Device Management

SL1 version 8.14.0

Table of Contents

Introduction 7
What is a Device? 8
What is a Device Record? 8
What is a Device Class? 9
What is a Device Category? 9
How Does SL1 Manage Devices? 10
What is Discovery? 11
What is a Credential? 11
What is a Virtual Device? 12
What are Component Devices? 13
What is a Dynamic Application? 13
What is an SL1 Agent? 14
What is Virtualization? 14
What is an Asset Record? 14
Using the Devices Page 16
Viewing Devices 17
Viewing Additional Data about a Device 18
Aligning a Device with a Different Organization 18
Adding Devices with Discovery 18
What is Discovery? 19
What are Credentials? 19
Prerequisites for Discovering Devices on the Devices Page 20
Adding Devices Using Universal or Guided Discovery 20
Adding Devices Using Unguided Discovery 24
Working with Discovery Sessions 32
Using the Device Investigator 33
Adding Metrics to the Investigator Tab 36
Using the Info Drop-Down on the Device Investigator Page 38
Comparing Devices on the Investigator Tab 39
Using Device Tools 40
Combining Charts on the Investigator Tab 41
Running a Device Report 42
Overview of the Device Investigator Tabs 42
The Settings Tab 43
The Attributes Tab 45
The Collections Tab 46
The Configs Tab 50
The Events Tab 51
The Interfaces Tab 51
The Journals Tab 53
The Map Tab 54
The Monitors Tab 54
The Notes Tab 55
The Ports Tab 55
The Processes Tab 56
The Redirects Tab 57
The Relationships Tab 57
The Schedules Tab 58
The Services Tab 59
The Software Tab 60

The Thresholds Tab 61
The Tickets Tab 62
Working with Device Classes 63
Working with Device Categories 64
Assigning Icons to Devices, Device Classes, and Device Categories 67
Using the Device Manager Page 69
Viewing the List of All Devices 70
Device Manager Preferences 73
Filtering the List of Devices 73
Special Characters 75
Using the Advanced Filter with the List of Devices 78
Generating a Report for Multiple Devices 80
Generating a Report for a Single Device 82
Viewing the List of Component Devices 84
Availability for Component Devices 87
Viewing Children Devices 88
Filtering the List of Component Devices 88
Using the Advanced Filter with the List of Component Devices 89
Bulk Actions in the Device Management Page 91
Bulk Actions for Component Devices 92
Bulk Merging and Unmerging of Devices 94
Performing a Bulk Device Merge 95
Performing a Bulk Device Unmerge 97
Device Relationships 100
What are Device Relationships? 101
Viewing the List of Device Relationships 101
Filtering the List of Device Relationships 104
Viewing a Relationship for a Single Device 105
The Device View Page 107
Event Correlation 108
Defining Device Relationships 108
Device Categories that Don't Support Parent-Child Devices 110
Events that May Not Be Displayed in the Events Page 111
Defining Event Correlation 111
Layer-2 Topology Collection 114
CDP Topology Collection 115
LLDP Topology Collection 116
Layer-3 Topology Collection 118
Managing a Single Device with the Device Administration Panel 120
What is the Device Administration Panel? 121
Actions Menu 124
Device Properties 127
Viewing Read-Only Information About the Device 128
Editing Device Settings 129
Identification 130
Monitoring & Management 130
Preferences 134
Adding an IP Address to a Device 135
Removing an IP Address from a Device 137
Managing Device IPs 138
Clearing the Device Cache 140
Aligning a Secondary Credential 142

Adding the Device to a Device Group 144
Creating a Ticket About the Device 146
Adding a Note to a Device 148
Aligning Custom Attributes with a Device 151
Creating a New Extended Custom Attribute 152
Deleting an Extended Custom Attribute from a Device 154
Associating a Product SKU with the Device 155
Merging Devices 156
Merging Individual Devices 157
Unmerging Individual Devices 159
Performing Administrative Tasks for One or More Devices 161
Shortcut Keys for Device Administration panel 162
Device Toolbox 164
What is the Device Toolbox? 164
Accessing the Device Toolbox page 164
Viewing the Session Logs 167
Managing Device Classes and Device Categories 169
Device Classes 170
Generic | SNMP 171
Non-SNMP 171
Component 171
Agent-Only Device Classes 171
Viewing the List of Device Classes 172
Filtering the List of Device Classes 174
Special Characters 175
Creating Device Classes 177
Creating a New Device Class of Type "SNMP-Enabled" 177
Editing an SNMP-Enabled Device Class 181
Creating a New Device Class for a Device with Device Class "Generic | SNMP" 181
Creating a New Device Class for Devices That Do Not Support SNMP 184
Applying the New Device Class 189
Maintaining the New Device Class During Auto-Discovery 190
Editing a Device Class That is Not SNMP-Enabled 190
Creating a Device Class of Type "Component" 191
Editing a Device Class of Type "Component" 193
Legacy Device Classes of Type "ICMP" 193
Managing Device Classes 194
Manually Changing the Device Class for a Device 194
Changing the Icon for a Device Class 196
Aligning One or More Device Classes with a Device Dashboard 196
Deleting One or More Device Classes 197
Device Categories 198
Viewing the List of Device Categories 198
"Pingable" Device Category 199
Creating a New Device Category 199
Editing a Device Category 201
Deleting a Device Category 201
Aligning One or More Device Categories with a Device Dashboard 202
Device Maintenance 203
What is Scheduled Maintenance? 204
What is User Maintenance? 205
The Maintenance Minimum Severity Setting 205

Enabling and Disabling User Maintenance for a Single Device 205
Enabling and Disabling User Maintenance for One or More Devices 208
Scheduling Maintenance for a Single Device 209
Viewing the Schedule Manager 209
Defining a Scheduled or Recurring Device Maintenance Window for a Single Device 210
Scheduling Maintenance for One or More Devices 213
Enabling or Disabling Scheduled Maintenance for One or More Devices 214
Deleting Scheduled Maintenance for One or More Devices 215
Managing Dynamic Applications 216
Viewing the List of Dynamic Applications 217
Searching and Filtering the List of Dynamic Applications 221
Special Characters 223
Viewing the Dynamic Applications Associated with a Device 226
Viewing the Status of a Dynamic Application 228
Found 229
Collect 229
How SL1 Manages Collect Status 230
Stopping Collection 230
Starting Collection 230
Collection Objects that are Excluded from Maintenance 231
Status of Objects for Deviation 231
Manually Associating a Dynamic Application with a Device 231
Editing the Credential Associated with a Dynamic Application 233
Performing Other Administrative Tasks for an Aligned Dynamic Application 234
Enabling or Disabling Objects 235
Restarting Automatic Maintenance of Collection Objects 235
Editing the Poll Frequency for a Dynamic Application on the Current Device 236
Stopping Data Collection for a Dynamic Application 236
Resetting Statistical Data for a Dynamic Application 237
Resetting Persistent Session Objects for a Dynamic Application 238
Testing Data Collection for a Dynamic Application 238
Removing Data Collected by a Dynamic Application 239
Bulk Un-Aligning Dynamic Applications 239
Setting Thresholds for Dynamic Applications 240
Dynamic Applications and Discovery 241
How Does SL1 Align Dynamic Applications During Discovery? 242
Queuing Discovery from the Dynamic Applications Manager Page 243
Device Thresholds and Data Retention 244
Global Settings for Thresholds 245
Device Thresholds 250
Bulk Management with Device Groups and Device Templates 260
What is a Device Group? 260
What is a Device Template? 262
Virtual Devices 265
What is a Virtual Device? 265
Defining a Virtual Device 266
Directing Data to a Virtual Device 267
Redirecting Log Data to a Virtual Device 268
Aligning a Dynamic Application with a Virtual Device 270
Customizing the User Interface for a Device 272
Custom Navigation 272
Editing a Custom Navigation tab 274

Vanishing & Purging Devices 277
Setting Vanish and Purge Thresholds 278
Viewing the List of Vanished Devices 279
Filtering the List of Devices 281
Using the Advanced Filters 282
Manually Purging Selected Devices 284
Setting One or More Devices to Never Purge 285
Device Dashboards 286
Viewing the List of Device Dashboards 287
Creating a Device Dashboard 288
Aligning Device Dashboards 289
Aligning a Device Dashboard with a Device 290
Aligning a Device Dashboard with a Device Class 291
Aligning a Device Dashboard with a Device Category 292
Aligning a Device Dashboard with a Dynamic Application 293
Editing a Device Dashboard 294
Deleting a Device Dashboard 294
Copying a Device Dashboard 295
Defining the Global Default for Device Dashboards 295
Unaligning a Device Dashboard 297
Moving Alignment for Device Dashboards 298
Using Custom Attributes 300
Custom Attributes 301
Viewing the List of Custom Attributes 301
Filtering the List of Custom Attributes 304
Viewing the List of Subscribers for a Custom Attribute 304
Creating Custom Attributes 306
Deleting One or More Custom Attributes 307
Custom Attributes in the ScienceLogic API 307
Using the ScienceLogic API to View, Create, and Edit Custom Attributes 308
Using a Dynamic Application to Create and/or Populate Custom Attributes 308
Using Custom Attributes to Define Device Groups 311
Viewing Custom Attributes in the Custom Table Widget 312

Chapter 1

Introduction

Overview

This manual describes how to discover and collect data from devices in SL1. It also describes how to configure and manage those devices in SL1 after they have been discovered.

> **NOTE:** For information about the data that SL1 collects from monitored devices, how to configure monitoring policies to collect that data, and how SL1 displays the data in the user interface, see the manual *Monitoring Device Infrastructure Health*.

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

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

This chapter includes the following topics:

What is a Device? 8
What is a Device Record? 8
What is a Device Class? 9
What is a Device Category? 9
How Does SL1 Manage Devices? 10
What is Discovery? 11
What is a Credential? 11
What is a Virtual Device? 12

What are Component Devices? *13*
What is a Dynamic Application? *13*
What is an SL1 Agent? *14*
What is Virtualization? *14*
What is an Asset Record? *14*

What is a Device?

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

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

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

What is a Device Record?

As part of monitoring your network, SL1 collects data using common networking protocols. Most collected data is associated with a device in SL1. A ***device record*** in SL1 can represent:

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

What is a Device Class?

In SL1, each device is associated with a device class. Typically, a ***device class*** maps to a make/model pair. When possible, SL1 automatically assigns each discovered device to a device class. Device classes determine:

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

SL1 includes already-defined device classes for the most popular hardware. The **Device Class Editor** page (System > Customize > Device Classes) allows advanced administrators to define new or legacy device classes in SL1 and to customize properties of existing device classes.

Most TCP/IP-compliant devices have an internally-defined class ID, called the System Object ID and abbreviated to SysObjectID. This SysObjectID is an SNMP OID defined by the manufacturer. Each manufacturer specifies a SysObjectID for each different hardware model. In SL1, each SNMP device class is associated with a SysObjectID. During initial discovery, SL1 searches each device for the SysObjectID and assigns each device to the appropriate device class.

SL1 also includes device classes for devices that do not support SNMP. These device classes are associated with values returned by nmap. SL1 runs nmap against each device during discovery.

What is a Device Category?

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

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

NOTE: "Reserved" device categories are those device categories required by SL1. These device categories cannot be edited or deleted. If a device category does not display the bomb icon ( ), the device category is a reserved device category and cannot be deleted.

How Does SL1 Manage Devices?

- Using discovery, SL1 automatically locates or *discovers* all hardware and hardware-components in your network. SL1 can also automatically discover most software applications running in your network.
- Using Dynamic Applications, SL1 can automatically discover component devices.
- During discovery, devices are categorized by device class and device category for quick identification. You can customize device classes and device categories and also define custom device classes and device categories.
- On the SL1 **Devices** and **Device Manager** pages, you can view details about each discovered device, including IP address and MAC address, operating system, hardware components (like CPU, RAM, swap, file systems), interfaces, open ports, and installed software.
- For each device, you can use the **Device Administration** panel or the **Device Investigator** page to define configuration and policies for the device.
- For each device, you can use the **Device Reports** panel or the **Device Investigator** page to view details about the device, including graphical reports.
- SL1 can monitor bandwidth usage for each discovered network interface. SL1 can generate reports and billing documents for each network interface.

NOTE: SL1 includes pre-defined events (sometimes called "alerts" in other applications). An ***event*** is a message that is triggered when a specified condition is met. Among other things, an event can signal that a server has gone down, that a device is exceeding CPU or disk-space thresholds, that communication with a device has failed, or simply display the status of a device or component. You can define and customize events to best fit your infrastructure. Events can be viewed through SL1, sent to users' email accounts, and sent to users' pagers or cell phones.

- You can define customized performance thresholds and hardware thresholds for a device. SL1 can generate events based on these thresholds.
- SL1 monitors availability and latency for each device. You can define availability and latency thresholds. SL1 also generates graphical reports on each device's availability and latency.
- SL1 monitors open ports. Based on user-defined policies, SL1 can generate an event when a new port is opened on any device in the network.
- SL1 can monitor port-availability for each port in the network.
- SL1 can discover and monitor the hardware components of each device.
- SL1 can discover and monitor the software running on each device.
- SL1 can monitor system processes and Windows services running on a device. Based on user-defined policies, SL1 can generate an event when a process or service is running or when a process or service is not running and should be.
- You can use ***device groups*** and ***device templates*** to automate the configuration and policies for multiple devices.

- You can create a virtual device to store data that you want to manage with SL1 but that cannot be associated with a traditional device or that you do not want associated with a traditional device.
- You can monitor ***ESX servers*** and ***VMware "guest" devices*** as you would monitor any other hardware-based device.
- You can create parent and child relationships between devices. These relationships allow you to use a single solution to resolve problems for the related devices.
- You can create ***asset records*** for one, multiple, or all devices in the network. SL1 automatically populates as many fields as possible, using information retrieved during discovery.
- SL1 includes an exhaustive list of real-time, dynamic, graphical reports to display trends and status for individual devices, groups of devices, or the entire network. These reports can be saved in multiple formats and can be printed.

What is Discovery?

Discovery is the tool that automatically finds all the hardware-based devices, hardware components, and software applications in your network. You must provide the discovery tool with a range or list of IP addresses and/or a list of fully-qualified domain names (hostnames), and the discovery tool determines if a device, hardware component, or software application exists at each IP address. For each device, hardware component, or software application the discovery tool "discovers", the discovery tool can collect a list of open ports, DNS information, SSL certificates, list of network interfaces, device classes to align with the device, topology information, and basic SNMP information about the device.

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

For more information about discovery, see the ***Discovery & Credentials*** manual.

What is a Credential?

Credentials are access profiles (usually username, password, and any additional information required for access) that allow SL1 to retrieve information from devices and from software applications on devices.

- Discovery uses SNMP credentials to retrieve SNMP information during initial discovery and nightly auto-discovery. If SL1 can connect to a device with an SNMP credential, SL1 deems that device "manageable" in SL1.
- Dynamic Applications use credentials to retrieve SNMP information, database information, SOAP information, XML information, XSLT information, and WMI information.
- Proxied Web Services use SOAP/XML Host credentials to pass authentication information to external web services.

- SL1 includes a type of credential called "Basic/Snippet" that is not bound to a specific authentication protocol. You can use this type of credential for Dynamic Applications of type "WMI", of type "snippet", and when defining system backups. "Basic/Snippet" credentials can also be used for monitoring Windows devices using PowerShell.
- SL1 includes a type of credential that allows SL1 to communicate with an LDAP or Active Directory system. For details on integrating SL1 with LDAP or Active Directory, see the manual ***Using Active Directory and LDAP***.
- SL1 includes a type of credential that allows Dynamic Applications of type "Snippet" to use SSH to communicate with a remote device. To use these Dynamic Applications, you must define an SSH credential.
- SL1 includes a type of credential that allows Dynamic Applications to retrieve data from Windows devices. If you align a Dynamic Application for PowerShell with a PowerShell credential, SL1 assumes that you want to use its built-in agentless transport to communicate with Windows devices.

If necessary, a single device can use multiple credentials. If more than one agent or application is running on the device, each agent or application can be associated with its own credential. During discovery, SL1 will use the appropriate credential for each agent.

For example, suppose you want SL1 to discover a device that supports SNMP v2. To retrieve SNMP data from that device, SL1 must use a valid SNMP v2 read-only community string. So we would first go to the device and define the SNMP read-only community string. Then we would return to SL1 and create a credential in the SL1 system, using that community string. This new credential would allow discovery to retrieve SNMP data from the device.

Now suppose this same device also includes a MySQL database. Suppose you want SL1 to use a Dynamic Application to monitor that database. To retrieve data from the database, SL1 must use a valid username and password for that database. So we would first go to the device that hosts the MySQL database and create a database username and database password for SL1 to use. Then we would return to SL1 and create a credential in the SL1 system. The credential would include the database username and database password for the MySQL database. This credential would allow the Dynamic Application to retrieve data about the MySQL database.

For more information about credentials, see the ***Discovery & Credentials*** manual.

What is a Virtual Device?

A ***virtual device*** is a container for collected data. A virtual device can be used when you want to:

- Monitor a device or application that doesn't support TCP/IP, SNMP, or both. The device's data can be pushed to SL1 via another method (for example, email) and stored in a virtual device.
- Monitor multiple SNMP agents on a single device. In such a case, one of the SNMP agents (for example, a hardware agent) can be associated with the device and another SNMP agent (for example, an agent that monitors a software application) can be associated with a virtual device.
- Isolate and monitor specific parameters separately from their originating device. For example, you might want to monitor a database and keep its data separate from the hardware data you are collecting from the host device.

For more information about virtual devices, see the *Virtual Devices* section.

What are Component Devices?

SL1 uses Dynamic Applications to retrieve data from a management device and discover each entity managed by that management device. SL1 then uses that retrieved data to create a device for each managed entity. In some cases, the managed entities are nested.

- In SL1 a managed entity is called a ***component device***. A component device is an entity that runs under the control of a physical management device.
- In SL1, the ***root device*** is the physical device that manages one or more component devices.
- In SL1, a ***parent device*** is a device that has associated entities modeled as component devices. A parent device can be either a root device or another component device.

For example, in a Cisco UCS system, SL1 might discover a physical server that hosts the UCS manager. SL1 might discover a chassis as a component device. The chassis is a child device to the physical server; the physical server is the root device. SL1 might also discover a blade as a component device that is part of the chassis. The blade is a child device to the chassis. The chassis is the parent device.

The **Device Components** page (Devices > Device Components) displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices.

What is a Dynamic Application?

Dynamic Applications are the customizable policies that tell SL1 what data to collect from devices and applications. For example, suppose you want to monitor a MySQL database running on a device in your network. Suppose you want to know how many insert operations are performed on the MySQL database. You can create or edit a Dynamic Application that monitors inserts. Every five minutes (for example), SL1 could check the number of insert operations performed on the MySQL database. SL1 can use the retrieved data to trigger events and/or to create performance reports.

SL1 includes Dynamic Applications for the most common hardware and software. You can customize these default Dynamic Applications to suit your environment. You can also create custom Dynamic Applications.

Dynamic Applications in SL1 support a variety of protocols to ensure that SL1 can always communicate with the devices and applications in your network and retrieve information from them. Dynamic Applications can use the following protocols to communicate with devices:

- SNMP
- SQL
- XML
- SOAP
- XSLT (uses SOAP and XSLT to convert XML data to a new format)
- WMI (Windows Management Instrumentation), including WMI and WBEM

- Windows PowerShell
- Custom Python applications (called "snippets") for proprietary or more complex data retrieval

What is an SL1 Agent?

An ***SL1 agent*** is a program that runs on a device or element monitored by SL1. An agent collects data from the device, interface, or other element and pushes that data back to SL1. You can install and use multiple agents, as needed.

Because an agent is always running on a device, an agent can collect more granular data than can be collected by polling the device periodically. You can monitor devices using agents or by SL1 polling the device, or you can use both methods.

For more information about monitoring devices with the agent, see the ***Monitoring with the SL1 Agent*** manual.

What is Virtualization?

Virtualization is when multiple virtual machines run on a single hardware platform. Each virtual machine is a software-based implementation of a computer that executes programs like a hardware-based computer. A virtual machine provides a platform on which you can run an operating system and software applications. For example, a single server could contain a virtual machine running Windows and Windows applications, another VM running Linux and Linux applications, another VM running BSD and BSD applications, and another running Macintosh OS and Macintosh applications.

A hypervisor is the software that allows one or more virtual machines to run on a single hardware platform. The hypervisor software allows the virtual machines to share the RAM, CPU, and disk space on the hardware platform.

Each virtual machine can run its own operating system. A virtual machine can provide an alternate instruction set from the hardware-based computer.

Virtual machines are frequently used to:

- Run multiple operating systems on a single computer.
- Consolidate hardware servers and run multiple server applications on a single server.
- Provide multiple, isolated development environments.

What is an Asset Record?

An ***asset record*** is a collection of relevant information about an asset. In SL1, asset records are usually created for hardware devices.

In SL1, asset records can contain information about:

- The name, make, and model of a device.

- The serial number of a device.
- Function and status of the device.
- Networking information, like host ID, IP address, and DNS server for the device.
- Hardware information like amount of memory, CPU, and BIOS or EPROM version.
- Physical location of the device.
- Vendor information for the device, including PO or check number, warranty policy, and service policy.
- Description of the network interface.
- Description of each hardware component (if applicable).
- Description of installed software (if applicable).

SL1 will populate as many fields as possible automatically, using data retrieved during discovery and collections. You can enter values in all the fields or in only those fields that are required for your business processes.

You can specify which asset fields will be populated from data retrieved during discovery and collections and which fields will be populated manually. To specify this behavior, go to the **Asset Automation** page (System > Settings > Assets).

Chapter 2

Using the Devices Page

Overview

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

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

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

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

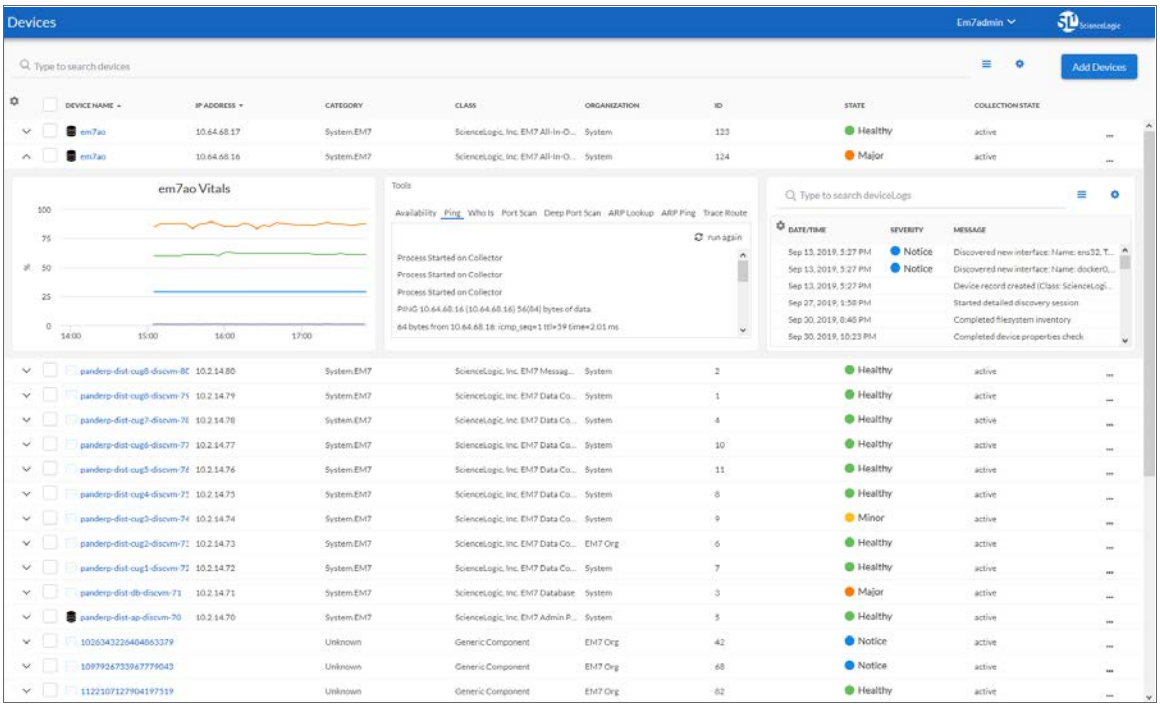
This chapter includes the following topics:

Viewing Devices 17
Adding Devices with Discovery 18
Using the Device Investigator 33
Overview of the Device Investigator Tabs 42
Working with Device Classes 63
Working with Device Categories 64
Assigning Icons to Devices, Device Classes, and Device Categories 67

Viewing Devices

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

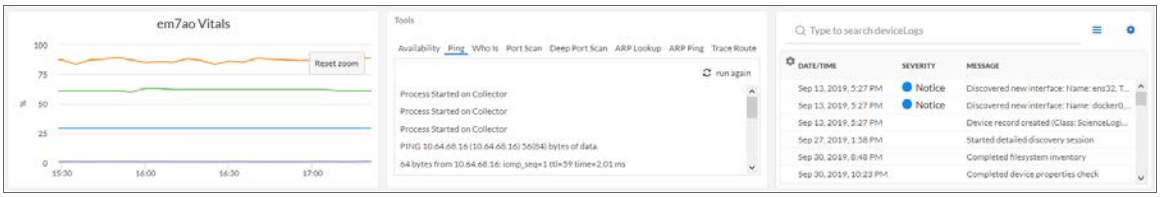
To navigate to the **Devices** page, click the Devices icon ( ):



TIP: To view the number of available devices, scroll down to the end of the list of devices and click the first checkbox next to the ***Select Columns*** icon ( ). The number of devices displays at the bottom of the screen. Click the first checkbox again to deselect all the devices, or click **Deselect All**.

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** graphs, the **Tools** pane, and the **Logs** pane. The **Vitals**graph displays data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. The **Tools** pane provides access to a set of network diagnostic tools. The **Logs** pane displays a list of events associated with that device.

You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.

> **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.

Aligning a Device with a Different Organization

To align a device with a different organization:

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

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

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

Adding Devices with Discovery

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

What is Discovery?

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

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

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

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

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

What are Credentials?

Credentials are access profiles (usually username, password, and any additional information required for access) that allow SL1 to retrieve information from devices and from software applications on devices.

- Discovery uses SNMP credentials to retrieve SNMP information during initial discovery and nightly auto-discovery. If SL1 can connect to a device with an SNMP credential, SL1 deems that device "manageable" in SL1.
- Dynamic Applications use credentials to retrieve SNMP information, database information, SOAP information, XML information, XSLT information, and WMI information.
- Proxied Web Services use SOAP/XML Host credentials to pass authentication information to external web services.
- SL1 includes a type of credential called "Basic/Snippet" that is not bound to a specific authentication protocol. You can use this type of credential for Dynamic Applications of type "WMI", of type "snippet", and when defining system backups. "Basic/Snippet" credentials can also be used for monitoring Windows devices using PowerShell.
- SL1 includes a type of credential that allows SL1 to communicate with an LDAP or Active Directory system. For details on integrating SL1 with LDAP or Active Directory, see the manual ***Using Active Directory and LDAP***.
- SL1 includes a type of credential that allows Dynamic Applications of type "Snippet" to use SSH to communicate with a remote device. To use these Dynamic Applications, you must define an SSH credential.
- SL1 includes a type of credential that allows Dynamic Applications to retrieve data from Windows devices. If you align a Dynamic Application for PowerShell with a PowerShell credential, SL1 assumes that you want to use its built-in agentless transport to communicate with Windows devices.

- If necessary, a single device can use multiple credentials. If more than one agent or application is running on the device, each agent or application can be associated with its own credential. During discovery, SL1 will use the appropriate credential for each agent.

Prerequisites for Discovering Devices on the Devices Page

To discover all of the devices on your network:

1. Make a note of the range of IP addresses used on your network. If your device does not have an IP address, make a note of the name of the root device. If you need help, ask your network administrator.
2. An Organization must exist in SL1 for the new devices. If you need to create an Organization go to the **Organizations** page (Registry > Accounts > Organizations).
3. A Collector Group must exist in SL1 that can reach the target device using a valid network path for the needed protocol. For example, UDP 161 for SNMP and general ICMP traffic for Ping. If you don't know what Collector Group to use, consult an SL1 Architecture diagram or ask your SL1 System Administrator. You can access collector information on the **Collector Group Management** page (System > Settings > Collector Groups).
4. You must create or use an existing credential in the classic user interface. You can access credential information on the **Credential Management** page (System > Manage > Credentials). Because credential problems are the most common cause for discovery failure, you can test any credential that you create on the **Credential Tests** page (System > Customize > Credential Tests).
5. Similarly, if you want to use a device template with a discovery session, you must use an existing template in SL1. You can access device templates on the **Configuration Templates** page (Devices > Templates).
6. The Grant All user needs to be used to access new discovery workflow, as the SYS_SETTINGS_LICENSES_PAGE and SYS_SETTINGS_CUGS_PAGE access keys are needed to get collector or collector group information. For more information, see the **Access Keys** page (System > Manage > Access Keys).

Adding Devices Using Universal or Guided Discovery

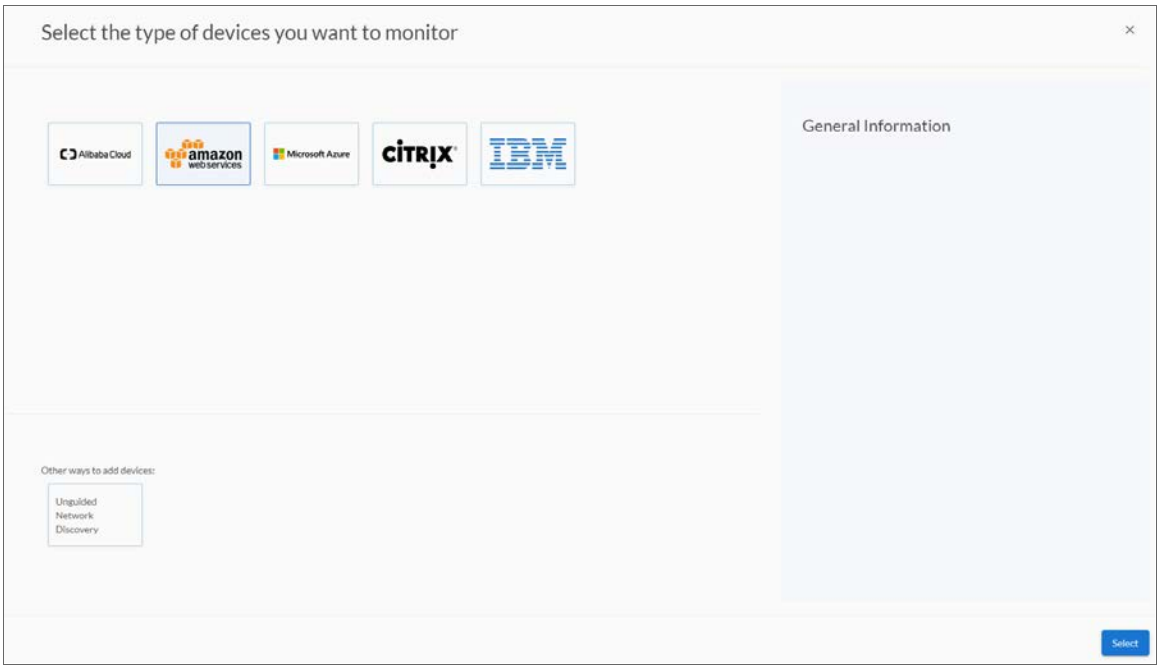
On the **Devices** page, you can add or "discover" new devices for monitoring in SL1. You add devices by creating a ***discovery session***, which searches for devices on the network you specify.

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

NOTE: The following procedure uses Amazon Web Services as an example of the discovery type. Some steps and fields will vary depending on the discovery type.

To run a guided or Universal Discovery:

1. On the **Devices** page, click the **[Add Devices]** button. The **Select** page appears:



2. Select a discovery type for the devices you want to discover, such as **Amazon Web Services**. Additional information about the requirements for device discovery appears in the **General Information** pane to the right.

> **NOTE:** If you want to do a more general discovery, you can select one of the options in the **Other ways to add devices** pane, such as **Unguided Network Discovery**. For more information, see *Adding Devices Using Unguided Discovery*.

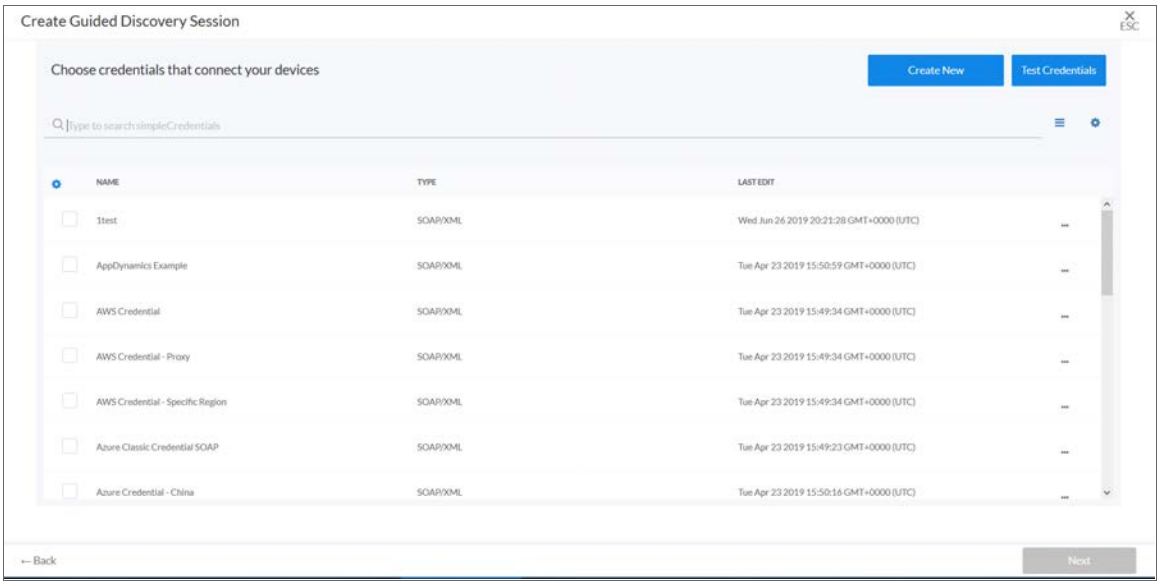
3. Click **[Select]**. The first **Create Guided Discovery Session** page displays the following list of requirements for Discovery (in this example, the requirements are for Amazon Web Services):

   - The name of the root device
   - The credentials you need to access the API

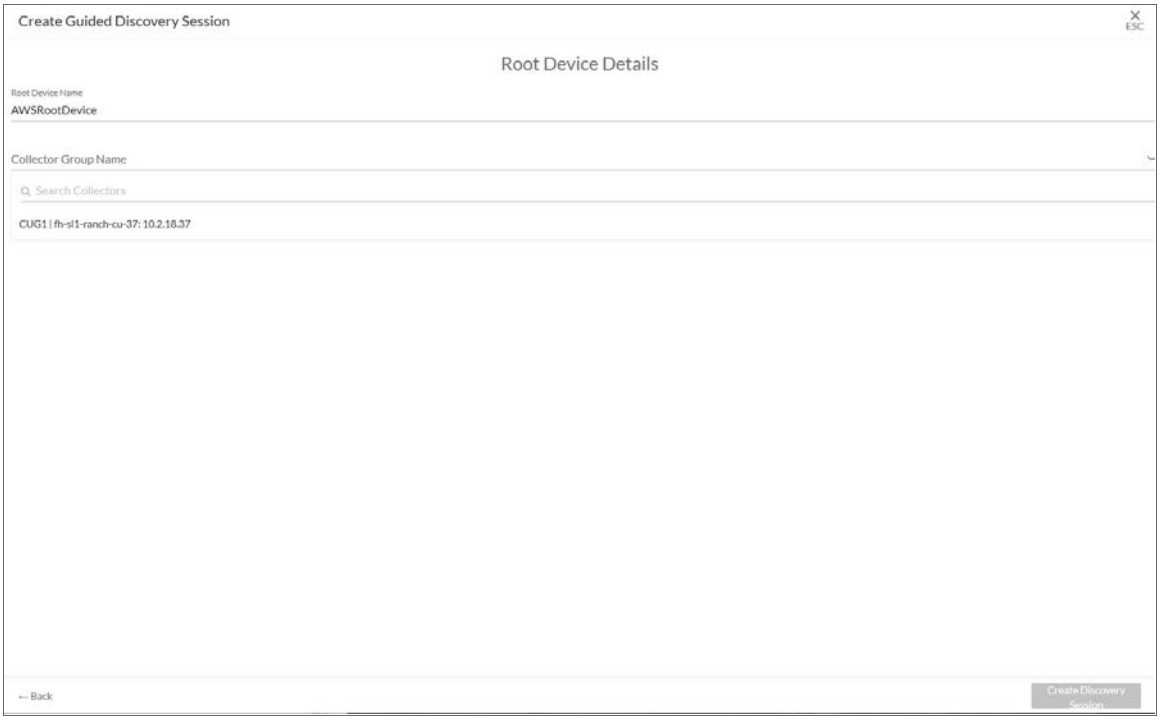
4. Click **[Next]**. The second **Create Guided Discovery Session** page appears.
5. Complete the following fields:

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

6. Click **[Next]**. The **Credentials** page of the Create Guided Discovery Session process appears:



7. If the credential you need is not in the list, click the **[Create New]** button to open the **Create Credential** window, where you can specify the name and organization for the credential, the third-party username and password, and other data such as Cloud Type and Proxy information. Click **[Save]** to save the credential and return to the **Credentials** page of the **Create Guided Discovery Session** page.
8. To edit a credential on the **Credentials** page, click the **[Actions]** button (⋯) for the credential, select *Edit*, and edit that credential as needed. Click the **[Save]** button on the Edit Credential window to save your updates.
9. To test a credential on the **Credentials** page, click the **[Test Credentials]** button. On the **Credential Test Form** window, specify the test type, credential, hostname or IP, and collector, and then click the **[Run Test]** button.
10. On the **Credentials** page of the Create Guided Discovery Session process, select a credential to allow SL1 to access a device and click **[Next]**. The **Root Device Details** page appears:



11. Complete the following fields:

    - ***Root Device Name***. Type the name of the root device for the application you want to monitor (in this case, an Amazon Web Services root device).
    - ***Collector Group Name***. Select an existing collector group to communicate with the discovered devices. Required.

