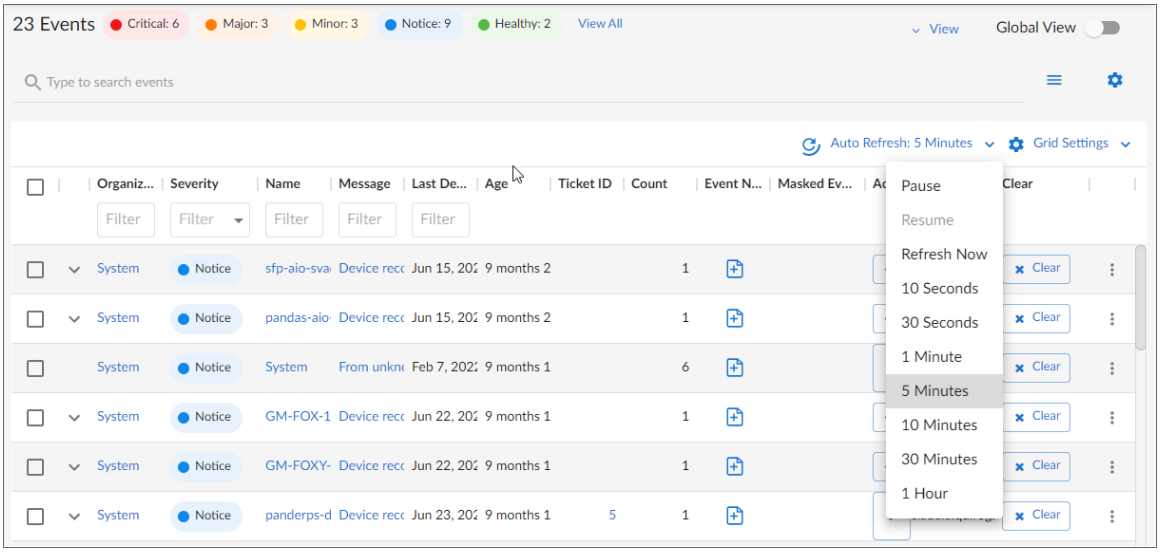
- The date and time when the action was executed
- The automation policy that triggered the action

- The name of the action policy
- The result of the action

Refreshing the Events Page

You can refresh the **Events** page manually or set it to auto-refresh.

To refresh the **Events** page manually, click the **Auto Refresh** icon and select **Refresh Now**.



To enable auto-refresh:

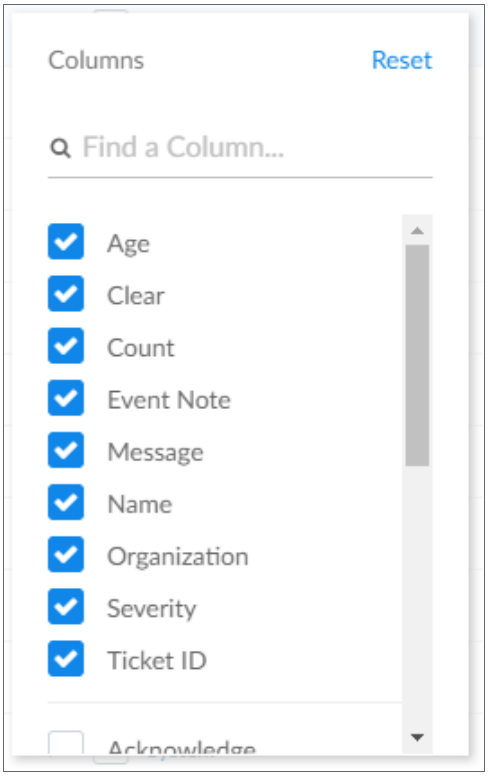
1. On the **Events** page, click the ***Auto Refresh*** drop-down menu.
2. In the **Refresh interval** drop-down, select the desired refresh interval for the page. Options range from 10 seconds to 60 minutes.

Customizing the Events Page

You can deselect columns that you do not want to see in the **Events** page, and select additional columns including custom attributes.

To select columns:

1. Click on the gear icon (⚙) in the top left of the **Events** page.
2. In the **Columns** menu, select the columns you want to add or deselect columns you want to hide. If you can't find a column, use the search field to find it by name. If you have created any Custom Attributes, these will appear in this list as well:

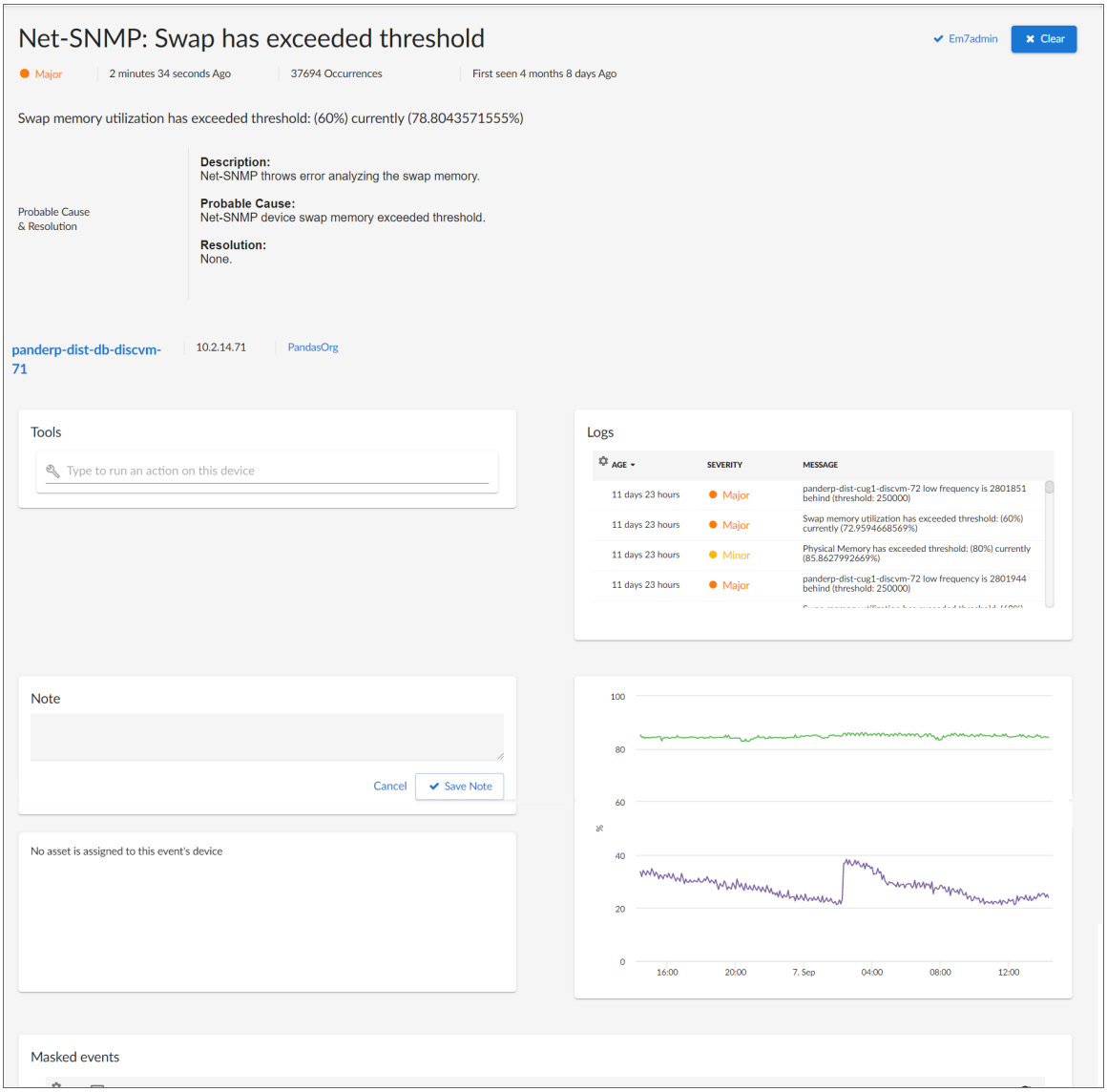


NOTE: For more information about Custom Attributes, see the ***Device Management*** manual.

3. When you have finished making your selections, click outside the **Columns** menu to close it.

Using the Event Investigator

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



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

The top pane of the **Event Investigator** page contains basic event details. From this pane, you can also acknowledge or clear the event.

> **TIP:** On the **Event Investigator** page, click the name of an aligned device to go to the **Investigator** page for that device. You can also click the name of the aligned organization to view its **Organizational Summary** page.

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

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

Using the Action Runner

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

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

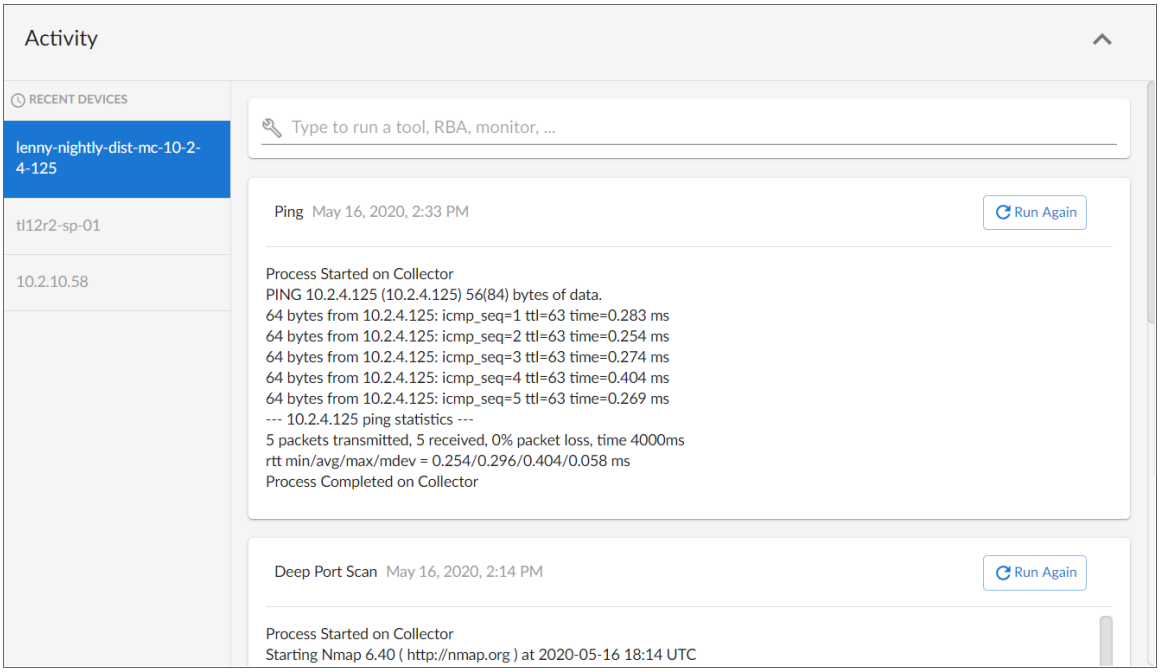
NOTE: For more information about user-initiated actions, see the chapter on "Automation Policies" in the ***Run Book Automation*** manual.

To use the **Action Runner**:

1. Access the **Action Runner** for events in one of the following ways:
    - On the **Action Runner** page, open the Event Drawer for a particular event. Click the search bar in the **Tools** pane.
    - On the **Action Runner** page, click the search bar in the **Tools** pane.
    - Click the **[Activity]** button in the navigation bar at the top of any page in Skylar One. Click the search bar.
2. When you click the search bar, a list displays the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:
    - ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
    - ***Ping***. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by Skylar One to communicate with the device) and waits for a reply. Skylar One 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, Skylar One uses the appropriate IPv6 ping command.
    - ***Who Is***. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
    - ***Port Scan***. Displays a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
    - ***ARP Lookup***. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.
    - ***ARP Ping***. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.
    - ***Trace Route***. Displays the network route between Skylar One and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, Skylar One uses the appropriate IPv6 traceroute command.

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

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



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

Responding to Events

When events occur, there are multiple ways you can respond to them when in ***Global View*** mode:

- ***Acknowledge***. Lets other users know that you are aware of an event and are working on a response.
- ***Add a Note***. Adds custom text to an event. You can view notes from the **Events** page or the **Event Investigator** page. You can also include notes in automation actions.
- ***Clear***. Removes an instance of an event from the **Events** page. The cleared instance is no longer displayed.
- ***Create External Ticket***. Creates a new ticket for the event if you are using an external ticketing system instead of Skylar One. For more information, see the "Events and Tickets" chapter of the ***Events*** manual.

- ***Align External Ticket***. Aligns this event with an existing ticket if you are using an external ticketing system instead of Skylar One. For more information, see the "Events and Tickets" chapter of the ***Events*** manual.

Selecting Multiple Events

On the **Events** page, 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 at the bottom of the page to acknowledge or clear those events simultaneously.

If you do *not* want to acknowledge or clear the selected events, click the **[Deselect All]** 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.

Acknowledging and Clearing Events

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

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

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

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

To acknowledge and clear events:

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

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

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

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

Viewing and Editing Event Notes

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

To view or edit an event note:

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

   TIP: You can also edit an event note on the **Events** page by clicking the **[Actions]** button ( ) for that event and selecting *Edit Event Note*. This is helpful if you have hidden the ***Event Note*** column on the **Events** page. To add or edit an event note for multiple events, check the box next to the events for which you want to edit the note, then click the **[Edit Note]** button at the top of the inventory table.

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

Creating and Aligning Event External Tickets

If your Global Manager system has the *necessary configuration*, you can create an external ticket from an event while in ***Global View*** mode.

To create and align event external tickets, on the **Events** page or the **Event Investigator** page for a specific event, click the **[Actions]** button ( ) for the event and do one of the following:

- Select *Create External Ticket*. When you do so, Skylar One sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic to create the ticket on the external system.
- Select *Align External Ticket*. When you do so, the **Align External Tickets** modal appears. From the drop-down list, select the existing external ticket that you want to align to the event, and then click **[Align]**. (Alternatively, if you want to unalign an external ticket, select the external ticket from the drop-down list and click **[Unalign]**.)

NOTE: The external ticket references that are available for selection in the **Align External Tickets** modal come from a unique list that is a combination of all available external ticket references in all stacks across your Global Manager system. If a stack returns the same reference as another stack, only one entry for that reference will appear in the list.

NOTE: If a stack in your Global Manager system does not have the *Create/View External Ticket* option selected in the ***Event Console Ticket Life Ring Button Behavior*** setting, an error message will appear if you attempt to create an external ticket for an event that originated on that stack.

TIP: You can bulk align/unalign tickets to multiple events that originate from the same stack. To do so, select one or more events from the **Events** page and then click **[Align]** or **[Unalign]** at the bottom of the page. If you attempt to align/unalign tickets to multiple events that originate from different stacks, you will receive an error message.

Chapter 6

Viewing Global Business Services

Overview

This chapter describes how to view business services in a Skylar One (formerly SL1) Global Manager system. You can view business services on the **Business Services** page, which you can access by clicking the Business Services icon ( ). From there, you can select a service from the list to view detailed data on the *Service Investigator* page for that service.