NOTE: The contents of this page might vary depending on the discovery type you selected at the start of the Guided Discovery.

12. Click the **[Create Discovery Session]** button. A summary of the new discovery session appears on this page.
13. Click **[Close]**.

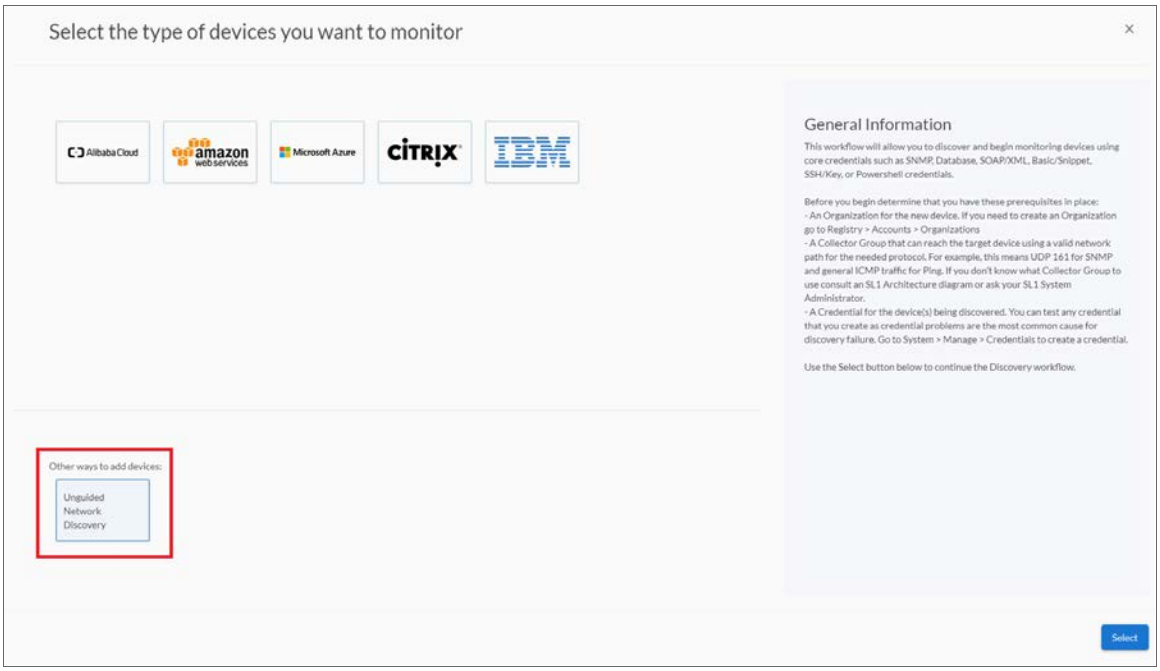
> **NOTE:** The results of a guided discovery do not display on the **Discovery Sessions** page (Devices > Discovery Sessions).

Adding Devices Using Unguided Discovery

Instead of running a Universal Discovery for a specific discovery type, you can run an "unguided" discovery to find a range of devices using core credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or PowerShell credentials.

To run an unguided discovery:

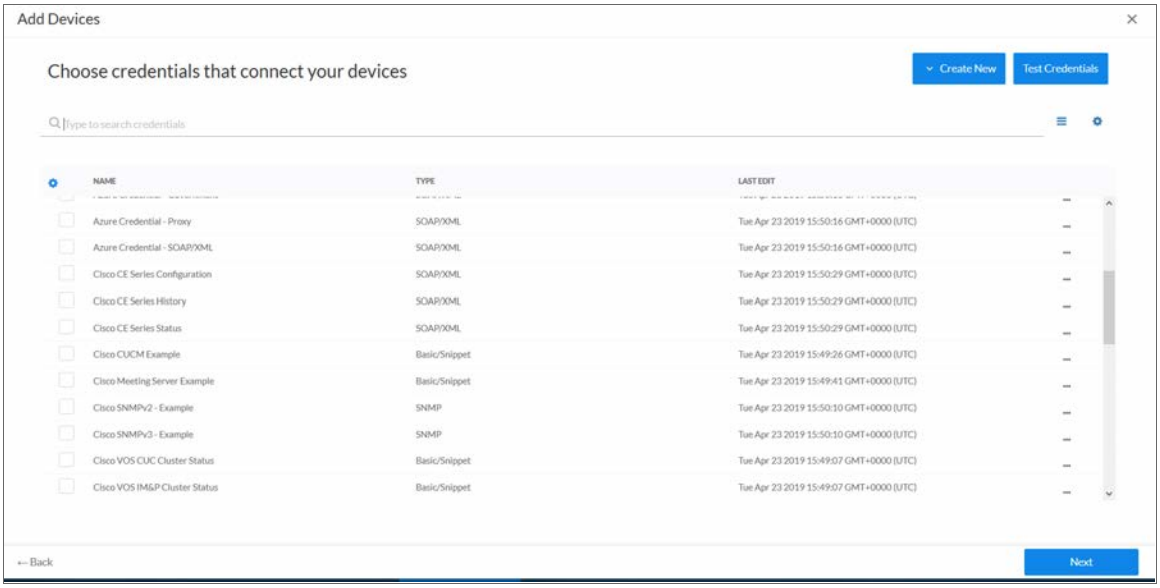
1. On the **Devices** page, click the **[Add Devices]** button. The **Select** page appears:



2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:

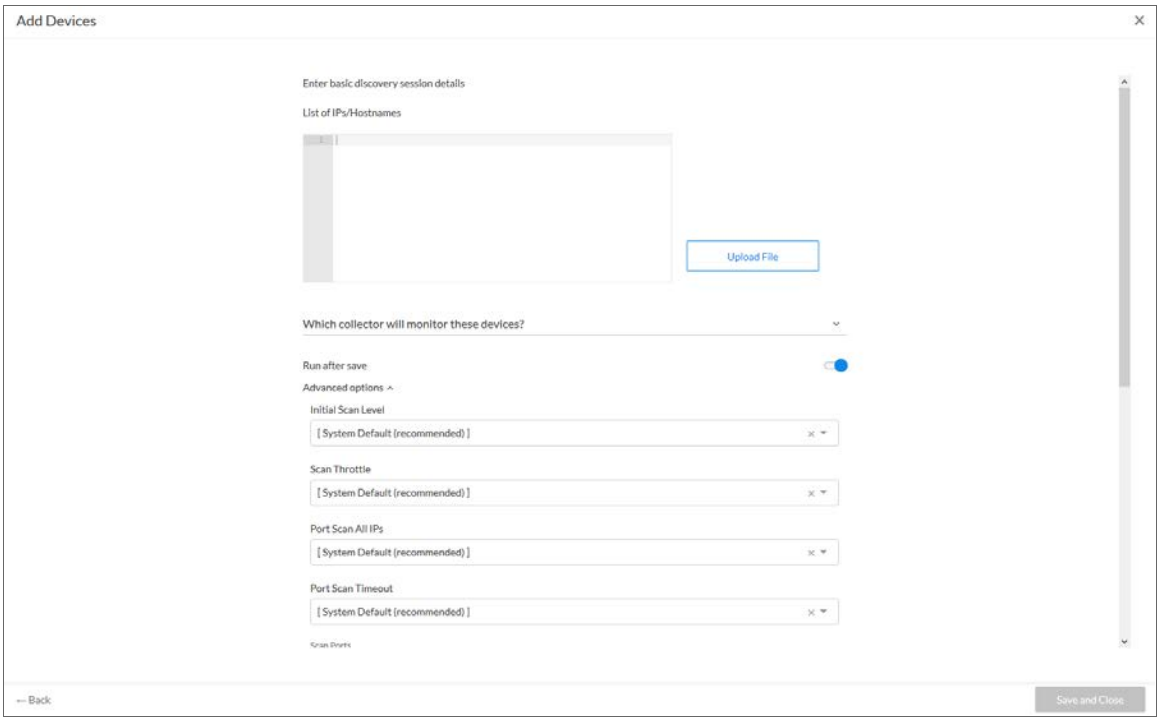
    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. Type a short description of the discovery session. You can use the text in this description to search for the discovery session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

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



6. If the credential you need is not in the list, click the **[Create New]** button to open the **Create Credential** window, where you can specify the name and organization for the credential, the third-party username and password, and other data such as Cloud Type and Proxy information. Click **[Save]** to save the credential and return to the **Credentials** page of the **Add Devices** wizard.
7. To edit a credential on the **Credentials** page, click the **[Actions]** button (⋯) for the credential, select *Edit*, and edit that credential as needed. Click the **[Save]** button on the Edit Credential window to save your updates.
8. To test a credential on the **Credentials** page, click the **[Test Credentials]** button. On the **Credential Test Form** window, specify the test type, credential, hostname or IP, and collector, and then click the **[Run Test]** button.

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



10. Complete the following fields:

    - ***List of IPs/Hostnames***. Provide a list of IP addresses, hostnames, or fully-qualified domain names for SL1 to scan during discovery. This field is required. In this field, you can enter a combination of one or more of the following:

        - One or more *single IPv4 addresses* separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
        - One or more *ranges of IPv4 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 – 10.20.30.254".
        - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
        - One or more *ranges of IPv6 addresses* with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0-2001:DB8:0:0:0:0:0:0003".
        - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
        - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

TIP: You can also click the **[Upload File]** button to upload a comma-separated list of IPs.

- ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
- ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.
- ***Advanced options***. Click the down arrow icon ( ) to access additional discovery options.

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

  - ***Initial Scan Level***. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:

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

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

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

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

    - *6. Deep Discovery*. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a

faster TCP/IP connection method. Discovery will also perform *3. Discover SSL Certificates, 2. Initial Population of Apps*, and *1. Model Device Only*.

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

- ***Scan Throttle***. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the ***IP Address/Hostname Discovery List*** field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- ***Port Scan All IPs***. For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior) in the classic user interface for SL1.
  - *Enabled*. SL1 will scan all discovered IP addresses for open ports.
  - *Disabled*. SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
- ***Port Scan Timeout***. For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
  - *System Default (recommended)*. Use the value defined in the **Behavior Settings** page (System > Settings > Behavior).
  - Choices between 60 to 1,800 seconds.
- ***Scan Ports***. Specify a list of ports to scan, separated by colons (:). The default is *21:22:25:80:136*.
- ***Interface Inventory Timeout (ms)***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

- If you specify a value in this field and do not apply a device template to this discovery session, the ***Interface Inventory Timeout*** setting in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page (System > Settings > Thresholds).

- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.

  - During the execution of this discovery session, SL1 uses the value in this field first. If you delete the default values and do not specify another value in this field, SL1 uses the value in the **Global Threshold Settings** page.

  - If you specify a value in this field and do not apply a device template to this discovery session, the ***Maximum Allowed Interfaces*** setting in the **Device Thresholds** page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the **Global Threshold Settings** page.

- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces.

  - *Selected*. SL1 will not attempt to discover interfaces for each device in the discovery session. For each discovered device, the ***Bypass Interface Inventory*** checkbox on the **Device Investigator [Settings]** tab will be selected.

  - *Not Selected*. SL1 will attempt to discover network interfaces, using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value.

- ***Discover Non-SNMP***. Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.

  - *Selected*. SL1 will discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** field. These devices will be discovered as "pingable" devices.
  - *Not Selected*. SL1 will not discover devices that don't respond to the SNMP credentials selected in the ***SNMP Credentials*** fields.

- ***Model Devices***. Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:

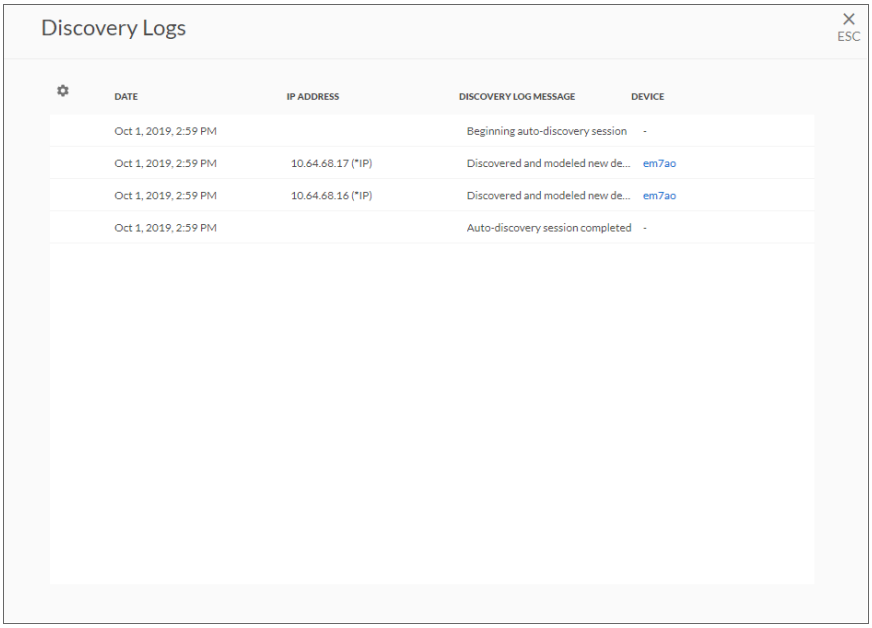
  - *Enabled*. When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.

  - *Disabled*. If a device is not modeled, you cannot access the device through the **Device Manager** page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor

and manage with SL1. For the amount of time specified in the ***Device Model Cache TTL (h)*** field, a user can manually model the device from the **Discovery Session** window.

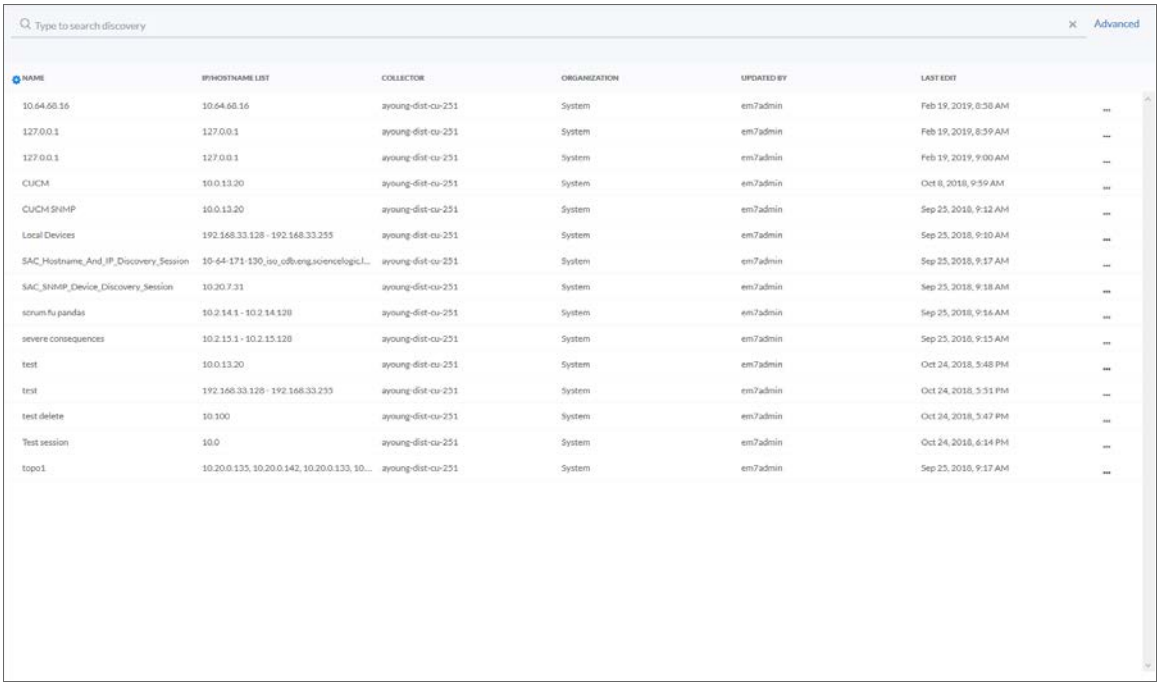
- ***Enable DHCP***. Specifies whether or not the specified range of IPs and hostnames use DHCP.
  - *Selected*. SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
  - *Not Selected*. SL1 will perform normal discovery.
- ***Device Model Cache TTL (h)***. Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the ***Model Devices*** option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the **Discovery Session** window.
- ***Log All***. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the ***IP Address/Hostname Discovery List*** field, even if the results are "No device found at this address."
  - *Selected*. This discovery session will use verbose logging.
  - *Not Selected*. This discovery session will not use verbose logging.
- ***Apply Device Template***. As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on ***Device Groups and Device Templates***.

11. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
12. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device:



Working with Discovery Sessions

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

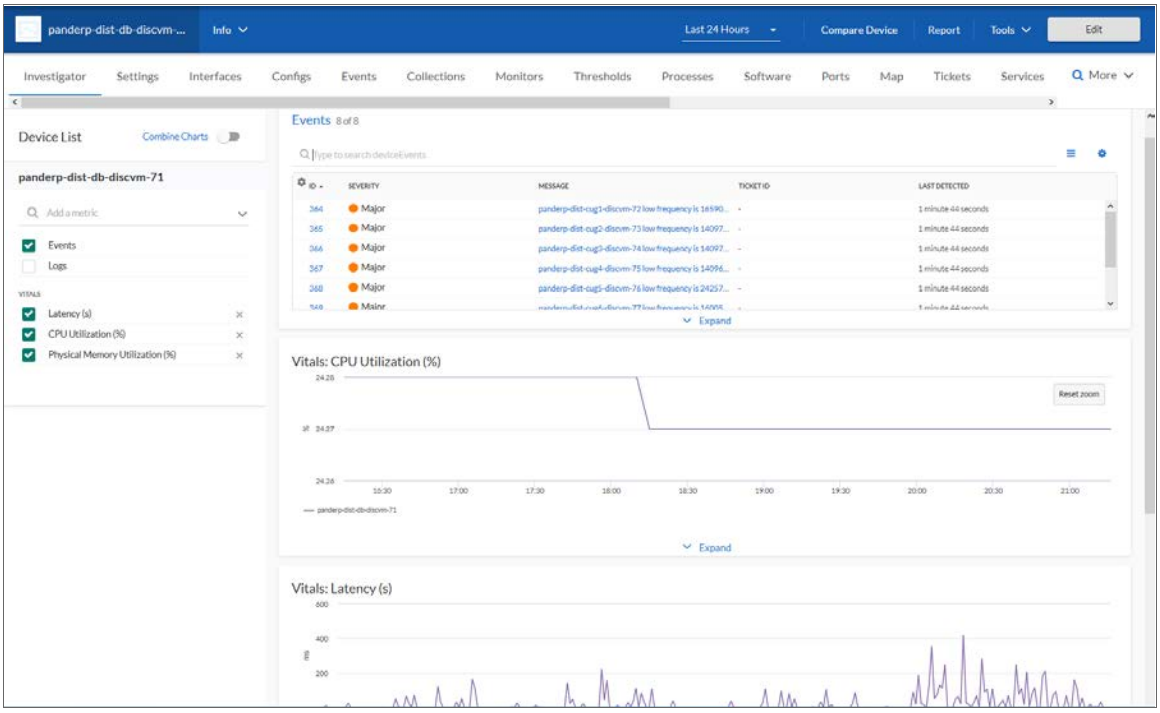


On this page you can click the **[Actions]** button (⋯) for a session and select one of the following actions:

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

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 all the data associated with a device. The tabs are similar to the tabs on the **Device Administration** and **Device Properties** panels in the classic user interface.

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

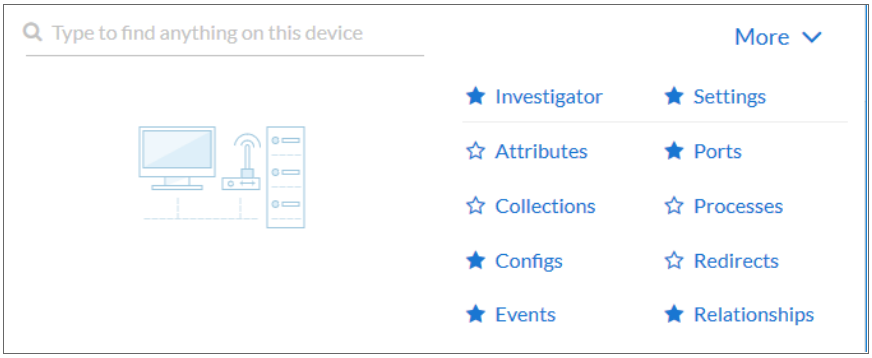
The **Device Investigator** page can include the following menus and buttons:

- *Info*. This drop-down list on the **[Investigator]** tab displays additional information about the device, along with the most recently updated values for uptime and collection time.
- ***Time span filter***. This drop-down list on the **[Investigator]** tab allows you to adjust the time span that appears in all the metrics on the **[Investigator]** tab. The default filter is *Last 24 Hours*, but you can select a time span of Last Hour, Last 3 Hours, Last 6 Hours, Last 12 Hours, Last 24 Hours, Last 3 Days, Last 5 Days, Last 7 Days, Last 30 Days, Last 60 Days, Last 90 Days, Last Year, or Last 2 Years.
- *Compare Devices*. This button on the **[Investigator]** tab lets you select one or more devices to compare with the device you have currently selected.
- *Report*. This button lets you generate a detailed report on the device.
- *Tools*. This button opens the **Tools** pane, which provides access to a set of network tools for the device.
- *Combine Charts*. This option on the **[Investigator]** tab lets you create a new widget that displays data from all of the other widgets on this page.

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*. Lets you manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more. You can also set user maintenance preferences and disable or enable collection on that device.
- *Attributes*. Lists the custom descriptive fields that are currently aligned with this device. On this tab, you can add and remove extended custom attributes to this device.
- *Collections*. Lets you align or unalign Dynamic Applications with this device, enable or disable collection for the Dynamic Applications, and run a Dynamic Application. You can also change credentials and update the poll frequency for a Dynamic Application.
- *Configs*. Displays configuration information collected from the device by Dynamic Applications. If this device does not have any configuration data, this tab does not appear.
- *Events*. Displays a list of active and cleared events for the device. You can acknowledge events from this tab and add event notes.
- *Interfaces*. Displays information about the interfaces used by the device. If this device does not use interfaces, this tab does not appear.
- *Journals*. Displays journal entry information collected from the device by Dynamic Applications.
- *Map*. Opens a map of that device and the devices it is related to (for systems that have the **Maps** page enabled).
- *Monitors*. This tab lets you define monitoring policies for the device.
- *Notes*. Displays notes and attachments associated with the device. You can also edit and create notes.
- *Ports*. Displays a list of all open ports on the device.
- *Processes*. Displays a list of system processes running on the device.

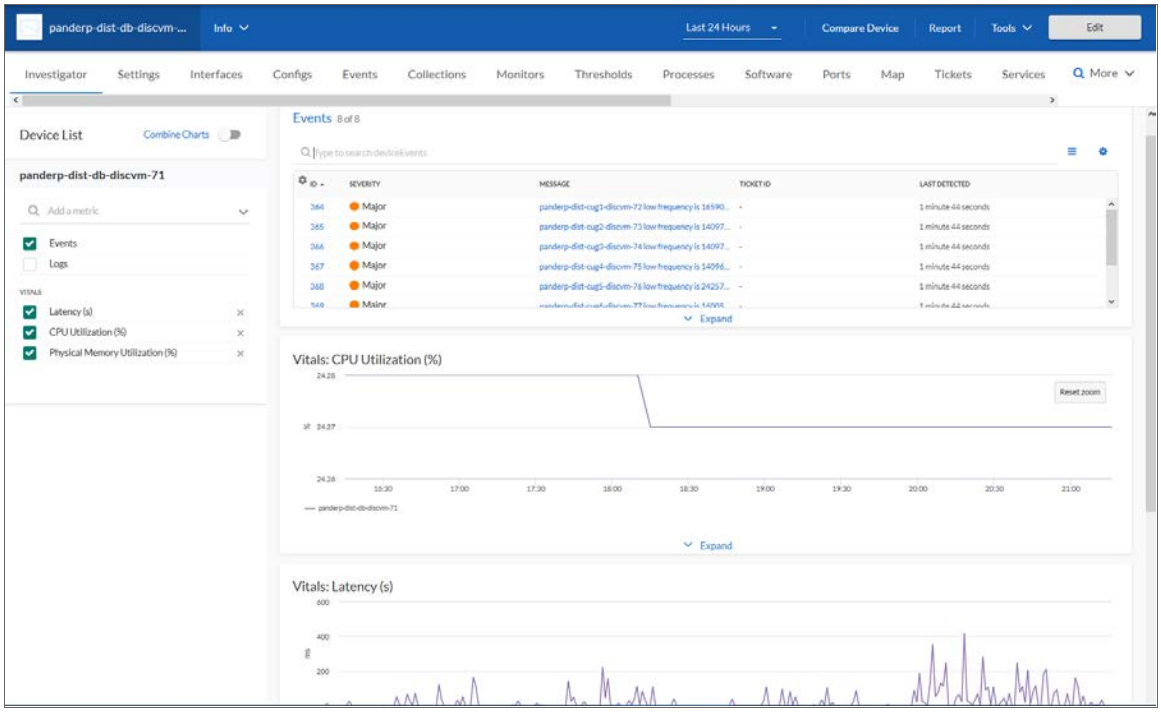
- *Redirects*. Allows you to redirect logs entries from an IP-based device to the current device. This is most useful when the current device is a virtual device.
- *Relationships*. Displays information about parent-child relationships between devices.
- *Schedules*. Allows you to view and manage all the scheduled processes you have defined in your system.
- *Services*. Displays a list of all Windows services enabled on the device.
- *Software*. Displays a list of all the software installed on the device.
- *Thresholds*. Lets you define space and performance thresholds for a device.
- *Tickets*. Displays all open, pending, or working tickets associated with the device.
- **More**. This drop-down lets you select additional tabs to display on the **Device Investigator** page by clicking the star icon next to the tab name. You can search for specific items on a tab, such as Device Class, Uptime, or Category, and the relevant tab will appear in the search results. You can also remove a tab by clicking the star icon again, turning it from blue to white. Your tab selections are saved and remain in place even after you log out:



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

Adding Metrics to the Investigator Tab

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

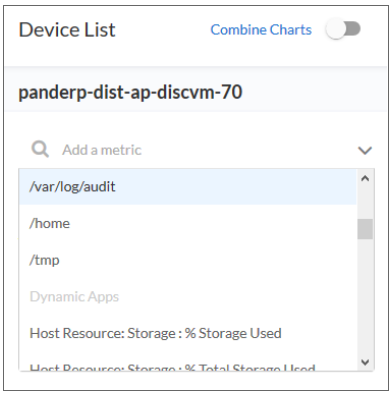


The list of metrics that appears in the **Device List** pane depends on the type of device. For most devices, the following metrics appear by default:

- ***Events***. Displays a 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 **Events** to go to the **[Events]** tab for that device.
- ***Logs***. Displays a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting. You can also click on the column headers for ***Date/Time***, ***Source***, ***Event ID***, ***Severity***, and ***Message*** to sort by that column.
- ***Latency***. Displays a widget for latency for the device over time, in milliseconds. Latency means the amount of time it takes SL1 to communicate with the device.
- ***CPU Utilization***. Displays a widget for the total amount of CPU used over time, as a percentage of all available CPU.
- ***Physical Memory Utilization***. Displays a widget for the physical memory usage over time, in percent.

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

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



2. Select a metric from the list, or type the name of a metric and select it from the list. The metric is added to the **Device List** pane, and a corresponding widget appears in the right-hand pane.
3. Some metrics might require you to make additional selections, such as the network interfaces associated with a device. Click the field and add one or more additional metrics, as needed.

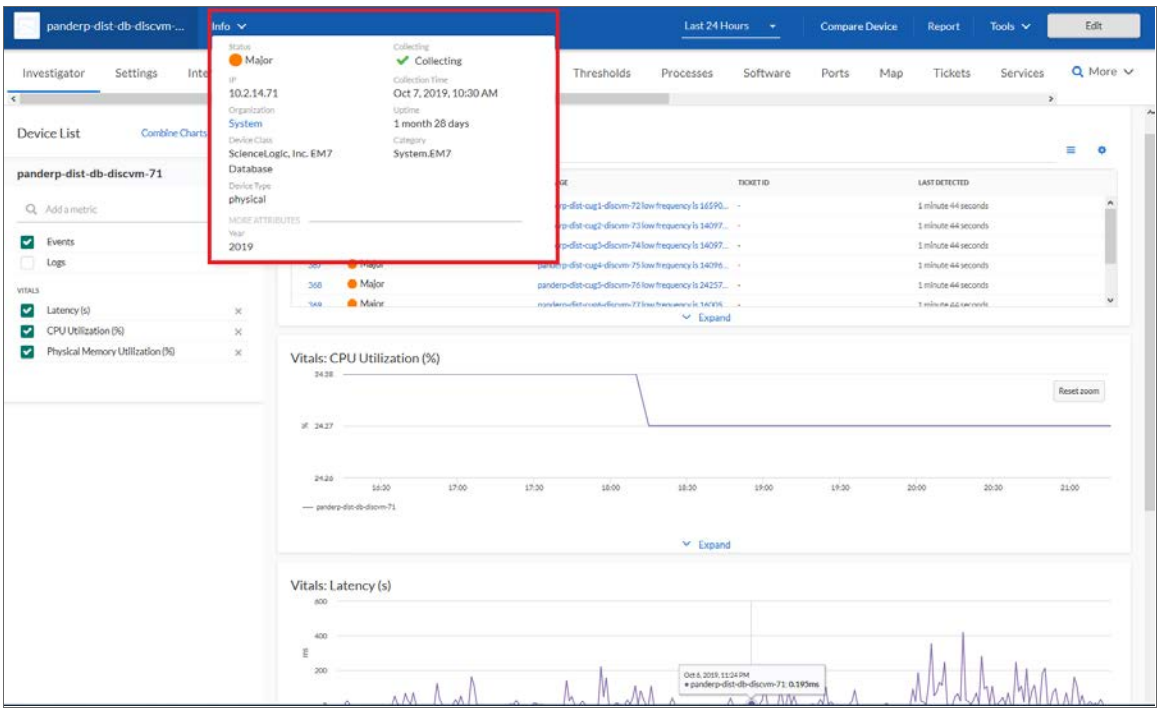
> **NOTE:** You can select up to eight additional metrics per widget.

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

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

Using the Info Drop-Down on the Device Investigator Page

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



The ***Info*** drop-down displays the following information for the device:

- ***Status***. The status of the device.
- ***Collecting***. Indicates that the device collection is "Collecting" with a green check mark icon ( ), meaning SL1 is periodically collecting data from the device, or "Not Collecting" with a prohibition icon ( ), meaning the SL1 is not currently collecting data from the device.
- ***IP***. IP address of the device.
- ***Collection Time***. Date and time of the most recent collection.
- ***Organization***. The organization to which this device belongs. Click the organization name to view a detail page for the organization.
- ***Uptime***. The number of days and hours that the device has been continuously up and communicating with SL1.
- ***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".

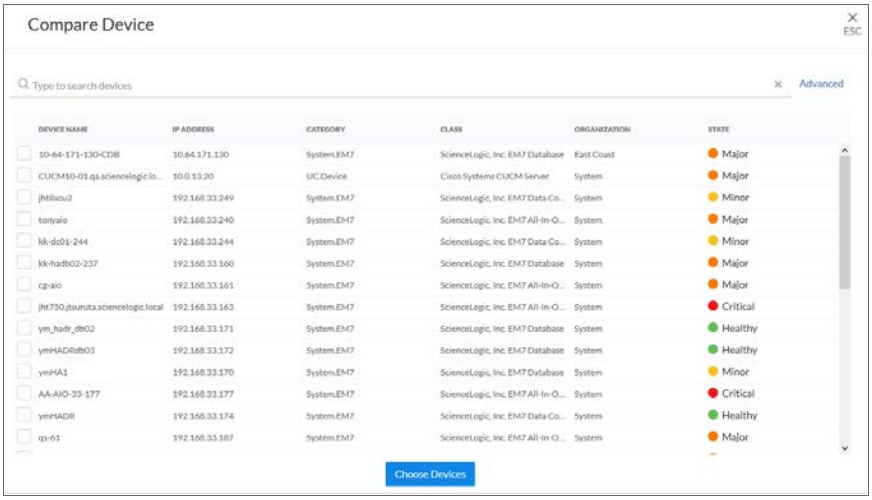
- ***Device Type***. Specifies whether the device is a physical device or a virtual device.
- **More Attributes**. This lower section lists any custom attributes that might be aligned with this device.

Comparing Devices on the Investigator Tab

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

To compare devices:

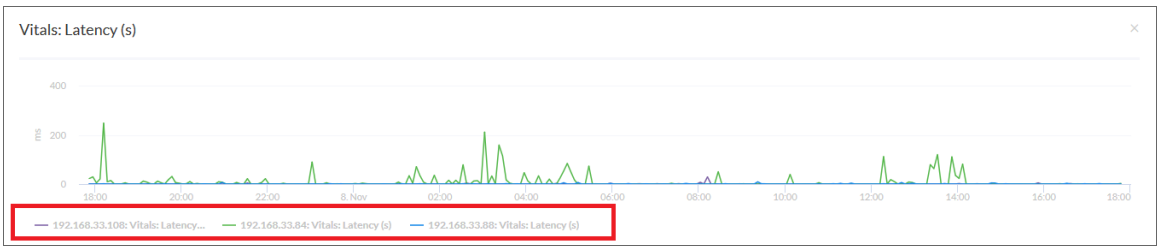
1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Compare Device]** button. The **Compare Device** modal page appears:



2. Select devices from the list and then click the **[Choose Devices]** button.

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

3. The selected devices are added to the Device List on the **[Investigator]** tab, using the same set of metrics that the current device is using. You can click on the name of an individual device in the Device List to go to that device's Investigator page. In the right-hand pane, each widget displays the data from all of the devices:



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

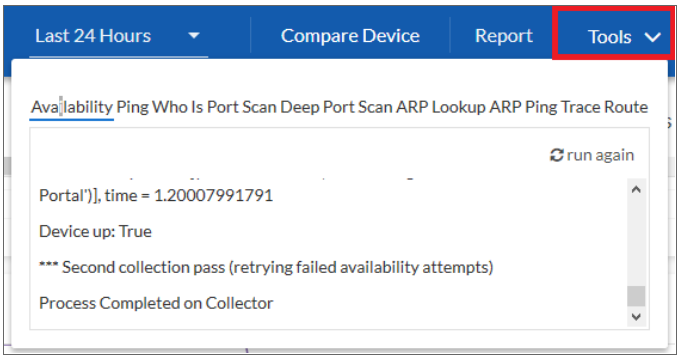
NOTE: You can also *combine the charts* for all of the devices you are comparing by clicking the **Combine Charts** toggle.

Using Device Tools

On the **Device Investigator** page, you can click the **Tools** menu to display the **Tools** pane. The **Tools** pane provides access to a set of network tools. The **Tools** pane lets you to run diagnostics on a device without leaving SL1.

The **Tools** menu appears only for devices where the tools are relevant and can be used. For example, if a device does not have an IP address, only the Availability tool will be available, and the following tools will not appear for that device and its events: Ping, Who IS, Port Scan, AP, and Trace Route.

NOTE: The **Tools** pane will not display if the user does not have permissions for device tools.



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

You can access the following tools from the **Device Investigator** page for a device:

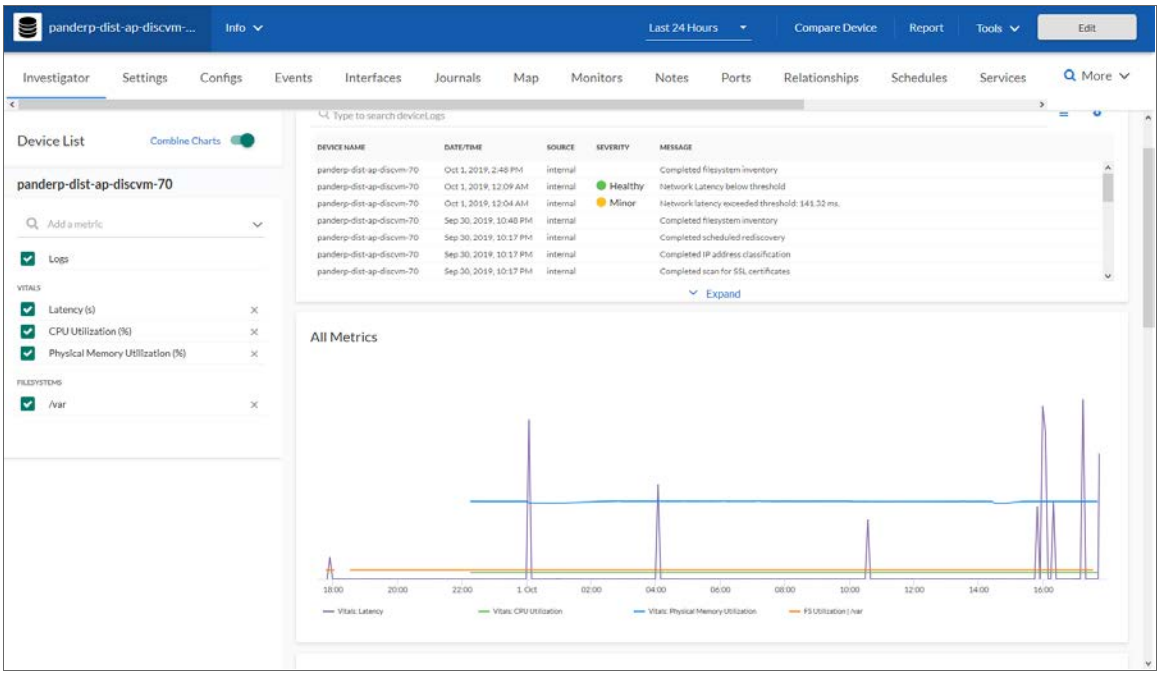
- ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
- ***Ping***. Displays statistics returned by the ping tool. The ping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

Combining Charts on the Investigator Tab

On the **[Investigator]** tab of the **Device Investigator** page, you can combine charts to see all of the data in a single chart. Combining charts displays multiple metric types in one chart.

To combine charts:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **Combine Charts** toggle. The **All Metrics** chart appears:



2. To hide a metric from the **All Metrics** chart, click the metric label in the legend on the graph's x-axis. You can click the metric label again to add the metric back to the graph.

Running a Device Report

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

1. On the **Device Investigator** page, click the **[Report]** button in the top navigation bar. The **Device Report** modal page appears.
2. From the ***Select Type*** drop-down, select the type of report you want to generate. You can select *Full Report*to get all of the metrics, or you can select a single metric for the device, such as *Status*, *Processes*, or *Health*.
3. In the ***Select Format*** drop-down, select the format for the report. Options include *HTML*, *PDF*, *DOC*, *XLS*, or *CSV*.
4. Click **[Create Report]** to generate the report.

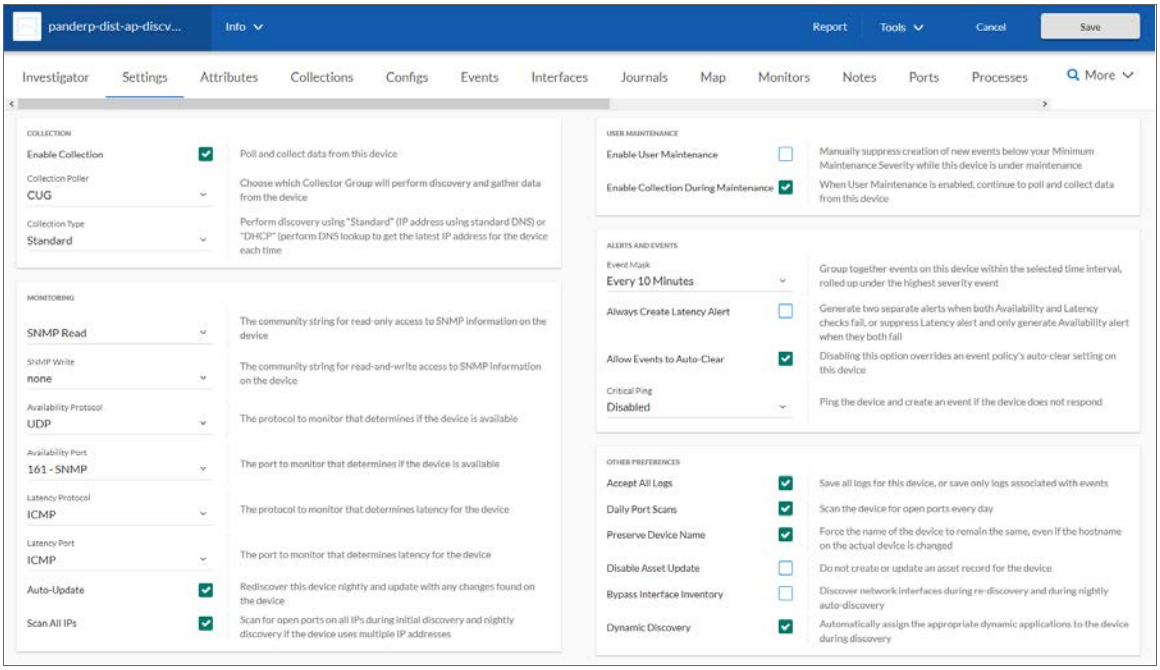
Overview of the Device Investigator Tabs

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

The 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]**.



Set the following collection preferences:

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

Set the following monitoring preferences:

- ***SNMP Read***. Select the community string for read-only access to SNMP information on the device.
- ***SNMP Write***. Select the community string for read-and-write access to SNMP information on the device.
- ***Availability Protocol***. Select the protocol to monitor that determines if the device is available.
- ***Availability Port***. Select the port to monitor that determines if the device is available.
- ***Latency Protocol***. Select the protocol to monitor that determines latency for the device.
- ***Latency Port***. Select the port to monitor that determines latency for the device.

- ***Auto-Update***. This checkbox specifies whether or not you want SL1 to perform a nightly discovery of the device and update records with changes to the device. If this field is unchecked, SL1 will not perform nightly discovery. Changes to the device, including newly opened ports, will not be recorded by SL1.
- ***Scan All IPs***. If the device uses multiple IP Addresses, SL1 will scan for open ports on all IPs during initial discovery and nightly discovery.

Set the following user maintenance preferences:

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

Set the following alerts and events preferences:

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

Set the following device preferences:

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

- *Not Selected*. SL1 will attempt to discover network interfaces for this device during re-discovery and nightly auto-discovery using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value specified in the **Device Thresholds** page.

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

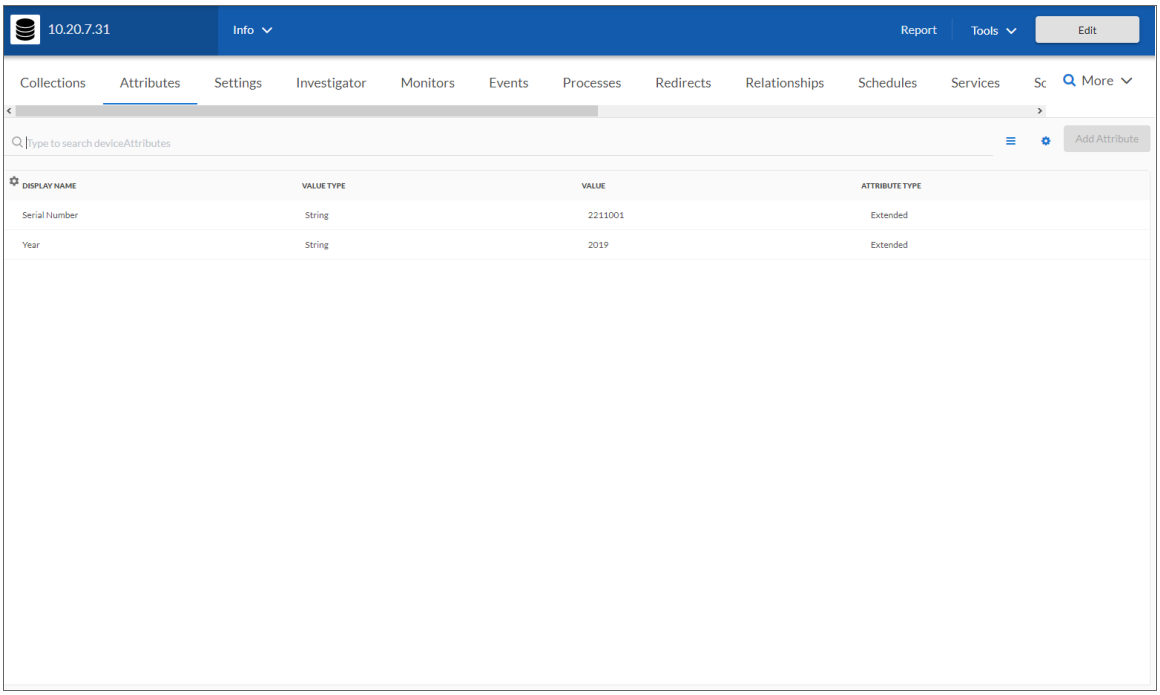
The Attributes Tab

Custom Attributes are name-value pairs. You can use custom attributes to add custom descriptive fields to assets, devices, interfaces, themes, and vendors. In SL1, you can create and update custom attributes via the API, in configuration Dynamic Applications, and in the **Custom Attribute Manager** page. Custom attributes can be used to dynamically define device groups and can be viewed with the custom table widget.

There are two categories of custom attributes:

- **Base Custom Attributes**. These custom attributes are applied to each member of an element type. For example, a base attribute for devices would be applied to all devices.
- **Extended Custom Attributes**. These custom attributes are applied individually to one or more members of an element type. For example, you could apply the custom attribute cisco_ios_version only to those asset records for Cisco devices; you would not want to assign this custom attribute to all asset records.

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



> **NOTE:** Before you can add a custom attribute to a device, you might need to create that custom attribute on the **Custom Attribute Manager** page (Manage > Custom Attributes) or on the classic **Custom Attribute Manager** page (System > Manage > Custom Attributes).

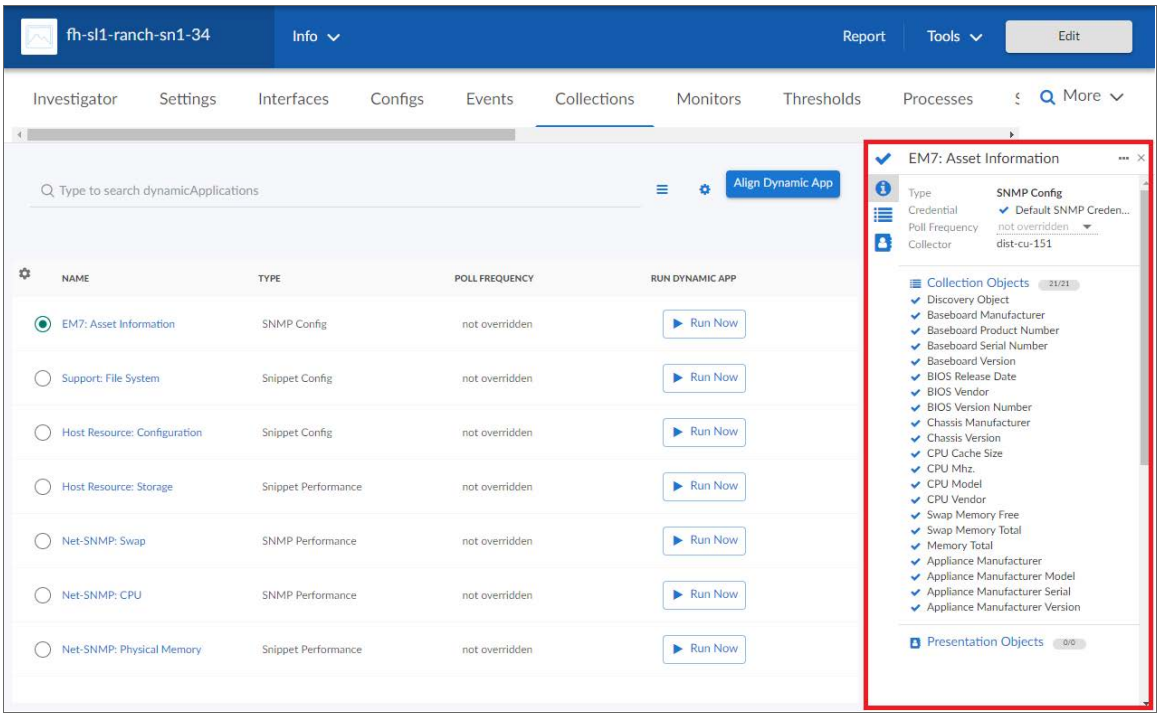
To add and edit custom attributes for a device on the **[Attributes]** tab:

1. Click **[Edit]** on the **[Attributes]** tab for the device and click **[Add Attribute]**. The **Align Extended Attribute** window appears.
2. Complete the following fields:
   - ***Attributes***. Select the name of the custom attribute.
   - ***Attribute value***. Specify a text or numeric value for the attribute, based on its value type.
3. Click **[Add Attribute]**. The custom attribute is added to the list on the **[Attributes]** tab.
4. To edit an attribute in the list, select that attribute and edit the ***Attribute value*** field in the **Edit** window.
5. To unalign an attribute, select that attribute and click **Unalign Attribute** in the **Edit** window.
6. When you are done adding, editing, or unaligning attributes, click **[Save]**.

The Collections Tab

On the **[Collections]** tab, you can align or unalign Dynamic Applications with this device, enable or disable collection for the Dynamic Applications, and run a Dynamic Application. You can also update the poll frequency and change the credential for a Dynamic Application.

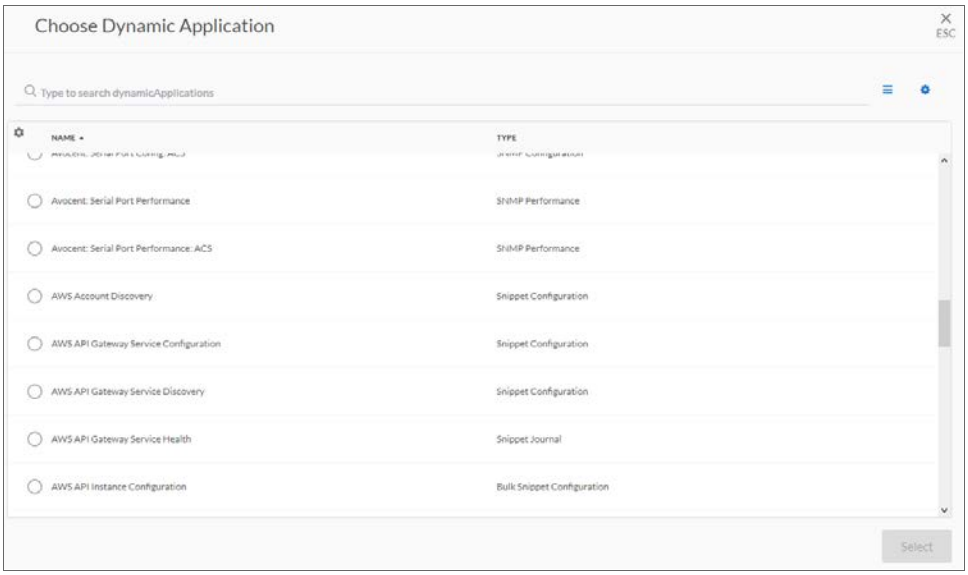
To view more information about a Dynamic Application, select that Dynamic Application from the list. An information pane appears on the right with details about that Dynamic Application and its collection objects and presentation objects:



TIP: Click the gear icon ( ) in the top left of the **Events** page and select additional columns as needed, including **Credential, Poll Frequency**, and **Run Dynamic App**.

To align a Dynamic Application:

1. On the **[Collections]** tab for the device, click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
2. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears:



3. Select the Dynamic Application you want to align and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. Click *Choose Credential*. The **Choose Credential** window appears.
5. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
6. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

TIP: To *unalign* a Dynamic Application from a device, click the **[Actions]** button (⋯) for that Dynamic Application and select *Unalign Dynamic App*.

7. To run the new Dynamic Application immediately, click the **[Actions]** button (⋯) for that Dynamic Application and select *Run Now*. You can also select *Run Now* from the **[Actions]** button (⋯) on the information pane for the Dynamic Application. A status window displays the status and relevant logs for the dynamic application.

TIP: To enable or disable all collection for a Dynamic Application, click the **[Actions]** button (⋯) for that Dynamic Application and select *Enable Collection* or *Disable Collection* as needed. When you unalign a Dynamic Application, you also delete the data it has collected.

After a Dynamic Application is aligned with a device, you can select that Dynamic Application to see the status of its collection objects. The following icons represent the different collection object statuses:

Icon	Status
	Found and collecting
	Found and not collecting
	Not found and collecting

To change the poll frequency and collection status for a Dynamic Application:

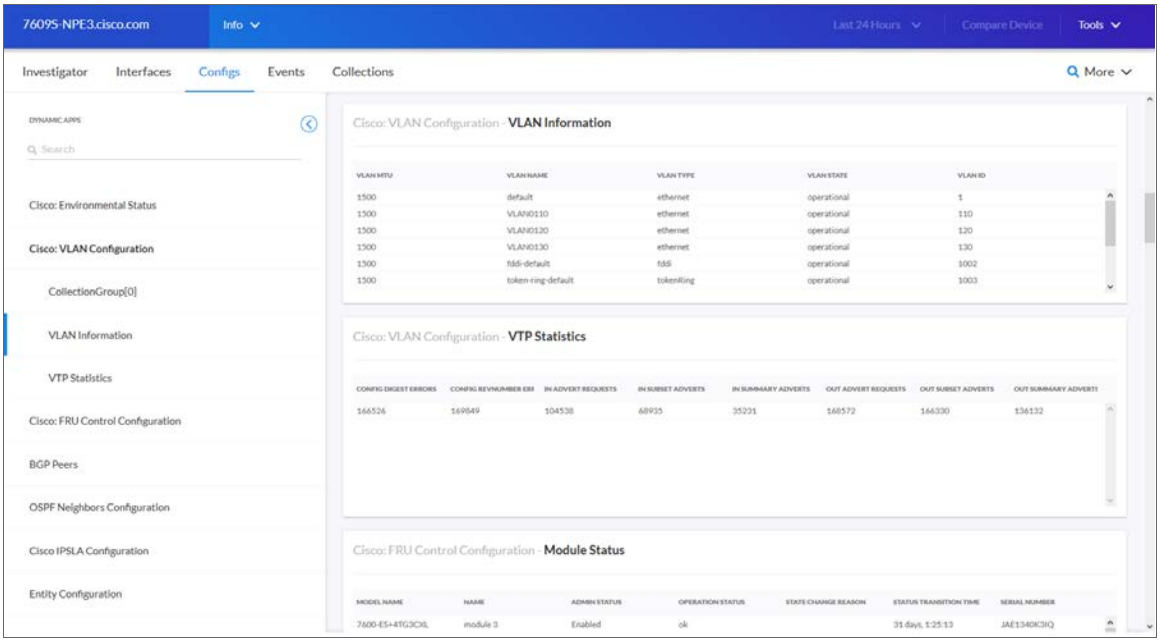
1. On the **[Collections]** tab for the device, click **[Edit]** and select the Dynamic Application you want to update. The information pane for the Dynamic Application appears.
2. From the ***Poll Frequency*** drop-down, select how often you want the Dynamic Application to poll the device. Your options range from *1 minute* to *24 hours*, or you can select *Default* to not change the frequency.
3. You can disable collection for individual collection objects and presentation objects by clicking the **[Actions]** button (⋯) for an object in the information pane and selecting *Disable Collection*. Start collection for a disabled object by clicking the **[Actions]** button (⋯) and selecting *Enable Collection*.

TIP: You can also use the information pane to change the credential aligned with this Dynamic Application. Click the name of the credential at the top of the information pane and select a different credential from the **Choose Credential** window.

4. Click **[Save]**.

The Configs Tab

On the **[Configs]** tab of the **Device Investigator** page, you can view configuration information that has been collected from the device by Dynamic Applications. All objects of type "config" are included on the **[Configs]** tab. Usually, "config" objects contain static information about hardware and configuration settings, such as serial numbers, version numbers, and hardware status.



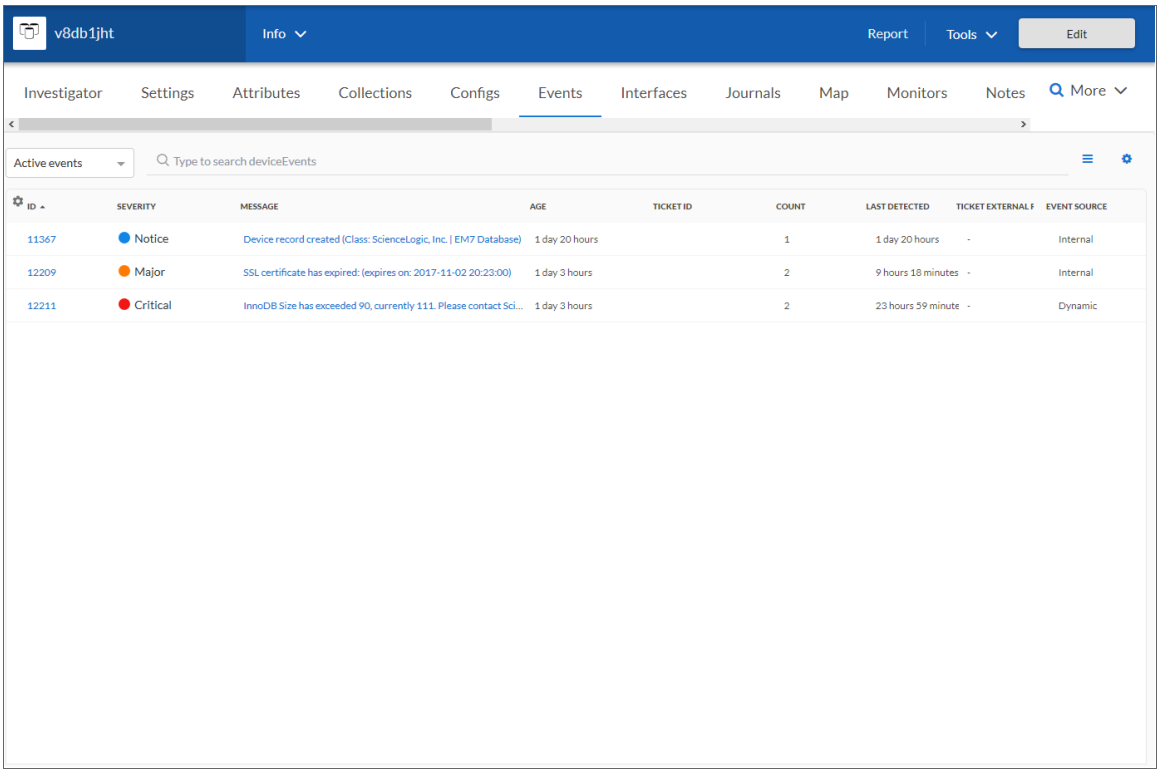
The pane on the left displays a list of Dynamic Applications associated with the device. To view the configuration data collected by a Dynamic Application, select it from the **Dynamic Apps** section on the left.

You can enable change detection for an object in the in the **Collections** tab (System > Manage > Dynamic Applications > Create/Edit), in the ***Change Alerting*** field. If an object's value has changed, it will be underlined on the **Configuration Report** page. You can then click on the object's value in the **Configuration Report** page and view a list of historical values for the object. Any configuration data that has changed since the last time you visited this tab displays as underlined.

The data displayed on this tab is read-only.

The Events Tab

On the **[Events]** tab of the **Device Investigator** page, you can view a list of events for the device:



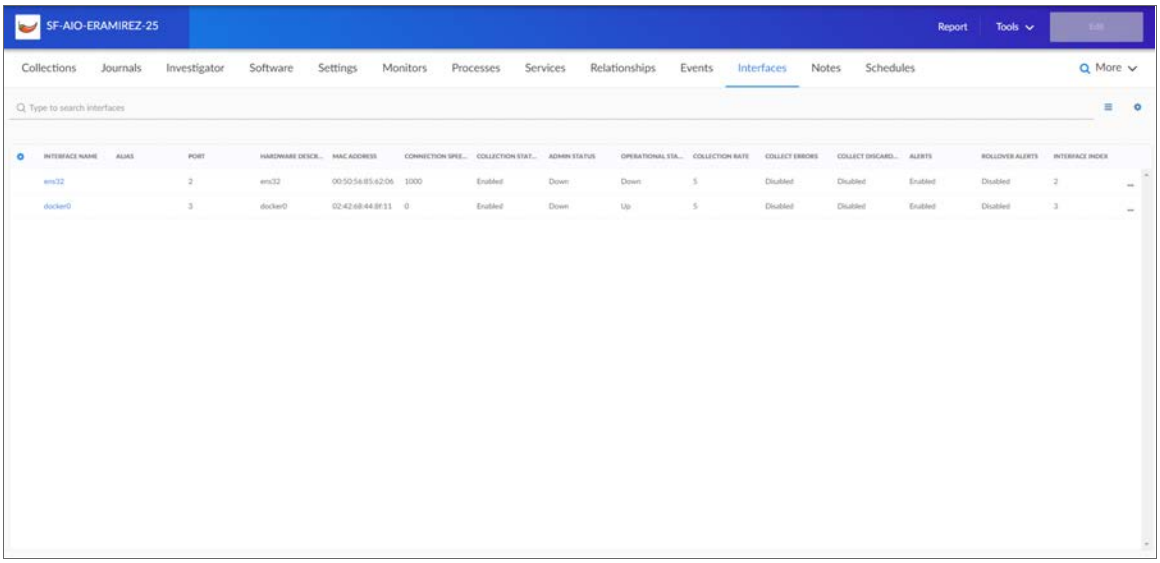
Click the ***Select Columns*** icon ( ) to add or remove columns to the table, such as *Ticket ID*, *Last Detected*, *Ticket External Reference*, and *Age*.

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.

TIP: To view the **Event Investigator** page for an event on this tab, click the linked text in the **ID** or the **Message** column.

The Interfaces Tab

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



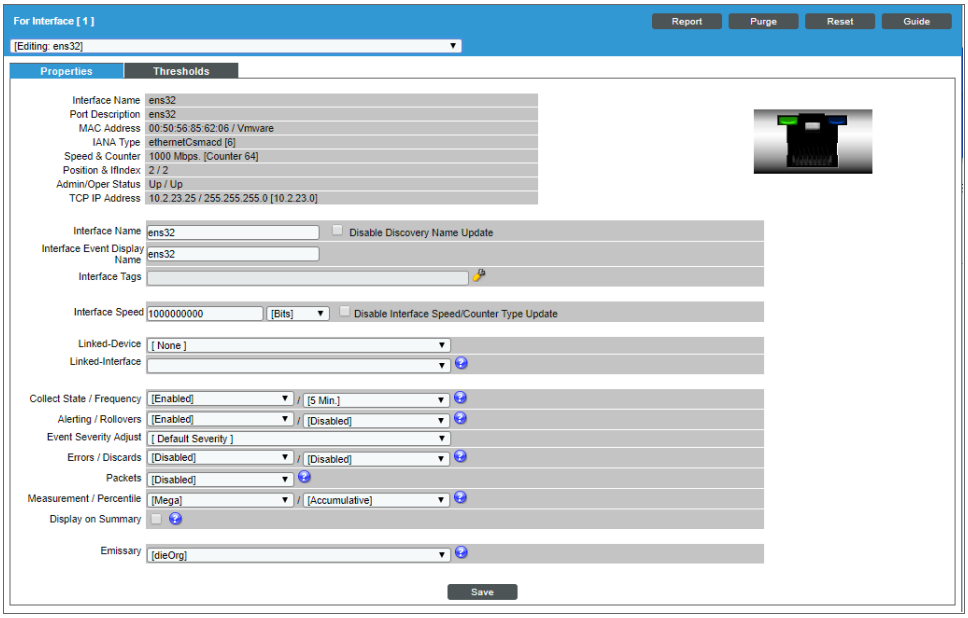
The data displayed on this tab is read-only.

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

- ***Interface Name***. The name of the network interface. You can open the **Interface Properties** page in a pop-up window by clicking the interface name from the list.
- ***Alias***. The name assigned by SL1 to the interface.
- ***Port***. Port of the interface.
- ***Hardware Description***. Description of the network interface. Usually a description of a network-interface card.
- ***MAC Address***. Short for Media Access Control Address. A unique number that identifies the interface. MAC Addresses are defined by the hardware manufacturer.
- ***Connection Speed***. The amount of data per second that can pass through the network interface.
- ***Collection State***. Specifies whether the platform monitors the network interface and collects data from the network interface for reports. Can be either *Disabled* or *Enabled*.
- ***Admin Status***. Specifies how the network interface has been configured on the device. Can be one of the following:
    - *Up*. Network interface has been configured to be up and running.
    - *Down*. Network interface has been purposefully disabled.
- ***Operational Status***. Specifies current state of the network interface. Can be one of the following:
    - *Up*. Network interface is transmitting and receiving data.
    - *Down*. Network interface cannot transmit and receive data.

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

Clicking an ***Interface Name*** opens the **Interface Properties** page for that interface:



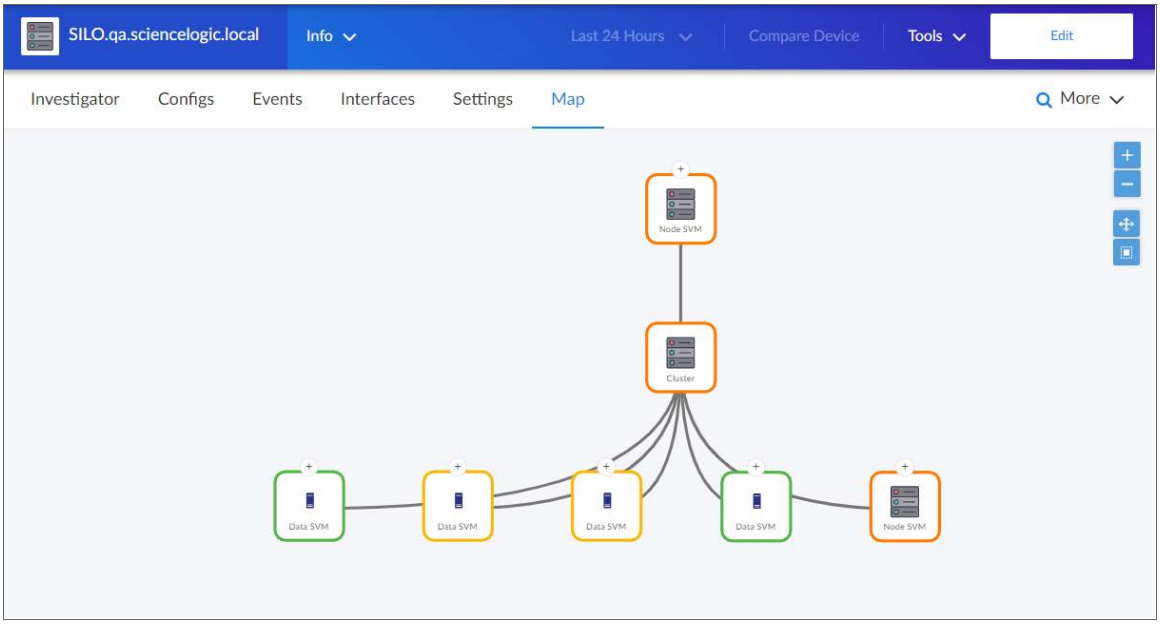
The Journals Tab

The **[Journals]** tab of the **Device Investigator** page displays journal entry information collected from the device by journal Dynamic Applications. All information from Dynamic Applications of type journal are included in the **Journal View** page. Journal Dynamic Applications store information in log format; for example, telephone call records or access logs.

For details on the **Journal View** page, see the ***Snippet Dynamic Application*** manual.

The Map Tab

The **[Map]** tab in the **Device Investigator** page displays a map of the device and all of the devices with which the device has relationships.



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

The Monitors Tab

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

The **Monitoring Policies** page allows you to define policies that monitor:

- ***System processes***. Monitors the device and look for the specified system process.
- ***Domain-name availability and lookup speed***. Monitors the availability and lookup time for a specific domain-name server and a specific record on a domain name server.
- ***Email round-trip speed***. Monitor the amount of time it takes to send an email message from SL1 to an external mail server and then back to SL1.
- ***SOAP and XML transaction speeds***. Monitors any server-to-server transactions that use HTTP and can post files or forms. (for example, SOAP/XML, email, or RSS feeds). Periodically, SL1 sends a request and some data and then examines the result of the transaction and compares it to a specified expression match.
- ***TCP/IP port availability***. Monitors ports for availability every 5 minutes. If a port is not available, SL1 creates an event. The data gathered by the port policy is used to create port-availability reports.
- ***Web-content availability***. Monitors a website for specific content. SL1 will periodically check the website for

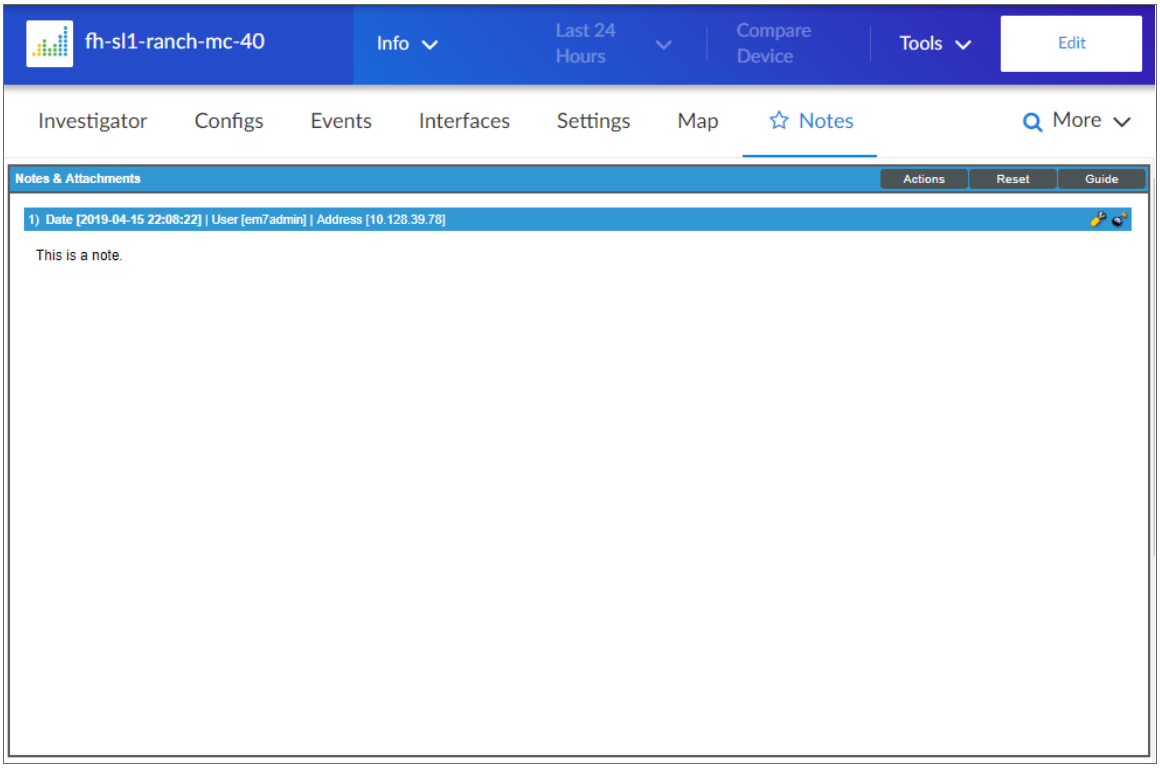
specified content. If the content cannot be found on the website, SL1 will generate an event.