Use the following menu options to navigate the Skylar One user interface:

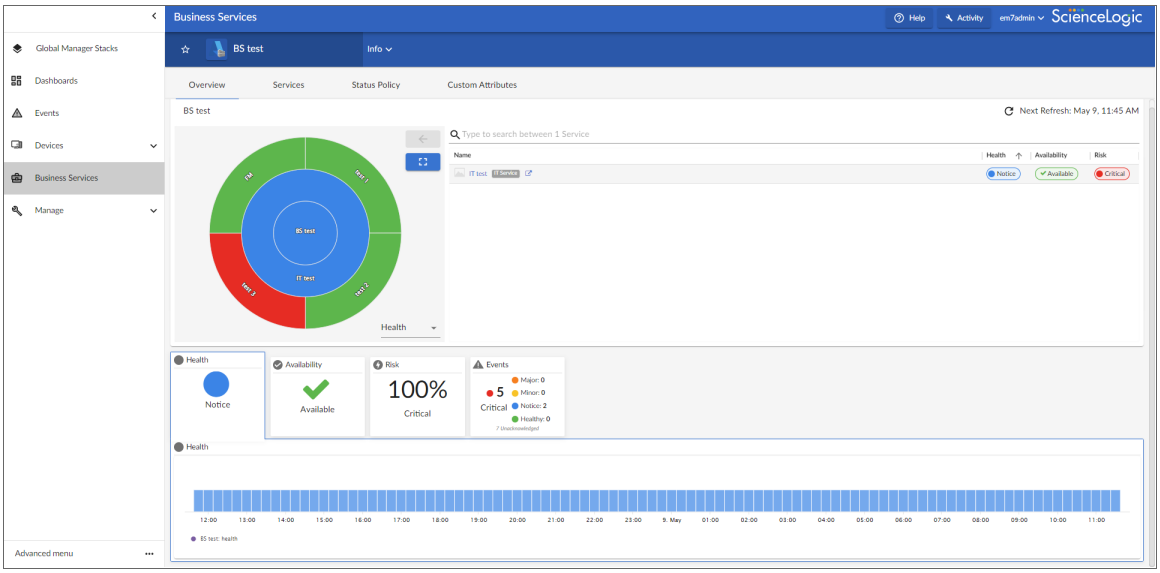
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter covers the following topics:

Viewing the Global List of Business Services

The **Business Services** page displays a list of the business, IT, and device services that you have access to, as well as some basic info and the health, availability, and risk metrics for each service.

To navigate to the **Business Services** page, click the **Business Services** icon ( ), then click the name of the business service you would like to view details about:



The **[Global View]** button on the **Business Services** page is toggled on by default to display a list of business, IT, and device services across all of the stacks in your Global Manager system. You cannot toggle the **[Global View]** button off for business services.

TIP: If you are looking for a very specific set of services, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing and Advanced Search" topic in the ***Introduction to Skylar One*** manual.

For each service, the Business Services page displays the following information:

- ***Name.*** The name of the service.
- ***Description.*** A description of the service.
- ***Service Type.*** Indicates the service type. Values include Business Service, IT Service, Device Service, or a custom service page.
- ***Organization.***The organization that owns the service.
- ***Contact User.***The user who should be contacted with any questions about the service.
- ***Availability.***The service's current availability value.
- ***Health.***The service's current health value.
- ***Risk.*** The service's current risk value.
- ***Policy.***The service' policy associated with the service.
- ***Stack ID.*** The numeric ID of the stack on which the service was discovered.
- ***Stack Name.*** The name of the stack on which the service was discovered.
- ***Last Updated By.*** The username of the user who last updated the service.
- ***Date Updated.*** The date and time at which the service was last updated.
- ***RCA Options.*** Indicates whether Root Cause Analysis is enabled or disabled for the service.

- ***Contact Organization.*** The organization that should by contacted with any questions about the service.

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

NOTE: You can configure your column fields by clicking the gear icon (⚙) below the **[Global View]** toggle, then by adding and removing different column fields by selecting and deselecting the checkboxes, respectively.

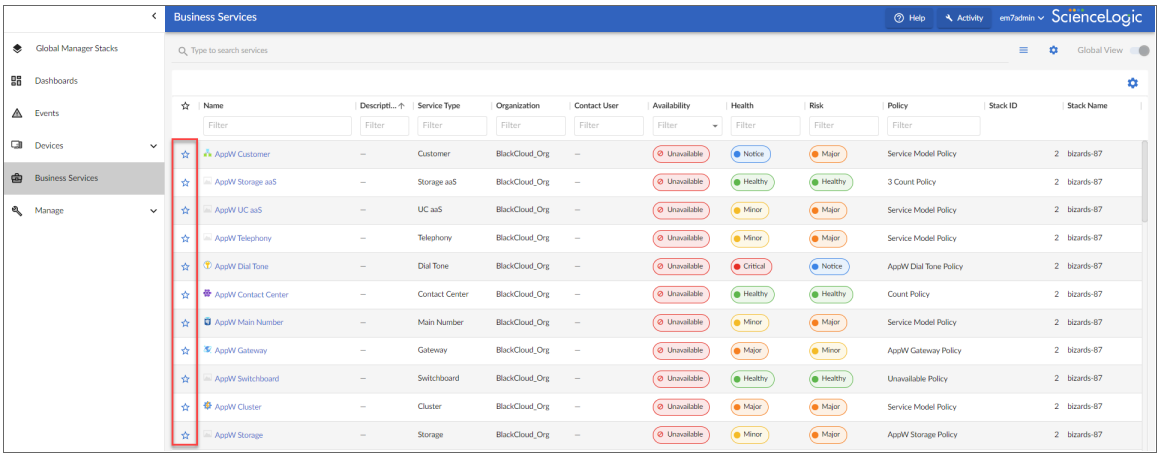
TIP: You can filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see "Filtering Inventory Pages" in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

Favoriting Business Services

In Skylar One, you can select one or more services so that they always display at the top of the list on the **Business Services** page. This process is called ***favoriting*** services or ***favorite*** service.

For example, on the Business Services page pictured below, click the ***Favorite Service*** star icon (☆) to add or remove the service from your favorites list. Click the icon (★) again to remove the favorite status.



You can then sort your Business Services by their favorite status.

With favorite services, you can:

- View your favorite service at the top of the **Business Services** page by default.
- Include favorites in the multi-sort function.
- Filter services by favorite.

Using the Service Investigator

You can view detailed data about a specific service by clicking the service name on the **Business Services** page to open the **Service Investigator** page.

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

- *Overview*
- *Services/Devices*
- *Status Policy*
- *Custom Attributes*

Each of these tabs is described in the following sections.

The Overview Tab

The **[Overview]** tab provides a single-page view of your services. This tab enables users to determine the ***behavioral correlation*** between a service's health, availability, and risk values and the events, anomalies, or other causes that might be impacting those values. This behavioral correlation feature provides users with a "big picture" view of the service and enables them to determine the root cause of any problems the service might be experiencing and then troubleshoot those problems.

The **[Overview]** tab consists of the following widgets:

- *Sunburst widget*
- *Health, Availability, and Risk* widgets
- *Changes widget*
- *Events widget*

Each of these widgets is described in the following sections.

Sunburst Widget

The top dashboard widget of the **[Overview]** tab displays either a *Sunburst* chart view or a *Map* view of your services. Use the drop-down menu in the top left corner of the widget to select which view you want to appear.

When you select the *Sunburst* view:

- The left pane includes a sunburst chart that displays the current Health, Availability, and Risk values for the service, as well as for any constituent IT services or device services that belong to that top-level service. For device services, the sunburst includes the device name and Health values for any devices that belong to the service. Additionally, this pane indicates the maximum number of constituent services or devices that will be used for computing health, availability, and risk.
- The right panel includes a list of constituent services or devices. Each service in this panel includes icons that represent that service's Availability, Health, and Risk metrics; devices include icons that represent each device's Health value. The right panel also includes a search bar at the top of the panel that enables you to search for specific constituent services or devices.

In the sunburst chart, the center circle represents the selected service. The selected service drives the context for the page title and **Info** drawer, as well as all the other panels and widgets on the **[Overview]** tab. This means that the right panel, widgets, and other elements on the page will all reflect the metrics for the service in the center circle of the sunburst.

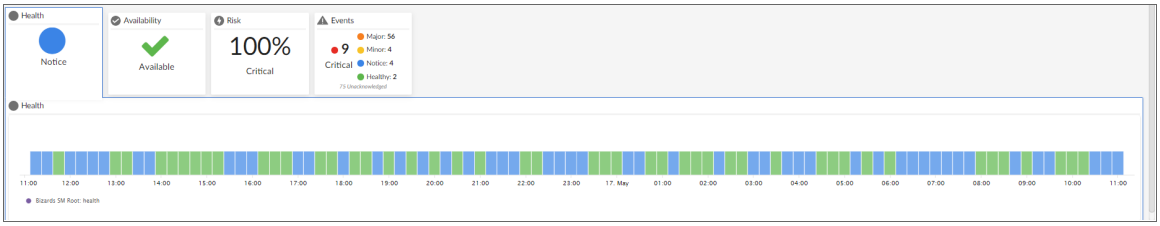
You can navigate through services on the widget in the following ways:

- In the left panel, you can click any of the constituent IT services or device services in the sunburst to select that service. To return to the parent IT service or business service, click the center circle or click the **[Back]** button.
- In the right panel, you can click the service name of any of the constituent IT services or device services to select that service. To return to the parent IT service or business service, click the breadcrumb links that appear in the top-left corner of the widget.

By default, the sunburst displays the Health value for the selected service and its constituent services or devices. To view the current Availability or Risk value for the selected service, click the drop-down button in the lower-right corner of the left pane and select *Availability* or *Risk*.

To collapse the sunburst widget, click the up arrow icon (^) in the top-right corner of the widget. To reopen it, click the down arrow icon (v).

Health, Availability, and Risk Widgets



The **Health**, **Availability**, and **Risk** widgets display a time series chart with the historical values of those metrics for the selected service from each polling cycle over the previous 24 hours.

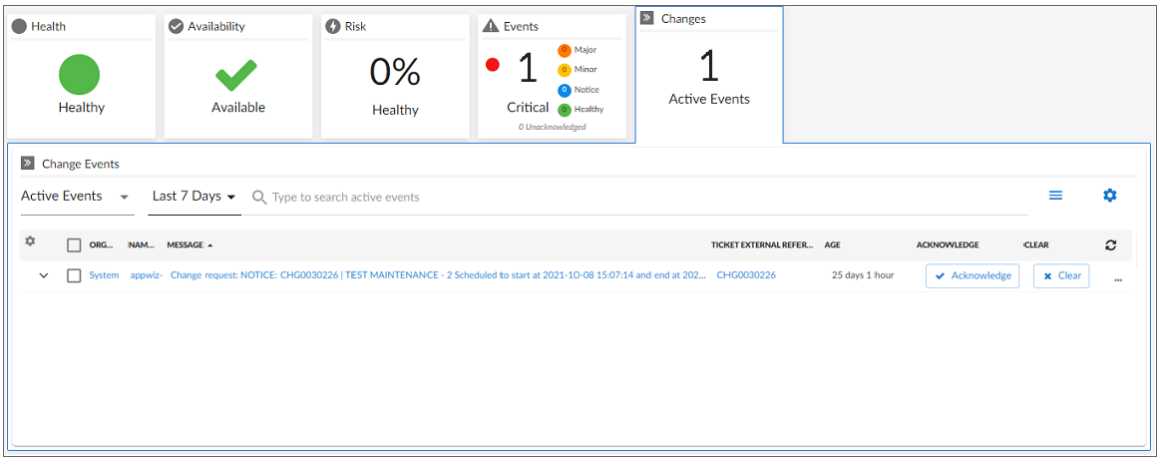
From these widgets, you can do the following:

- Hover your mouse over the chart to view the value for each polling cycle from the previous 24 hours.
- Click and drag your mouse over a series of bars in the chart to zoom in on that specific timespan. To return to the 24-hour view, click **[Reset zoom]**.
- Click a specific polling cycle to view the historic Health, Availability, and Risk values for that polling cycle.

TIP: If the ***RCA Options*** field is enabled, you can also view Root Cause Analysis information for the service to help you troubleshoot the root cause of a particular Health, Availability, or Risk value for a specific polling cycle. To view Root Cause Analysis information, click one of the polling cycles in the time series chart.

Changes Widget

NOTE: The **Changes** widget appears only if it has been properly configured and enabled. For more information, see the "Configuring and Enabling the Changes Widget" section of the ***Business Services*** manual.



The **Changes** widget is available to customers who have purchased Configuration and Change Management as part of their Skylar One Standard or Premium subscription. This widget displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, including both active and cleared change events.

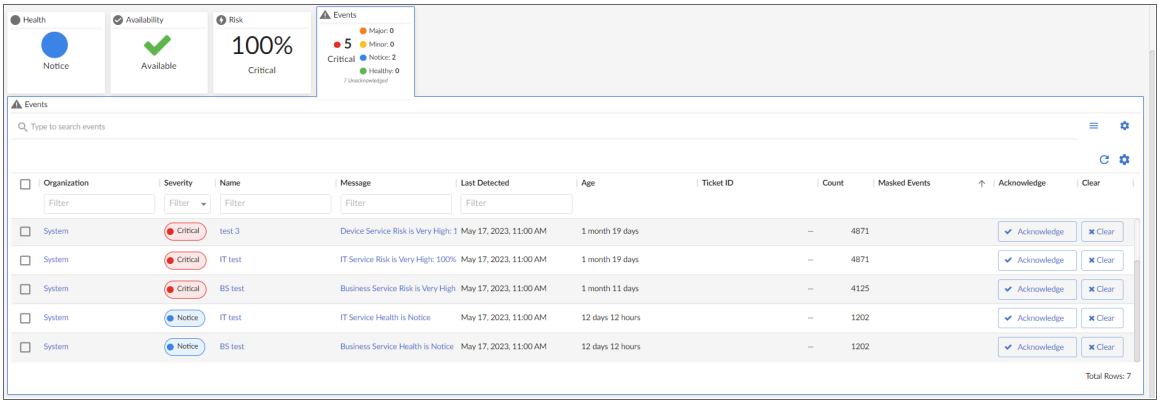
The **Changes** widget tile displays the number of active change events that are impacting the service. Events on the widget will automatically clear after 30 minutes.

From the **Changes** widget, you can do the following:

- Use the drop-down menu to choose which type of change events display in the widget: *Active Events* or *Cleared Events*.
- Filter and search for events by their date; either by 5, 7, 14, 30 days, or more than 30 days.
- Use the ***Search*** field to search for specific change events.
- For active events that are aligned to devices, click the down-arrow icon (⌄) next to the event to open the Event Drawer panel, which displays 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 timespan by clicking the **[Reset zoom]** button.
    - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
    - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.
- View the **Organizational Summary** page for the organization aligned with an active event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with an active event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for an active event by clicking the link in the ***Message*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with an active event by clicking the link in the ***Ticket External Reference*** column.

- For ServiceNow integrations, view the ServiceNow ticket associated with a cleared event by clicking the link in the ***External Ticket*** column.
- Acknowledge an active event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an active event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from an active event.
- View the event policy for an active event.
- Select multiple active events for action using the check boxes next to the events.

Events Widget



The **Events** widget displays a list of events for the selected service. This widget has much of the same functionality as the **Events** page.

> **NOTE:** The **Events** widget tile displays the number of events of each severity type, after masking, that are currently impacting the service. When opened, the **Events** widget lists all events impacting the service, including masked events. Therefore, the number of events that appear in the widget tile might be smaller than the number of events that appear in the opened widget.

From the **Events** widget, you can do the following:

- Use the search field to search for specific events.
- For events that are aligned to devices, click the down-arrow icon ( ) next to the event to open the Event Drawer panel, which displays 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 timespan by clicking the **[Reset zoom]** button.

    - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
    - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.
- View the **Organizational Summary** page for the organization aligned with the event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with the event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for the event by clicking the link in the ***Message*** column.
- View or edit event notes by clicking the **Note** icon ( ) in the ***Event Note*** column or by clicking the **[Actions]** button (···) and selecting *Edit Event Note*. Event notes 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 service or device you are monitoring.
- View more information about masked events by clicking the masked events icon ( ) in the ***Masked Events*** column. Masked events are related events that occur in quick succession on a single device or service that are rolled up and posted together under one event description, with only the highest severity event displayed.

> **NOTE:** For more information on masked events, see the "Viewing Events" topic in the **Events** manual.

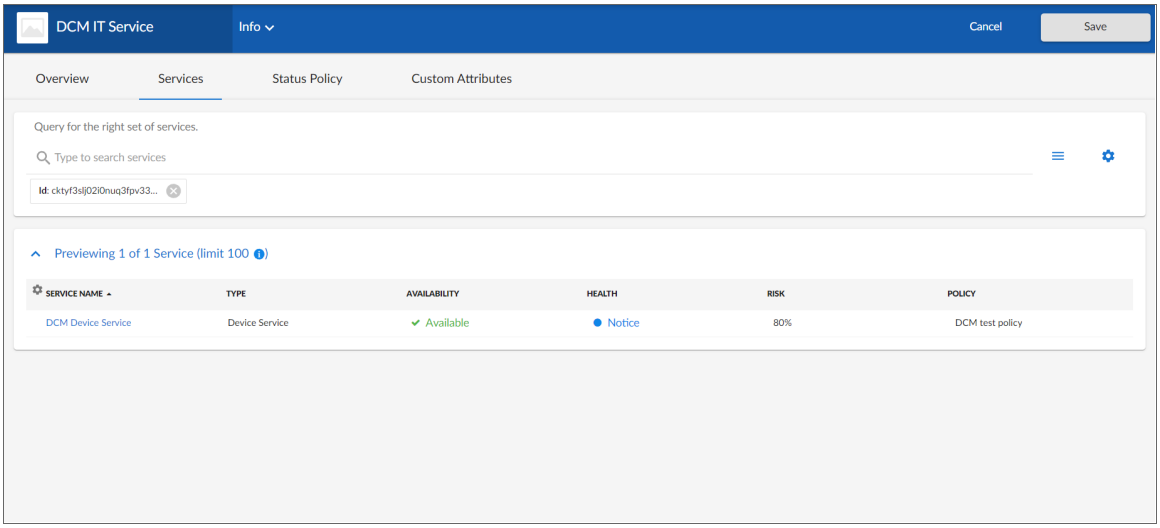
- Acknowledge the event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear the event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from the event.
- View the event policy.
- View a log of automations that have occurred for the event by clicking the **[Actions]** icon (···) and selecting *View Automation Actions*.
- Select multiple events for action using the check boxes next to the events.

> **NOTE:** For more information about events, see the ***Events*** manual.

The Services/Devices Tab

For business services and IT services, the **[Services]** tab displays the services currently being used in the service; for device services, the **[Devices]** tab displays devices included in the service.

You can edit the query at the top of the tab to control which services or devices appear on the page when you click **[Search]**.



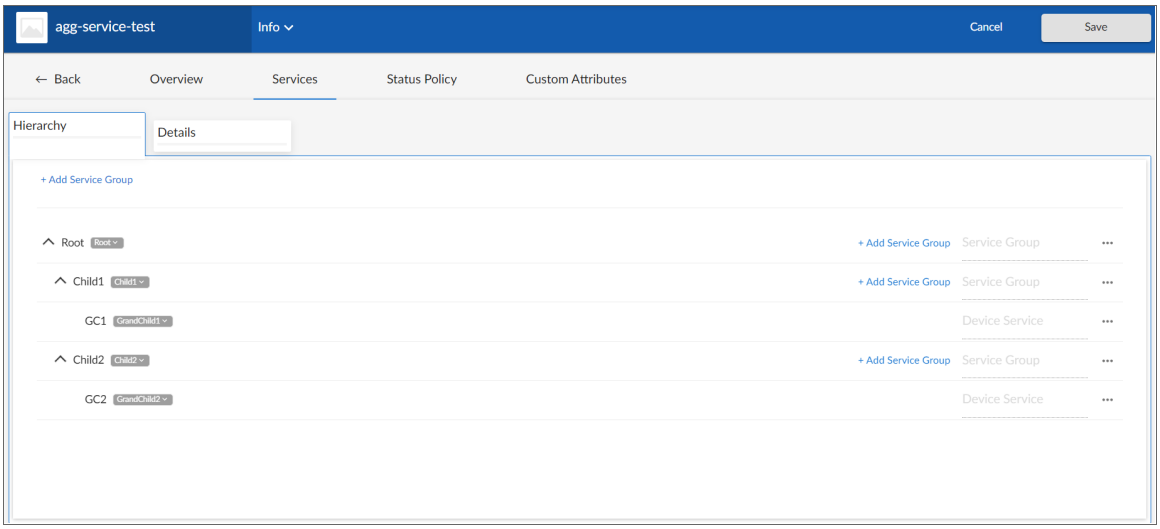
NOTE: The "ANY" search option is disabled on the **[Services]** or **[Devices]** tab.

NOTE: For more information about the **[Services]** or **[Devices]** tab for business services, IT services, and device services, see the section on "Creating Business, IT, or Devices Services" in the ***Business Services*** manual.

For Custom Service Models, the **[Services]** tab displays two tabs:

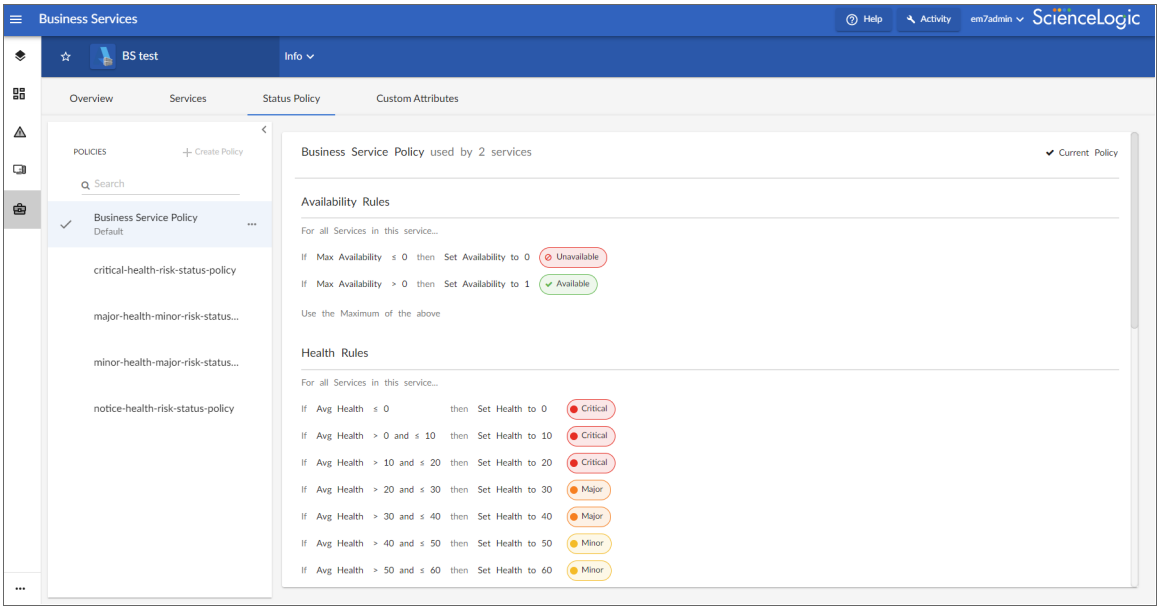
- ***Hierarchy***. Enables you to edit your service hierarchy by adding, moving, or deleting service groups.
- ***Details***. Includes two sub-tabs:
  - *Overview*. Enables you to update the managing organization and visible organizations for the individual levels within your service model hierarchy.
  - *Status Policy*. Enables you to create a new status policy or apply an existing status policy for the individual levels within your service model hierarchy.

NOTE: You cannot make changes for Business Services in Global Manager. For more information about the **[Services]** tab for service models, see the section on "Creating a Custom Service Model" in the ***Business Services*** manual.



The Status Policy Tab

The **[Status Policy]** tab displays a list of all the policies of that service type that are currently in the system and that can be chosen to associate with the service being viewed.



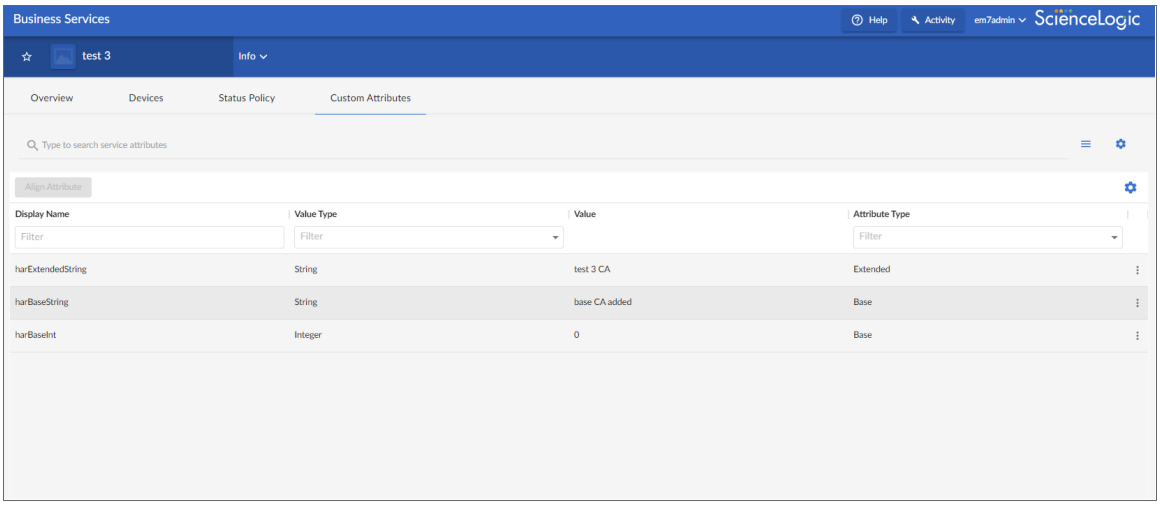
NOTE: Global Manager is read-only. For more information about selecting or changing a service policy, see the section on "Selecting a Service Policy" in the ***Business Services*** manual. For more information about creating a new service policy, see the section on "Creating a Service Policy" in the ***Business Services*** manual.

Depending on the thresholds you configured on the **Business Services Thresholds** page (Business Services > Thresholds), Skylar One generates an alert message if a threshold is crossed.

NOTE: For more information about thresholds, see the section on "Managing Service Thresholds" in the ***Business Services*** manual.

The Custom Attributes Tab

The **[Custom Attributes]** tab displays a list of all of the custom attributes that are aligned with your service.



Custom Attributes are customized name-value pairs. You can use custom attributes when importing services from an integrated system to handle incoming properties that are not defined in Skylar One.

There are two categories of custom attributes:

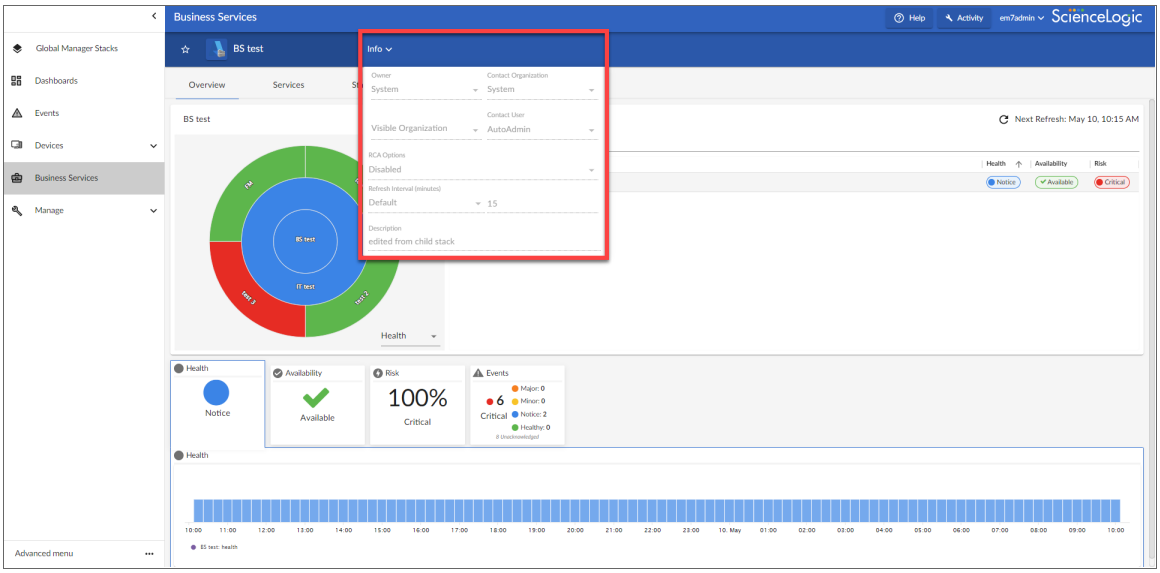
- **Base Custom Attributes**. Base custom attributes for services are aligned to all services. Therefore, all base custom attributes in your Skylar One system that have a ***Resource Type*** of *Service* will appear on the **[Custom Attributes]** tab for all services. You can edit the value of a base custom attribute for a particular service, but you cannot unalign a base custom attribute from a service.
- **Extended Custom Attributes**. Extended custom attributes that have a ***Resource Type*** of *Service* can be aligned individually to one or more services. For example, you could align an extended custom attribute only to those services to which the custom field applies. You can also edit an extended attribute value for a particular service or unalign an extended custom attribute from a service.

NOTE: Custom attributes cannot be used in dashboards for business services.

NOTE: For more information about custom attributes, see the "Custom Attributes" chapter in the ***Device Management*** manual or the "Using the Service Investigator" chapter in the ***Business Services manual***.

Using the Info Drawer on the Service Investigator Page

The **Info** drawer at the top of the **Service Investigator** page displays the following:



NOTE: The **Info** drawer is read-only in Global Manager. For more information, see the "Using the Service Investigator" chapter in the ***Business Services*** manual.

- ***Owner***. The organization that owns the service.
- ***Contact Organization***. The organization that should be contacted with any questions about the service.
- ***Visible Organizations***. A list of organizations from which you can select devices to use in Device Services or IT Services. For example, if you selected Acme for this field, then any service that is aligned with Acme can access devices in the Acme organization. This implies the devices can be included in IT Services. There are two uses for Visible Organizations:
    1. *Device Services*. Allow the inclusion of devices from the owning organization, as well as the visible organizations.
    2. *IT Services*. Allow the inclusion of Device Services from the owning organization, as well as the visible organizations.
- ***Contact User***. The user who should be contacted with any questions about the service.

- ***RCA Options***. Allows you to enable or disable the Root Cause Analysis feature, an advanced feature for troubleshooting. For more information, see the "Using the Root Cause Analysis Feature" section in the ***Business Services*** manual.
- ***Refresh Interval (minutes)***. Allows users with edit permissions to edit the Health-Availability-Risk (HAR) Har Provider's Poll Frequency time. The value allows a minimum of 1 minute and a maximum of 24 hours (in minutes). Default minute value is 15 minutes.
- ***Description***. A description of the service. You can use this field as a metadata tagging field that can be exploited in the search by a parent service. For example, if a collection of Device Services all have a description of "Shared Infrastructure", then an IT Service can search to include every Device Service in the same organization that has a description of "Shared Infrastructure". As you add more "Shared Infrastructure" device services, the IT Service will automatically expand to include them. This makes building service trees quick and self-maintaining, without resorting to rigid service names.
- ***Include devices from visible organizations***. Allows you to include devices from other organizations in a Device Service. Turn the toggle on (blue) to include other organizations' devices; turn it off (gray) to exclude other organizations' devices. This option appears only on the **Service Investigator** page for Device Services.

Chapter 7

Viewing and Creating Global Dashboards

Overview

This chapter describes how to view and create global dashboards in a Skylar One (formerly SL1) Global Manager system. You can create and use dashboards on the **Dashboards** page, which you can access by clicking the Dashboards icon ( ).