- ***Windows services***. Monitors the device and look for the specified service.

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

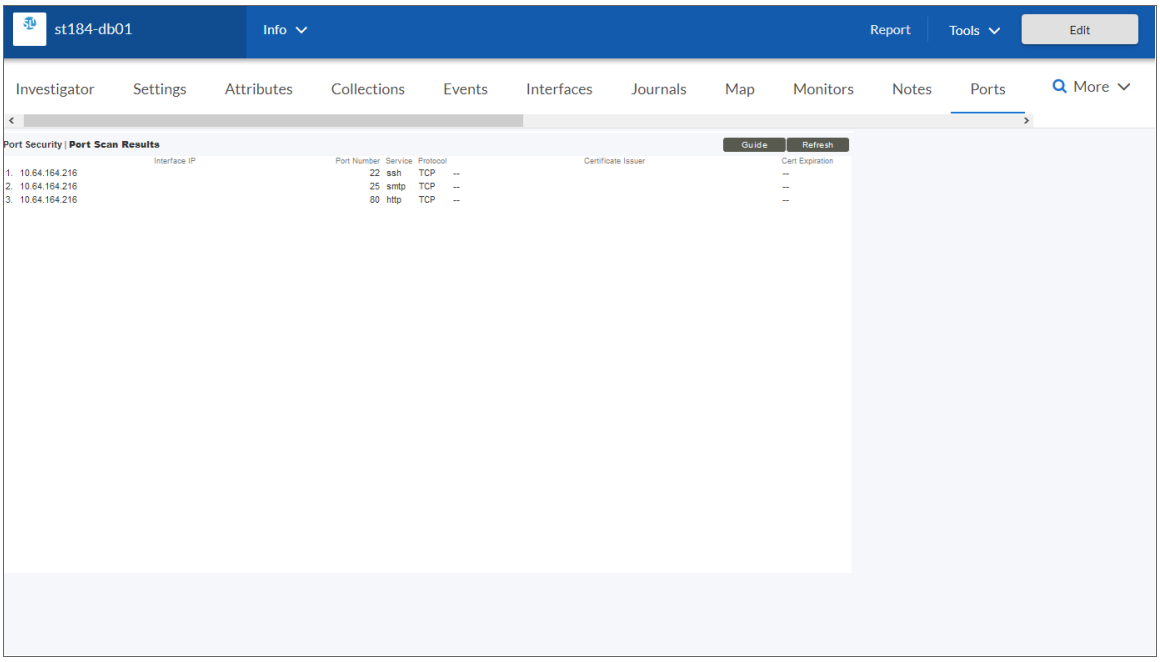
The Notes Tab

On the **[Notes]** tab of the **Device Investigator** page, you can view a list of all comments and attachments associated with the device properties. You can create a new note by selecting the **[Notepad Editor]** button in the **Notes & Attachments** page or *Notepad Editor* from the **[Actions]** menu.



The Ports Tab

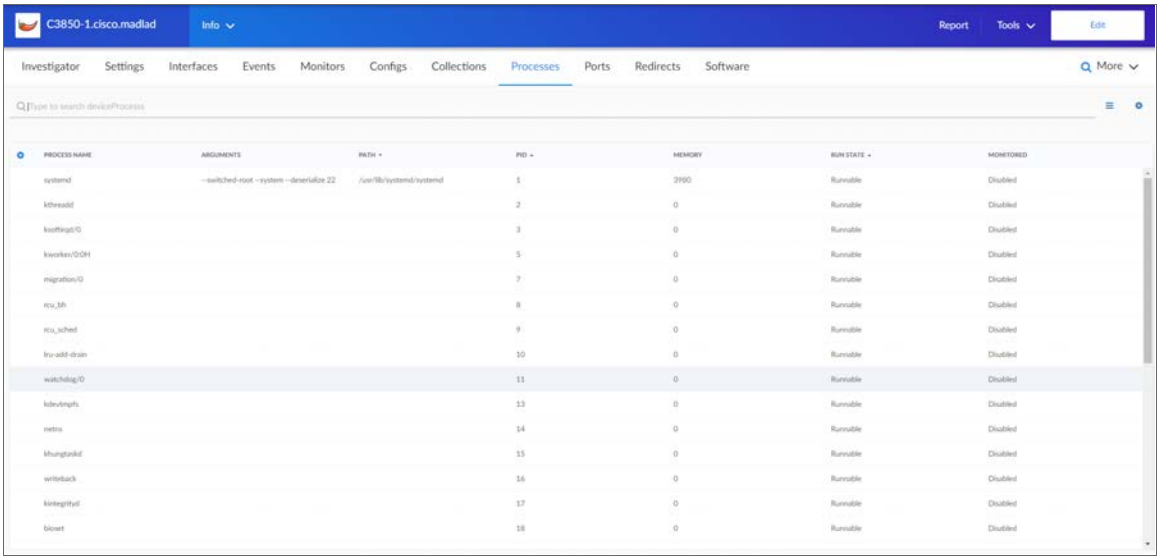
The **[Ports]** tab in the **Device Investigator** page displays a list of all open ports on a device. Every night, SL1 scans all the ports of each managed device. If any new ports are opened, SL1 adds the port to the list in the **Port Security** page.



The Processes Tab

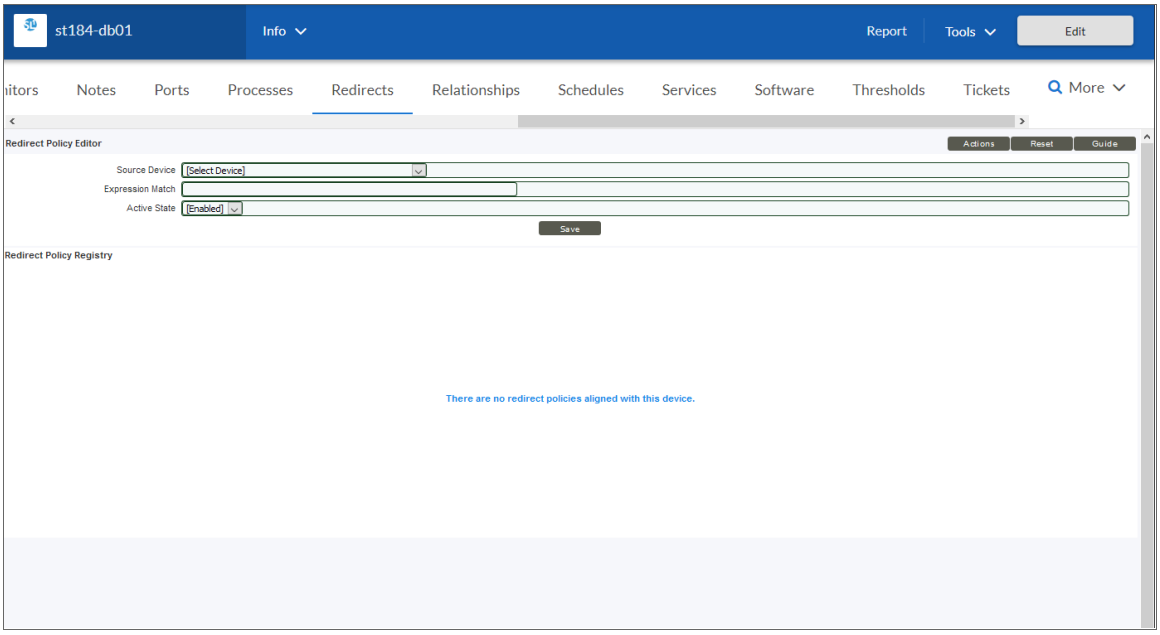
The **[Processes]** tab in the **Device Investigator** page displays information about the processes running on the device. A ***process*** is a program that is currently running on a monitored device or has been run in the past and is currently idle. Sometimes a process is called a task.

To keep your device running efficiently and to maintain security, the **Processes** tab helps you manage processes on your device. The **Processes** taballows you to easily view details about each process running on the device.



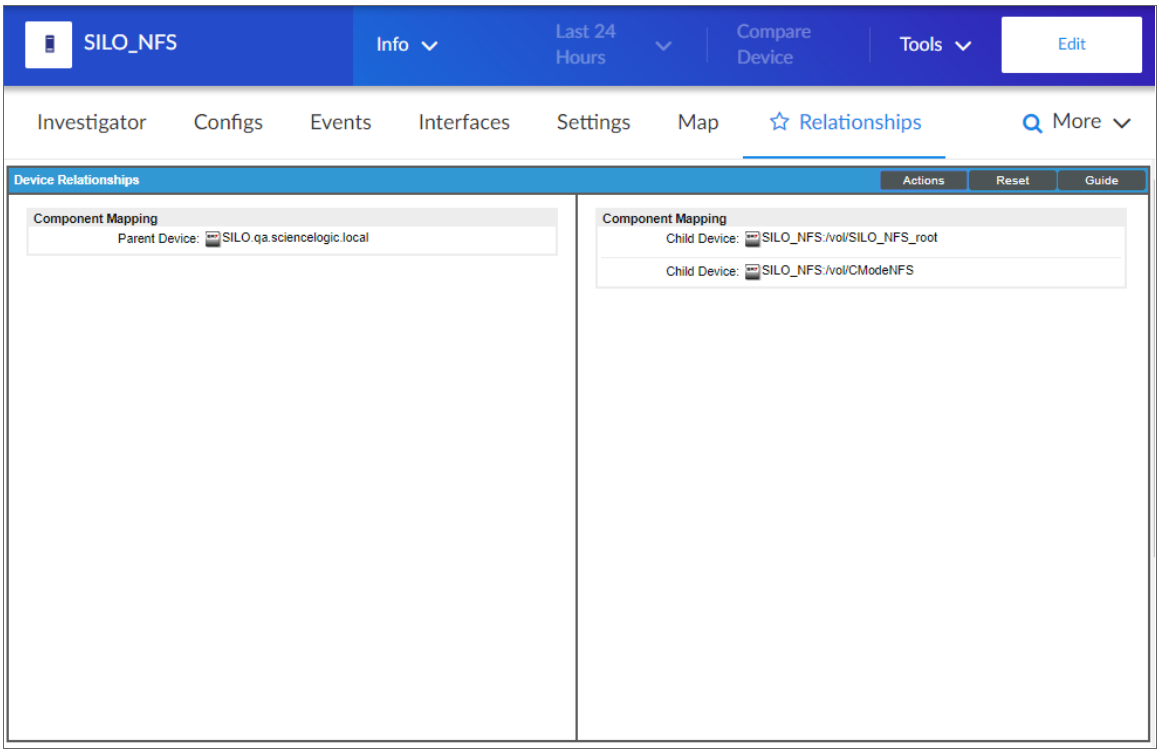
The Redirects Tab

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



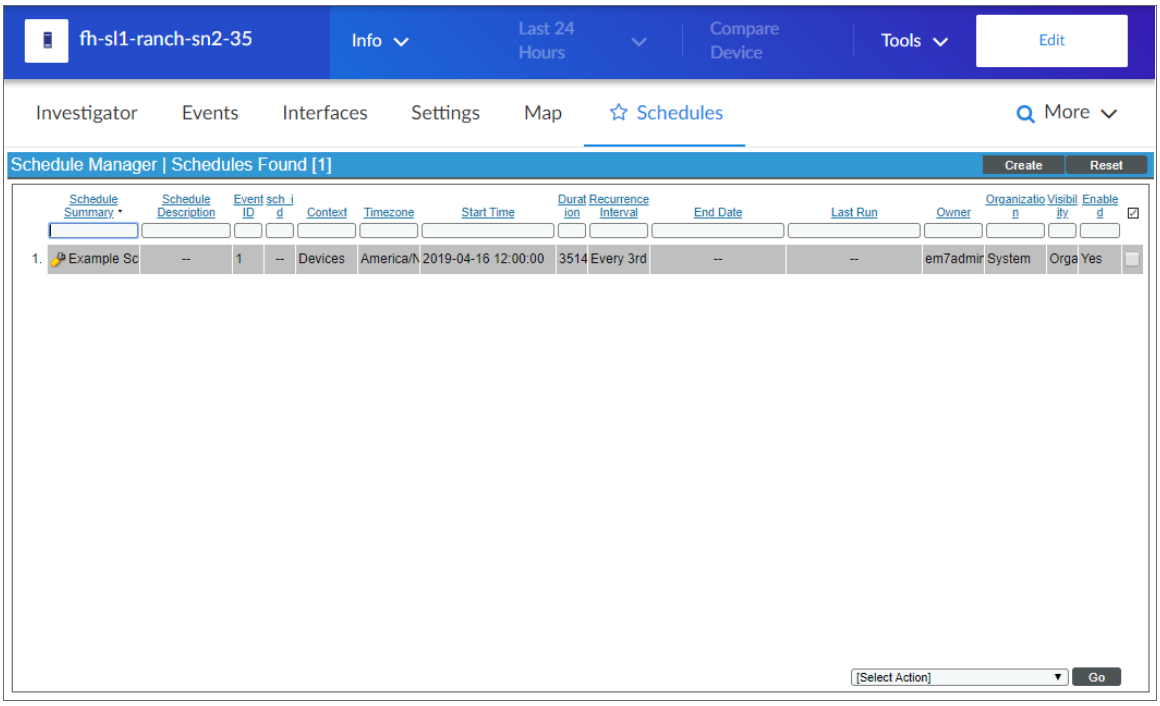
The Relationships Tab

The **[Relationships]** tab of the **Device Investigator** page displays information about parent-child relationships between devices.



The Schedules Tab

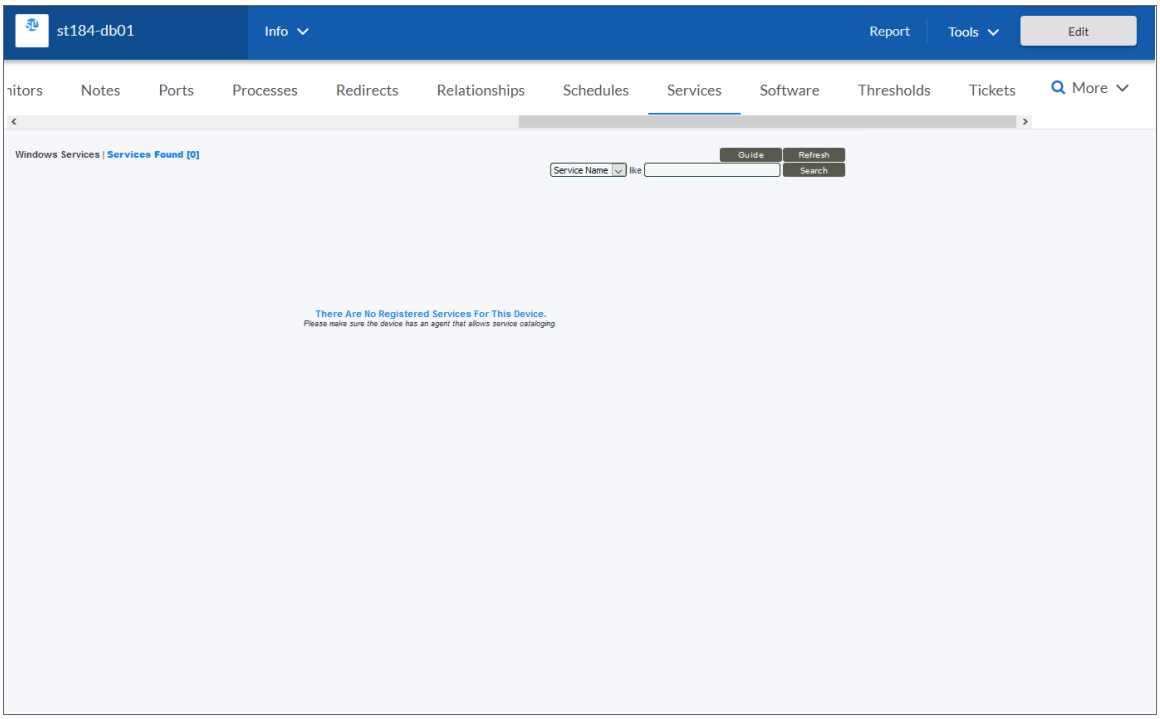
On the **[Schedules]** tab of the **Device Investigator** page you can manage all the scheduled process you have defined in your system. You can define scheduled tasks for a number of things, such as backup management, dashboards, devices, and Run Book Automation policies.



The Services Tab

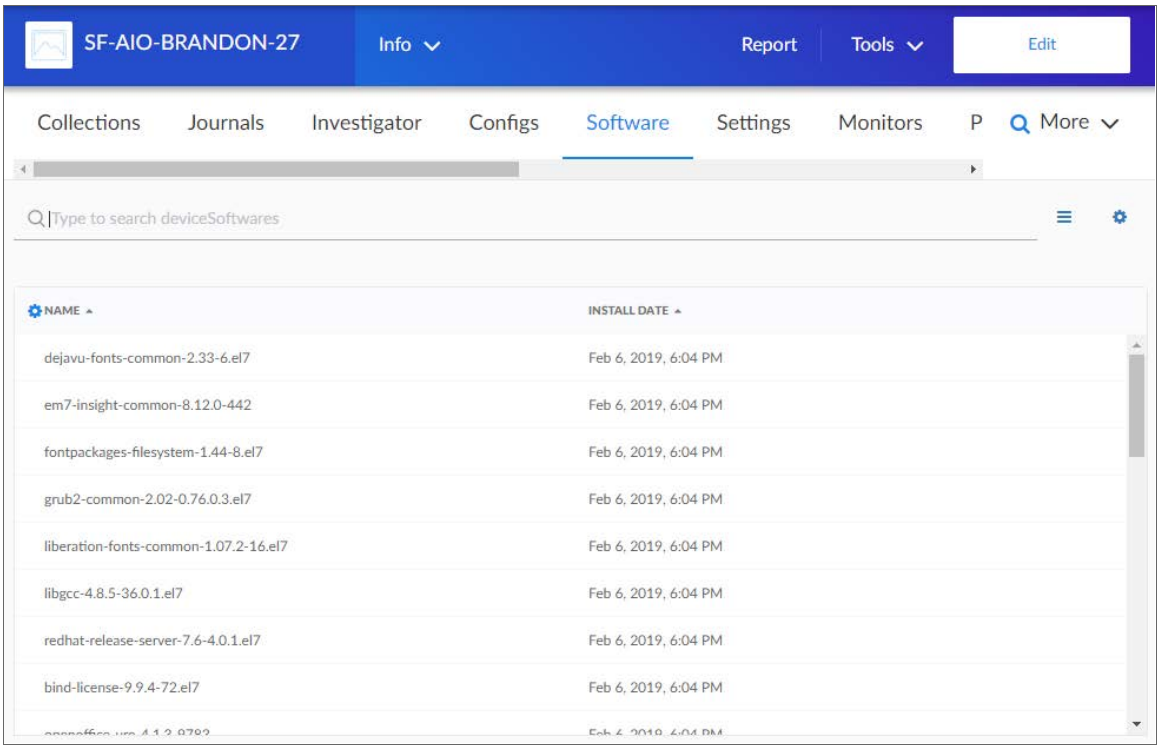
The **[Services]** tab in the **Device Investigator** page displays a list of all Windows services enabled on the device. Windows Services are long-running applications. These applications typically do not have a user interface or produce any visual output. Any messages associated with the service are typically written to the Windows Event Log. Services can be configured to start automatically when the computer is booted. Services do not require a logged in user in order to execute.

To keep your device running efficiently and to maintain security, the **[Services]** tab helps you manage services on your device. The **[Services]** tab allows you to easily view details on all the services running on the device.



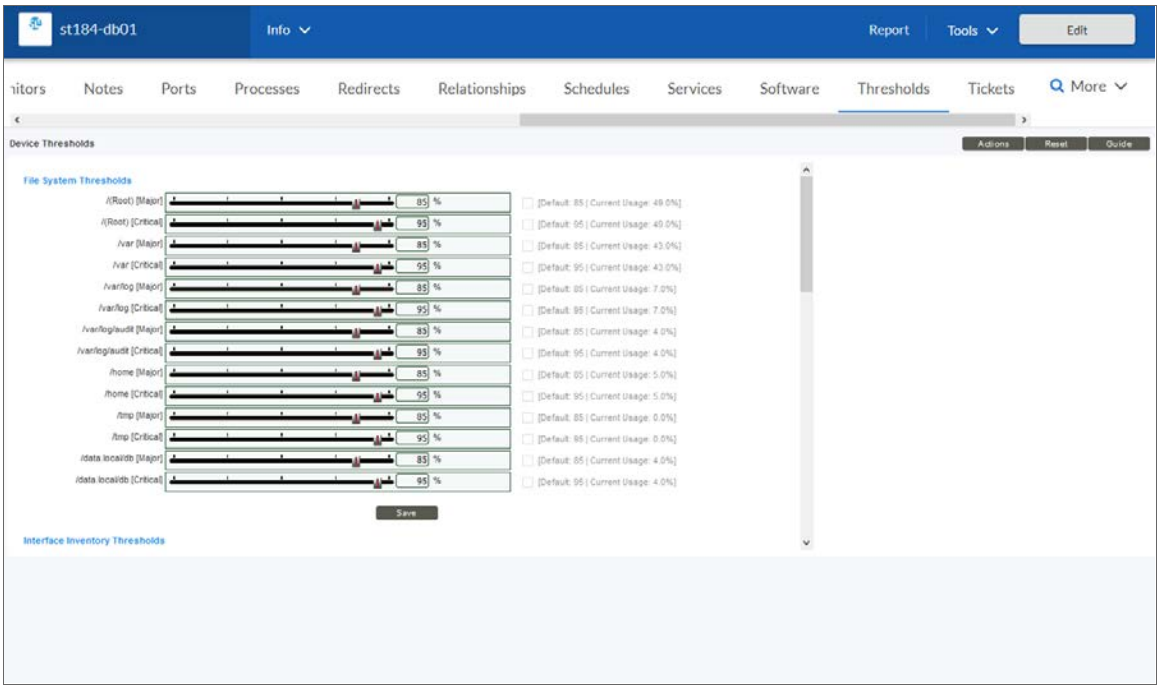
The Software Tab

The **[Software]** tab in the **Device Investigator** page displays a list of all the software installed on the device. If possible, the installation date is also displayed.



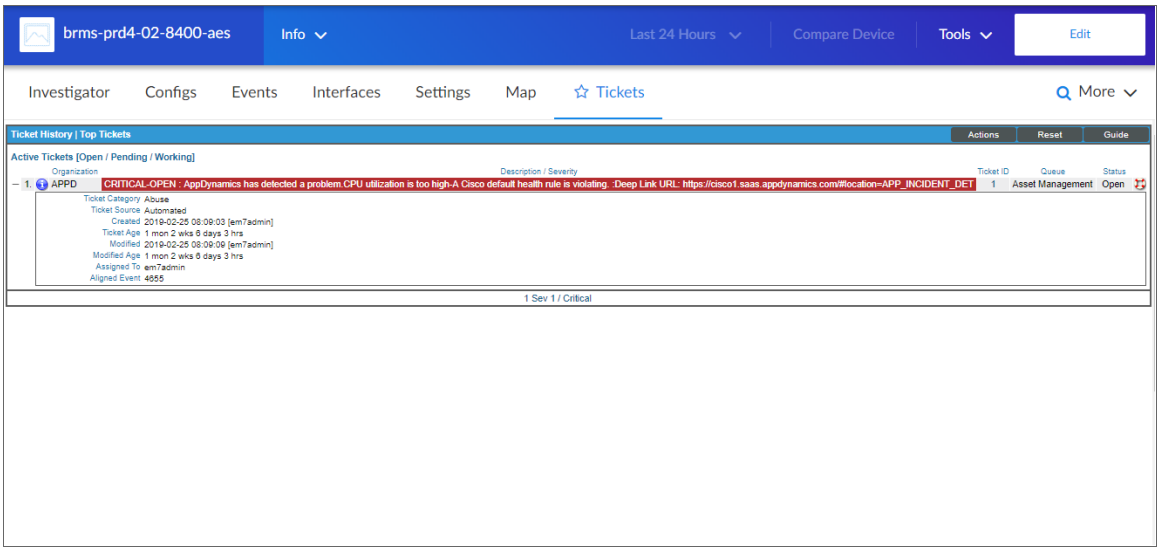
The Thresholds Tab

On the **[Thresholds]** tab of the **Device Investigator** page, you can define usage and performance thresholds and data retention thresholds for a device. When these thresholds are exceeded, SL1 will generate an event for the device.



The Tickets Tab

The **[Tickets]** tab in the **Device Investigator** page displays all tickets associated with the device. This page displays critical information about each ticket. If you require more detail, you can access the**Ticket Editor** from this page by clicking on the ticketing icon ( ). For details on creating tickets, see the manual ***Ticketing***.



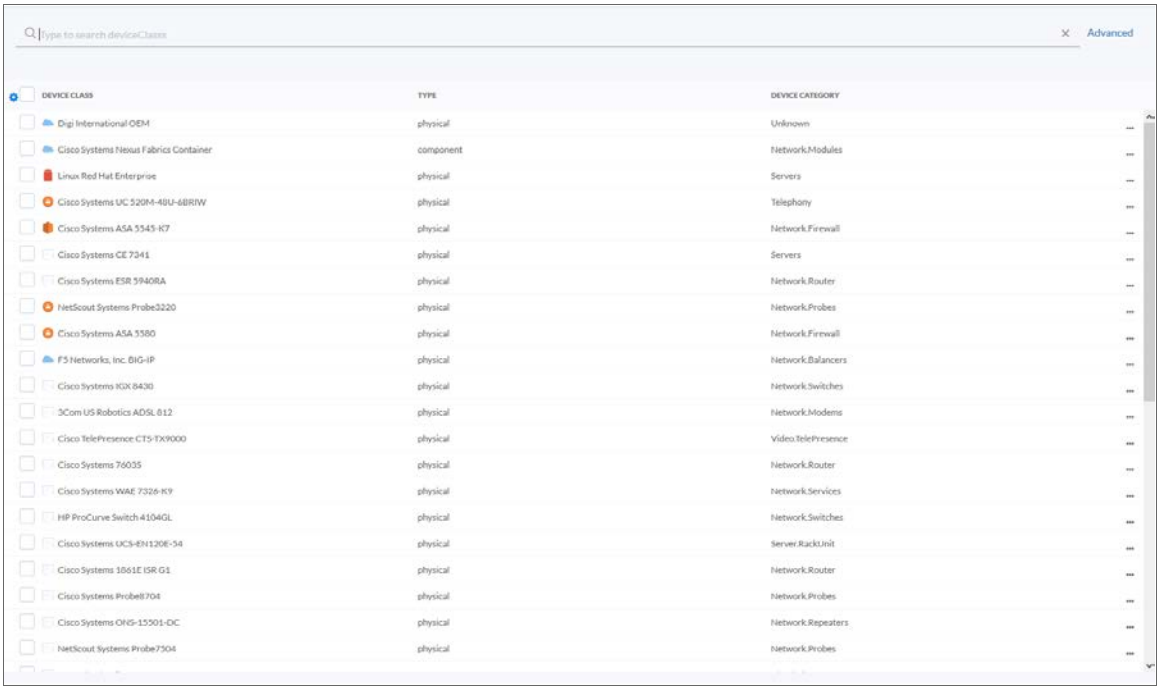
Working with Device Classes

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

Device classes determine:

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

On the **Device Classes** page (Devices > Device Classes), you can view a list of existing device classes in SL1.

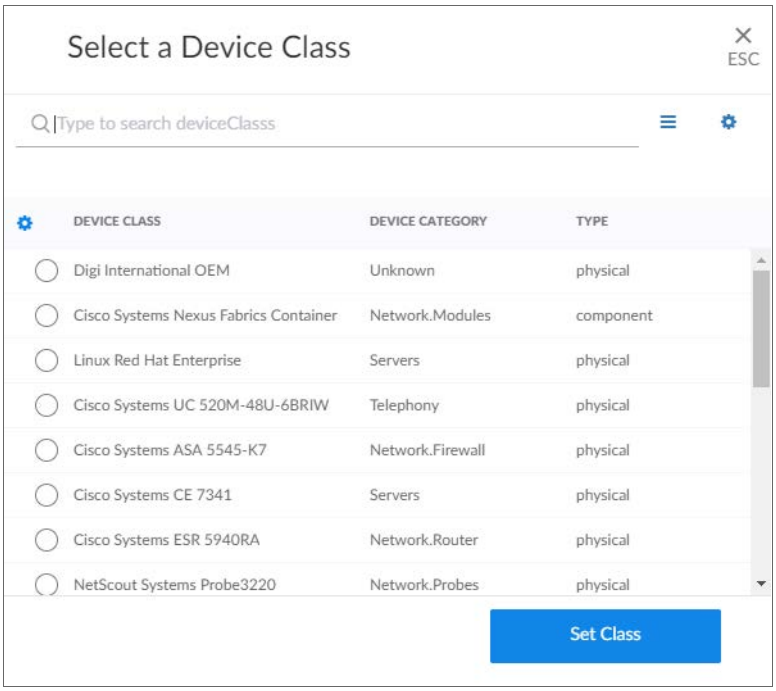


TIP: Click the **Choose Columns** icon ( ) to enable the **Vendor** and **Model** columns in the **Device Classes** page.

To assign a device class to a device:

1. Go to the **Devices** page and select the device to which you want to assign a device class.
2. On the **Device Investigator** page, click **[Edit]**.

3. Click the **Info** drop-down and click the ***Device Class*** field. The **Select a Device Class** window appears:



4. The **Select a Device Class** window displays a searchable list of available device classes, and the category and type for each class. Select the device class you want to assign, then click the **[Set Class]** button.

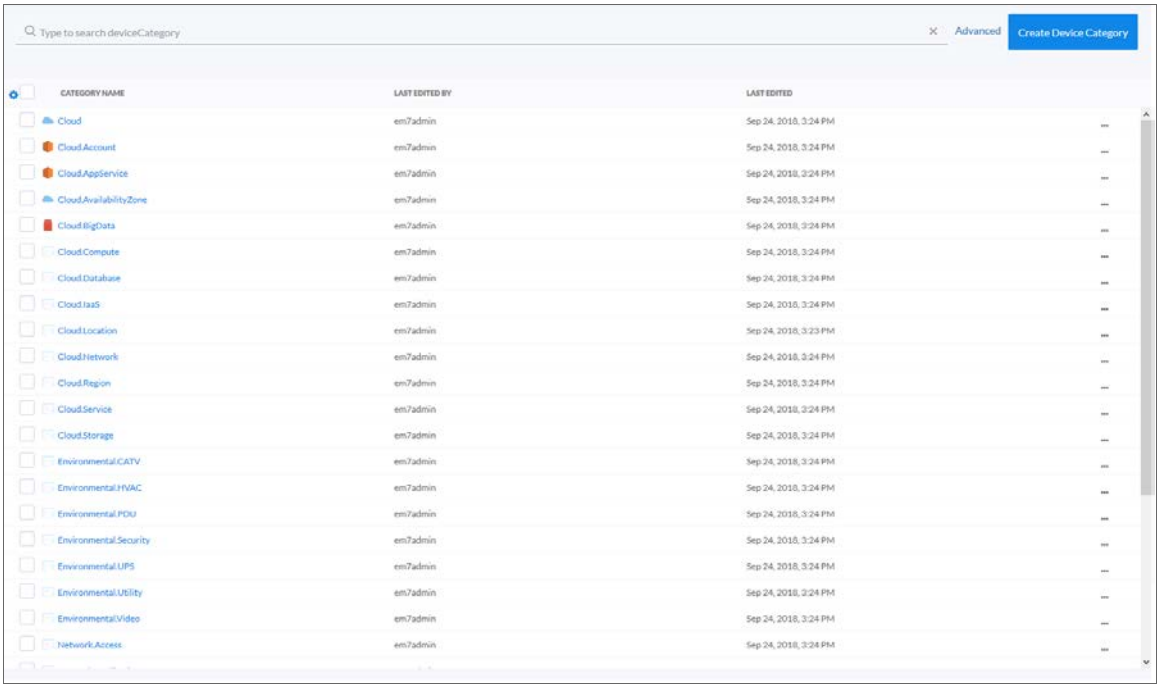
5. Click the **[Save]** button on the **Device Investigator** page to save your changes.

Working with Device Categories

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

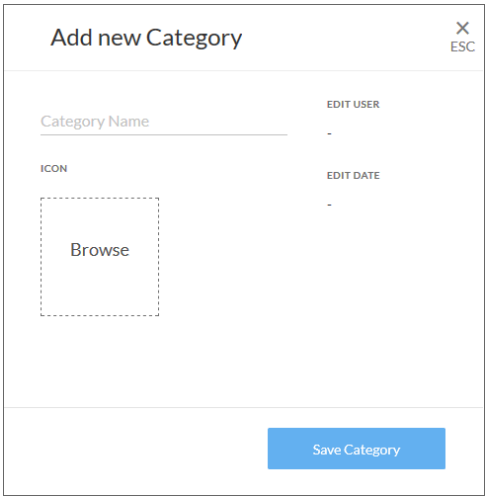
Device categories are paired with device classes to organize and describe discovered devices. The device class usually describes the manufacturer. The device category describes the function of the hardware. Each device class can include a device category.

On the **Device Categories** page (Devices > Device Categories), if you have the proper permissions, you can view a list of existing device categories, create and edit device categories, and duplicate device categories. You can also assign an icon to a specific device category, and those icons will appear on the **Device Categories** page. The icons also appear on Maps as well as Device Investigator, Service Investigator, and Application Investigator pages.



To create a new device category:

1. On the **Device Categories** page (Devices > Device Categories), click the **[Create Device Category]** button. The **Add New Category** window appears:



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

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

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

To duplicate a device category:

1. On the **Device Categories** page, locate the device category that you want to duplicate.
2. Click the ***Actions*** button (⋯) for that device category and select *Duplicate*.
3. A duplicate of that device category will appear with the word "copy" appended to the original name. Click on the name of the device category to edit the category name.