Use the following menu options to navigate the Skylar One user interface:

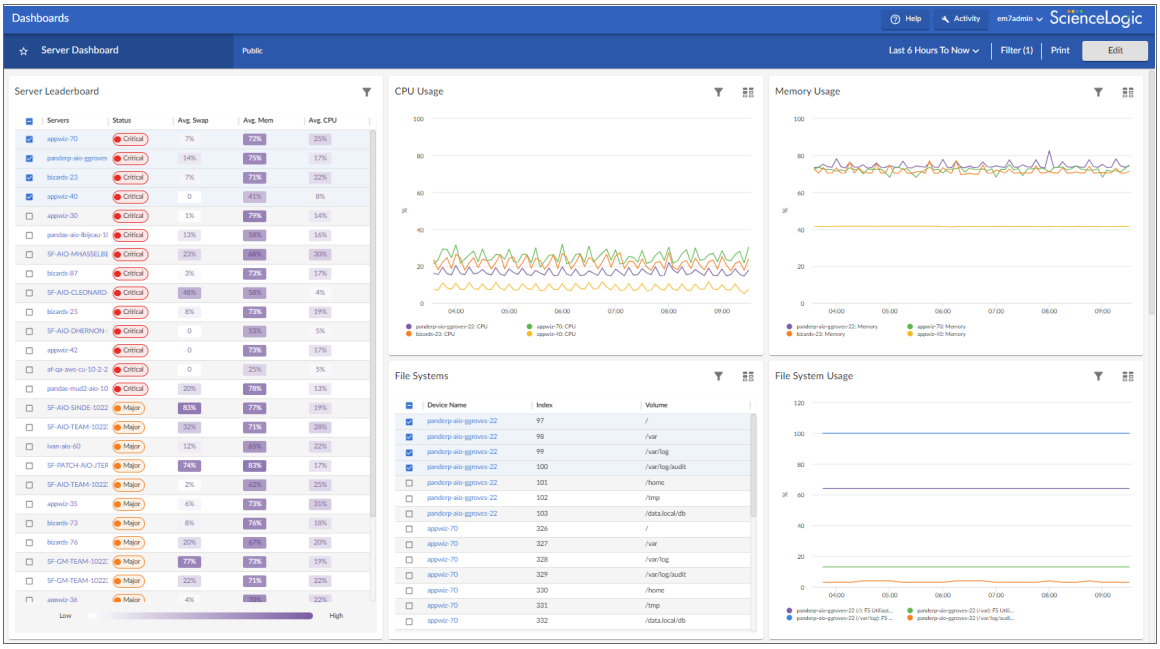
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

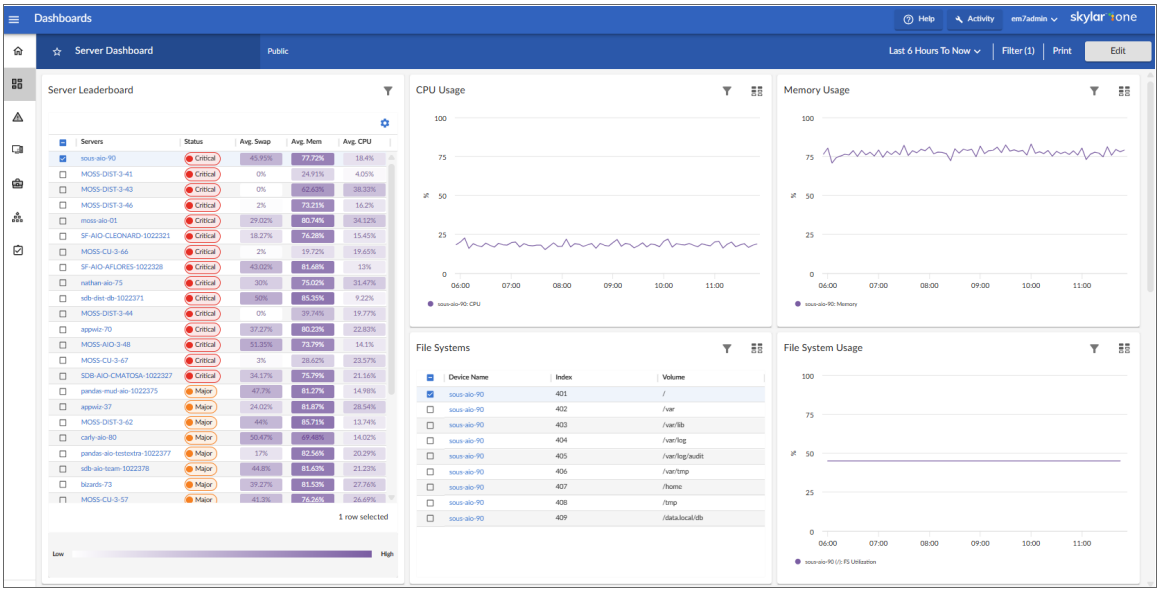
This chapter covers the following topics:

What is a Dashboard?

A ***dashboard*** is a page that displays one or more graphical reports, called ***widgets***. These widgets appear in their own pane, and display charts, tables, and text.

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.





To define a widget, you first select from a list of pre-defined widget definitions, and then customize what will be displayed by the selected widget by supplying values in the option fields provided by that widget.

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

TIP: If you are looking for a very specific set of dashboards, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

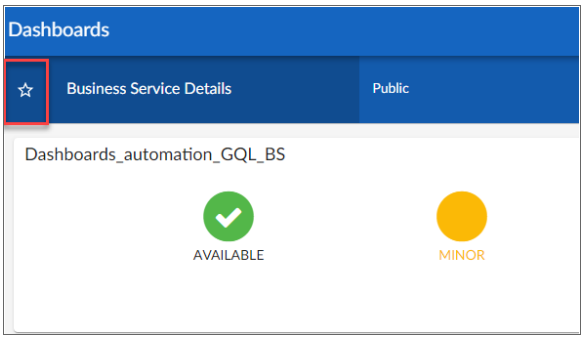
TIP: If an item name displays as a hyperlink in a dashboard, you can click that link to go to the relevant detail or Investigator page for that item. You can click dashboard links to the Investigator pages for devices or events.

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

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on "Adjusting the Row Density" in the ***Introduction to Skylar One*** manual.

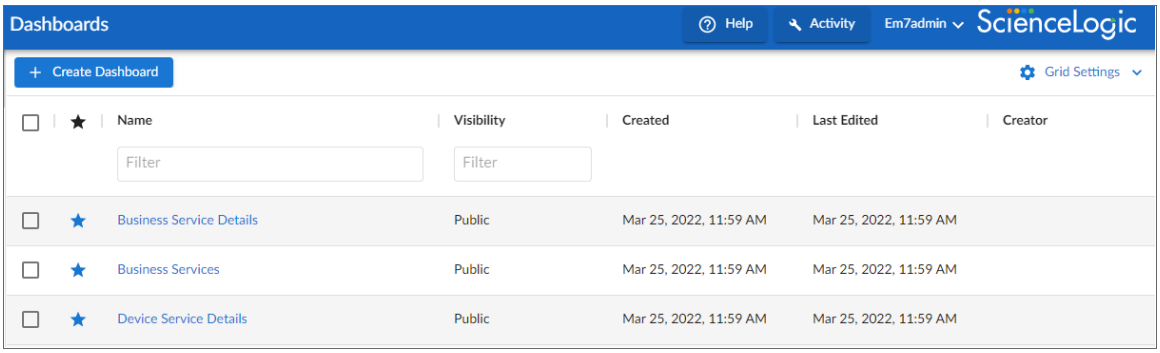
Favorite Dashboards

In Skylar One, this feature is called ***favoriting*** dashboards or ***favorite*** dashboard. For example, in the Business Service Details dashboard pictured below, you can select the ***Favorite Dashboard*** star icon to add/remove the dashboard from your favorites list. You can then sort your Dashboards by their favorite status.



With favorite dashboards, users can:

- View their favorited dashboard(s) at the top of the Dashboard Inventory list by default.
- Include favorites in the multi-sort function.
- Filter dashboards by favorite.



Leaderboard Widgets 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:

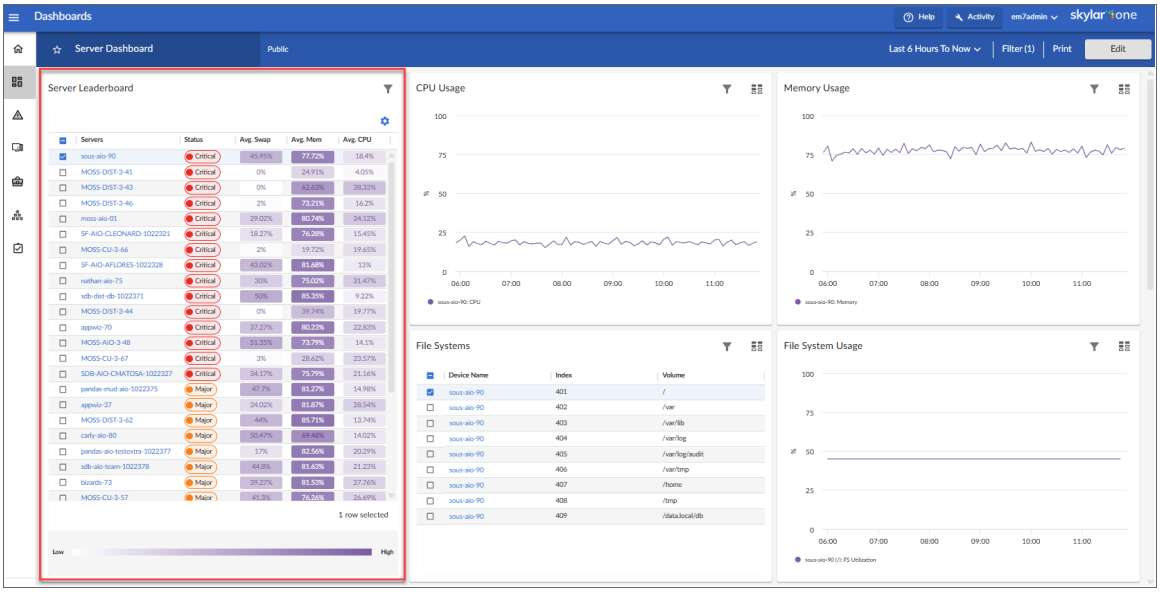
In Skylar One, this feature is called ***driving*** data or driving the ***context*** of a dashboard widget. For example, in the Server leaderboard widget pictured above, if you select one or more servers on the leaderboard widget, the other widgets in the dashboard will display data about just the servers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

NOTE: You can use the ***Display zeroes*** toggle when editing a Top-N or Bottom-N widget to enable the widget to show or hide zero results.

To use a leaderboard widget:

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

2. Select one or more items on the leaderboard widget. The other widgets in the dashboard update with data only for the selected item or items.

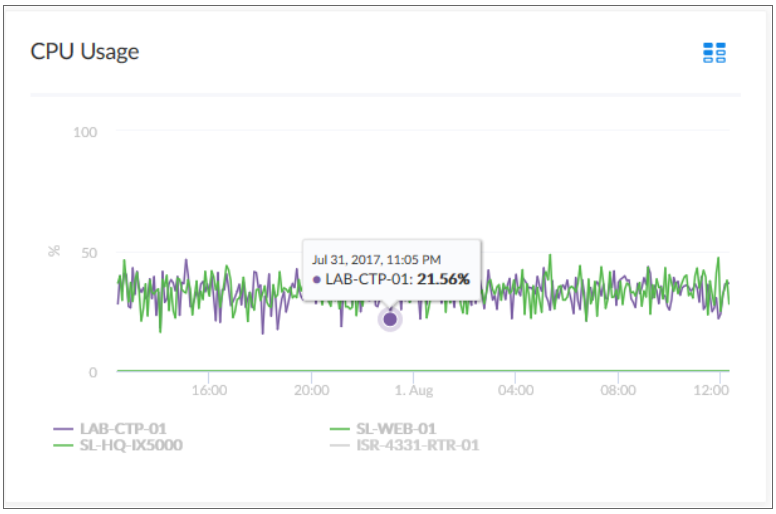


Widget Legends

The items you select in a leaderboard on the **Dashboards** page also appear at the bottom of each widgets 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 a Leaderboard widget on the **Dashboards** page, 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** page, you can control the display of a widget, such as changing the time span of data displayed in all the widgets, or zooming in or out on widget data.

You can also use the **[Filter (X)]** button to narrow down the data displayed in all widgets. The variable X is the number of filters applied to the dashboard.

> **NOTE:** Widgets on the **Dashboards** page have header text that indicates the number of filters applied.

Using the Time Span Filter

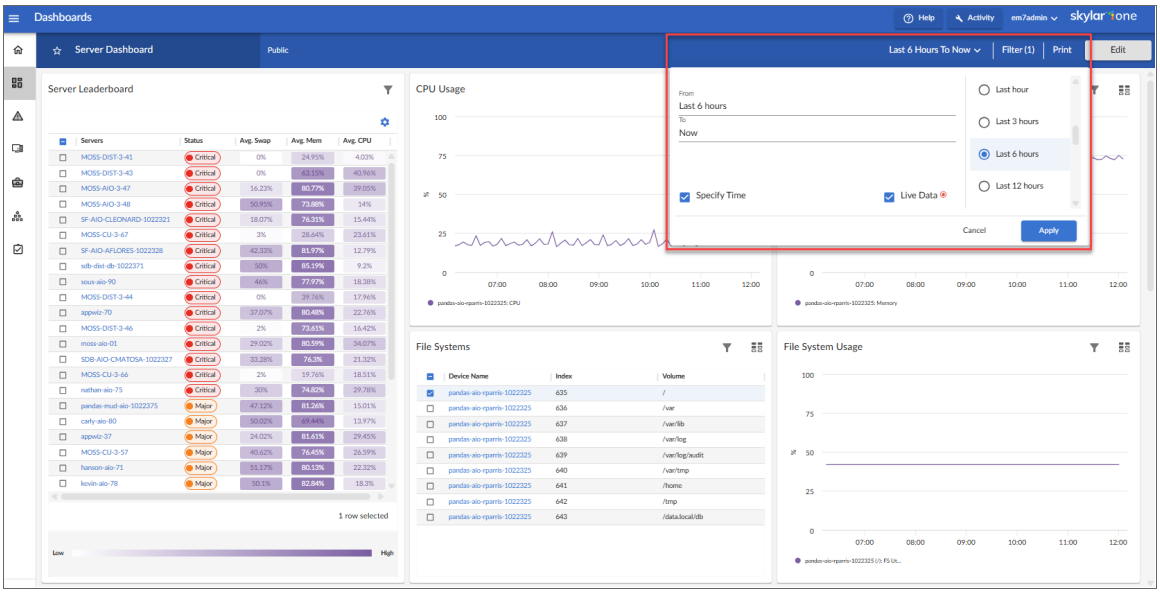
You can use the ***Time span filter*** on the **Dashboards** page to adjust the time span of data that appears in all the widgets on a dashboard. The default time span is *Last 6 Hours to Now*, but you can update the time span of data reflected in a dashboard by clicking the time span button and doing one of the following:

- Selecting an absolute time range from the list, such as *Yesterday* or *This week so far*. When you do so, Skylar One automatically updates the *From* and *To* fields with the corresponding dates and times.
- Selecting a relative time span from the list, ranging from *Last Hour* up to *Last 2 Years*. When you do so, Skylar One automatically updates the *From* and *To* fields with the corresponding dates and times.
- Clicking the calendar icons in the *From* and *To* fields to select the exact historical range of data that you want to display in the dashboard.

Optionally, you can also select one or both of the following options in addition to your time span selection:

- Select the ***Specify Time*** checkbox to specify the exact times (in addition to dates) that you want to display in the dashboard.
- Select the ***Live Data*** checkbox to set the ***To*** field to *Now*, so that every time the dashboard is refreshed, it will display the most recently polled data. If this checkbox is not selected, the ***To*** field is set to an absolute date and time for the dashboard. The dashboard automatically refreshes every five minutes.

After selecting a time span, click **[Apply]** to update the dashboard.



NOTE: The time span filter does not impact the list of events that appears in Events table widgets.

NOTE: If you select an historical time span, single-value widgets and tables will display the latest data point from the specified time span.

TIP: If you see a gap in a line on a graph, that means that Skylar One did not collect any data during that time frame.

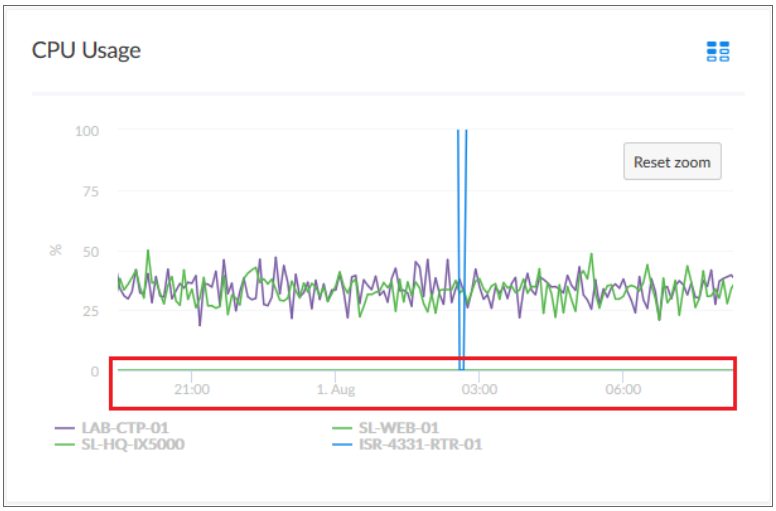
Zooming in on a Time Span

You can edit the time span of a line chart widget on the **Dashboards** page 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 on the **Dashboards** page by Organization or Device. The search process for the **[All Filters]** button works just like the Search feature works on other pages.

To filter dashboard data with the **[Filter (X)]** button:

1. On any of the dashboards, to temporarily filter the dashboard, click the **[Filter (X)]** button in the top right-hand corner of the **Dashboards** page. If you want to save the filters you apply, click the **[Edit]** button and then click **[Dashboard Filters]**. The **Default Data** window appears.
2. Click in one of the fields and type your filter text. As you type, Skylar One 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.
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 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.
7. Click the **[Apply]** button to apply your filters and settings.
8. If you are in **Edit** mode, click **[Save]** to save your filters. When the applied filters are saved, every user viewing it from that point on will view the dashboard with that filter and can adjust it temporarily.

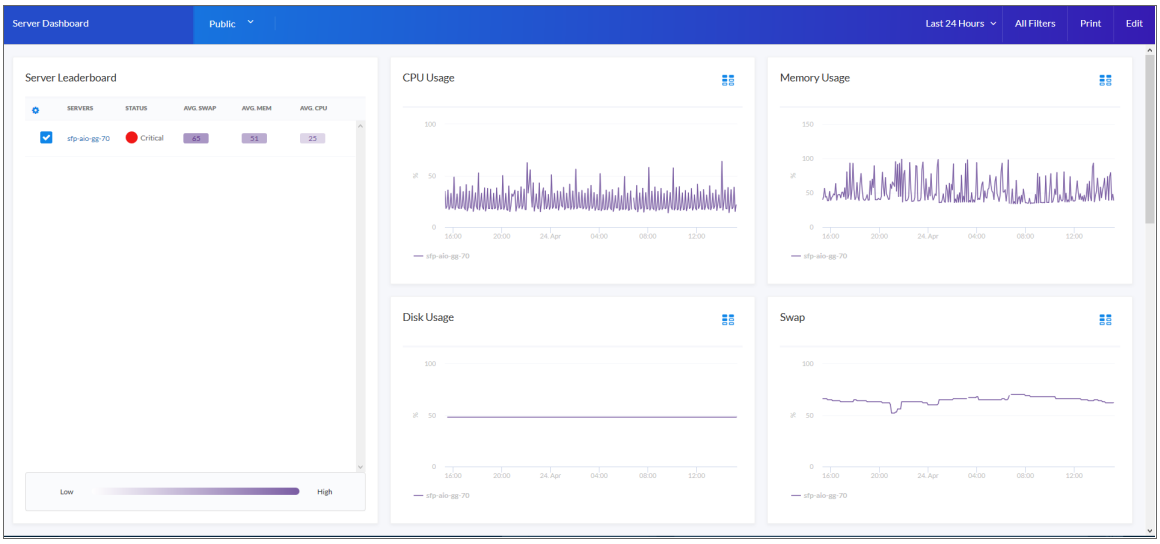
Focusing on One Device in a Dashboard

You can use a leaderboard or table widget to focus on just one device in a dashboard on the **Dashboards** page. 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** page, select a dashboard with a device leaderboard, such as **Server Dashboard**.
2. In the leaderboard or table widget, take note of the ID for that device.
3. If you don't have **ID** enabled as a Device Property in the table, hover over the link for the device you want to view. 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.sciencelogic.com/inventory/devices/detail/23**.

4. Click the **[All Filters]** button and enter the device ID into the ***By Device*** field. When the search options appear, select ***id<device ID>***, then click the **[Apply]** button. When the page refreshes, only the specified device appears in the dashboard:



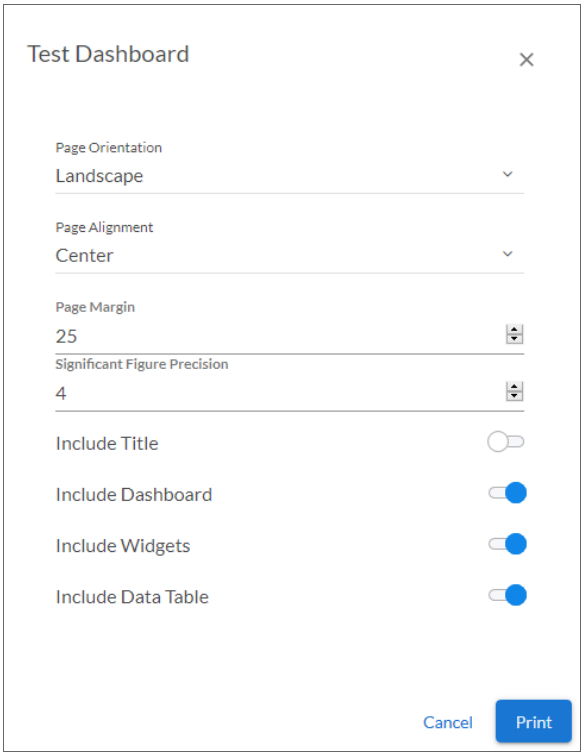
5. Alternatively, you can add **?deviceId=*<device ID>*** to the existing URL for the Server Dashboard, where ***<device ID>*** is the number you found in step 2. For example, if the original URL for the Server Dashboard is **https://em7.sciencelogic.com/dashboards/server-dashboard**, you would update 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.
6. To return to the default view for the dashboard, clear the ***By Device*** field in the **[All Filters]** menu or delete the **?deviceId=*<device ID>*** from the URL.

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** page and click the name of the dashboard you want to print. The dashboard page appears.
2. Click the **[Print]** button on the main navigation bar. A **Print** dialog appears:



3. Complete the following fields:
   - ***Page Orientation***. Select from *Portrait* or *Landscape* orientation for the output. The default is Landscape.
   - ***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).
   - ***Significant Figure Precision***. Specify the maximum number of numerals that you want to appear after the decimal point when data is presented in the output. The default is 4.
   - ***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. Skylar One generates a PDF version of the dashboard.

Creating a Dashboard for Global Manager

Skylar One includes several system default dashboards, but you can also create your own dashboards that are customized to your specific data visualization needs.

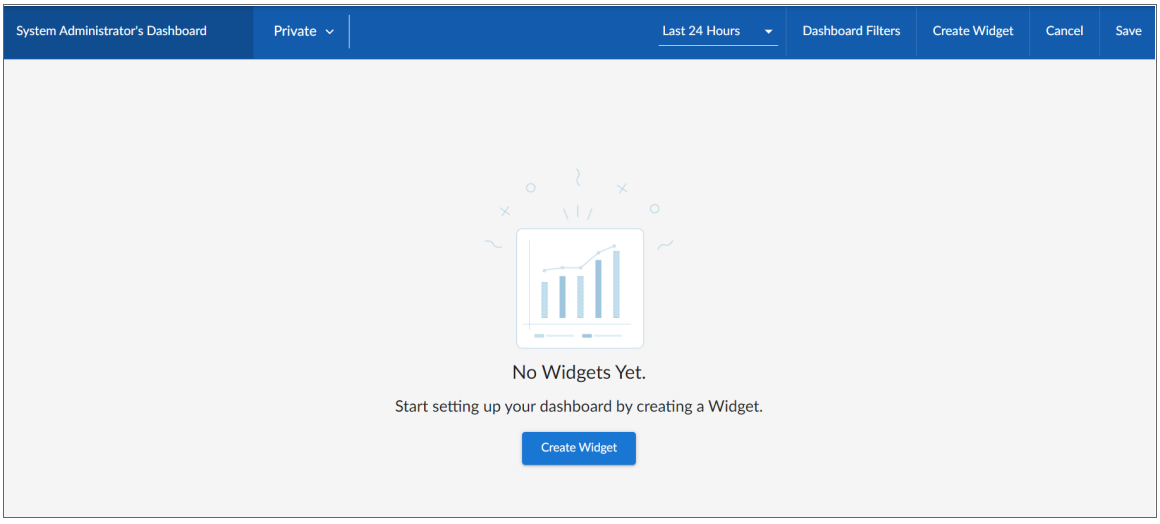
In a Global Manager system:

- When the **[Global View]** button on the **Dashboards** page is toggled ***on***, you can create and view dashboards that display data from all of your monitored stacks.
- When the **[Global View]** button on the **Dashboards** page is toggled ***off***, you can create and view dashboards that display data only for devices on the Global Manager system itself.

When you create a dashboard, you are defining a container that will display widgets. You must define a name for the dashboard, specify the space for one or more widgets, and determine the settings for those widgets. Each widget displays a report about data in Skylar One.

To create a new dashboard for your Global Manager system in Skylar One:

1. On the **Dashboards** page (), click the **[Global View]** button to toggle it on, and then click the **[Create Dashboard]** button. An empty dashboard page appears:



2. Click the ***Name*** field at the top left corner 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.

3. Create one or more widgets for your dashboard. For more information, see the next section, *Creating Dashboard Widgets*.

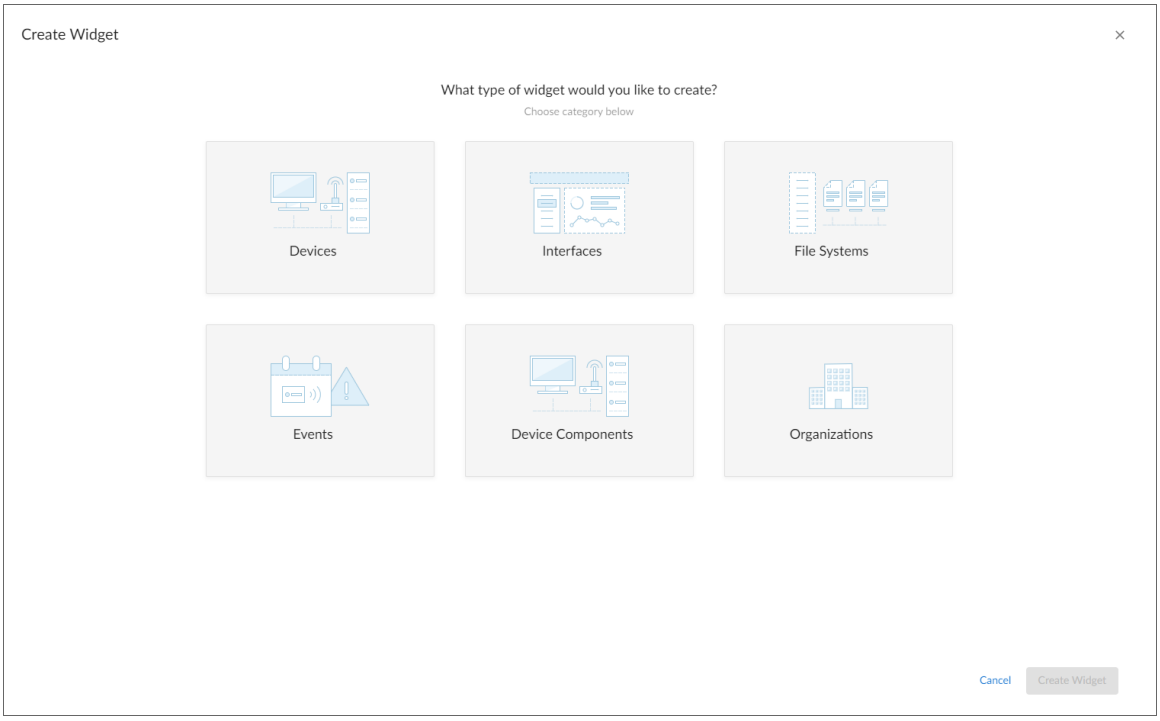
4. Determine the dashboard's visibility settings. For more information, see the section *Sharing a Dashboard*.
5. Click **[Save]** in the top right corner of the page.

Creating Dashboard Widgets

A dashboard is a container for one or more widgets that display reports about data in Skylar One. You can create widgets that are customized to display the specific data that you want to appear in your dashboard.

To create a dashboard widget for a Global Manager dashboard:

1. On the **Dashboards** page, toggle on the **[Global View]** button and then click the **[Create Dashboard]** button to create a new dashboard or click the name of an existing dashboard that you want to edit.
2. If you are creating a new dashboard, click the **[Create Widget]** button. If you are editing an existing dashboard, click the **[Edit]** button and then click the **[Create Widget]** button. The **Create Widget** page appears:



3. Select a widget type by clicking the relevant box. Your options include:

NOTE: Depending on your system configuration, you might not see all widget types.

- ***Devices***. Displays data based on devices and Dynamic Applications.

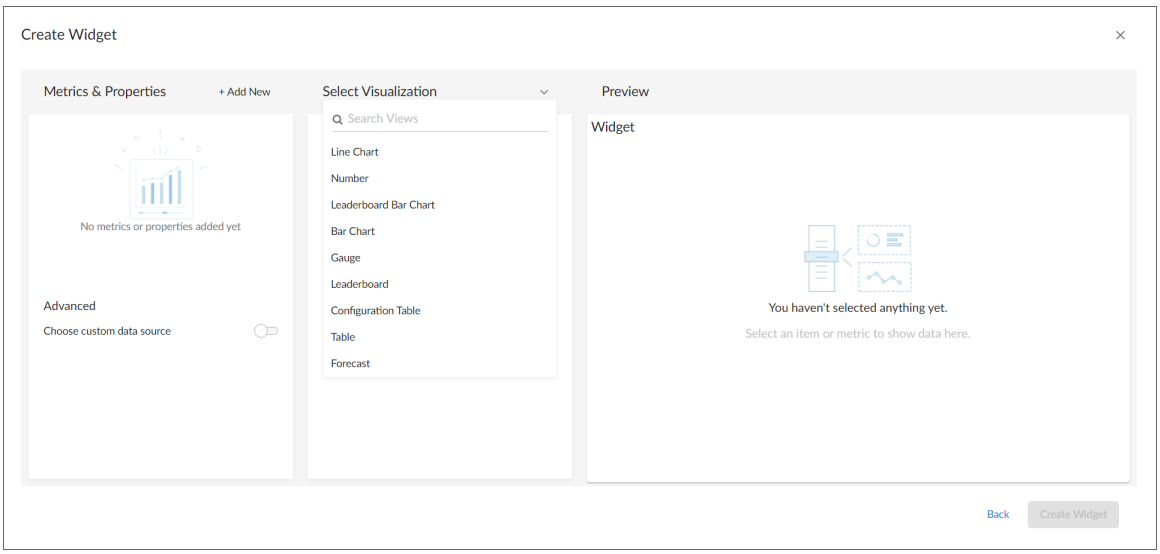
- ***Interfaces***. Displays data about network interfaces.
- ***File Systems***. Displays data about disk space used, in percent, for devices.
- ***Events***. Displays data about the events that exist for devices.
- ***Device Components***. Displays data about entities that run under the control of another device (in a parent-child relationship).
- ***Organizations***. Displays data about selected organizations, and can drive context to Devices, Interfaces, File Systems, and Events widgets.

TIP: Because of the way data and relationships are used and presented in Device Component widgets, ScienceLogic recommends the following best practices when creating a Device Component widget:

- Using a *Table visualization*
- *Selecting the **Filter data specifically in this widget** option* and *Filtering by* parent device so that the widget returns the root level of the Device Component Map tree, based on the root level's Device Class
- *Enabling the widget to drive a context of Type "Device Component"* for other widgets
- Creating additional Device widgets that subscribe to that Device Component context, using additional filtering options as necessary to ensure the correct devices display in the widget

NOTE: You can add Organizations widgets to dashboards only when the **[Global View]** button is toggled off.

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



4. Complete the fields on the page to customize the widget. For more information about each of the ways you can customize a widget, see the following sections:
    - *Selecting How the Widget Displays Data*
    - *Adding Metrics and Properties to a Widget*
    - *Specifying Which Items Will Appear in a Widget*

> **TIP:** As you make updates to the widget, your selections will be reflected in the **Preview** pane on the right side of the page.