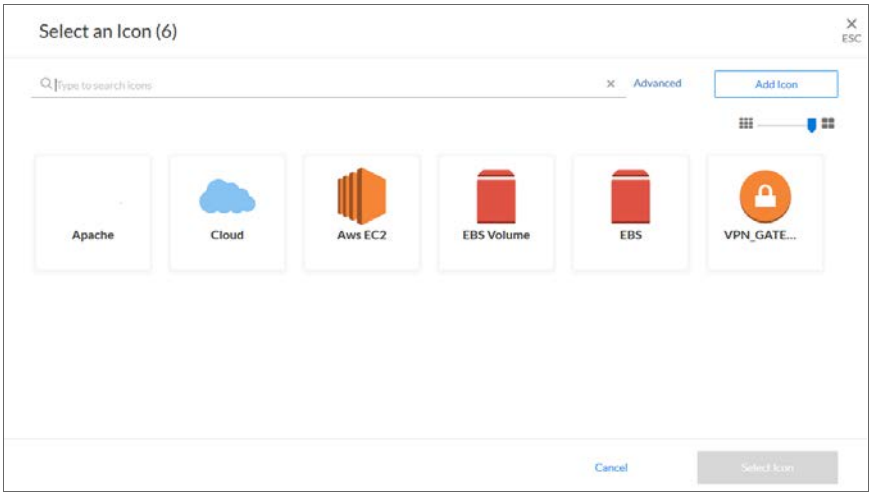
To edit a device category:

1. On the **Device Categories** page, locate the device category that you want to edit.
2. Click the name of the device category to open the category details page.
3. You can edit the ***Category Name*** and ***Icon***. When you are finished making changes, click the **[Save Category]** button.

Assigning Icons to Devices, Device Classes, and Device Categories

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

1. On the **Devices**, **Device Classes** (Devices > Device Classes), or **Device Categories** (Devices > Device Categories) pages, locate the device, device class, or device category for which you want to add an icon.
2. Click the ***Actions*** button (⋯) for that item and select *Assign Icon*. The **Select an Icon** window appears:



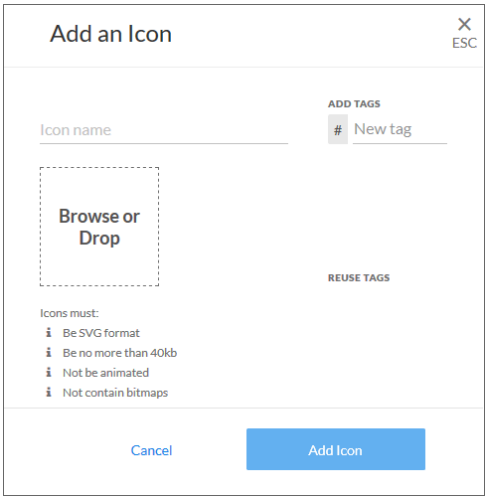
TIP: To assign more than one device, class, or cateogry to an icon, select the checkboxes to the left of those devices and click ***Assign Icon*** in the blue bar at the bottom of the screen.

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

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

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

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



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

Chapter 3

Using the Device Manager Page

Overview

After running discovery for the first time, you can view the list of discovered devices on the **Device Manager** page (Devices > Device Manager).

> **NOTE:** The list of devices on the **Device Manager** page matches the list of devices on the **Devices** page, but the **Device Manager** page includes additional functionality, which will be covered in this chapter.

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

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

This chapter includes the following topics:

Viewing the List of All Devices 70
Device Manager Preferences 73
Filtering the List of Devices 73
Special Characters 75
Using the Advanced Filter with the List of Devices 78
Generating a Report for Multiple Devices 80
Generating a Report for a Single Device 82
Viewing the List of Component Devices 84
Availability for Component Devices 87

Viewing Children Devices 88
Filtering the List of Component Devices 88
Using the Advanced Filter with the List of Component Devices 89
Bulk Actions in the Device Management Page **91**
Bulk Actions for Component Devices **92**
Bulk Merging and Unmerging of Devices **94**
Performing a Bulk Device Merge 95
Performing a Bulk Device Unmerge 97

Viewing the List of All Devices

After running discovery for the first time, you can view the list of discovered devices in the **Device Manager** page. To access the **Device Manager** page, go to Devices > Device Manager (or Registry > Devices > Device Manager in the classic user interface):

The **Device Manager** page displays the following information about each device:

TIP: To sort the list of devices, click on a column heading. The list will be sorted by the column value, in ascending order. To sort the list by descending order, click the column heading again.

- ***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.
- ***Device Hostname***. For devices that are discovered and managed by hostname (instead of IP address), this field displays the fully qualified hostname for the device.
- ***IP Address***. The IP address of the device.

- ***Device 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/Sub-Class.
- ***Device Class/Device Sub-Class***. The manufacturer (device class) and type of device (sub-class). The Device Class/Sub-Class is automatically assigned during discovery, at the same time as the Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by SL1.
- ***Organization***. The Organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. Condition can be one of the following:
    - *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.

NOTE: The appearance of the ***Current State*** field depends upon value in the ***Show Severity Badges*** field in your user preferences. If the ***Show Severity Badges*** field is enabled, the value in the ***Current State*** column will be displayed as a color-coded badge. If the ***Show Severity Badges*** field is not enabled, the value in the ***Device Name*** column and the value in the ***Current State*** column will be painted with the severity color.

- ***Collection Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in the **Collector Group Management** page (System > Settings > Collector Groups) and specify a primary Data Collector and an optional failover collector. A Data Collector server is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).
- ***Collection State***. Collection state can be one of the following:
    - *Active*. SL1 is collecting data from the device.
    - *Unavailable*. SL1 cannot connect to the device, and will not collect data from the device until the device becomes available.
    - *Disabled*. SL1 is not currently collecting data from the device.
    - *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. SL1 cannot collect data from the device at this time.
- ***SNMP Credential***. Primary credential used by SL1 to retrieve SNMP information about the device.

NOTE: Your organization membership(s) might affect the display in the ***SNMP Credential*** column. For details, see the ***Discovery and Credentials*** manual.

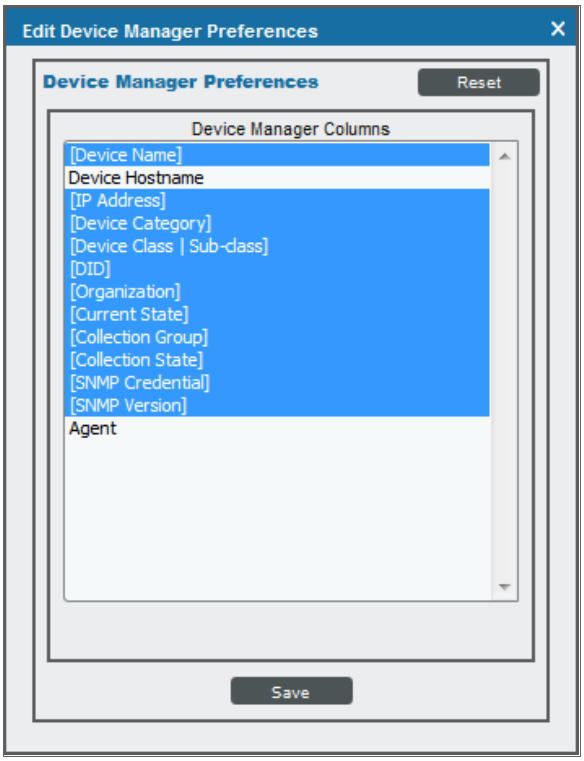
- ***SNMP Version***. The version of SNMP used by the ***SNMP Credential***.
- ***SL Agent***. Indicates if the SL1 agent is installed on the device. If the agentis installed on the device, see SL Agent column displays a gear icon that can be used to access agent settings. For more information about editing Agent settings, see the ***Monitoring Using the Agent*** manual. The ***SL Agent*** column does not appear on the **Device Manager** page by default. For more information about adding or removing columns on the **Device Manager** page, see the *Device Manager Preferences* section.
- ***Tools***. Displays icons for managing devices. The choices are:
    - *Device Administration* ( ). Leads to the **Device Properties** page, where you can define basic device parameters and parameters for discovery. From the **Device Properties** page, you can also access the other pages in the *Device Administration* tools.
    - *Device Management* ( ). Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the **Device Reports** panel. For details on Device Reports, see the manual ***Monitoring Device Infrastructure Health***.
    - *Root Device* ( ). Indicates that the device is a ***component device***. Leads to the **Device Properties** page of the root device for the component device. In SL1, the ***root device*** is the physical device that hosts the system that manages the component device.
    - *Parent Device* ( ). Indicates that the device is a ***component device***. Leads to the **Device Properties** page of the parent device for the component device. In SL1, the ***parent device*** can be either another component device or a physical device. A parent device can be either: a the component device between the current component device and the next layer in the component-device hierarchy or a root device.
    - *Interfaces* ( ). Leads to the **Interfaces Found** page, where you can view details about each network interface on the device. For details on device interfaces, see the ***Device Management*** manual.
    - *Print Report* ( ). Generates a report for the selected icon. Spawns the **Report Selector** page, where you can specify the information to include in the report (Full Report, Status, Config, Hardware, Notes, Software, Processes, Network, Events, and Health) and the format in which the report will be generated (Create Report as HTML Document, Create Report as PDF Document, Create Report as MS Word Document, or Create Report as MS Excel Document).
    - *Create Ticket* ( ). Leads to the **Ticket Editor** page, where you can define and file a new ticket for the device. For details on creating tickets, see the manual ***Ticketing***.
    - *View Asset Record*( ). This icon appears if an asset record has already been defined for the device. This icon leads to the **Asset Properties** page, where you can view the asset record for the device.
    - *Create Asset Record* ( ). This icon appears if an asset record has not been defined for the device. This icon leads to the **Asset Properties** page, where you can create an asset record for the device.
    - *Checkbox* ( ). Applies the action in the ***Select Action*** drop-down to the device. To select all checkboxes (i.e., to select all devices), select the large red check icon.

Device Manager Preferences

The **Device Manager Preferences** page allows you to customize the display and behavior of the **Device Manager** page. To access this page, go to the **Device Manager** page, select the **[Actions]** menu, and then choose *Device Manager Preferences*.

In the **Device Manager Preferences** page, you can customize the following:

- ***Device Manager Columns***. In this list, you can select the default columns to be displayed in the **Device Manager** page.



NOTE: When you edit the list of columns in the ***Device Manager Columns*** field, the selected list of columns in the **Account Preferences** page is automatically updated. When you edit the list of columns in the **Account Preferences** page, the selected list of columns in this page is updated.

Filtering the List of Devices

You can filter the list on the **Device Manager** page by one or more parameters. Only devices that meet all the filter criteria will be displayed in the **Device Manager** page.

To filter by each parameter except ***Current State***, enter text into the desired filter-while-you-type field. The **Device Manager** page searches for devices that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list of devices is dynamically updated as you type. Text matches are not case-sensitive.

You can also use special characters to filter each parameter.

Filter the list by one or more of the following parameters:

- ***Device Name***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching device name.
- ***Device Hostname***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching hostname.
- ***IP Address***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching IP address.
- ***Device Category***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching device category.
- ***Device Class***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching device class.
- ***DID***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching device ID.
- ***Organization***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching organization.
- ***Current State >=.*** Specifies the device's current state. Only those devices that match all the previously selected fields and have the specified condition will be displayed. A device's condition is determined by its most severe, outstanding event. The choices are:
    - *>=Healthy*. Include devices with a condition of "Healthy" or greater. This will include all devices.
    - *>=Notice*. Include devices with a condition of "Notice" or greater. This means, include devices with a condition of "Notice", "Minor", "Major", and "Critical".
    - *>=Minor*. Include devices with a condition of "Minor" or greater. This means, include devices with a condition of "Minor", "Major", and "Critical".
    - *>=Major*. Include devices with a condition of "Major" or greater. This means, include devices with a condition of "Major" and "Critical".
    - *>=Critical*. Include devices with a condition of "Critical" or greater. This means, include devices with a condition of "Critical", because there is no "greater" condition.
- ***Collection Group***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching Collector Group.
- ***Collection State***. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching Collection State.
- ***SNMP Credential***. You can enter text to match, including special characters, and the **Device Manager**r page will display only devices that have a matching SNMP credential.

- *SNMP Version*. You can enter text to match, including special characters, and the **Device Manager** page will display only devices that have a matching SNMP version.

TIP: To return to the default list of events, select the **[Reset]** button.

Special Characters

You can include the following special characters to filter by each column except those that display date and time:

NOTE: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:

  "dell, micro" matches all values that contain the string "dell" OR the string "micro".

- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:

  "dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

  "!dell" matches all values that do not contain the string "dell".

  "!^micro" would match all values that do not start with "micro".

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!^" would match null values.

  "!$" would match null values.

  "!*" would match null values.

  "happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

  "hel*er" would match "helpers" and "helicopter" but not "hello".

  "325*" would match "325", "32561", and "325000".

  "*000" would match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

  "l?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

  "135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502"

String

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

  "^sci" would match "scientific" and "sciencelogic", but not "conscious".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!^micro" would match all values that do not start with "micro".

  "!^$" would match all values that are not null.

  "!^" would match null values.

- $ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

  "ter$" would match the string "renter" but not the string "terrific".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!$" would match null values.

NOTE: You can use both ^ and $ if you want to match an entire string and only that string. For example, "^tern$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

Numeric

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

  "1-5 "would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

  "1-" matches 1 and greater. So would match 1, 2, 6, 345, etc.

  "-5" matches 5 and less. So would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

  ">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

  "<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

  "=>7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

  "=<12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

  "=-5 " would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contains the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!0$". Matches only text that does not end with "0".
- "!^silo$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!^". Matches null values, typically represented as "--" in most pages.
- "!$". Matches null values, typically represented as "--" in most pages.

- "!^$". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*l*o$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- "!^s*i*l*o$". Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol' and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- " !silo ". Matches text that does not contain "silo".
- " !^silo$ ". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.
- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n*SAN$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

Using the Advanced Filter with the List of Devices

In the **Device Manager** page, you can specify one or more parameters to filter the display of devices. Only devices that meet all the filter criteria will be displayed.

The Advanced Filter Tool allows you to make selections instead of manually typing in a string to filter on.

TIP: To select multiple entries in the Advanced Filter Tool, hold down the **<Ctrl>** key and left-click the entries.

After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.

To reset each field and apply no filters, select the **[Reset]** button.

To access the Advanced Filter Tool:

1. Go to the **Device Manager** page.
2. Click on the funnel icon ( ).
3. The Advanced Filter Tool will display advanced filters for each column in the page.

NOTE: Unlike the "find while you type" feature, the Advanced Filter Tool is not applied to the list of devices until you select the **[Apply]** button.

4. In the Advanced Filter Tool, you can filter by one or more of the following filters.

    - ***Device Name***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Manager** page will display only devices that have a matching device name.
    - ***Device Hostname***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Manager** page will display only devices that have a matching hostname.
    - ***IP Address***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Manager** page will display only devices that have a matching IP address.
    - ***Device Category***. Select from a list of device categories that have member devices. The **Device Manager** page will display only devices that have a matching device category.
    - ***Device Class | Sub-class***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Manager** page will display only devices that have a matching device class or sub-class.
    - ***DID***. In the *From* and *To* field, you can specify a range of device IDs. The **Device Manager** page will display only devices that fall within that range of device IDs.
    - ***Organization***. Select from a list of organizations that have member devices. The **Device Manager** page will display only devices that have a matching organization.
    - ***Current State***. You can select from a list of device states. The **Device Manager** page will display only devices that have a matching state.
    - ***Collection Group***. Select from a list of collection groups that have member devices. The **Device Manager** page will display only devices that have a matching collection group.

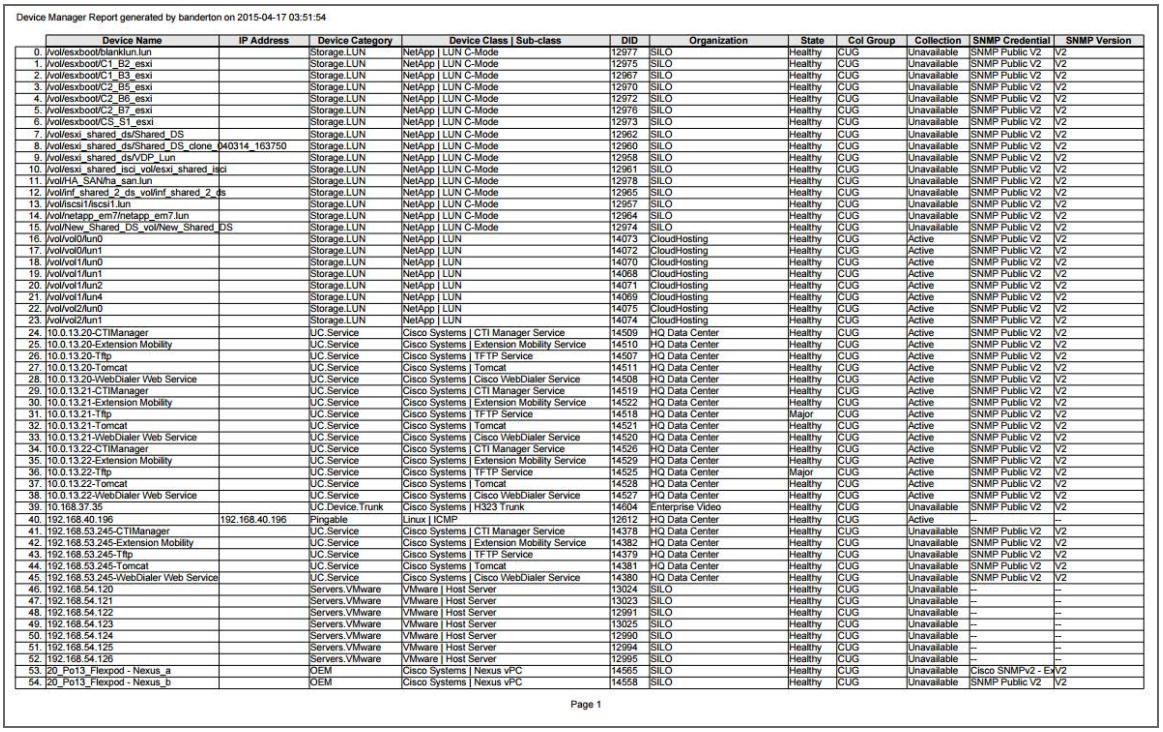
- ***Collection State***. Select from a list of collection states that have member devices. The **Device Manager** page will display only devices that have a matching collection state.
- ***SNMP Credential***. Select from a list of SNMP credentials that have member devices. The **Device Manager** page will display only devices that have a matching SNMP credential.
- ***SNMP Version***. Select from a list of SNMP versions that have member devices. The **Device Manager** page will display only devices that have a matching SNMP version.
- ***SL Agent***. Select either *Yes* or *No*. *Yes* indicates that the agent is installed on the device. *No* indicates that the agent is not installed on the device. The **Device Management** page will display only devices that either have or do not have the agent installed.

5. After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
6. To reset each field and apply no filters, select the **[Reset]** button.

TIP: You can perform an advanced filter and then perform a second advanced filter on the results of the first advanced filter. You can continue to modify and apply an advanced filter multiple times.

Generating a Report for Multiple Devices

From the **Device Manager** page (Devices > Device Manager), you can generate a report on all devices in SL1 or on multiple devices in SL1. The report will be in .xlsx format and will contain all the information displayed in the **Device Manager** page.



Device Manager Report generated by banderton on 2015-04-17 03:51:54

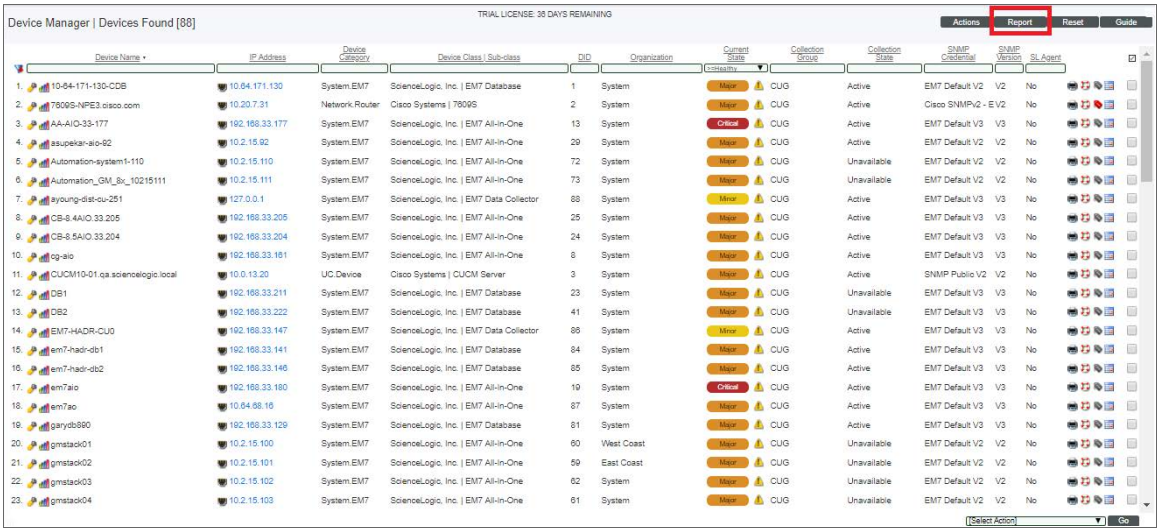
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	State	Col Group	Collection	SNMP Credential	SNMP Version
0.	/vol/esxboot/blankIun.lun		Storage.LUN	NetApp | LUN C-Mode	12977	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
1.	/vol/esxboot/C1_B2_esxi		Storage.LUN	NetApp | LUN C-Mode	12975	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
2.	/vol/esxboot/C1_B3_esxi		Storage.LUN	NetApp | LUN C-Mode	12967	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
3.	/vol/esxboot/C2_B5_esxi		Storage.LUN	NetApp | LUN C-Mode	12970	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
4.	/vol/esxboot/C2_B6_esxi		Storage.LUN	NetApp | LUN C-Mode	12972	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
5.	/vol/esxboot/C2_B7_esxi		Storage.LUN	NetApp | LUN C-Mode	12976	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
6.	/vol/esxboot/CS_S1_esxi		Storage.LUN	NetApp | LUN C-Mode	12973	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
7.	/vol/esxi_shared_ds/Shared_DS		Storage.LUN	NetApp | LUN C-Mode	12962	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
8.	/vol/esxi_shared_ds/Shared_DS_clone_040314_163750		Storage.LUN	NetApp | LUN C-Mode	12960	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
9.	/vol/esxi_shared_ds/VDP_Lun		Storage.LUN	NetApp | LUN C-Mode	12958	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
10.	/vol/esxi_shared_isci_vol/esxi_shared_isci		Storage.LUN	NetApp | LUN C-Mode	12961	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
11.	/vol/HA_SAN/ha_san.lun		Storage.LUN	NetApp | LUN C-Mode	12978	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
12.	/vol/inf_shared_2_ds_vol/inf_shared_2_ds		Storage.LUN	NetApp | LUN C-Mode	12965	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
13.	/vol/iscsi1/iscsi1.lun		Storage.LUN	NetApp | LUN C-Mode	12957	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
14.	/vol/netapp_em7/netapp_em7.lun		Storage.LUN	NetApp | LUN C-Mode	12964	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
15.	/vol/New_Shared_DS_vol/New_Shared_DS		Storage.LUN	NetApp | LUN C-Mode	12974	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
16.	/vol/vol0/lun0		Storage.LUN	NetApp | LUN	14073	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
17.	/vol/vol0/lun1		Storage.LUN	NetApp | LUN	14072	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
18.	/vol/vol1/lun0		Storage.LUN	NetApp | LUN	14070	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
19.	/vol/vol1/lun1		Storage.LUN	NetApp | LUN	14068	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
20.	/vol/vol1/lun2		Storage.LUN	NetApp | LUN	14071	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
21.	/vol/vol1/lun4		Storage.LUN	NetApp | LUN	14069	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
22.	/vol/vol2/lun0		Storage.LUN	NetApp | LUN	14075	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
23.	/vol/vol2/lun1		Storage.LUN	NetApp | LUN	14074	CloudHosting	Healthy	CUG	Active	SNMP Public V2	V2
24.	10.0.13.20-CTIManager		UC.Service	Cisco Systems | CTI Manager Service	14509	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
25.	10.0.13.20-Extension Mobility		UC.Service	Cisco Systems | Extension Mobility Service	14510	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
26.	10.0.13.20-Tftp		UC.Service	Cisco Systems | TFTP Service	14507	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
27.	10.0.13.20-Tomcat		UC.Service	Cisco Systems | Tomcat	14511	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
28.	10.0.13.20-WebDialer Web Service		UC.Service	Cisco Systems | Cisco WebDialer Service	14508	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
29.	10.0.13.21-CTIManager		UC.Service	Cisco Systems | CTI Manager Service	14519	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
30.	10.0.13.21-Extension Mobility		UC.Service	Cisco Systems | Extension Mobility Service	14522	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
31.	10.0.13.21-Tftp		UC.Service	Cisco Systems | TFTP Service	14518	HQ Data Center	Major	CUG	Active	SNMP Public V2	V2
32.	10.0.13.21-Tomcat		UC.Service	Cisco Systems | Tomcat	14521	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
33.	10.0.13.21-WebDialer Web Service		UC.Service	Cisco Systems | Cisco WebDialer Service	14520	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
34.	10.0.13.22-CTIManager		UC.Service	Cisco Systems | CTI Manager Service	14526	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
35.	10.0.13.22-Extension Mobility		UC.Service	Cisco Systems | Extension Mobility Service	14529	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
36.	10.0.13.22-Tftp		UC.Service	Cisco Systems | TFTP Service	14525	HQ Data Center	Major	CUG	Active	SNMP Public V2	V2
37.	10.0.13.22-Tomcat		UC.Service	Cisco Systems | Tomcat	14528	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
38.	10.0.13.22-WebDialer Web Service		UC.Service	Cisco Systems | Cisco WebDialer Service	14527	HQ Data Center	Healthy	CUG	Active	SNMP Public V2	V2
39.	10.168.37.35		UC.Device.Trunk	Cisco Systems | H323 Trunk	14604	Enterprise Video	Healthy	CUG	Unavailable	SNMP Public V2	V2
40.	192.168.40.196	192.168.40.196	Pingable	Linux | ICMP	12612	HQ Data Center	Healthy	CUG	Active	--	--
41.	192.168.53.245-CTIManager		UC.Service	Cisco Systems | CTI Manager Service	14378	HQ Data Center	Healthy	CUG	Unavailable	SNMP Public V2	V2
42.	192.168.53.245-Extension Mobility		UC.Service	Cisco Systems | Extension Mobility Service	14382	HQ Data Center	Healthy	CUG	Unavailable	SNMP Public V2	V2
43.	192.168.53.245-Tftp		UC.Service	Cisco Systems | TFTP Service	14379	HQ Data Center	Healthy	CUG	Unavailable	SNMP Public V2	V2
44.	192.168.53.245-Tomcat		UC.Service	Cisco Systems | Tomcat	14381	HQ Data Center	Healthy	CUG	Unavailable	SNMP Public V2	V2
45.	192.168.53.245-WebDialer Web Service		UC.Service	Cisco Systems | Cisco WebDialer Service	14380	HQ Data Center	Healthy	CUG	Unavailable	SNMP Public V2	V2
46.	192.168.54.120		Servers.VMware	VMware | Host Server	13024	SILO	Healthy	CUG	Unavailable	--	--
47.	192.168.54.121		Servers.VMware	VMware | Host Server	13023	SILO	Healthy	CUG	Unavailable	--	--
48.	192.168.54.122		Servers.VMware	VMware | Host Server	12991	SILO	Healthy	CUG	Unavailable	--	--
49.	192.168.54.123		Servers.VMware	VMware | Host Server	13025	SILO	Healthy	CUG	Unavailable	--	--
50.	192.168.54.124		Servers.VMware	VMware | Host Server	12990	SILO	Healthy	CUG	Unavailable	--	--
51.	192.168.54.125		Servers.VMware	VMware | Host Server	12994	SILO	Healthy	CUG	Unavailable	--	--
52.	192.168.54.126		Servers.VMware	VMware | Host Server	12995	SILO	Healthy	CUG	Unavailable	--	--
53.	20_Po13_Flexpod - Nexus_a		OEM	Cisco Systems | Nexus vPC	14565	SILO	Healthy	CUG	Unavailable	Cisco SNMPv2 - Ex	V2
54.	20_Po13_Flexpod - Nexus_b		OEM	Cisco Systems | Nexus vPC	14558	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2

Page 1

NOTE: If you want to include only specific devices in the report, use the "search as you type" fields at the top of each column. You can filter the list of devices by one or more column values. You can then generate the report, and only the devices displayed in the **Device Manager** page will appear in the report.

To generate a report about all or multiple devices:

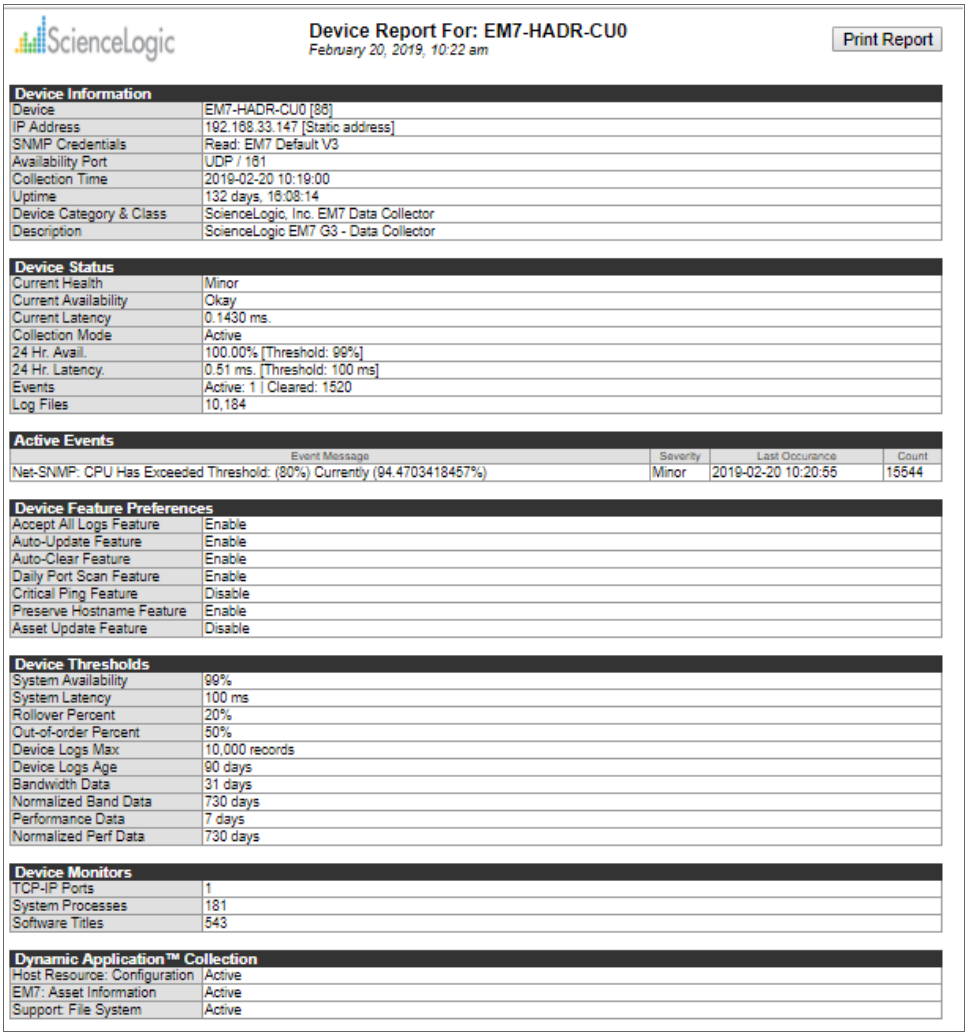
1. Log in to SL1.
2. Go to the **Device Manager** page (Devices > Device Manager).



3. If you want to filter the list of devices, use the "search as you type" fields at the top of each column. You can filter the list of devices by one or more column values.
4. Select the **[Report]** menu in the upper right.
5. When prompted, specify the output format for the report and if you want to save it to disk.

Generating a Report for a Single Device

From the **Device Manager** page (Devices > Device Manager), you can generate a detailed report on a single device. You can specify the information to include in the report (Full Report, Status, Config, Hardware, Notes, Software, Processes, Network, Events, Health) and the format in which the report will be generated (Create Report as HTML Document, Create Report as PDF Document, Create Report as MS Word Document, Create Report as MS Excel Document).



ScienceLogic

Device Report For: EM7-HADR-CU0
February 20, 2019, 10:22 am

Print Report

Device Information	
Device	EM7-HADR-CU0 [86]
IP Address	192.168.33.147 [Static address]
SNMP Credentials	Read: EM7 Default V3
Availability Port	UDP / 161
Collection Time	2019-02-20 10:19:00
Uptime	132 days, 16:08:14
Device Category & Class	ScienceLogic, Inc. EM7 Data Collector
Description	ScienceLogic EM7 G3 - Data Collector

Device Status	
Current Health	Minor
Current Availability	Okay
Current Latency	0.1430 ms.
Collection Mode	Active
24 Hr. Avail.	100.00% [Threshold: 99%]
24 Hr. Latency.	0.51 ms. [Threshold: 100 ms]
Events	Active: 1 | Cleared: 1520
Log Files	10,184

Active Events

Event Message	Severity	Last Occurance	Count
Net-SNMP: CPU Has Exceeded Threshold: (80%) Currently (94.4703418457%)	Minor	2019-02-20 10:20:55	15544

Device Feature Preferences	
Accept All Logs Feature	Enable
Auto-Update Feature	Enable
Auto-Clear Feature	Enable
Daily Port Scan Feature	Enable
Critical Ping Feature	Disable
Preserve Hostname Feature	Enable
Asset Update Feature	Disable

Device Thresholds	
System Availability	99%
System Latency	100 ms
Rollover Percent	20%
Out-of-order Percent	50%
Device Logs Max	10,000 records
Device Logs Age	90 days
Bandwidth Data	31 days
Normalized Band Data	730 days
Performance Data	7 days
Normalized Perf Data	730 days

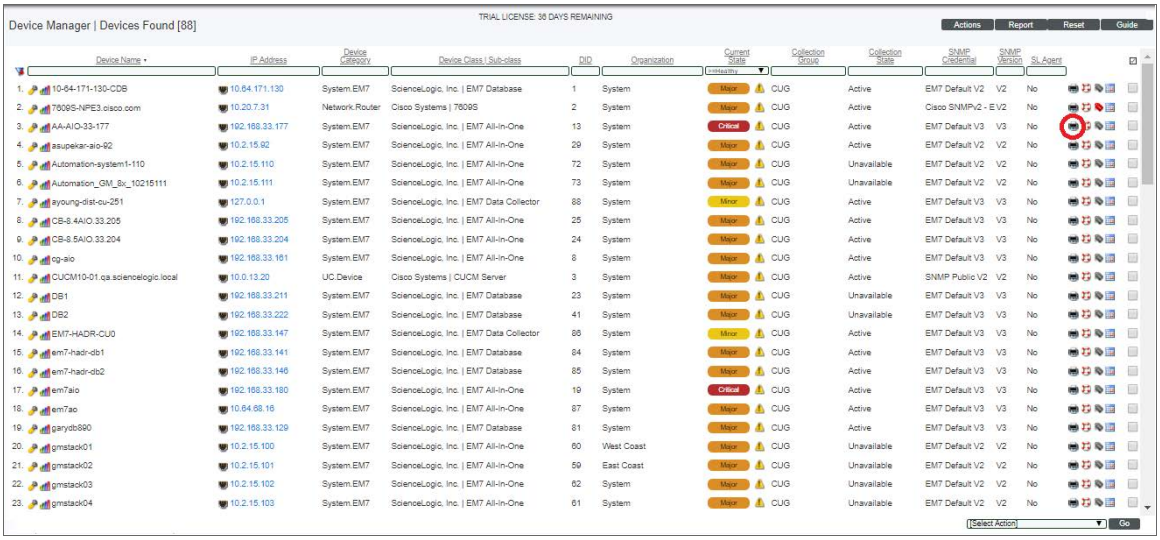
Device Monitors	
TCP-IP Ports	1
System Processes	181
Software Titles	543

Dynamic Application™ Collection	
Host Resource: Configuration	Active
EM7: Asset Information	Active
Support: File System	Active

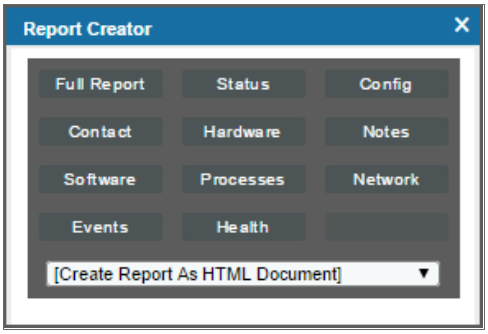
To generate a detailed report on a single device:

1. Log in to SL1.

2. Go to the **Device Manager** page (Devices > Device Manager).



3. In the **Device Manager** page, find the device for which you want to generate a detailed report. Select the printer icon ( ) for that device.
4. The **Report Creator** modal page appears. In the **Report Creator** modal page, you can specify which information to include in the device report and the format in which the report will be generated.