5. When you are finished customizing the widget, click the **[Create Widget]** button to save the new widget. If this button is grayed out, review the settings on the page for errors or missing information in required fields.
6. On the dashboard page, click **[Save]**.
7. To add more widgets to the dashboard, click the **[Edit]** button under the main tab bar and repeat this procedure for each new widget.

Selecting How the Widget Displays Data

On the **Create Widget** page, click the ***Select Visualization*** drop-down list to select how you want the widget to display data.

The visualization options that you can select vary by widget type; not all options appear for all widget types. If only one visualization option is available for the selected widget type, then that visualization option will be selected automatically.

> **TIP:** Some widgets (such as leaderboard widgets) ***drive*** the data or "context" for other widgets in the dashboard, while other widgets ***receive*** the data or "context" from that driving widget. When a widget drives context for other widgets, that means you can select one or more items in the driving widget and it will determine the data that appears in the receiving widgets by displaying data only for the items selected. For more information, see the section on *Specifying Which Items Appear in a Widget*.

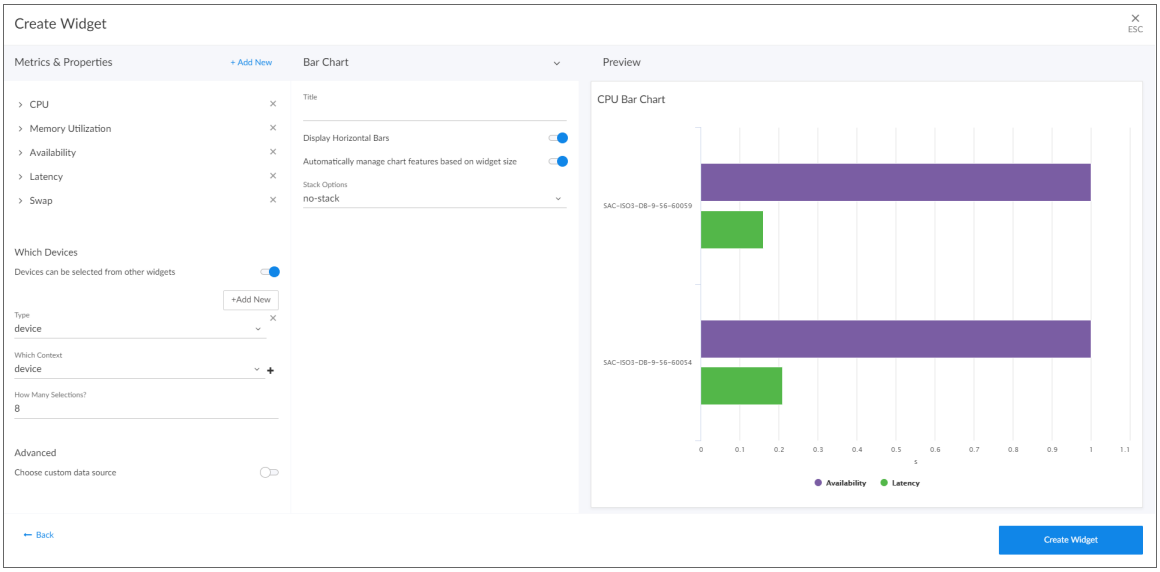
The available visualization options are discussed in the following sections:

- *Bar Chart*
- *Configuration Table*
- *Forecast*
- *Gauge*
- *Leaderboard*
- *Leaderboard Bar Chart*
- *Line Chart*
- *Number*

- *Pie Chart*
- *Table*

Bar Chart Widgets

Bar Chart widgets display one or more metrics as a colored vertical or horizontal bar or bars. Selecting a single item can *drive* data or "context" to other widgets:

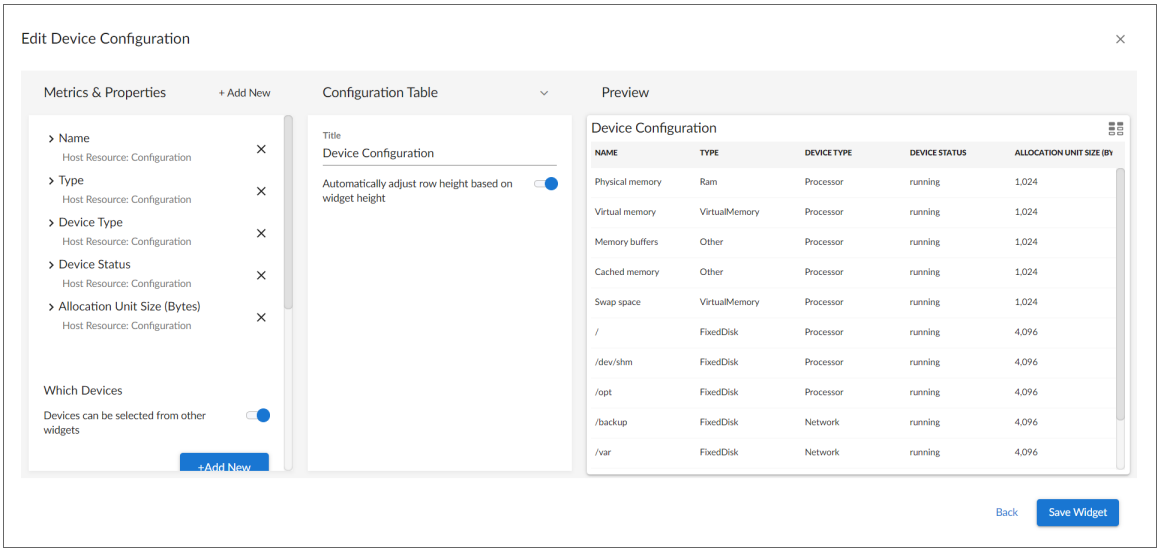


If you select *Bar Chart*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Display Horizontal Bars***. Select this toggle to display bars horizontally.
- ***Automatically manage chart features based on widget size***. Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.
- ***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*.

Configuration Table Widgets

Configuration Table widgets display configuration Dynamic Application data for a single device in a boxed set of rows and columns. A configuration table widget *receives* data or "context" from other widgets:

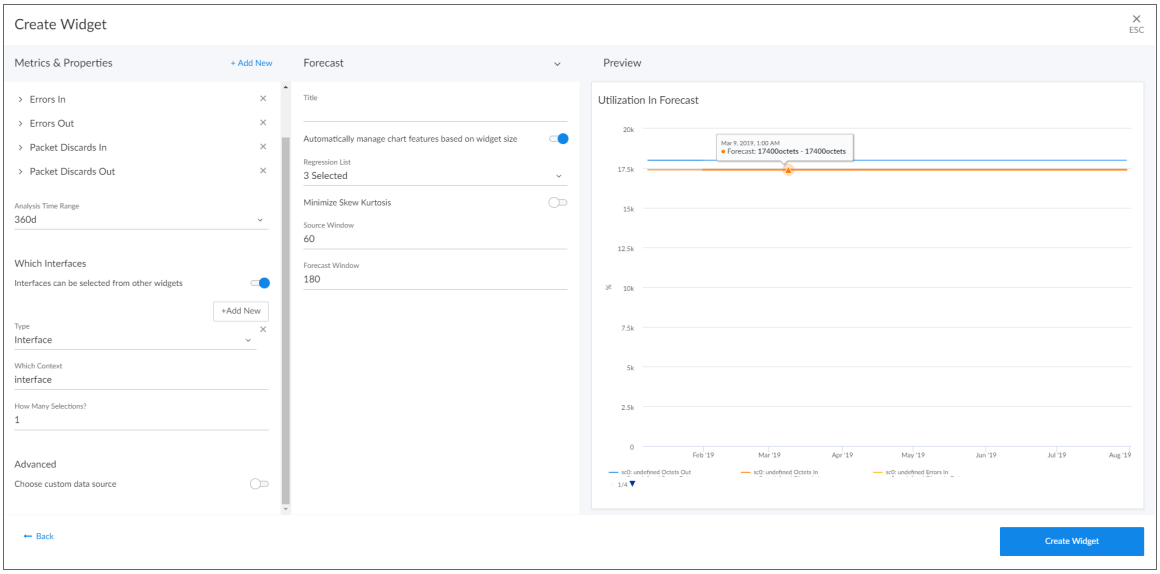


If you select *Configuration Table*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Automatically adjust row height based on widget height.*** Select this toggle if you want the widget to dynamically adjust the height of the rows in the table when the size of the widget is adjusted.
- ***Select Row Height***. Select the relative height of the rows in the table. Choices are *Small*, *Medium*, or *Large*. This field appears only if the toggle is not selected in the ***Automatically adjust row height based on widget height*** field.

Forecast Widgets

Forecast widgets display projected forecast data for a specific object and collection metric using historical data and selected regression methods:



If you select *Forecast*, complete the following fields:

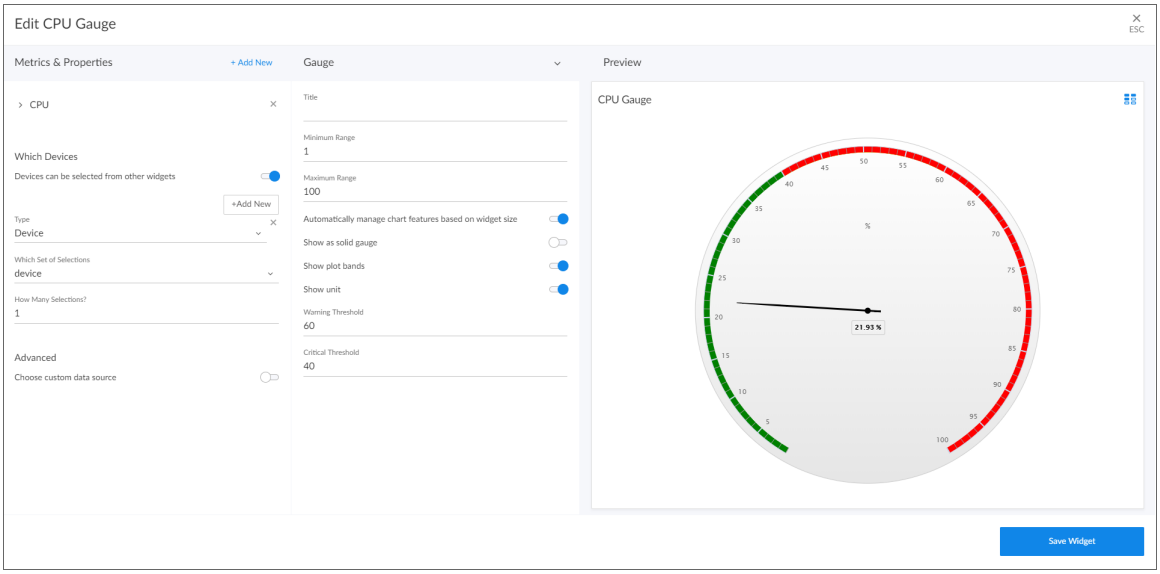
- ***Title***. Enter a title for the widget.
- ***Automatically manage chart features based on widget size.*** Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.
- ***Automatically scale y-axis***. Select this toggle to have the y-axis of a line chart automatically scale to fit the data. Toggling this off allows you to set a Maximum and Minimum value for the y-axis.
- ***Step line***. Select this toggle to display the line chart in which the points are connected by horizontal and vertical line segments.
- ***Threshold Line***. Specify a number that represents the threshold for a line chart.
- ***Regression List***. Select the regression method or methods you want Skylar One to try when calculating the forecast data in a forecast widget. You can select multiple types of regression, and Skylar One 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. Skylar One will then determine which regression method(s) of those you have chosen will best model the forecast data. Options include:
    - *Average Regression*. The forecast for future values is equal to the average of the historical data.
    - *Drift Regression*. The forecast for future values increases or decreases based on the average change observed in historical data over time.

- *Exponential Least Squares Regression*. The forecast for future values is an exponential curve determined by the best fit between a set of data points.
- *Least Squares Regression*. The forecast for future values is a straight line determined by finding the best fit between a set of data points.
- *Logarithmic Least Squares Regression*. The forecast for future values is a logarithmic curve determined by the best fit between a set of data points.
- *Naive Regression*. The forecast for future values is the same as the last collected value.
- *Null Regression*. The forecast for future values is generated using random samples of collected data where some elements are constant.
- *Seasonal Drift Regression*. The forecast for future values increases or decreases based on the average change in historical data from the same season of the year (for example, same month of the previous year).
- *Seasonal Weighted Regression*. The forecast for future values is determined by finding the best fit between a set of data points, which have all been weighted to increase or decrease their influence, and adjusting based on historical data collected from the same season of the year (for example, same month of the previous year).
- *Seasonal Naive Regression*. The forecast for future values is the same as the last collected value from the same season of the year (for example, same month of the previous year).

- ***Minimize Skew Kurtosis***. Select this toggle button to enable transformation of the source data into a normal distribution by compensating for skewness (lack of symmetry in the data set distribution) and kurtosis (heaviness or lightness of data outliers relative to a normal distribution) in the data, which makes the data easier to read. For example, you might select this toggle if you want to normalize the distribution of a data set that is asymmetrical or has a very high or low number of outliers.
- ***Source Window***. Specify the number of days from which the widget will gather data for the forecast. The default is 60 days.
- ***Forecast Window***. Specify the number of days of forecast data that you want the widget to display. The default is 180 days.

Gauge Widgets

Gauge widgets display 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:



TIP: If you change the order of the Warning and Critical Thresholds, you can invert the gauge colors so that as numbers increase on the gauge, the numbers correspond with red/yellow/green instead of green/yellow/red.

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

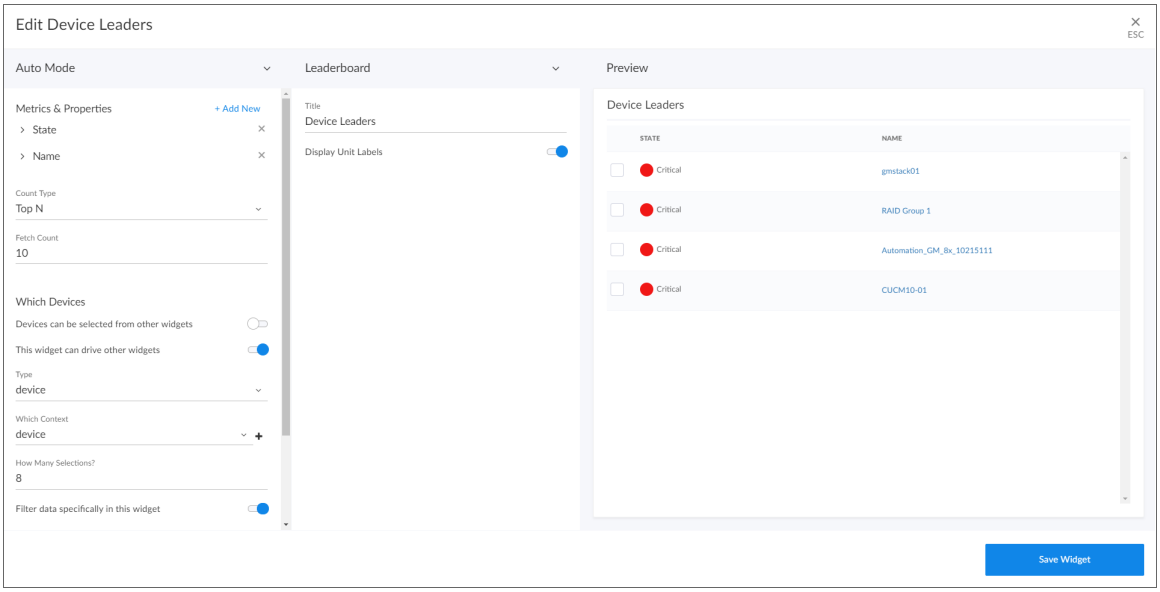
If you select *Gauge*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Minimum Range***. Specify the upper limit of a gauge. The default is 0.
- ***Maximum Range***. Specify the upper limit of a gauge. The default is 100.
- ***Automatically manage chart features based on widget size***. Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.
- ***Show as solid gauge***. Select this toggle to display the gauge as a solid bar.
- ***Show plot bands***. Select this toggle to show the plot bands on a gauge.
- ***Show unit***. Select this toggle to display the current value on a gauge).

- ***Warning Threshold***. Specify where you want the yellow warning portion of a gauge to start. The default is 60.
- ***Critical Threshold***. Specify where you want the red critical portion of a gauge to start. The default is 80.

Leaderboard Widgets

Leaderboard widgets display 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:



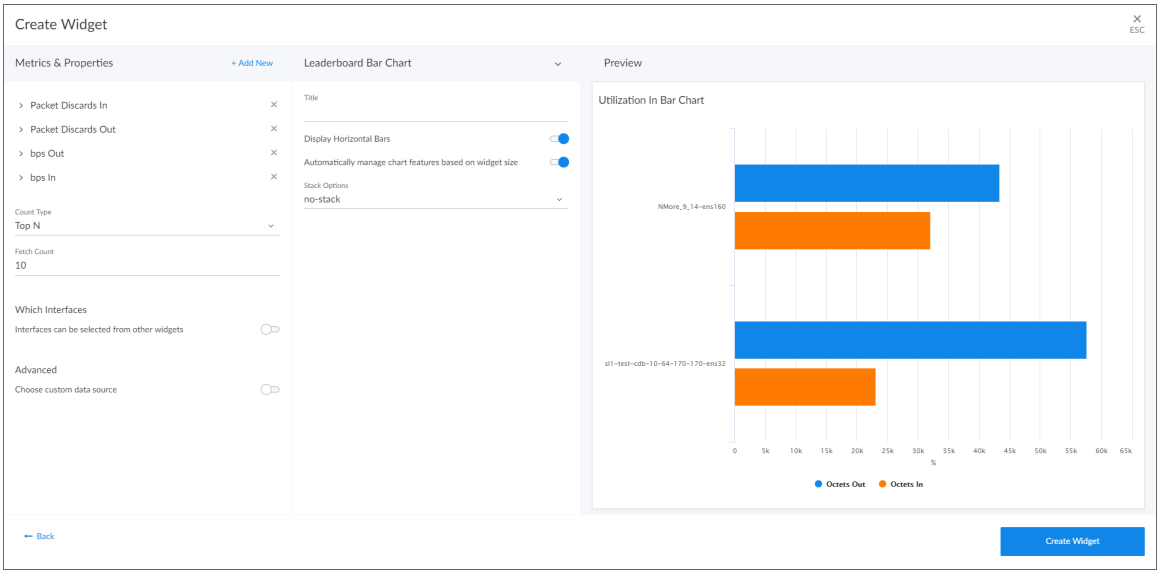
NOTE: You can use the ***Display zeroes*** toggle when editing a Top-N or Bottom-N widget to enable the widget to show or hide zero results.

If you select *Leaderboard*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Display Unit Labels***. Select this toggle to display relevant unit labels, such as "KB" or "%" along with the values in the widget.
- ***Display Icon***. Select this toggle to display the icon associated with each item in a table.
- ***Automatically adjust row height based on widget height***. Select this toggle if you want the widget to dynamically adjust the height of the rows in the leaderboard when the size of the widget is adjusted.

Leaderboard Bar Chart Widgets

Leaderboard Bar Chart widgets display 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:



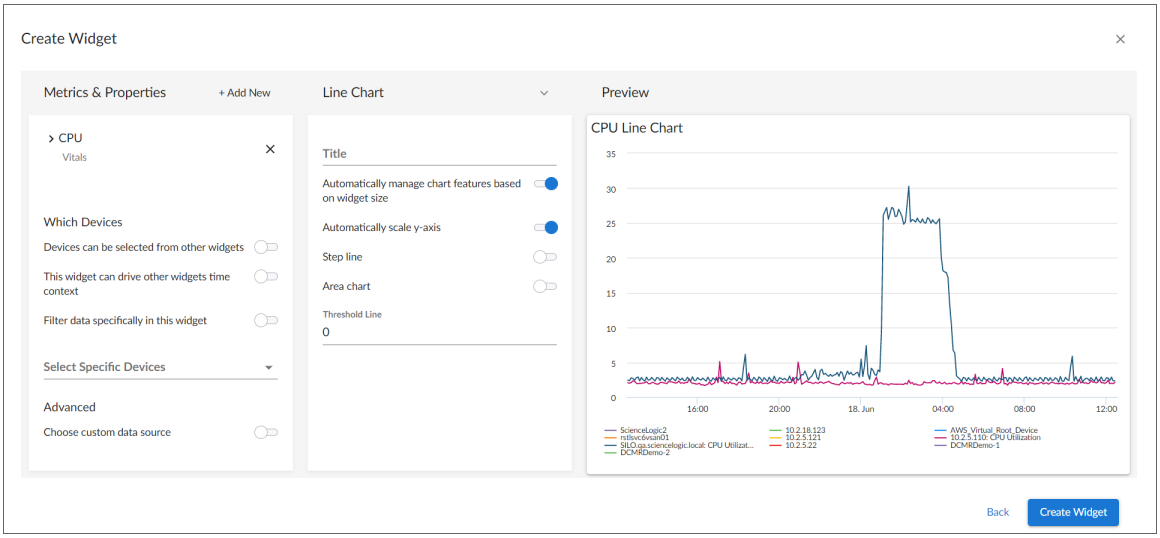
NOTE: You can use the ***Display zeroes*** toggle when editing a Top-N or Bottom-N widget to enable the widget to show or hide zero results.

If you select *Leaderboard Bar Chart*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Display Horizontal Bars***. Select this toggle to display the chart bars horizontally instead of vertically.
- ***Automatically manage chart features based on widget size***. Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.
- ***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* .
- ***Customize Labels***. For Device, File System, and Interface widgets only. Specify if you want to display only Device labels; only Device Index, File System, or Interface labels, depending on the widget type; or all labels in your bar chart.

Line Chart Widgets

Line Chart widgets display data as a series of data points over time connected by straight line segments. This enables you to view changes over time for the specific item and metric. You can click on a point in time on the line chart to display the exact metric value collected for that time. You can also zoom in on a specific time period for a better view by clicking and dragging your mouse over that time period.

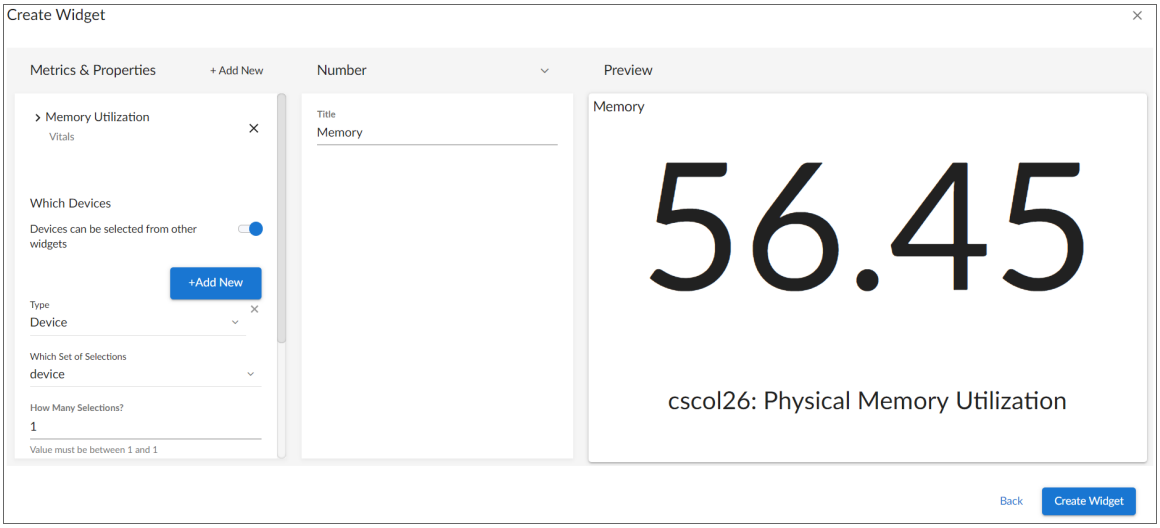


If you select *Line Chart*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Automatically manage chart features based on widget size***. Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.
- ***Automatically scale y-axis***. Select this toggle to have the y-axis of a Line Chart automatically scale to fit the data. Toggling this off allows you to set a Maximum and Minimum value for the y-axis.
- ***Step line***. Select this toggle to display the line chart in which the points are connected by horizontal and vertical line segments.
- ***Area chart***. Select this toggle to display the line chart as an area chart with the region beneath the line colored in.
- ***Stack Options***.If Area Chart is enabled, you can specify how you want to display data in a line chart. Your options include *no-stack* (show each value as its own bar), *normal* (show all values in one bar), and *percent* .
- ***Threshold Line***. Specify a number that represents the threshold for a line chart.

Number Widgets

Number widgets display data as a single number to highlight an important metric for a device or event. The size of the number and the 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:



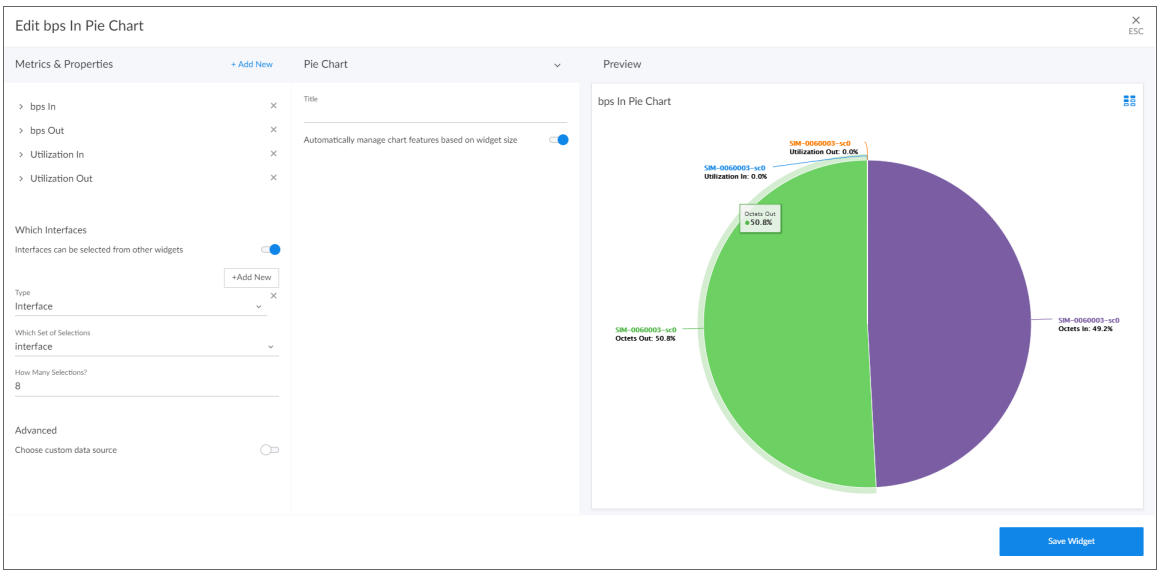
NOTE: If you create a number widget and you select more than one item on the widget driving data or "context" to that widget, the number widget displays data for only the *first* item you selected in the driving widget. For more information, see the section on

If you select *Number*, complete the following field:

- ***Title***. Enter a title for the widget.

Pie Chart Widgets

Pie Chart widgets display data metrics as a percentage of a whole:

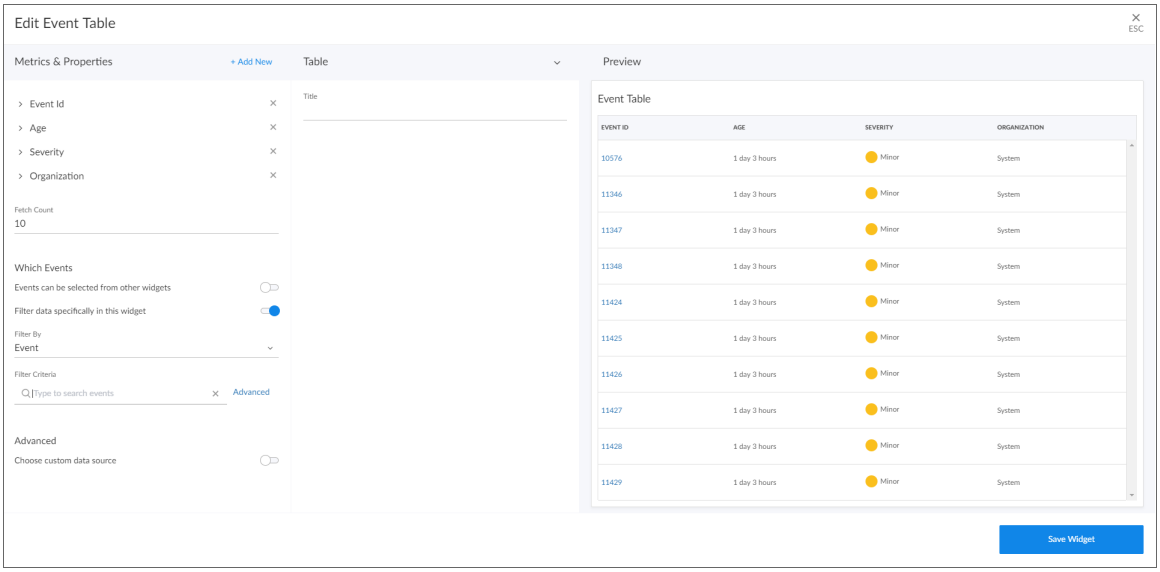


If you select *Pie Chart*, complete the following fields:

- ***Title***. Enter a title for the widget.
- ***Automatically manage chart features based on widget size***. Select this toggle if you want the widget to dynamically hide the chart's features (labels and legends) when the size of the widget is adjusted. For more information, see the *Resizing and Moving Widgets on a Dashboard* section.

Table Widgets

Table widgets display data in a boxed set of rows and columns. A table widget can be used to *drive* data or "context" to other widgets. If you have an Event, Device, or Service table, selecting its name or ID takes you to its detail page:



If you select *Table*, complete the following fields:

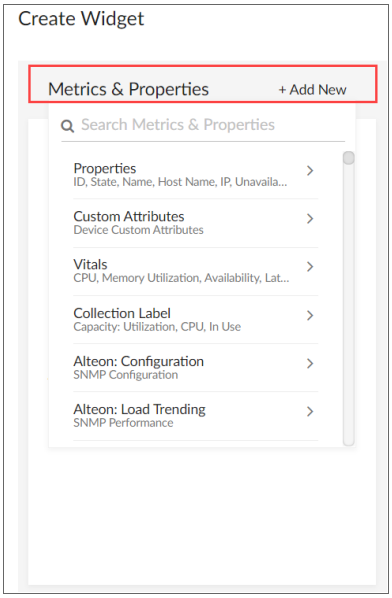
- ***Title***. Enter a title for the widget.
- ***Display Unit Labels***. Select this toggle to display relevant unit labels, such as "KB" or "%" along with the values in the widget.
- ***Display Icon***. Select this toggle to display the icon associated with each item in a table.
- ***Automatically adjust row height based on widget height.*** Select this toggle if you want the widget to dynamically adjust the height of the rows in the table when the size of the widget is adjusted.
- ***Select Row Height***. Select the relative height of the rows in the table. Choices are *Small*, *Medium*, or *Large*. This field appears only if the toggle is not selected in the ***Automatically adjust row height based on widget height*** field.

Adding Metrics and Properties to a Widget

On the **Create Widget** page, you can specify the metrics and properties that you want to appear in your widget.

To add a metric type or property to a widget:

1. On the **Create Widget** page, click the ***Metrics & Properties*** label or click **+ Add New**. A drop-down list displays a list of metric types and properties from which you can choose:



NOTE: The metric types and properties that you can select are specific to the widget type you selected; not all options appear for all widget types.

2. Select a metric type. Your possible options include:
    - ***Properties***. These metrics contain basic device information, including ID, State, Name, Host Name, Interface ID, IP, Index, Index Label, Collector Group, Device Class, and Unavailable. Name, Host Name, and State are commonly used for leaderboard widgets.
    - ***Custom Attributes***. These metrics contain any custom attributes you created in Skylar One. Custom attributes are name-value pairs that you can use to add custom descriptive fields to assets, devices, interfaces, themes, and vendors. For more information, see the ***Device Management*** manual.
    - ***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.