5. Select one of the following to specify the information to include in the device report:

   - **[Full Report]**. Includes information about device status, status of all device policies, status of all monitors, status of hardware components, status of all thresholds defined for the device, a list of all active events associated with the device, and information about the last collection time and last entry to the device log.
   - **[Status]**. Includes information about device status, status of all monitors, status of hardware components, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
   - **[Config]**. Includes status of all monitors, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.

- **[Contacts]**. Includes contact information for the device's organization and contact information for all vendors and warranty/support accounts.
- **[Hardware]**. Includes overview of hardware components for the device.
- **[Notes]**. Includes all notes created in the **Notepad Editor** page.
- **[Software]**. Displays a list of software installed on the device.
- **[Processes]**. Displays a list of all processes running on the device.
- **[Network]**. Includes information about network ports and network configuration.
- **[Events]**. Includes a list of all active events associated with the device.
- **[Health]**. Includes information about device status, status of all monitors, status of all Dynamic Applications associated with the device, status of all thresholds defined for the device, and a list of all active events associated with the device.

6. Select from the following list of formats in which the report can be generated:

   - Create Report as HTML Document
   - Create Report as PDF Document
   - Create Report as MS Word Document
   - Create Report as MS Excel Document
   - CSV - Comma Separated Values

Viewing the List of Component Devices

You can view the list of component devices from the **Device Components** page. To view the list of component devices:

1. Go to the **Device Components** page (Devices > Device Components).

2. The **Device Components** page displays the following about each device:

TIP: To sort the list of devices, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again.

- ***Plus-sign icon*** (+). Clicking on this icon expands the device and displays the children devices underneath the device. Each device that displays a plus-sign icon has children devices.
- ***Minus-sign icon*** (−). Clicking on this icon collapses the device and hides the children devices for this device. Each device that displays a minus-sign icon has children devices.
- ***Device Name***. Name of the device. For devices running SNMP, component devices, or devices with DNS entries, the name is discovered automatically. For root devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The IP address of the device. Appears only for physical devices.
- ***Device Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the as Device-Class/Sub-Class.
- ***Device-Class/Device Sub-Class***. The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during discovery, at the same time as the as Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by SL1.
- ***Organization***. The Organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. Condition can be one of the following:
    - *Critical*. Device has serious problem that requires immediate attention.

- *Major*. Device has problem that requires immediate attention.
- *Minor*. Device has less-serious problem.
- *Notice*. Device has an informational event associated with it.
- *Healthy*. Device is running with no problems.

- ***Collector Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in System > Settings > Collector Groups and specify one or more Data Collectors. A Data Collector is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups)
- ***Collection State***. Collection state can be one of the following:
  - *Active*. SL1 is currently collecting data from the device.
  - *User-Disabled*. Collection has been manually disabled for this device by a user. SL1 will not collect data from the device until a user manually re-enables collection.
  - *Unavailable*. The device is currently unavailable, so SL1 cannot collect data from the device at this time.
  - *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. SL1 cannot collect data from the device at this time.
- ***Tools***. Displays icons for managing devices. The choices are:
  - *Device Administration (* *)*: Leads to the **Device Properties** page, where you can define basic device parameters and parameters for auto-discovery. From the **Device Properties** page, you can also access the other pages in the Device Administration tools
  - *Device Management (* *)*: Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the Device Management tools.
  - *Interfaces (* *)*. Leads to the **Interfaces Found** page, where you can view details about each network interface on the device.

- *Print Report* ( ). Generates a report for the selected device. Opens the **Report Selector** modal page, where you can specify the information to include in the report (Full Report, Status, Config, Hardware, Notes, Software, Processes, Network, Events, Health) and the format in which the report will be generated (HTML Document, PDF Document, MS Word Document, MS Excel Document, CSV File).
- *Create Ticket* ( ). Leads to the **Ticket Editor** page, where you can define and file a new ticket for the device.
- *View Asset Record* ( ). This icon appears if an asset record has already been defined for the device. This icon leads to the **Asset Properties** page, where you can view the asset record for the device.
- *Create Asset Record* ( ). This icon appears if an asset record has not been defined for the device. This icon leads to the **Asset Properties** page, where you can create an asset record for the device.
- *Checkbox* ( ). Applies the action in the **[Select Action]** drop-down to the device. To select all the checkboxes, select the large red check icon.

Availability for Component Devices

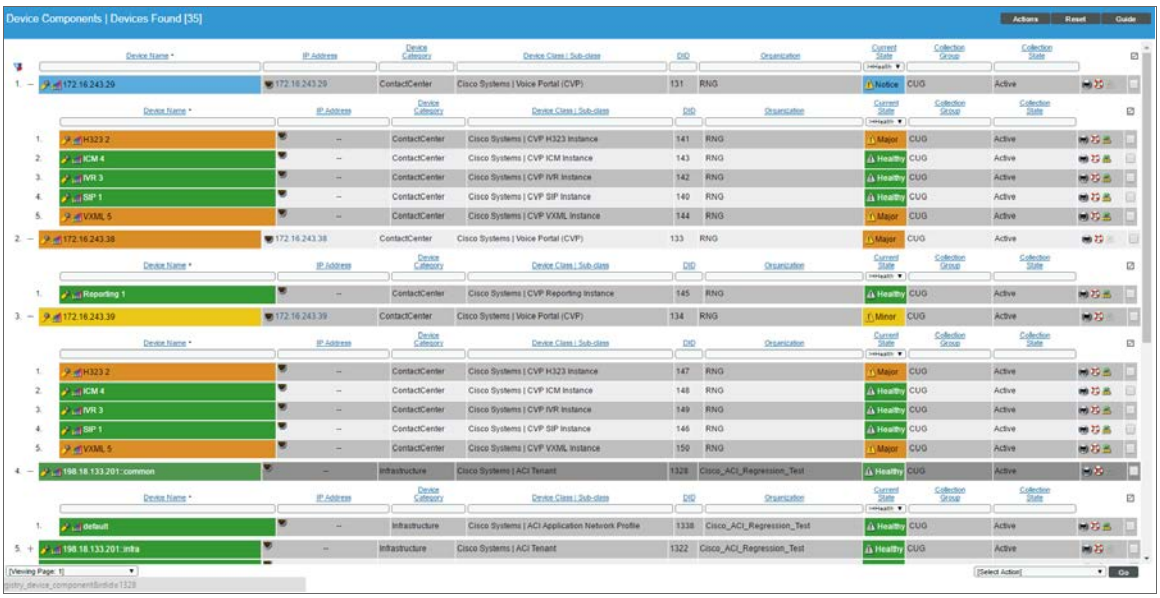
The following rules apply to the availability state for component devices:

- Component devices can use a Component Identifier to monitor availability. However, in a tree of component devices, some component devices might have a component identifier for availability and others might not. For example, suppose a component device has a component identifier for availability, and SL1 considers that component device "unavailable". All the descendents of that component device that do not have their own component identifier for availability will be considered unavailable. As soon as SL1 finds a descendent with its own component identifier for availability, SL1 stops checking that descendent and its descendents for availability. Component devices without their own component identifier for availability inherit their availability from their nearest ancestor that has a component identifier for availability.
- For trees that include merged devices, so include both hardware devices and component devices, SL1 skips over the hardware devices and allows them to use a network-based protocol to determine availability. For example, suppose you have a tree like this:
  - Grandparent device is a component device with a component identifier for availability. SL1 has determined that the grandparent device is unavailable.
  - Child device is a hardware device that uses ICMP and ping to determine availability. When SL1 evaluates the grandparent's component identifier, SL1 skips over this device. ICMP and ping determine the availability of this device.
  - Grandchild device is a component device that does not have its own component identifier for availability. When SL1 evaluates the grandparent's component identifier, SL1 assigns the grandparent's availability to this grandchild device.
- If all the hosts in a cluster are powered off or unavailable in a VMware system, both the hardware-based hosts and the associated component devices will display the value *Unavailable* in the ***Collection State*** column. When at least one host in the cluster becomes available, some or all of the associated component devices will also become available.

Viewing Children Devices

You can view component child devices of a root device in the **Device Components** page. If that child device also serves as a root device, you can also view its component child devices, and so forth. To view component children devices for root devices:

1. Go to the **Device Components** page (Devices > Device Components).
2. In the **Device Components** page, find the root device for which you want to view its component children. Select its plus sign icon (+).
3. The device will be expanded to display the component children devices below the root device.



4. You can select the plus sign icon for each component child device that also serves as a root device. To collapse the component child devices, select their minus sign icon (—).

Filtering the List of Component Devices

You can filter the list on the **Device Components** page by one or more parameters. Only component devices that meet all the filter criteria will be displayed in the **Device Components** page.

To filter by each parameter except ***Current State***, enter text into the desired filter-while-you-type field. The **Device Components** page searches for component devices that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list is dynamically updated as you type. Text matches are not case-sensitive.

You can also use special characters to filter each parameter.

Filter the list by one or more of the following parameters:

- ***Device Name***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching device name.
- ***IP Address***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching IP address.
- ***Device Category***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching device category.
- ***Device Class | Sub-Class***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching device class.
- ***DID***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching device ID.
- ***Organization***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching organization.
- ***Current State >=.*** Specifies the device's current state. Only those devices that match all the previously selected fields and have the specified condition will be displayed. A device's condition is determined by its most severe, outstanding event. The choices are:
    - >=*Healthy*. Include devices with a condition of "Healthy" or greater. This will include all devices.
    - >=*Notice*. Include devices with a condition of "Notice" or greater. This means, include devices with a condition of "Notice", "Minor", "Major", and "Critical".
    - >=*Minor*. Include devices with a condition of "Minor" or greater. This means, include devices with a condition of "Minor", "Major", and "Critical".
    - >=*Major*. Include devices with a condition of "Major" or greater. This means, include devices with a condition of "Major" and "Critical".
    - >=*Critical*. Include devices with a condition of "Critical" or greater. This means, include devices with a condition of "Critical", because there is no "greater" condition.
- ***Collection Group***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching Collector Group.
- ***Collection State***. You can enter text to match, including special characters, and the **Device Components** page will display only devices that have a matching Collection State.

TIP: To return to the default list of events, select the **[Reset]** button.

Using the Advanced Filter with the List of Component Devices

You can use the Advanced Filter tool to select one or more parameters to filter the display of devices in the **Device Components** page. Only devices that meet all the filter criteria will be displayed.

TIP: To select multiple entries in the Advanced Filter tool, hold down the <Ctrl> key and left-click the entries.

- After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
- To reset each field and apply no filters, select the Reset button.

To access the Advanced Filter tool:

1. Go to the **Device Components** page (Devices > Device Components).
2. Click on the funnel icon ( ).
3. The Advanced Filter Tool will display advanced filters for each column in the page. You can filter by one or more of the following parameters:

NOTE: Unlike the "*filter-while-you-type*" feature, the Advanced Filter tool is not applied to the list of devices until you select the ***Apply*** button

- ***Device Name***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Components** page will display only devices that have a matching device name.
- ***IP Address***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Components** page will display only devices that have a matching IP address.
- ***Device Category***. Select from a list of device categories that have member devices. The **Device Components** page will display only devices that have a matching device category.
- ***Device Class | Sub-class***. In the *Match Any* fields, you can enter one or more text strings to match, including special characters. The **Device Components** page will display only devices that have a matching device class or sub-class.
- ***DID***. In the *From* and *To* field, you can specify a range of device IDs. The **Device Components** page will display only devices that fall within that range of device IDs.
- ***Organization***. Select from a list of organizations that have member devices. The **Device Components** page will display only devices that have a matching organization.
- ***Current State***. You can select from a list of device states. The **Device Components** page will display only devices that have a matching state.
- ***Collection Group***. Select from a list of collection groups that have member devices. The **Device Components** page will display only devices that have a matching collection group.
- ***Collection State***. Select from a list of collection states that have member devices. The **Device Components** page will display only devices that have a matching collection state.

4. After selecting the desired filters, clickthe **[Apply]**button to filter the list of devices.
5. To reset each field and apply no filters, clickthe**[Reset]** button.

TIP: You can perform an advanced filter and then perform a second advanced filter on the results of the first advanced filter. You can continue to modify and apply an advanced filter multiple times.

Bulk Actions in the Device Management Page

The **Device Manager** page Devices > Device Manager) contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once.

To apply an action to multiple devices:

1. In the **Device Manager** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the red checkbox ( ) at the top of the page.

2. In the ***Select Action*** drop-down list, select one of the following actions:

   - ***Delete Devices***. Deletes all selected devices from SL1. Tickets associated with the device are unlinked from the device, but are not deleted.
   - ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device template to all selected devices. You can also make one-time changes to the template, and those changes will be applied only to the selected devices. For details on using device templates, see the manual ***Device Groups and Device Templates***.
   - ***Clear Device Logs***. Deletes data from the device's log files. For details on device logs, see the manual ***Monitoring Device Infrastructure Health***.
   - ***Create Asset Record***. Creates an asset record for each selected device. For details on asset records, see the ***Asset Management*** manual.

- ***Schedule Maintenance***. Leads to the **Maintenance Schedule** page. In this page you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, SL1 will not generate events about the selected devices. You can choose to disable or enable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate events for the devices. For details on scheduling maintenance, see the section on *Maintenance*.
- ***Find Collection Label Duplicates***. Leads to the **Duplicates** page. In this page, you can view a list of devices where the Collection Labels have more than one possible presentation object aligned. From this page, you can manually align a single presentation object with a Collection label for a device. For more information on Collection Labels, see the manual ***Monitoring Device Infrastructure Health***.
- ***Change Collection State***. Changes the status of the device in SL1. The choices are:
    - *Active*. SL1 polls the device on a regular basis and updates the data displayed in SL1.
    - *Disabled*. SL1 does not poll the device. Data displayed in SL1 is not updated.
- ***Change User Maintenance Mode***. Changes the user maintenance mode setting for the selected devices. For details on user maintenance mode, see the section on *Maintenance*.
- ***Change Collector Group***: Changes the Data Collector(s) used to collect data from the device. Choose from the list of all Collector Groups in SL1. When you select one of the collector groups, each selected device will by polled by the collectors in the collector group. This option does not appear for All-In-One Appliances. For details on collector groups and their relationships to devices, see the manual ***System Administration***.
- ***Move To Organization***: Associates a device with an organization. The list of choices will include all organizations in SL1. For details on organizations in SL1, see the manual ***Organizations and Users***.
- ***Align SNMP Read Credential***. This option applies the selected credential to all selected devices. The selected devices will use the selected credential as their primary credential. Secondary credentials will remain unchanged. Choose from a list of all SNMP Read credentials in SL1 (defined in the **Credential Management** page [System > Manage > Credentials]). For more details on Credentials, see the manual on ***Credentials and Discovery***.
- ***Add to Device Group***. This option aligns the selected devices with the selected device group. The selected devices will then appear in Device Group Views and will inherit the properties of the device group, including scheduling, access, and visibility.
- ***Align to Device Dashboard***. This option aligns the selected device dashboard with the selected device group. Choose from a list of all device dashboards in SL1 (defined in the **Device Dashboards** page [System > Customize > Device Dashboards]). For more details on Device Dashboards, see the *Device Dashboards* section.

Bulk Actions for Component Devices

The **Device Components** page (Devices > Device Components) contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once.

To apply an action to multiple devices:

1. In the **Device Components** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the red checkbox (☑) at the top of the page.
2. In the ***Select Action*** drop-down list, select one of the following actions:

    - ***Delete Selected Devices***. Deletes all selected devices from SL1. Tickets associated with the device are unlinked from the device, but are not deleted.

NOTE: To delete a root device and its associated component devices, use the option ***Delete Selected Devices (recursive)***.

- ***Delete Selected Devices (recursive)***. Deletes all selected devices from SL1. If one or more of the selected devices is a root device with one or more component devices as children, this option deletes the root device and the component devices. Tickets associated with the deleted device are unlinked from the device, but are not deleted.
- ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device templates to all selected devices. You can also make one-time changes to the template, that will be applied only to the selected devices.
- ***Clear Device Logs***. Deletes data from the device's log files.
- ***Schedule Maintenance***. Leads to the **Maintenance Schedule** page. In this page, you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, SL1 will not generate events about the selected devices. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate events for the devices.
- ***Create Asset Record***. Automatically creates an asset record for the device. SL1 automatically populates as many fields as possible, using retrieved data.
- ***Change Collection State***. Changes the status of the device in SL1. The choices are:
    - *Active*. SL1 polls the device on a regular basis and updates the data displayed in SL1.
    - *Active (recursive)*. SL1 polls the device on a regular basis and updates the data displayed in SL1. SL1 also polls all children devices (of the selected device) on a regular basis and updates their data.
    - *Disabled*. SL1 does not poll the device. Data displayed in SL1 is not updated.
    - *Disabled (recursive)*. SL1 does not poll the device. SL1 does not update data about the device. SL1 also does not poll any children devices (of the selected device) and does not update data about the children devices.
- ***Change Collector Group***. Changes the collector group used to collect data from the device. Choose from the list of all collector groups and virtual collector groups in SL1. When you select one of the collector groups, each selected device will by polled by the collectors in the collector group. For All-In-One Appliances, you can select only the built-in Collector Group and any virtual Collector Groups.
    - If you align a device with a virtual Collector Group, SL1 will store all historical data from all aligned devices, but will no longer perform collection on those devices or trigger events for these devices.

- ***Move to Organization***. Associates a device with an organization. The list of choices will include all organizations in SL1.
- ***Align SNMP Read Credential***. This option applies the selected credential to all selected devices. The selected devices will use the selected credential as their primary credential. Secondary credentials will remain unchanged. Choose from a list of all SNMP Read credentials in SL1 (defined in System > Manage > Credentials).
- ***Add to Device Group***. This option aligns the selected devices with the selected device group. The selected devices will then appear in **Device Group Views** and will inherit the properties of the device group, including scheduling, access, and visibility.

3. Select the **[Go]** button. SL1 will apply the selected option to the selected devices.

Bulk Merging and Unmerging of Devices

If your SL1 system includes a physical device and a component device, you can merge those device records into a single record for easier monitoring. Merging consolidates the devices and their data—device fields, values, graphs, behaviors, and other user interface elements—providing you with a single set of data for the device. Additionally, merged devices consume only a single device license.

Merging does not remove, replace, or add any data; merging simply groups data together. When you merge a physical device and a component device, the device record for the component device no longer displays in the user interface, while the device record for the physical device displays in user interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the record for the physical device.

Merged devices can be unmerged back into individual device records, if needed.

The **Device Manager** page (Devices > Device Manager) contains options for the bulk merging or unmerging of multiple pairs of physical and component devices. These features are convenient if you have a large number of devices you want to merge or unmerge in a single session.

NOTE: You can merge only two individual devices together into a single merged device. To do so, you must have user permissions that allow merging and unmerging on both devices.

NOTE: When you merge devices, active events associated with the component device will be set to "cleared." The cleared events will not be associated with the physical device. If the devices are unmerged, the cleared events cannot be moved back to the component device.

CAUTION: Merging devices also merges the log data from each device. The log data cannot later be unmerged.

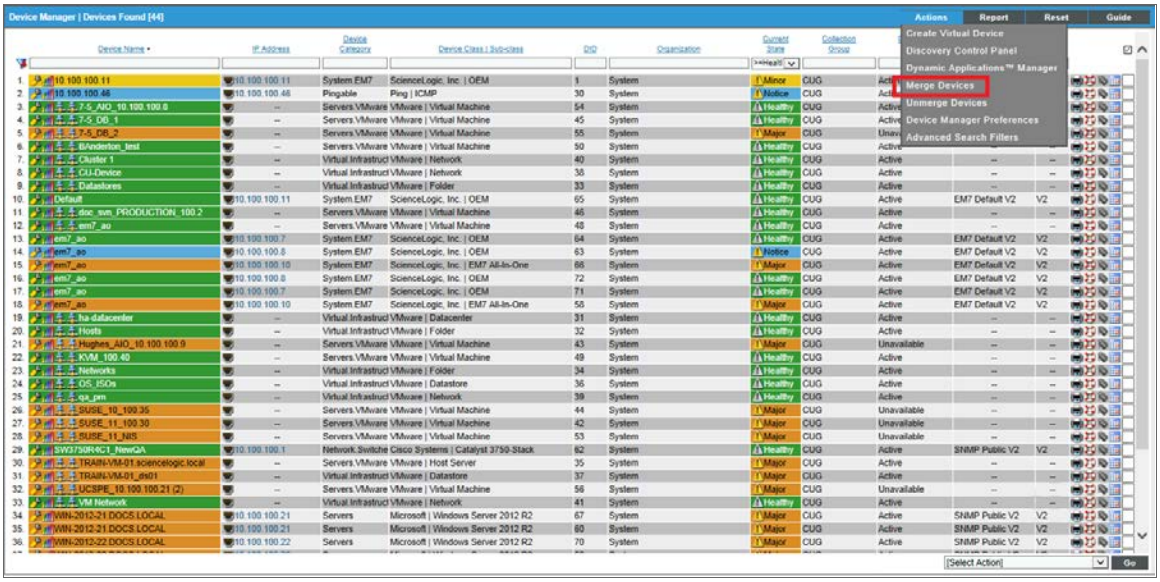
Performing a Bulk Device Merge

If you have a large number of devices to merge, you can perform a bulk device merge, which is more efficient than merging device pairs individually. A bulk device merge enables you to select from multiple pairs of devices—particularly those with matching IP addresses or device names—and choose the pairs to merge.

NOTE: If you have a small number of physical and component devices that you want to merge, you can merge each pair individually. For more information, see the *Merging Individual Devices* section.

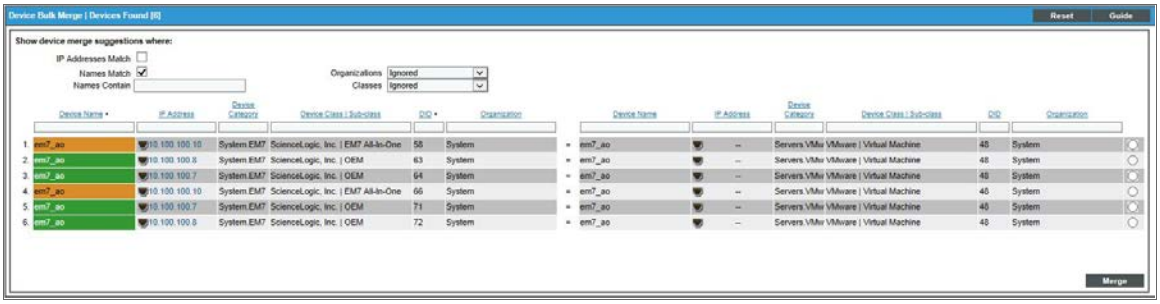
To perform a bulk device merge:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Select the **[Actions]** menu and then choose ***Merge Devices***.



TIP: Because of the potentially large number of devices that could be merged, no results display when the **Device Bulk Merge** page initially displays. You must select one of the checkboxes or begin typing a name in the ***Names Contain*** field for results to display on the page.

3. On the **Device Bulk Merge** page:



- Select the ***IP Addresses Match*** checkbox if you want the page to display a list of devices where the physical device and the component device a have matching IP addresses.
- Select the ***Names Match*** checkbox if you want the page to display a list of devices where the physical device and the component device have matching Device Names.
- If you want the page to display a list of devices that could be merged where the Device Names of the physical device and the component device contain the same character(s), enter those characters in the ***Names Contain*** field.
- In the ***Organizations*** field:
  - Select *Ignored* if you do not want to filter the list of devices based on the Organizations assigned to the physical device and the component device.
  - Select *Match* if you want to filter the list of devices to include only physical devices and component devices that have matching Organizations.
  - Select *Don't Match* if want to filter the list of devices to include only physical devices and component devices that do not have matching Organizations.
- In the ***Classes*** field:
  - Select *Ignored* if you do not want to filter the list of devices based on the Device Classes assigned to the physical device and the component device.
  - Select *Match* if you want to filter the list of devices to include only physical devices and component devices that are assigned matching Device Classes.
  - Select *Don't Match* if you want to filter the list of devices to include only physical devices and component devices that are assigned non-matching Device Classes.

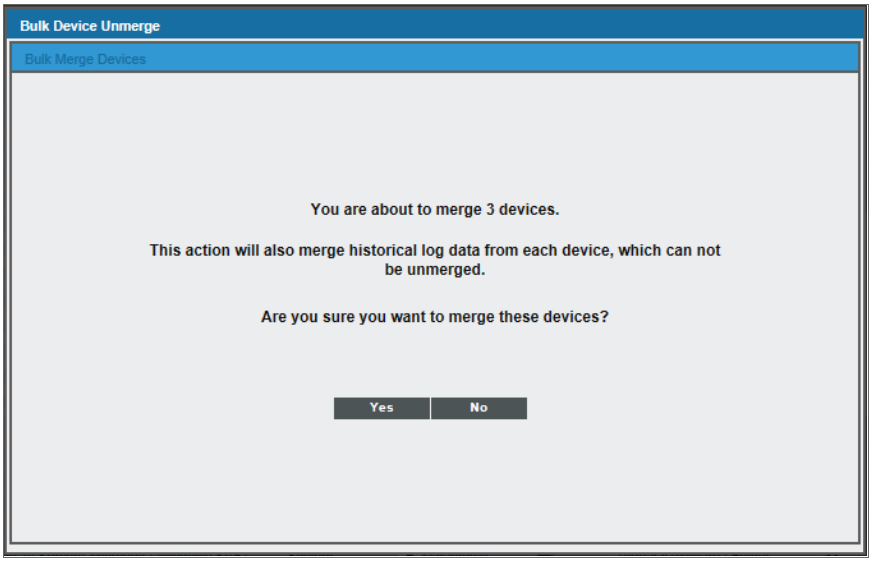
NOTE: You can make selections in the ***Organizations*** and ***Classes*** fields only after you make a selection or entry in the ***IP Addresses Match***, ***Names Match***, and/or ***Names Contain*** fields.

The **Device Bulk Merge**page displays a list of physical device and component device pairs that match your search criteria. Each numbered row indicates a pair of devices that could be merged.

4. Select the radio button(s) in the last column of each row of device pairs that you want to merge, then select the **[Merge]** button. The radio buttons are grouped per physical device, i.e., you can select only one row for each physical device.

NOTE: You can select each component device only once for merging. If you attempt to select the same component device in multiple rows, you will receive an error message when you select the **[Merge]** button.

5. A modal window displays that asks you to confirm the merge. Select the **[Yes]** button.



6. SL1 begins merging the selected devices. When the message, "Device Bulk Merge complete" displays, select the **[Close/Esc]** button.

NOTE: To view an updated list of devices that includes your merged devices, select the **[Reset]** button on the **Device Manager** page.

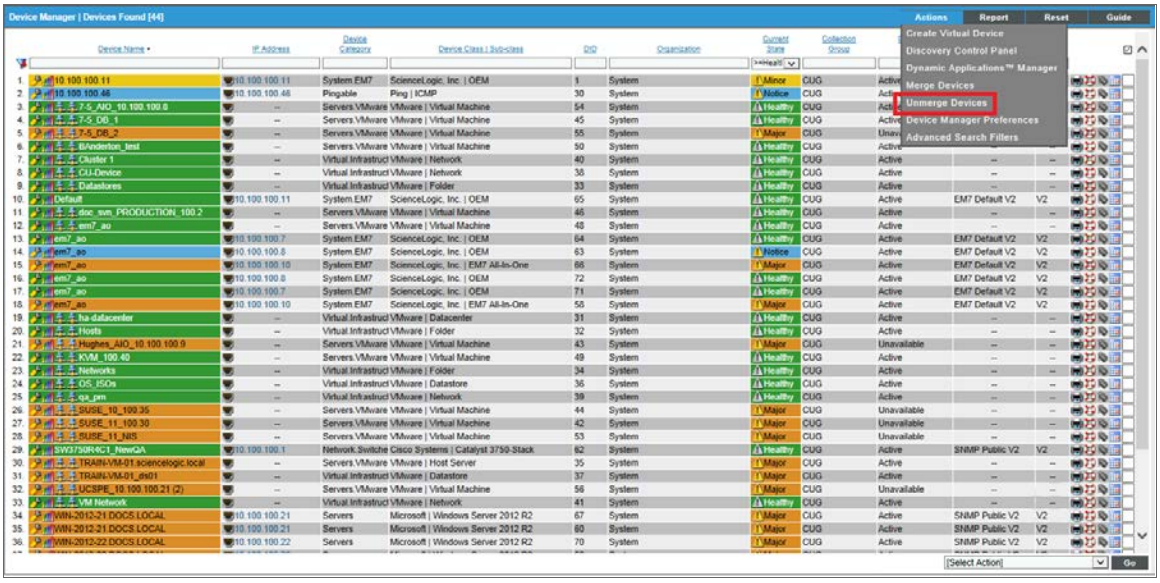
Performing a Bulk Device Unmerge

If you have a large number of devices to unmerge, you can perform a bulk device unmerge, which is more efficient than unmerging device pairs individually. A bulk device unmerge enables you to view a list of merged devices and select all of the devices you want to unmerge.

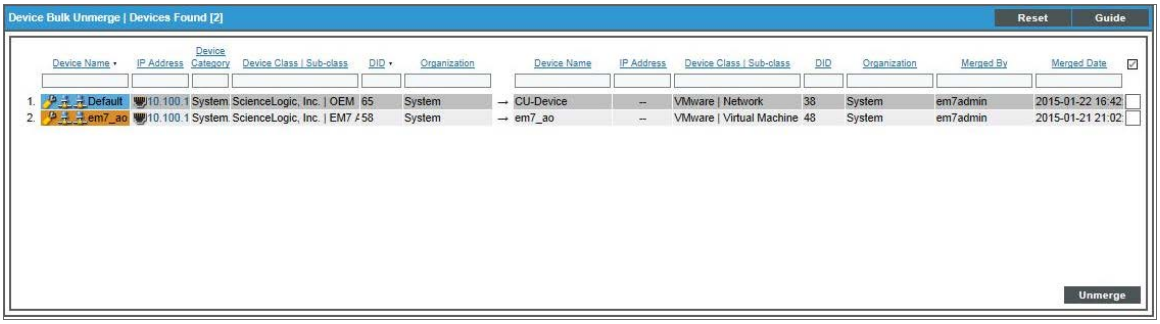
NOTE: If you have a small number of devices that you want to unmerge, you can unmerge each pair individually. For more information, see the *Unmerging Individual Devices* section.

To unmerge multiple devices:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Select the **[Actions]** menu and then choose ***Unmerge Devices***.



3. The **Device Bulk Unmerge** page displays a list of merged devices. Each numbered row indicates a pair of merged devices that can be unmerged. Select the checkboxes in the last column of each row of devices that you want to unmerge, then select the **[Unmerge]** button.



4. A modal window displays that asks you to confirm the unmerging. Select the **[Unmerge]** button.

5. When the message, "Device Bulk Unmerge complete" displays, select the **[Close/Esc]** button.

NOTE: To view an updated list of devices that includes your unmerged devices, select the **[Reset]** button on the **Device Manager** page.

Chapter 4

Device Relationships

Overview

This chapter describes device relationships in SL1.

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

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

This chapter includes the following topics:

What are Device Relationships? *101*
Viewing the List of Device Relationships *101*
Filtering the List of Device Relationships *104*
Viewing a Relationship for a Single Device *105*
The Device View Page *107*
Event Correlation *108*
Defining Device Relationships *108*
Device Categories that Don't Support Parent-Child Devices *110*
Events that May Not Be Displayed in the Events Page *111*
Defining Event Correlation *111*
Layer-2 Topology Collection *114*
CDP Topology Collection *115*
LLDP Topology Collection *116*

Layer-3 Topology Collection *118*

What are Device Relationships?

SL1 automatically defines parent and child relationships for certain devices. Users can also manually define some types of relationships. Devices can have the following types of relationships:

- Layer-2 devices and their clients. Layer-2 relationships are automatically discovered by SL1 and can be created in the **Subnet Map (L2)** page (Views > Topology Maps > Layer-2).
- Layer-3 devices and layer-2 devices. Layer-3 relationships are automatically discovered by SL1 and can be created in the **Layer 3 Map** page (Views > Topology Maps > Layer-3).
- Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in the CDP tables. CDP relationships are automatically discovered by SL1 and can be created in the **Subnet Map (CDP)** page (Views > Topology Maps > CDP).
- Network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in the LLDP tables. LLDP relationships are automatically discovered by SL1 and can be created in the **Views > Topology Maps > LLDP** page (Views > Topology Maps > LLDP).
- Component devices and their parent devices using Dynamic Application data. For example, virtual machines and their hypervisors.
- Device relationships between root devices, parent devices, and component devices (Component Mapping).
- Device relationships created using Dynamic Application data. For example, the Dynamic Applications in the VMware vSphere and NetApp PowerPacks are configured to create relationships between VMware Datastore component devices and their associated NetApp Volume component devices.
- Generic parent-child relationships, sometimes referred to as Event Correlation relationships or Ad-Hoc relationships, can be manually created. These relationships can be created in the **Device Children** page for the parent device.

NOTE: SL1 also automatically discovers relationships between VMWare hypervisors and VMWare virtual machines using SNMP data, but ***only for legacy versions VMWare ESX 3.5 and VMWare ESX 4.x***.

All device relationships are displayed as child and parent relationships. For example:

- A layer-2 switch is a parent device and a firewall attached to the switch is a child device.
- A layer-3 router is a parent device and a layer-2 switch attached to the router is a child device.
- A VMware ESX server is a parent device and a Linux VM on that server is a child device.

Viewing the List of Device Relationships

The **Device Relationships** page displays information about every parent-child relationship that has been automatically created by SL1 or manually defined by a user.

For each child device, the **Device Relationships** page displays at least the MAC address of the child interface and, if possible, the device name of the child device, the IP address associated with the child interface, the name of the child interface, and the manufacturer of the child interface.

For each parent device, the **Device Relationships** page displays the device name, the name of the parent interface, the MAC address of the parent interface, and the manufacturer of the parent interface.

For example, suppose a switch has been discovered by SL1. Suppose that 12 interfaces on that switch are in use. Suppose that only three of those 12 interfaces are connected to child interfaces that have been discovered by SL1. The **Device Relationships** page will display whatever ARP information SL1 can retrieve about the remaining nine child interfaces. In most cases, SL1 can retrieve the MAC address and manufacturer associated with the child interface, even if the child interface has not been discovered by SL1.

The relationships in the **Device Relationships** page are dynamically updated. If SL1 discovers a new relationship, SL1 updates the **Device Relationships** page.

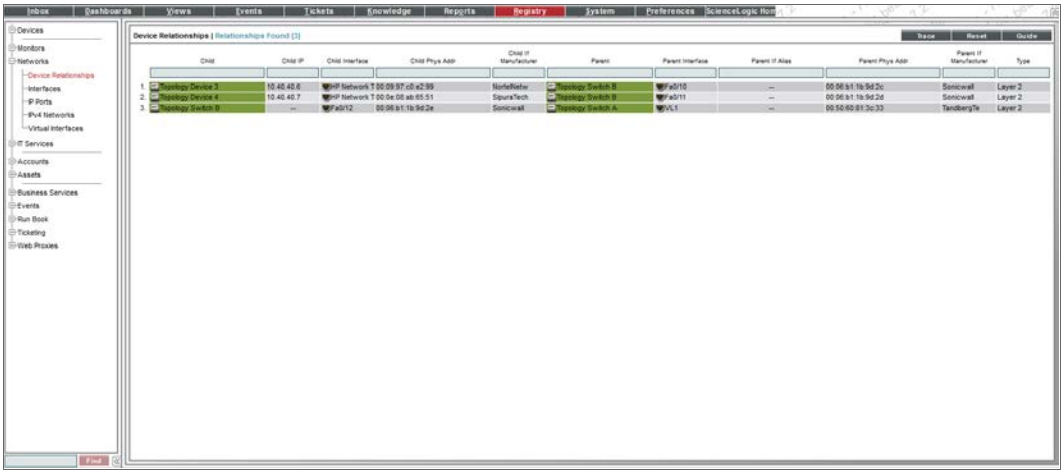
You can view information for each parent-child relationship between two devices managed by SL1 or for a single parent device managed by SL1 and an unknown child device. To view information on **Device Relationships**:

1. Go to the **Device Relationships** page (Registry > Networks > Device Relationships).

2. The **Device Relationships** page displays the following information:

TIP: You can sort the list of user device relationships by column. To sort by ascending column value, click on a column heading. To sort by descending column value, click on the same column heading a second time.