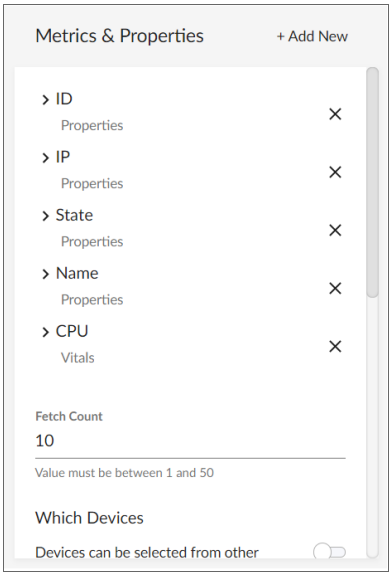
- ***Dynamic Application metrics***. These metrics contain the available Dynamic Applications that you can use as metrics in the widget, such as "AWS Custom Metrics" or "Cisco: BGP Peer Stats". This menu continually loads more Dynamic Applications as you scroll to the end of the list.
- ***Interface***: These metrics contain information about discovered network interfaces on the device, including Utilization In or Out, Errors In or Out, and Packet Discards In or Out. (This option appears only for Interface widget types.)
- ***File System***. These metrics contain information about the amount of disk space used, in percent. (This option appears only for File System widget types.)
- ***Polled Data***. These metrics contain information about agent polled data and return with a timestamp.

TIP: To locate a specific metric, type a search term in the ***Search Metrics & Properties*** field to filter the list of categories. Once you navigate to a selected category, you can search the list of metrics within that category.

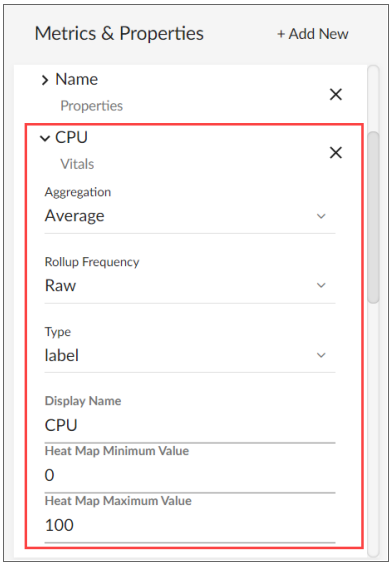
3. When you select a metric type, a new menu appears with a list of metrics and properties that you can add to your widget. Select one or more metrics or properties from the menu and then click the back-arrow icon (‹) to return to the main ***Metrics & Properties*** drop-down list.

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

4. 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:



5. To edit the settings for a specific metric, click the metric name or the forward-arrow icon (›) to access a menu for that metric. The forward-arrow icon will turn to a downward-arrow icon (⌄) and a list of settings will appear for that metric:



NOTE: Not all metrics have these additional settings.

The possible metric settings include:

- ***Aggregation***. Specify the method of aggregation (average, maximum, minimum) to display on the collected values for this metric.
- ***Analysis Time Range***. Optionally, update the time frame displayed in this widget. (This option applies only to forecast widgets).
- ***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. (This option applies only to leaderboard and table widgets.)
- ***Display Name***. Type a name for this metric as you want it to display in the widget.
- ***Display Zeroes***. Use this toggle when editing a Top-N or Bottom-N widget to enable the widget to show or hide zero results.
- ***Fetch Count***. Type the number of devices that you want to view on the widget. (This option applies only to line chart, leaderboard, leaderboard bar chart, table, and tile widgets.).

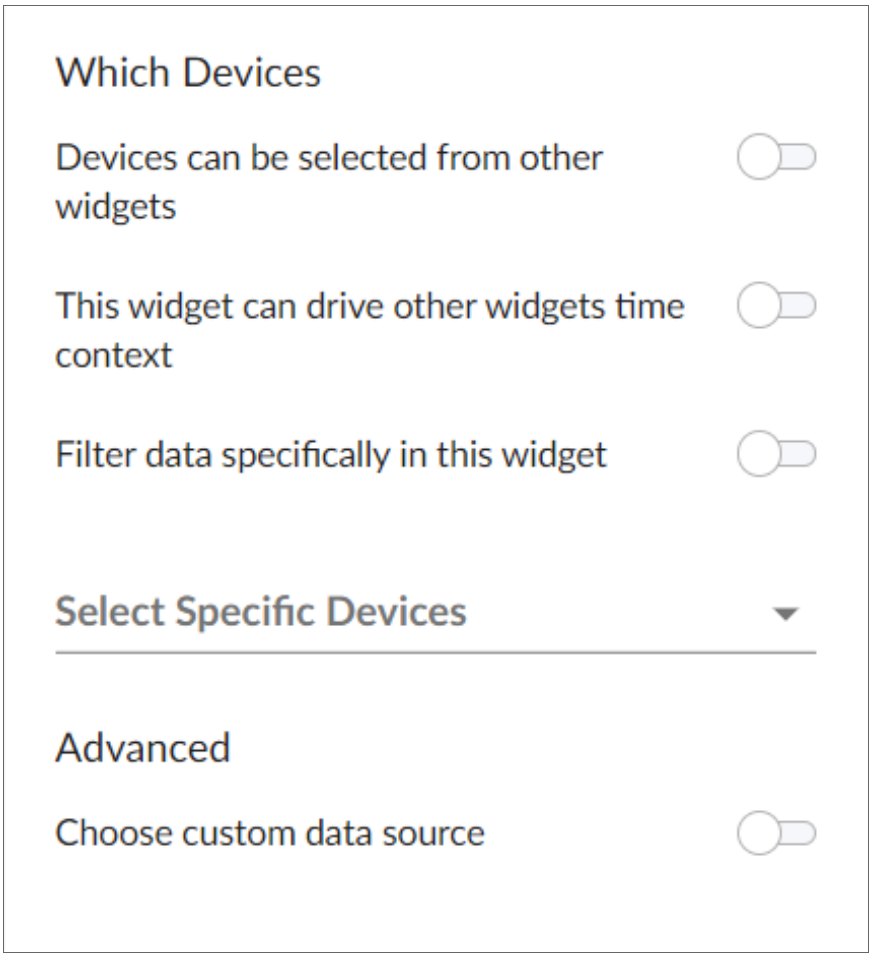
- ***Indexes***. Specify the index values that you want to be returned per device for this metric. Select one of the following options:
    - *First Index*. Returns only the first index value for this metric.
    - *Last Index*. Returns only the last index value for this metric.
    - *Multiple*. Specify the number of index values that you want to be returned per device for this metric. You can also select the ***Advanced Filters*** option, which enables you to search for specific indexes by index value, name, or metric presentation.

NOTE: This option applies only to device widgets.

- ***Maximum Value***. Specify the highest possible value to be displayed in the widget.
- ***Minimum Value***. Specify the lowest possible value to be displayed in the widget.
- ***Rollup Frequency***. Specify a type of normalized performance data (hourly, daily, or raw) for this metric. Raw data is stored up to the system threshold, and then "rolled-up" into hourly and then daily data as it gets further into the past. Certain widgets allow for "auto", which will display the best data for the timespan being viewed.
- ***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.
- ***Unit***. Optionally, specify the unit for this widget, such as a percentage or a unit of time.

Specifying Which Items Will Appear in a Widget

On the **Create Widget** page, there are several ways in which you can specify how Skylar One should determine the items that will appear in your widget.



In the ***Which <Items>*** section (where *<Items>* corresponds with the widget type you created), you can:

- Determine if the widget will *drive* data (or "context") to another widget or *receive* data (or "context") from another widget
- Filter a specific set of data in the widget
- Select specific devices or services that you want to appear in the widget
- Select the custom data source you want to use

To specify which items will appear in a widget, you can select one of the following options, more than one of the options, or none of the options in the ***Which <Items>*** section of the **Create Widget** page:

- ***<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 widgets from which you want to receive data:

    - ***Type***. Select a widget type that will drive data or "context" to this widget. The default type is based on the current widget type. For example, if you want a Device widget to drive data to this widget, select *Device*.

    - ***Which Set of Selections***. From the drop-down list, select the item type that the user will select to drive the data ("context") to this widget. The default selection type is based on the widget type you selected in the ***Type*** field. For example, if you want the user to select one or more devices in another Device widget to drive the data that appears in this widget, select *device*.

    - ***How Many Selections?*** Select the maximum number of items the user can select in the driving widget. For example, if you want the user to be able to select only 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 Set of Selections***, 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 current widget type. For example, if you want a Device widget to drive data to this widget, select *Device*.

    - ***Which Set of Selections***. 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 context to other widgets. The default context type is based on the widget type. Leaderboard Bar Chart widgets for events can have multiple contexts. Also, a File System or Interface widget can publish its file system or interface context as well as a secondary context of device.

    - ***How Many Selections?*** Select the maximum number of items the user can select in the driving widget. For example, if you want the user to be able to select only one device at a time, select *1*.

    - ***Auto Selection***. Select the number items that are automatically selected in the widget that drives context to other widgets.

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.

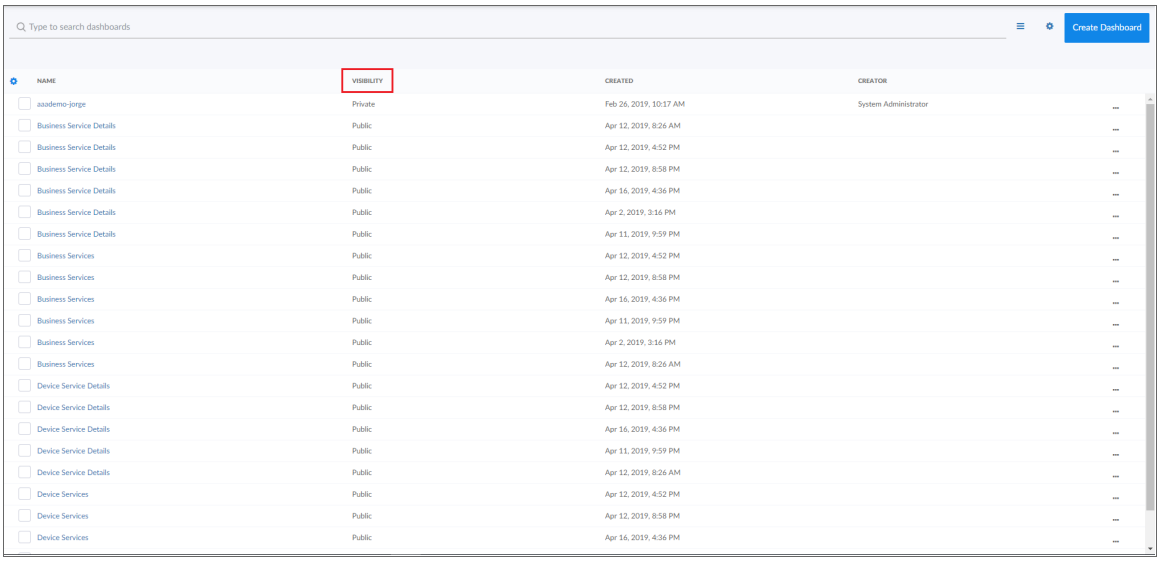
- ***Filter data specifically in this widget***. Select this option if you want to view a specific set of data in this widget. For example, you can create multiple leaderboard widgets in a dashboard that contain just the devices you want to view. If you select this option, complete one or both of the 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.
- ***Select Specific Devices***. If you are creating a widget for devices, select the specific devices that you want to include in the widget. These devices will appear ***in addition to*** any devices that would appear based on context receiving/driving or filtering.
- *Advanced*.
    - ***Choose custom data source***. Toggling this on will display the *Data Source* drop-down. Select the custom data source you wish to use, if applicable. This option is for advanced users only. Options include *Auto Mode* or various metric types.

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** page, the ***Visibility*** column lists whether a dashboard is public, private, or shared with only specific organizations.

The data within each dashboard is limited using multi-tenancy restrictions to allow only users with proper permissions and organization memberships to view data. There are four scenarios for dashboard visibility:

- ***Private***. Only the creator of the dashboard can view the dashboard.
- ***Public***. All users can view the dashboard.
- ***Shared to the System Organization***. Only administrator users can view the dashboard.
- ***Shared to Specified Organizations***. Members of the specified organization or organizations can view the dashboard.



To change the visibility of a dashboard:

1. Go to the **Dashboards** page and open the dashboard. Click the **[Edit]** button on the main navigation bar.
2. Next to the title of the dashboard, click the **Visibility** drop-down list and select one of the following options:
    - *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.
        - If you are an Administrator user and want to share a dashboard with only the System organization, select ***System*** from the organization list.
        - If you have dashboards that you want to share with users in other organizations, but not with System, select the organization(s) from the list and deselect ***System***.
3. After you set the visibility of your dashboard, click the **[Save]** button on the main navigation bar.

Editing a Dashboard

If you have the proper permissions, you can edit an existing dashboard by performing the following steps:

1. Go to the **Dashboards** page and click the name of the dashboard you want to edit. The dashboard page appears.
2. Click the **[Edit]** button on the main navigation bar.
3. Do one of the following:
    - If you want to add a widget to the dashboard, click the **[Create Widget]** button. For more information about creating widgets, see the section *Creating Dashboard Widgets*.

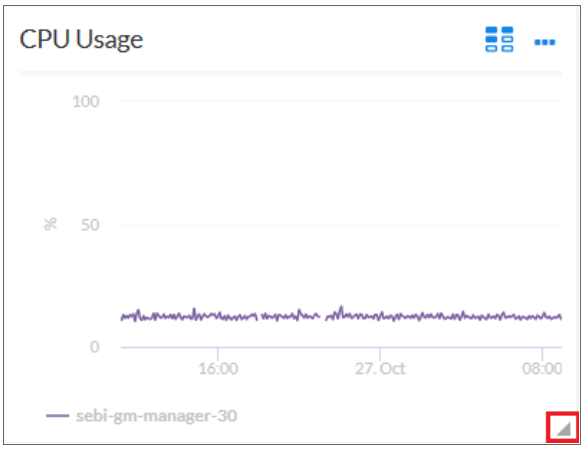
- If you want to edit an existing widget, click the **[Actions]** button (···) on that widget and select *Edit*. The **Edit** page appears.
- If you want to make a copy of an existing widget and then customize the new widget, click the **[Actions]** button (···) and select *Duplicate*. The new widget appears at the bottom of the dashboard. You can then click the **[Actions]** button (···) on that widget and select *Edit* to make changes to the widget.

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, click the **[Save]** button on the main navigation bar.

Resizing and Moving Widgets on a Dashboard

To resize and move widgets on a dashboard:

1. Go to the **Dashboards** page and click the name of the dashboard you want to edit. The dashboard page appears.
2. Click the **[Edit]** button on the main navigation 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. Widgets are based on a fractional grid of the dashboard screen size. You can snap the widget to 12 columns and 8 rows, which are proportional to the total size of the browser, and scale up or down as the browser does.



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.

If you selected the ***Automatically manage chart features based on widget size*** toggle when creating the widget, the widget will dynamically show or hide features of the chart, such as axis labels or the legend, depending on the effective size of the widget on the screen.

For example, if the widget is 1/2 of the height and 1/4 of the width of the dashboard, the widget might display at 500 by 400 pixels when viewed in a large browser on a 1080-pixel screen. This feature will

display all the surrounding information in the widget to the user when they have this much resolution to devote to the chart. However, if the same dashboard is viewed in a smaller resolution or screen, or the widget itself is resized to be a smaller fraction of the dashboard, features of the chart may automatically be hidden to maximize the amount of data that is displayed within the smaller panel.

Certain features are associated with widget height, such as table row height or horizontal axis labels, while other features are associated with widget width, such as vertical axis labels.

If you disable the ***Automatically manage chart features based on widget size*** toggle, you are presented with options to manually enable or disable each feature of each chart and table, and the size of the user's browser or widget display will not cause those features to appear or disappear.

Deleting a Dashboard

You can delete any dashboard that you have created, as well as any other dashboard in Skylar One.

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

To delete a dashboard:

1. On the **Dashboards** page, click the **[Actions]** 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.

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

International: +1-703-354-1010