NOTE: The **Device Relationships** page respects multi-tenancy rules. This means that you can view relationships in this page only if both devices are aligned with an organization of which you are a member.



- ***Child***. If the child device has been discovered by SL1, this column contains the name of the device and a link to the **Device Relationships** page for the child device.
- ***Child IP***. If the child device has been discovered by SL1, this column contains the IP address through which the child communicates with the parent device.
- ***Child Interface***. If the child device has been discovered by SL1, this column contains the name of the interface through which the child device communicates with the parent device and a link to the **Interfaces Found** page for the child interface.
- ***Child Phys Addr***. The physical address (MAC address) for the interface through which the child device communicates with the parent device.
- ***Child IF Manufacturer***. If included in the MAC address, the manufacturer of the child interface.
- ***Parent***. The name of the parent device and a link to the **Device Relationships** page for the parent device.
- ***Parent Interface***.The name of the interface through which the parent device communicates with the child device and a link to the **Interfaces Found** page for the parent interface.
- ***Parent IF Alias***. Easy-to-remember, human-readable name for the interface on the parent device.
- ***Parent Phys Addr***. The physical address (MAC address) for the interface through which the parent

device communicates with the child device.

- ***Parent IF Manufacturer***. If included in the MAC address, the manufacturer of the parent interface.
- ***Type***. Describes the relationship between the parent device and child device. Possible values are:
  - CDP
  - LLDP
  - Component Mapping
  - Component Relationship
  - Event Correlation
  - Layer-2
  - Layer-3
  - VMware

Filtering the List of Device Relationships

You can filter the list on the **Device Relationships** page by one or more parameters. Only device relationships that meet all the filter criteria will be displayed in the **Device Relationships** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Device Relationships** page searches for device relationships that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list is dynamically updated as you type. Text matches are not case-sensitive.

You can also use special characters to filter each parameter.

Filter by one or more of the following parameters:

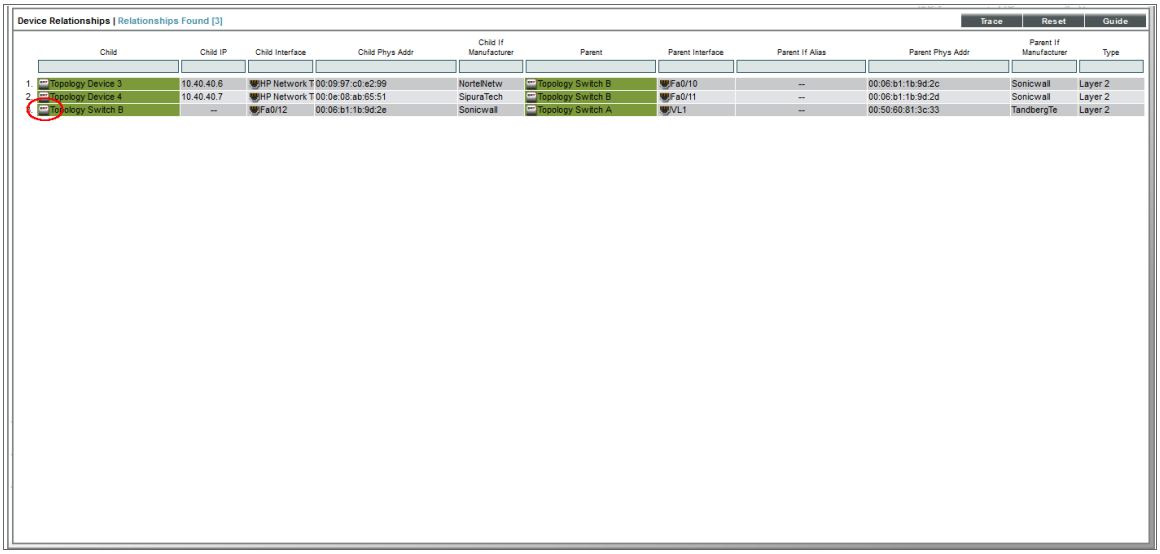
- ***Child***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching device name on the child device.
- ***Child IP***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching IP address on the child interface.
- ***Child Interface***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching name on the child interface.
- ***Child Phys Addr***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching MAC address on the child interface.
- ***Child IF Manufacturer***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching manufacturer for the child interface.
- ***Parent***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a device name on the parent device.

- ***Parent Interface***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching name on the parent interface.
- ***Parent IF Alias***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching IF alias on the parent interface.
- ***Parent Phys Addr***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching MAC address on the parent interface.
- ***Parent IF Manufacturer***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching manufacturer for the parent interface.
- ***Type***. You can enter text to match, including special characters, and the **Device Relationships** page will display only device relationships that have a matching type.

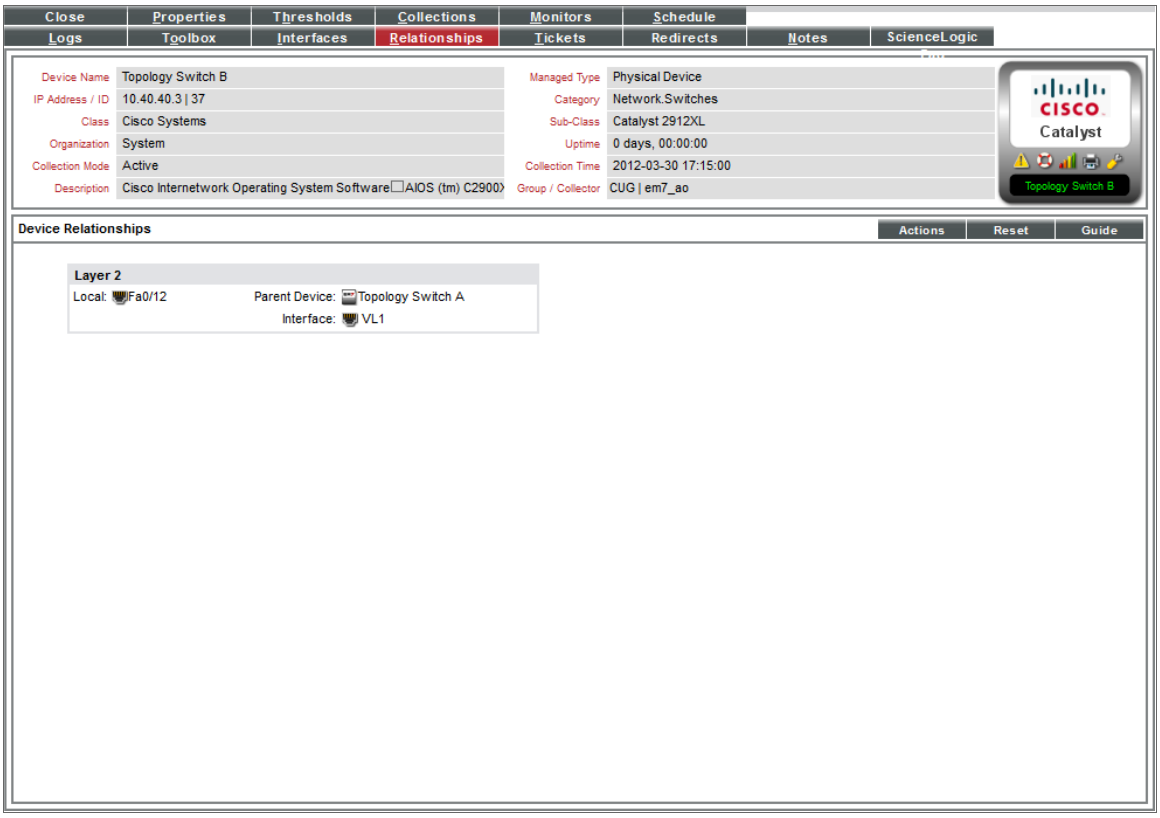
Viewing a Relationship for a Single Device

You can view all links for a single device in the **Device Relationships** page, in the **Device Properties** panel. To view all links for a single device:

1. Go to the **Device Relationships** page (Registry > Networks > Device Relationships) and click the Device Properties icon ( ) for the device you want to see relationships. If a link has been defined on a device, you can also go to the **Device Manager** page (Devices > Device Manager), click the wrench icon for a device ( ) and click the **[Relationships]** tab in the **Device Properties** pane.



2. The **Device Relationships** page appears. The left pane of the **Device Relationships** page displays links to parent devices. The right pane of the **Device Relationships** page displays links to child devices. For each relationship, the **Device Relationships** page displays the following information:



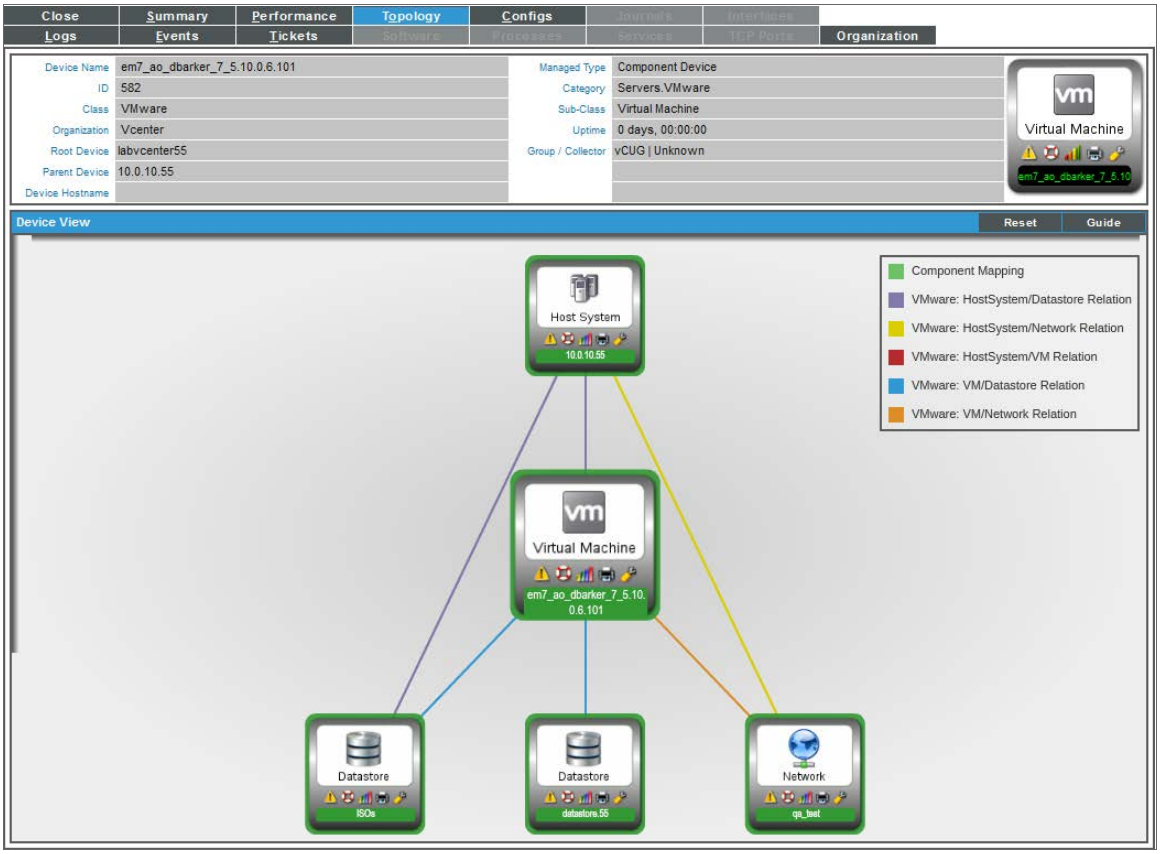
- ***Type of relationship***. Possible values are:
  - *Layer 2*. Layer-2 devices and their clients.
  - *Layer 3*. Layer-3 devices and layer-2 devices.
  - *VMware*. Hypervisors and their virtual machines.
  - *CDP*. Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables.
  - *LLDP*. Network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables.
  - *Event Correlation*. Relationships defined manually by users through the user interface.
  - *Component Mapping*. Relationships defined using Dynamic Applications.
- ***Child Interface***. Name of the interface through which the child device communicates with the parent device and a link to the **Interfaces Found** page for the child interface.
- ***Parent Device***. The name of the parent device and a link to the **Device Properties** page for the parent device.

- ***Parent Interface***. The name of the interface through which the parent device communicates with the child device and a link to the **Interfaces Found** page for the parent interface.

NOTE: Clicking on a device reloads the **Device Relationships** page and makes the selected device the primary device.

The Device View Page

The **Device View** page appears when a user clicks the **Topology** tab in the Device Reports panel. The **Device View** page displays a map of the device and all of the devices with which the device has relationships.



These relationships include:

- Layer-2 devices and their clients
- Layer-3 devices and Layer-2 devices
- Component devices and their parent devices. For example, virtual machines and their hypervisors and their virtual machines.

- Network devices that use CDP (Cisco Delivery Protocol) and devices that are specified as neighbors in CDP tables
- Links between network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables
- Network devices that use LLDP (Link Layer Delivery Protocol) and devices that are specified as neighbors in LLDP tables
- Links between network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables
- Device relationships between root devices, parent devices, and component devices (Component Mapping)
- Device relationships created with Dynamic Applications
- Manually created parent-child relationships that affect event correlation

NOTE: Double-clicking on a device reloads the **Device View** page and makes the selected device the primary device.

For details on the toolbars that appear in this page, see the ***Views*** manual.

Event Correlation

In SL1, event correlation means the ability to build parent-child relationships between devices and their events. When events are correlated, only the parent event is displayed in the **Events** page.

- In the **Events** page, the child events are rolled up and nested under the parent event and are displayed only if you click on the magnifying-glass icon ( ).
- For the parent event, the ***Count*** column will be incremented to indicate the number of correlated child events.

For details on event correlation, see the manual titled ***Events***.

Defining Device Relationships

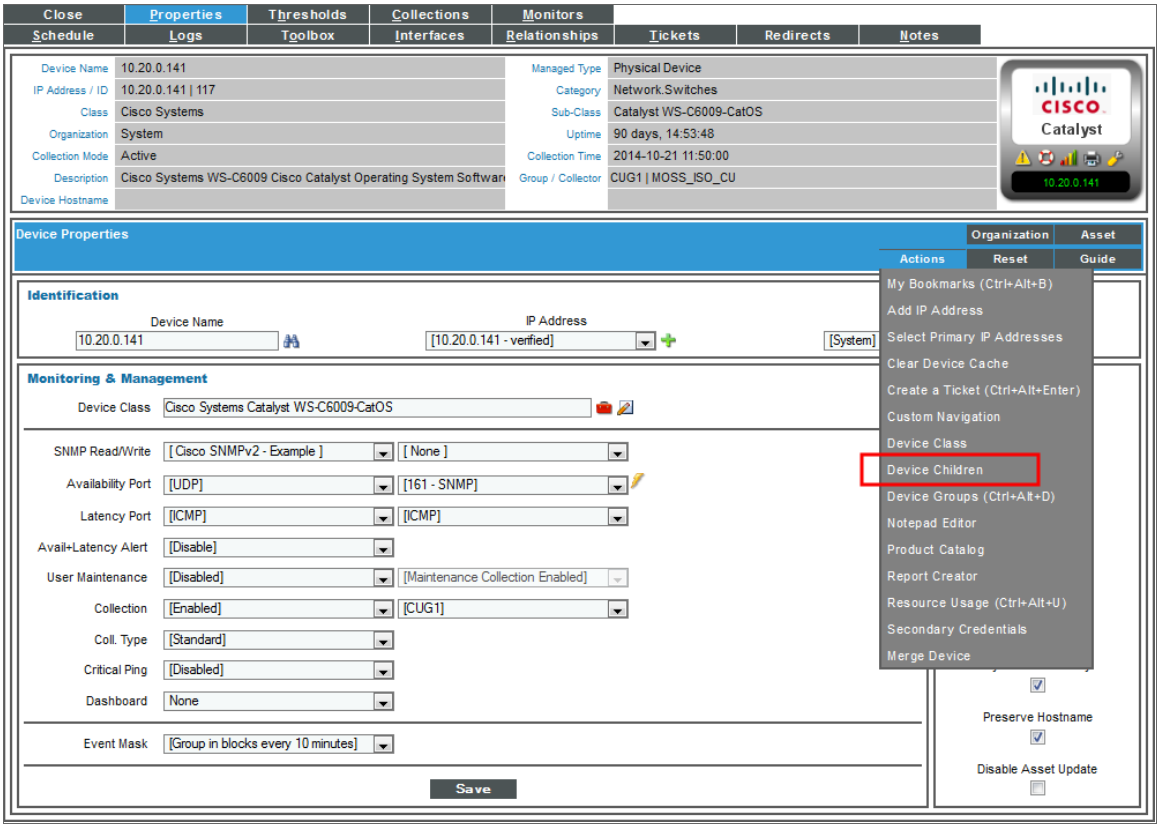
The **Device Children** modal page allows users to select one or more devices to become children of the currently selected device.

To add children to a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to add children devices. Select the wrench icon ( )for that device.

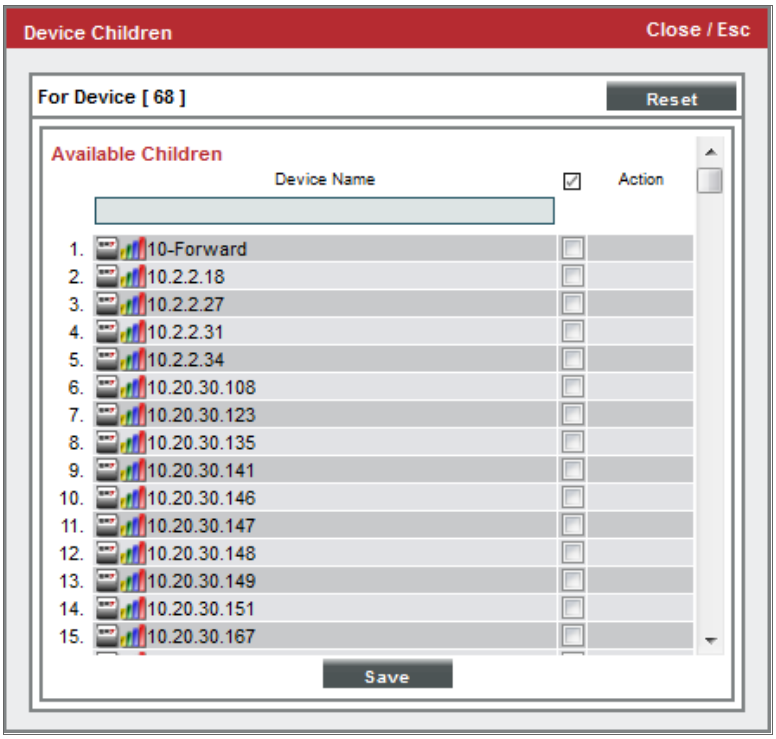
3. The **Device Properties** page appears:

> **NOTE**: You cannot create parent-child relationships for devices with a **Device Category** of *Virtual*.



4. In the **Device Properties** page, select the **[Actions]** menu. From the list of options, select *Device Children*.

5. The **Device Children** modal page appears.



6. In the **Device Children** page, select one or more devices to be children of the current device.
7. Select the **[Save]**button.

Device Categories that Don't Support Parent-Child Devices

A device category is a logical categorization of a device by primary function. SL1 uses device categories to group related devices in reports and views.

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

Devices that are members of the following device categories cannot be assigned children devices:

- Office Printers, Device Category #4
- Workstations, Device Category #6
- Environmental.Utility, Device Category #8
- Environmental.HVAC, Device Category #9
- Environmental.Security, Device Category #10
- System.Tape, Device Category #17

- Office.Copiers, Device Category #22
- Office.Facsimiles, Device Category #23
- Telephony.Phone, Device Category #36
- Office.Plotter, Device Category #40
- Pingable, Device Category #98
- Virtual, Device Category #97

To determine a device's device category, look in the *Category* field in any page in the **Device Administration** or **Device Management** pages.

Events that May Not Be Displayed in the Events Page

In SL1, there are four types of events that might not be displayed in the **Events** page:

- ***Rolled-up events***. Multiple occurrences of the same event on the same device. When the same event occurs multiple times on a single device, SL1 does not display each occurrence in the **Events** page. Instead, SL1 displays a single entry and notes the number of occurrences in the ***Count*** column.
- ***Suppressed Events***. Suppressed events do not appear in the **Events** page.
- ***Topology Events***. In SL1, event correlation or topology suppression means the ability to build parent-child relationships between devices and between events. When events are correlated, only the parent event is displayed in the **Events** page. The magnifying-glass icon ( ) appears to the left of the parent event. When you click on the magnifying-glass icon, the list of child events is displayed. The child events are rolled up under the parent event and are not displayed in the **Events** page. For the parent event, the count column will be incremented to indicate the number of correlated child events. Optionally, you can define event categories that allow SL1 to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event will be correlated with only events that are aligned with the same event category.
- ***Event Masks***. In the **Device Properties** page for each device, you can define an Event Mask. When a device uses the Event Mask setting, events that occur on a single device within a specified span of time are grouped together. In the **Events** page, masked events are displayed under a single event, the one with the highest severity. The magnifying-glass icon ( ) appears to the left of the event. When you click on the magnifying-glass icon, the list of all events that are masked under event is displayed.

Defining Event Correlation

To manually configure event correlation in the classic SL1 user interface, you must define two types of events:

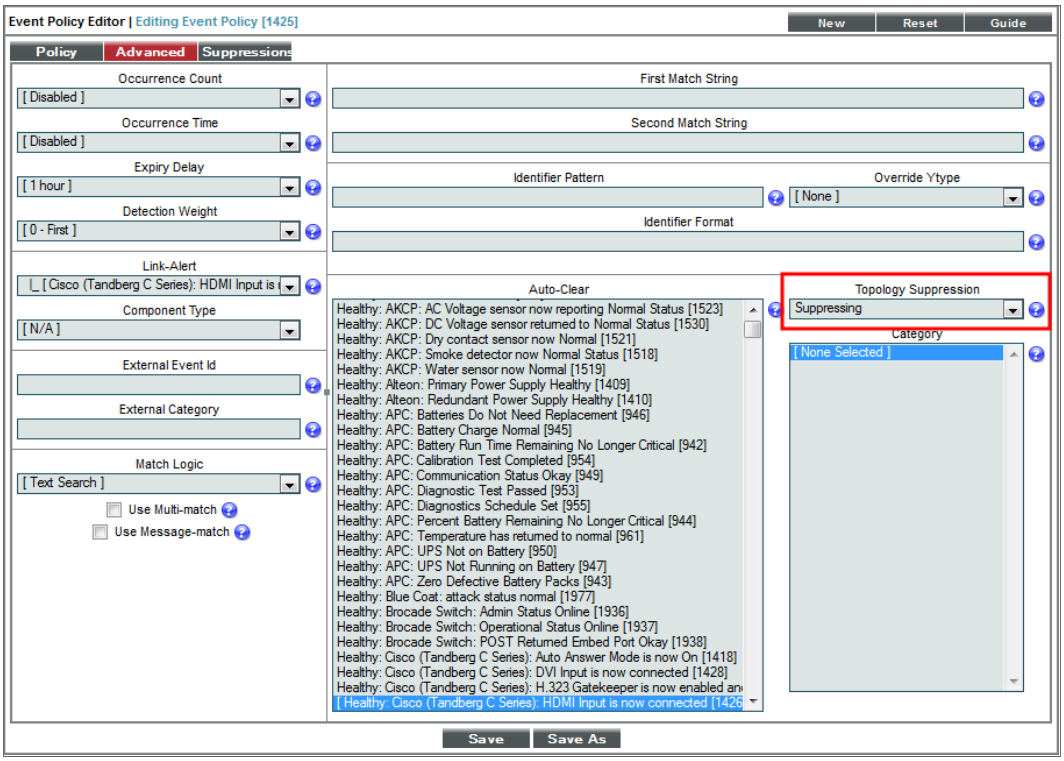
- ***Suppressing events***. If this event occurs on a parent device, SL1 will search all related children devices for ***suppressible*** events. On the children devices, all suppressible events will be suppressed. Only the suppressing event will appear in the **Events** page (or the **Event Console** page in the classic SL1 user interface) . The suppressible events will not appear in the **Events** page (or the **Event Console** page in the classic SL1 user interface) .

- ***Suppressible events***. This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

> **NOTE**: If you configure event categories, the suppressing and suppressible events must be associated with the same category for correlation to occur. If you do not configure event categories, each and every suppressing event that occurs on a parent device will cause SL1 to suppress **all suppressible** events on the associated children devices.

To define an event as a suppressing event on the **Event Policy Manager** page in the classic SL1 user interface):

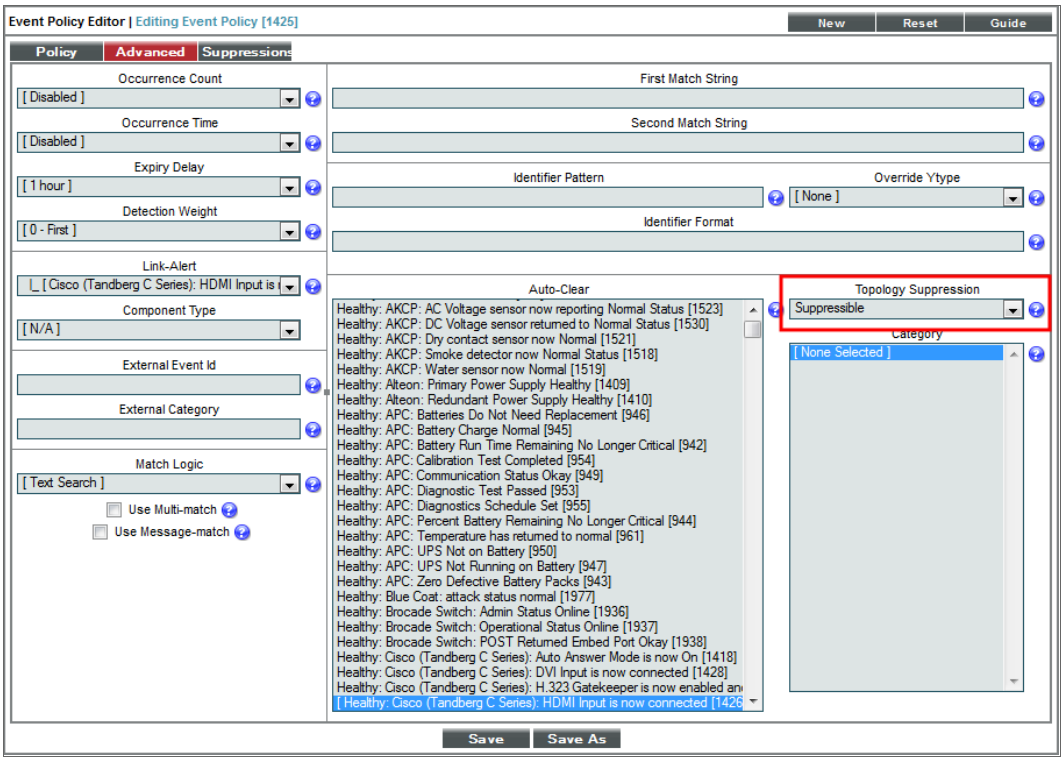
1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager.
2. On the **Event Policy Manager** page, click the wrench icon ( ) of the event that you want to define as the ***suppressing*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.



4. In the ***Topology Suppression*** field, select *Suppressing*.
5. Click **[Save]**. In the future, when this event occurs on a device, SL1 will check if the device is a parent device. If the device is a parent device, specified events (suppressible events) with the same category will be suppressed on the children devices.

To define an event as a suppressible event on the **Event Policy Manager** page in the classic SL1 user interface:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page , click the wrench icon ( ) of the event that you want to define as the ***Suppressible*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.



4. In the ***Topology Suppression*** field, select *Suppressible*.
5. Click **[Save]**. In the future, when this event occurs on a device, SL1 will check if the device is a child device. If the device is a child device, SL1 will check to see if a suppressing event with the same category has occurred on the parent device. If a suppressing event has occurred on the parent device, the specified event will be suppressed on the child device.

For example:

- Suppose you have a device named *Boise-DMZ*. Suppose this device is a Cisco Catalyst switch. Suppose we define this switch as a parent device.
- Suppose we have a device named *HQ-W2K3-VC01*. Suppose this device is a server. Suppose we define this server as a child device to *Boise-DMZ*.
- Suppose we define the event "Poller: Interface operationally down" as a suppressing event.
- Suppose we define the event "Poller: Device not responding" as a suppressible event.
- Suppose we associate both events with the same event category.

- If an interface goes down on the switch *Boise-DMZ*, SL1 will not be able to communicate with the server, *HQ-W2K3-VC01*, attached to the switch.
- So if the event "Poller: Interface operationally down" occurs on *Boise-DMZ*, the event "Poller: Device not responding" will be suppressed on the server *HQ-W2K3-VC01*. On the **Events** page (or the **Event Console** page in the classic SL1 user interface) , only the event "Poller: Interface operationally down" on the device *Boise-DMZ* will appear.

Layer-2 Topology Collection

A layer-2 topology record describes a direct network connection between a parent device (a Network Switch or Network Bridge) and a child device. The child device is either:

- Another bridge device discovered in SL1
- Another type of device that is discovered in SL1
- A device that is not discovered in SL1

Every hour, SL1 collects information from the Bridge-MIB from all discovered network switches and bridges. Network switches and bridges that support the Bridge-MIB report information about all MAC addresses for which that network switch or bridge has forwarding information.

During collection, SL1 performs the following steps:

- Compiles a list of all devices to poll. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Bridges" (ID 19). The ***Device Category*** is defined in the Device Class assigned to the device.
- If the ***Enable Community String Indexing (VLAN Topology)*** checkbox is selected in the **Behavior Settings** page (System > Settings > Behavior), SL1 compiles a list of vLANs for which data should be collected using the CISCO-VTP-MIB. A vLAN is added to the list of vLANs only if the vLAN state is 1 (operational) and the vLAN type is 1 (ethernet). If the ***Enable Community String Indexing (VLAN Topology)*** option is disabled, SL1 performs collection for vLAN 1 only.
- For each vLAN on each device, SL1 polls the Bridge-MIB to collect the list of all MAC addresses for which that network switch or bridge has forwarding information.
- SL1 stores a MAC address record if:
    - The status of the record is "3" (learned).
    - An ifIndex value was collected successfully for the associated port index.

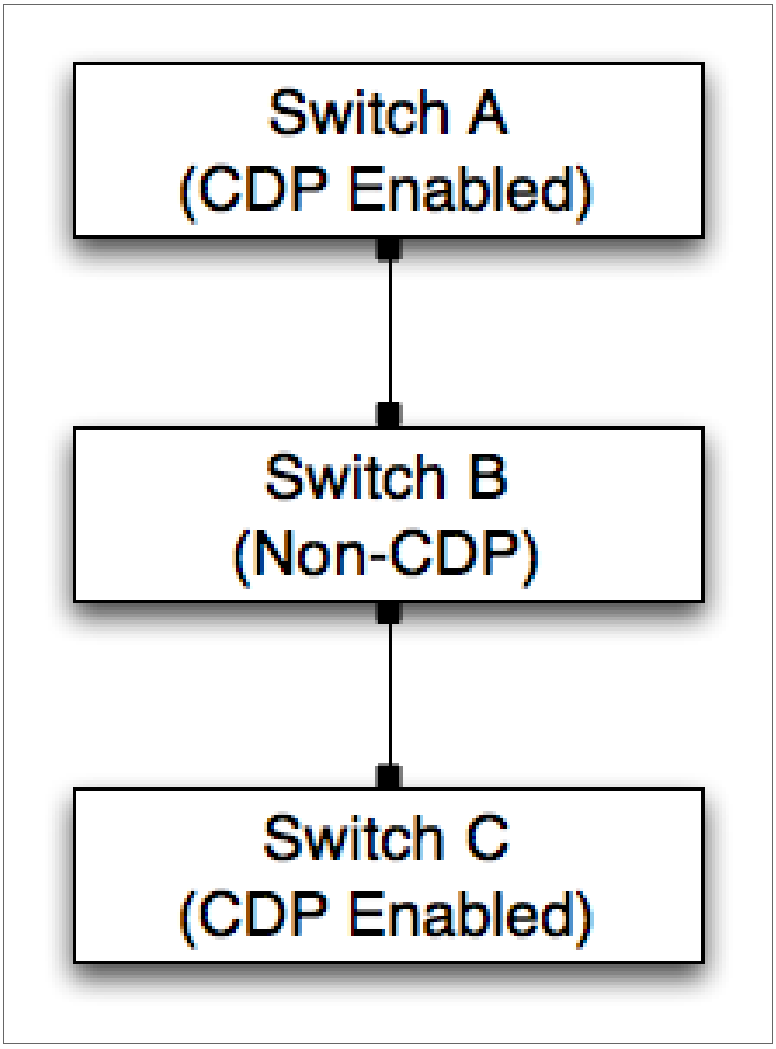
The information collected from the Bridge-MIB does not explicitly indicate which devices are directly connected to a network switch or bridge; switches and bridges will report forwarding information for MAC addresses that are several network hops away from the switch or bridge. A second "crunch" process creates layer-2 topology relationships by evaluating all of the collected MAC address records holistically.

CDP Topology Collection

A CDP Topology record describes a direct network connection between a parent device (a Network Switch or Network Router) and a child device. CDP stands for "Cisco Discovery Protocol," a proprietary standard that is used by networking devices to communicate configuration information to the other devices in the network. Devices that support CDP store and report information received about their immediate neighbors.

CDP is a proprietary protocol developed by Cisco and is not supported by all network hardware. If your network includes both CDP-enabled and non-CDP network switches and routers, the topology data reported by the CDP-enabled devices might not be accurate.

Suppose a network includes three switches connected in the following way:



- Switch A and Switch C, which are both CDP-enabled, broadcast CDP messages.
- Because Switch B is not CDP-enabled, the broadcast messages from Switch A will reach Switch C. Therefore, Switch C will report that it is directly connected to Switch A.
- Conversely, the broadcast messages from Switch C will reach Switch A. Therefore, Switch A will report that it is directly connected to Switch C.

In addition to the CDP data collected from the switches in this example, SL1 might also collect layer-2 topology data that can be used to create correct topology links. However, each discovered interface can be associated with only one topology record of ***any*** type. If a conflict exists between the collected CDP topology data and the collected layer-2 topology data, the CDP topology data takes precedence. In the example above, the CDP topology data will be inaccurate, but the layer-2 data might be accurate. Therefore, if your network includes both CDP-enabled and non-CDP network switches and routers, you might want to disable CDP topology collection in the **Behavior Settings** page (System > Settings > Behavior).

If CDP collection is enabled, SL1 collects information from the Cisco-CDP-MIB from all discovered network switches and routers. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Routers" (ID 1). The ***Device Category*** is defined in the Device Class assigned to the device. Network switches and routers that support the Cisco-CDP-MIB report the IP address and interface information for all directly connected devices that are CDP-enabled.

NOTE: Although SL1 polls all network switches and routers for CDP information, not all network switches and routers support CDP.

Each discovered interface can be associated with only one topology record of ***any*** type. Therefore, the same "crunch" process that creates layer-2 topology records is also responsible for creating the CDP records based on the collected data. However, unlike layer-2 topology records, the Cisco-CDP-MIB reports only directly connected devices. Therefore, if all associated interfaces are valid and available, there is a 1:1 mapping between collected CDP relationships and the CDP relationships created by the "crunch" process.

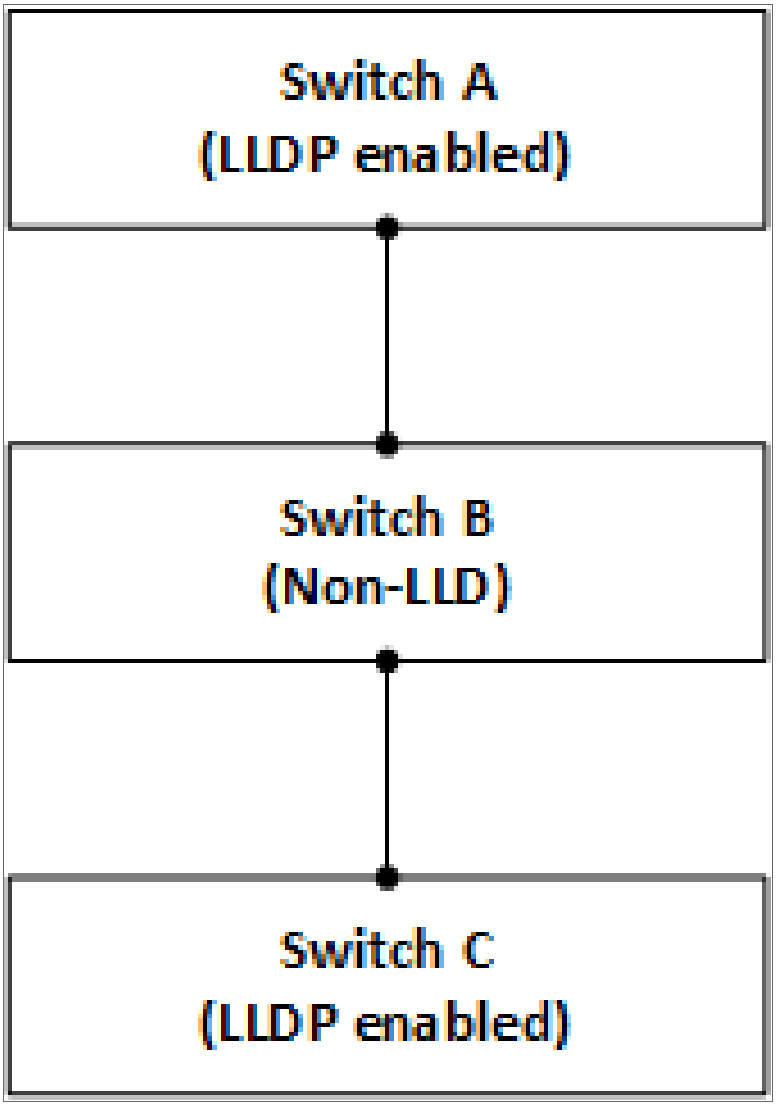
To view CDP maps, go to the **Subnet Map (CDP)** page (Views > Topology Maps >CDP). For details on viewing CDP maps, see the ***Views*** manual.

LLDP Topology Collection

An LLDP topology record describes a direct network connection between a parent device (a Network Switch or Network Router) and a child device. LLDP stands for "Link Layer Discovery Protocol," a standard used by networking devices to communicate configuration information to the other devices in the network. Devices that support LLDP store and report information received about their immediate neighbors.

If your network includes both LLDP-enabled and non-LLDP network switches and routers, the topology data reported by the LLDP enabled devices might not be accurate.

Suppose a network includes three switches connected in the following way:



- Switch A and Switch C, which are both LLDP-enabled, broadcast LLDP messages.
- Because Switch B is not LLDP-enabled, the broadcast messages from Switch A will reach Switch C. Therefore, Switch C will report that it is directly connected to Switch A.
- Conversely, the broadcast messages from Switch C will reach Switch A. Therefore, Switch A will report that it is directly connected to Switch C.

In addition to the LLDP data collected from the switches in this example, SL1 might also collect Layer-2 topology data that can be used to create correct topology links. However, each discovered interface can be associated with only one topology record of ***any*** type. If a conflict exists between the collected LLDP topology data and the collected Layer-2 topology data, the LLDP topology data takes precedence. In the example above, the LLDP topology data will be inaccurate, but the Layer-2 data might be accurate. Therefore, if your network includes both LLDP-enabled and non-LLDP network switches and routers, you might want to disable LLDP topology collection in the **Behavior Settings** page (System > Settings > Behavior).

If LLDP collection is enabled, SL1 collects information from the LLDP MIB from all discovered network switches and routers. SL1 polls devices that have a ***Device Category*** of "Network.Switches" (ID 2) or "Network.Routers" (ID 1). The ***Device Category*** is defined in the Device Class assigned to the device. Network switches and routers that support the Cisco-LLDP-MIB report the IP address and interface information for all directly connected devices that are LLDP-enabled.

NOTE: Although SL1 polls all network switches and routers for LLDP information, not all network switches and routers support LLDP.

Each discovered interface can be associated with only one topology record of ***any*** type. Therefore, the same "crunch" process that creates Layer-2 topology records is also responsible for creating the LLDP records based on the collected data. However, unlike Layer-2 topology records, the -LLDP MIB reports only directly connected devices. Therefore, if all associated interfaces are valid and available, there is a 1:1 mapping between collected LLDP relationships and the LLDP relationships created by the "crunch" process.

Layer-3 Topology Collection

Layer-3 topology records are created by performing a traceroute command from a Data Collector or the All-In-One Appliance to the discovered network hardware every two hours:

- For each "hop" in a traceroute that specifies an IP address associated with a discovered device, SL1 creates a layer-3 topology record that connects the device from the previous hop to the device for the current hop.
- Layer-3 topology records are created only when both devices are discovered; layer-3 topology records are not created when one or both of the two devices is unknown.
- If the IP address associated with a hop is associated with an unknown device, SL1 does not store that hop or any subsequent hops for that traceroute.
- Layer-3 topology records describe only that two devices are connected; layer-3 topology records do not describe which interfaces on those devices are connected.

For SL1 to create layer-3 topology records, the following requirements must be met:

- All traceroute commands for layer-3 topology collection originate from Data Collectors or an All-In-One Appliance. Therefore, the parent node(s) in the layer-3 topology is always a Data Collector or the All-In-One Appliance. For SL1 to create layer-3 topology records, all Data Collectors and All-In-One Appliances must be discovered.

- SL1 performs traceroute commands to devices that have the ***L3 Topology*** option enabled. The ***L3 Topology*** option is defined in the device class assigned to a device. For SL1 to perform layer-3 topology collection, at least one device in your system must have the ***L3 Topology*** option enabled in the device class.
- Your network configuration must allow the traffic generated by the traceroute commands. To test whether your network allows this traffic, go to the **Device Toolbox** page (by clicking the **[Toolbox]** tab in the **Device Administration** panel) for a device with the ***L3 Topology*** option enabled, and then click the **Traceroute** icon.

NOTE: A device that has the ***L3 Topology*** option disabled can still be associated with a layer-3 topology record. If an IP address associated with a device that has the ***L3 Topology*** option disabled appears as a "hop" in a traceroute command performed for a different device, the device with the ***L3 Topology*** option disabled will be associated with the layer-3 topology records that represent the hops to and from that device.

Chapter 5

Managing a Single Device with the Device Administration Panel

Overview

This chapter describes how to use the Device Administration Panel in SL1.

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

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

This chapter includes the following topics:

What is the Device Administration Panel? 121
Actions Menu 124
Device Properties 127
Viewing Read-Only Information About the Device 128
Editing Device Settings 129
Identification 130
Monitoring & Management 130
Preferences 134
Adding an IP Address to a Device 135
Removing an IP Address from a Device 137
Managing Device IPs 138
Clearing the Device Cache 140

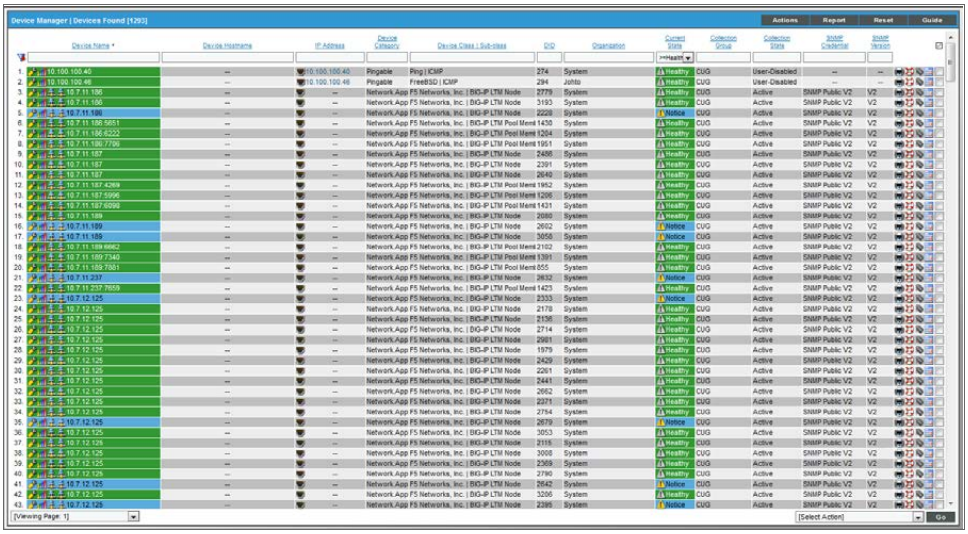
Aligning a Secondary Credential *142*
Adding the Device to a Device Group *144*
Creating a Ticket About the Device *146*
Adding a Note to a Device *148*
Aligning Custom Attributes with a Device *151*
Creating a New Extended Custom Attribute *152*
Deleting an Extended Custom Attribute from a Device *154*
Associating a Product SKU with the Device *155*
Merging Devices *156*
Merging Individual Devices *157*
Unmerging Individual Devices *159*
Performing Administrative Tasks for One or More Devices *161*
Shortcut Keys for Device Administration panel *162*

What is the Device Administration Panel?

The **Device Administration** panel allows you to define how SL1 will interact with a device. This includes defining the data that will be retrieved, the frequency with which SL1 will poll the device, and policies and thresholds that will generate events for the device.

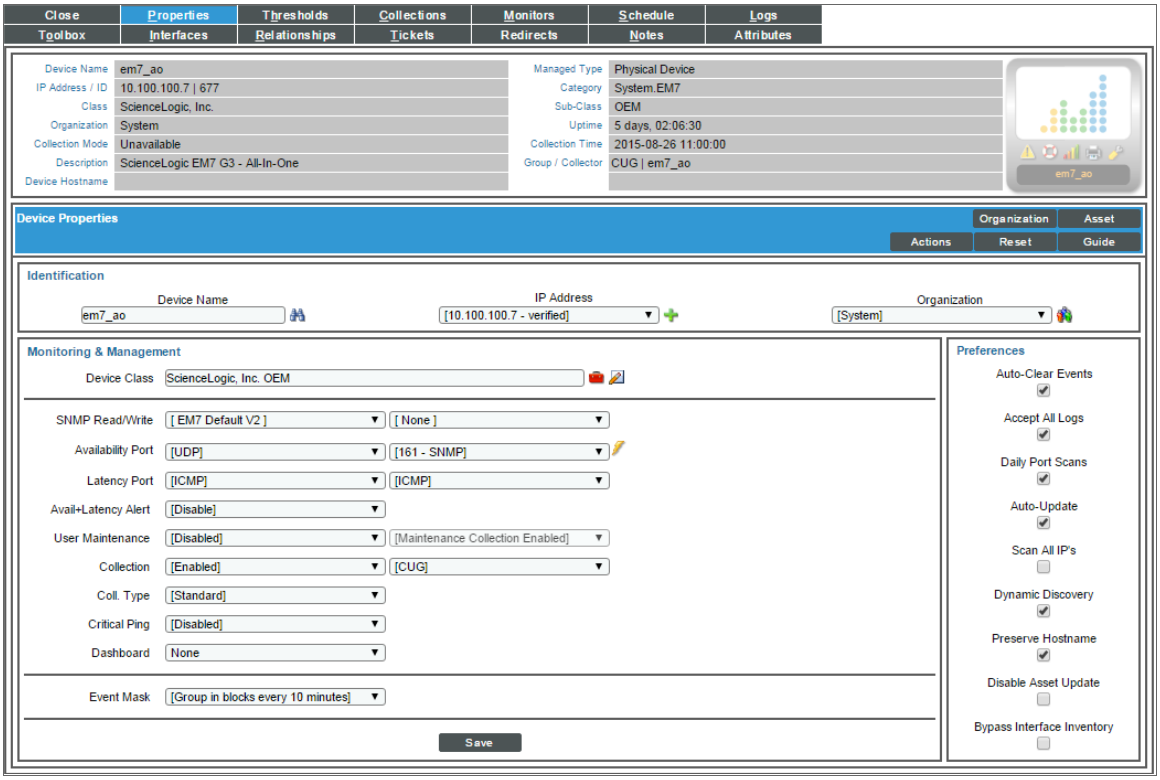
To access the **Device Administration** panel for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).



2. In the **Device Manager** page, find the device for which you want to access the **Device Administration** panel. Select its wrench icon ( ). The **Device Properties** page is displayed. From this page, you can access all the pages in the **Device Administration** panel.

3. 'The **Device Administration** tools include the following tabs and pages:

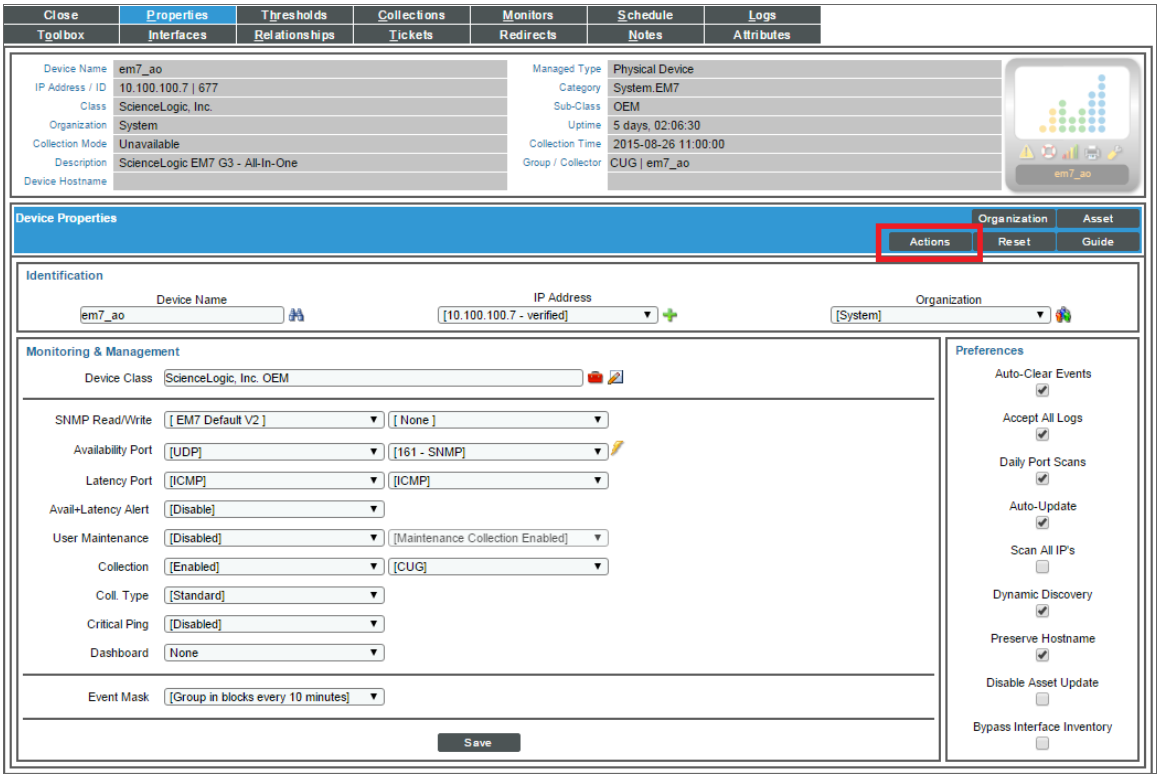


Tab	Description
Properties	In the **Device Properties** page, you can edit parameters that affect how SL1 "sees" the device and monitors the device.
Thresholds	The **Device Thresholds** page allows you to define usage and performance thresholds and data retention thresholds for a device. When these thresholds are exceeded, SL1 will generate an event for the device.
Collections	The **Dynamic Application Collections** page displays all the Dynamic Applications associated with the device. For Dynamic Applications of type "performance," the page displays report policies for each Dynamic Application. For Dynamic Applications of type "configuration," the page displays objects monitored by each Dynamic Application. You can specify a credential for use with the Dynamic Application for the specific device only. You can enable or disable one or more report policies for the specific device only. You can enable or disable monitoring of one or more objects for the specific device only.

Tab	Description
Monitors	The **Monitoring Policies** page allows you to define monitoring policies for a device. The **Monitoring Policies** page allows you to define policies that monitor: system processes, domain-name availability and lookup speed, email round-trip speed, SOAP and XML transaction speeds, TCP/IP port availability, web-content availability, and Windows services. **NOTE**: All these monitoring policies can generate events. SL1 uses the data collected by these policies to create performance reports and graphs.
Schedule	In the **Maintenance Schedule** page you can view, edit, and schedule downtimes for the device.
Logs	The **Device Logs & Messages** page displays all the messages SL1 has collected from the device and from SL1 about the device.
Toolbox	The **Device Toolbox** page provides access to common network tools. The list of tools available depends upon the type of device and the configuration of the device. This page allows you to access and run diagnostics on a device without leaving the user interface session.
Interfaces	The **Device Interfaces** page displays detailed information about each network interface on the device. From this page, you can view details about each individual interface and define bandwidth monitoring for the interface.
Relationships	The **Device Relationships** page displays information about parent-child relationships between devices. From this page, you can view details on the relationships between on layer-2 and layer-3 devices, hypervisors and their virtual machines, and other relationships.
Tickets	The **Ticket History** page displays all tickets associated with the device. This page displays critical information about each ticket. If you require more detail, you can access the**Ticket Editor** from this page.
Redirects	The **Redirection** page appears only for virtual devices. This page allows you to redirect logs entries from an IP-based device to a virtual device.
Notes	The **Notes & Attachments** page displays a list of all comments and attachments associated with the device properties. When you select the *Notepad Editor* option in the **Device Properties** page, the notes appear in this page.
Attributes	The **Attributes** page displays a list of custom attributes that are already aligned with the device. Additionally, the **Attributes** page enables you to assign a value to those custom attributes, create and align a new extended custom attribute with the device, or delete a custom attribute from a device.

Actions Menu

The pages in the **Device Administration** panel each include the **[Actions]** menu. The **[Actions]** menu allows you to perform many device-related tasks without requiring you to leave the current page. The **[Actions]** menu looks like a button and is located in the upper right of the page.



The following entries in the **[Actions]** menu appear only in the **Device Properties** page:

- ***Add IP Address***. Leads to the **Add IP Address** modal page, where you can define an additional IP address for the device. SL1 will continue to use the primary IP Address for communication with the device. For details, see the section on *Adding an IP Address to a Device*.
- ***Select Primary IP Addresses***. Leads to the **Select Primary IP Addresses** modal page, where you can define primary IP addresses and secondary IP addresses for the device. A primary IP address allows SL1 to align traps and syslog messages with the device. In the case of duplicate primary IP addresses, you can promote a secondary IP address to a primary IP address and demote the duplicated primary IP address.
- ***Clear Device Cache***. Selecting this option clears data about this device from the cache. For details, see the section on *Clearing the Device Cache*.
- ***Device Class***. Leads to the **Device Class** modal page, where you can select a device class to associate with the device. For details, see the section on *Device Classes and Device Categories*.

- ***Secondary Credentials***. Leads to the **Secondary Credentials** modal page, where you can associate additional credentials with the device. SL1 will then use the primary credential and the additional credentials during discovery for the device. For details, see the section on *Aligning a Secondary Credential*.

- ***Merge Device***. Allows you to merge the data from a component device and a physical device into a single record. When you merge a physical device and a component device, the device record for the component device is no longer displayed in the user interface; the device record for the physical device is displayed in user interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the physical device.

    - For *physical devices*, this option leads to the **Merge Devices** modal page, where you can view a list of component devices and select a component device to merge with the current physical device.
    - For *component devices*, this option leads to the **Merge Devices** modal page, where you can view a list of physical devices and select a physical device to merge with the current component device.

  For details, see the section on *Merging Devices*.

- ***Unmerge Device***. Appears only in the **Device Properties** page for physical devices. Prompts you to unmerge the component device that has been previously merged with the physical device. For details, see the section on *Merging Devices*.

NOTE: You can merge only one component device with a physical device.

NOTE: When you merge two devices, the historical device logs for those devices will be merged and are not unmerged when the ***Unmerge Device*** option is used.

NOTE: In Dashboard widgets, merged devices can be searched for and filtered by the device class or device category of the physical device or the device class or device category of the component device. If both device classes or device categories are selected, a merged device will appear twice in a single widget.

NOTE: When you merge two devices, active events associated with the component device will be set to "cleared". The cleared events will not be associated with the physical device. If the devices are unmerged, the cleared events cannot be moved back to the component device.

The following entry in the **[Actions]** menu appears only in the **Device Logs & Messages** page:

- ***Export Logs***. Allows you to export the log entries to a file on your local computer. You can save the exported file or save and view the exported file.

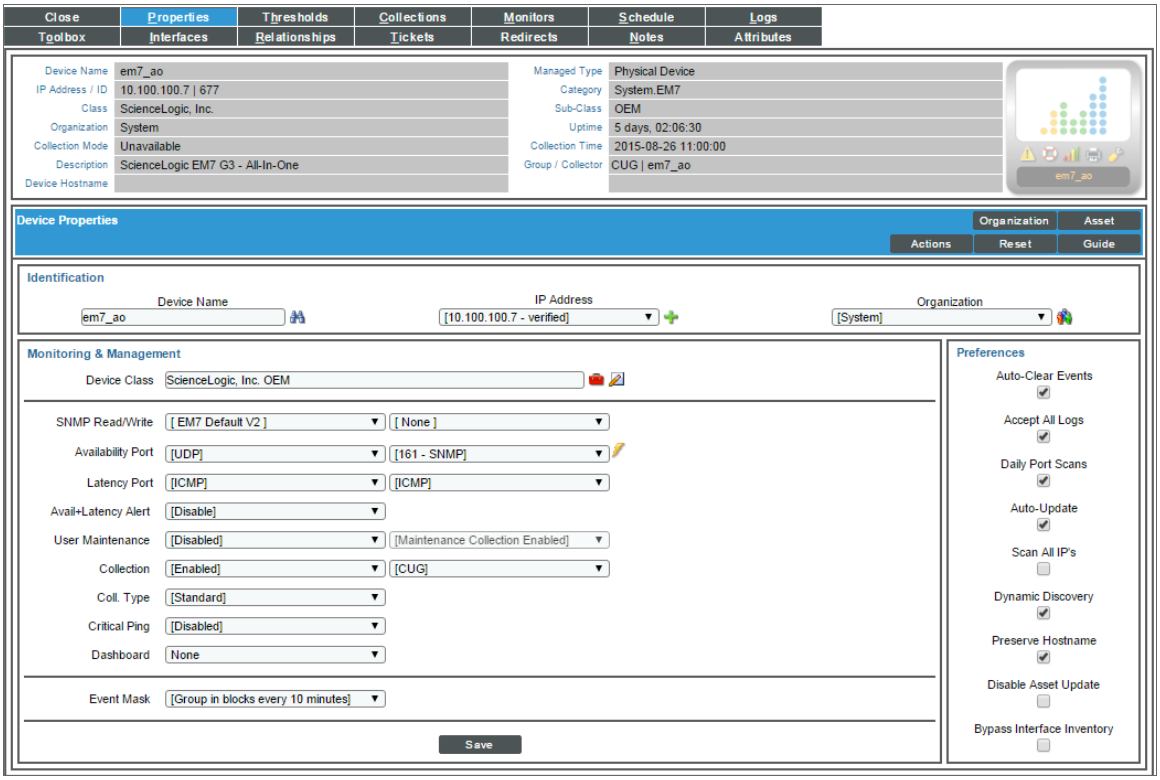
The following entries in the **[Actions]** menu appear on each page in the **Device Administration** panel:

- ***My Bookmarks***. Displays the **Administer Bookmarks** modal page, where you can access pre-defined bookmarks or save a new bookmark. For details, see the manual ***Customizing User Experience***.
- ***Create a Ticket***. Leads to the **Ticket Editor** page, where you can define a new ticket about the device. For details, see the section on *Creating a Ticket About the Device*.
- ***Custom Navigation***. Leads to the **Custom Navigation** modal page, where you can define a custom tab for the device administration panel for the current device. The custom tab will contain a link to an outside URL. For details, see the section on *Customizing the Interface for a Device*.
- ***Device Children***. Leads to the **Device Children** modal page, where you can add children devices to the current device. The current device will be the parent device. For details, see the section on *Defining Device Relationships*.
- ***Device Groups***. Leads to the **Device Groups** modal page, where you can assign the device to a device group or remove a device from a device group. For details, see the section on *Adding a Device to a Device Group*.
- ***Notepad Editor***. Leads to the **Notepad Editor** modal page, where you can enter a note to include with the device. The note will appear in the **Notes & Attachments** page for the device. For details, see the section on *Adding a Note to a Device.*
- ***Product Catalog***. Leads to the **Product Catalog** modal page, where you can associate a product SKU with the device or disassociate the device from a product SKU. For details, see the section on *Associating a Product SKU with a Device*.
- ***Report Creator***. Leads to the **Report Creator** modal page, where you can define a device report, including the information to include in the report and the format in which to generate the report. For details, see the section on *Generating a Report for a Single Device*.
- ***Resource Usage***. Leads to the **Resource Usage** modal page, where you can view the list of device logs and device statistics gathered by SL1 and also view where the data is stored and how many bytes of data are being stored.

Device Properties

The **Device Properties** page allows you to view basic, read-only information about a device and also to view and edit the device's parameters for discovery (collection).

The settings defined for the device in the **Device Properties** page override any system-wide settings.



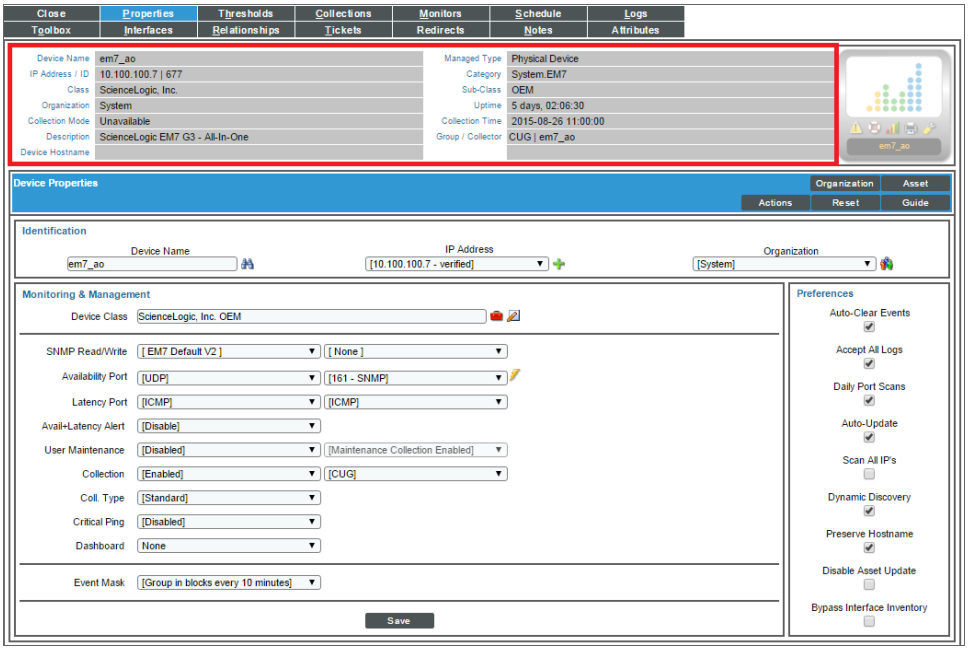
From the **Device Properties** page, you can:

- ***View Information about the Device***. This is described in the section on *Read-Only Information about the Device*.
- ***Edit the Discovery Parameters for the Device***. This is described in the section on *Editing Device Settings*.
- ***Edit the Device Class for the Device***. This is described in the section on *Device Classes*.
- ***Associate an Additional IP Address with the Device***. This is described in the section on *Adding an IP Address to a Device*.
- ***Remove an IP Address from the Device***. This is described in the section on *Removing an IP Address from a Device*.
- ***Manage Primary and Secondary IP Addresses for the Device***. This is described in the section on *Managing Device IPs*.

- ***Clear the Device Cache***. This is described in the section on *Clearing the Device Cache*.
- ***Define Child Devices***. This is described in the section on *Defining Device Relationships*.
- ***Associate a Secondary Credential with the Device***. This is described in the section on *Aligning a Secondary Credential*.
- ***Add the Device to a Device Group***. This is described in the section *Adding the Device to a Device Group*.
- ***Create a Ticket About the Device***. This is described in the section *Creating a Ticket About the Device*.
- ***Define Custom Navigation for the Device***. This is described in the section *Customizing the User Interface for a Device*.
- ***Add a Note to the Device***. This is described in the section *Adding a Note to a Device*.
- ***Associate a Product SKU with the Device***. This is described in the section *Associating a Product SKU with the Device*.
- ***Create or Edit an Asset Record for the Device***. This is described in the ***Asset Management*** manual.
- ***View Resource Usage for the Device***. This is described in the manual ***Monitoring Device Infrastructure Health***.
- ***Create a Report About the Device***. This is described in the manual ***Monitoring Device Infrastructure Health***.

Viewing Read-Only Information About the Device

Each page in the **Device Administration** panel and the **Device Reports** panel displays the following read-only information about the device:

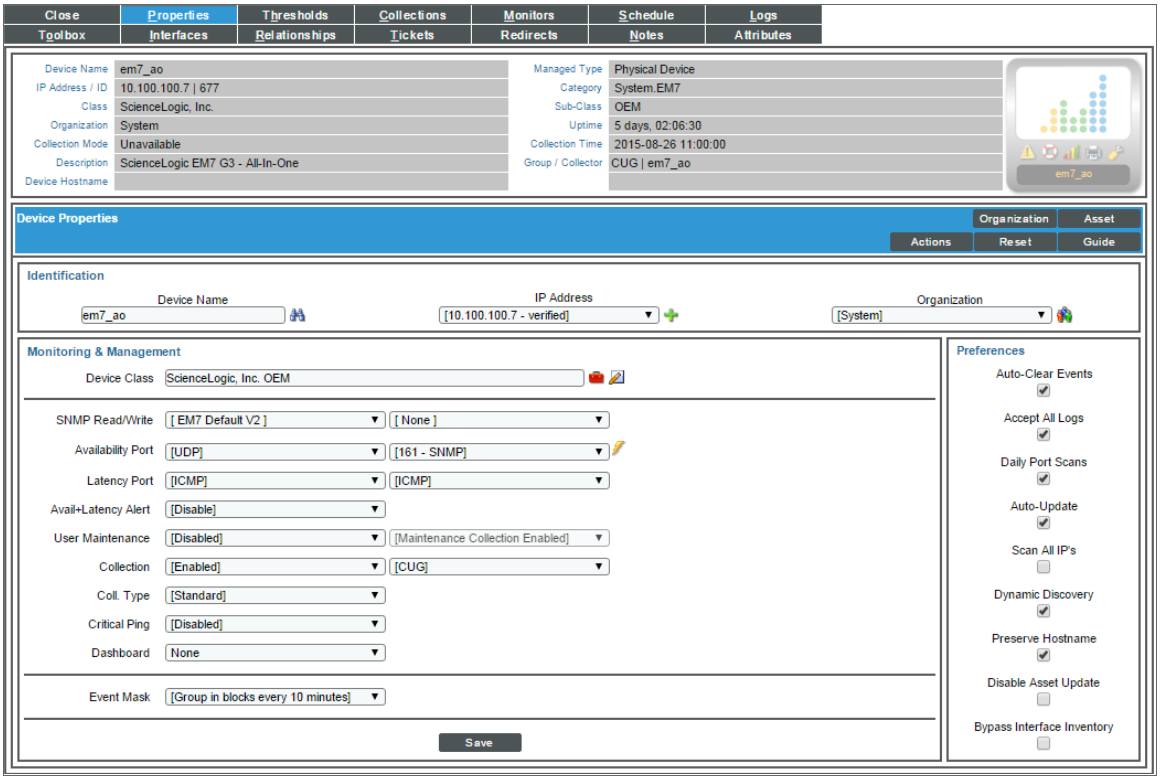


- ***Device Name***. Name of the device. Clicking on this field displays the **Device Properties** page for the device.
- ***IP Address /ID***. IP address of the device and the device ID of the device. The device ID is a unique numeric identifier, automatically assigned to the device by SL1. Clicking on this field displays the **Device Properties** page for the device.
- ***Class***. Device class for the device. A *device class* usually describes the manufacturer of the device.
- ***Organization***. Organization associated with the device. Clicking on this field leads to the **Organizational Summary** page for the device's organization.
- ***Collection Mode***. Collection mode. Choices are "active", meaning SL1 is periodically collecting data from the device, or "inactive", meaning the SL1 is not currently collecting data from the device. Clicking on this field executes the Remote Port Scanner and displays the **Remote Port Scanner** modal page.
- ***Description***. For SNMP devices, the SysDescr value as reported by the SNMP agent on the device. If a device does not support SNMP, this field appears blank.
- ***Root Device***. For component devices, displays the device name or IP address of the physical device where the system that manages the device resides. Clicking on this value displays the **Device Properties** page for the root device.
- ***Parent Device***. For component devices, displays the device name or IP address of the parent device. The parent device can be either another component device or a physical device. A parent device is the device between the current component device and the next layer in the component-device hierarchy. Clicking on this value displays the **Device Properties** page for the parent device.
- ***Device Hostname***. For devices that are discovered and managed by hostname (instead of IP address), this field displays the fully qualified hostname for the device.
- ***Managed Type***. Specifies the protocol used to discover the device and whether or not the device is a physical device or a virtual device. Clicking on this field executes an SNMP walk of the device's SNMP file and displays the **SNMP Walker** modal page.
- ***Category***. The device category associated with the device. The *device category* usually describes the function of the hardware.
- ***Sub-Class***. The device sub-class associated with the device. The sub-class usually described the model of a device.
- ***Uptime***. The number of days, hours, minutes, and seconds that the device has been continuously up and communicating with SL1. Clicking on this field displays the System Vitals Summary report.
- ***Collection Time***. The date and time that SL1 last collected data from the device.
- ***Group/Collector***. The Collector Group and specific collector used to last collect data from the device. For All-In-One Appliances, this field will contain the name of the default, built-in Collector Group.

Editing Device Settings

The fields in the **Device Properties** page affect how SL1 will discover and collect information about the device. Initially, SL1 uses system defaults, system-wide settings, and data retrieved during initial discovery of the device to populate these fields.

You can edit one or more of these fields for the device. The settings defined for the device in the **Device Properties** page override any system-wide settings (defined in the pages under System > Settings).



Identification

- ***Device Name***. The name of the device. If possible, SL1 retrieves the device name from the device. If the device is running SNMP or has a DNS entry, the name will be retrieved directly from the device. You can set the precedence for which of these names are used (SNMP system name or DNS entry) in the **Behavior Settings** page (System > Settings > Behavior). You can edit this name in the **Device Properties** page; however, the Device Name will not be changed on the actual device.
- ***IP Address***. The IP address that SL1 uses to communicate with the device. You can add additional IP addresses for the device. To change the IP address SL1 uses to communicate with the device (called the ***admin primary*** address), select a different IP address in this field.
- ***Organization***. Organization to which this device has been assigned. To assign this device to a different Organization, select an Organization from the drop-down list. To view details about the assigned organization, select the people icon ( ) to the right of this field.

Monitoring & Management

- ***Device Class***. Displays the *Device Class*. To assign a different device class to the device, select the toolbox icon ( ) to the right of this field. To edit the device's Device Class, select the pencil icon ( ) to the right of this field.

NOTE: If you incorrectly change a device's Device Class, SL1's nightly update will override the new Device Class and assign the device to the correct Device Class.

- ***SNMP Read***. The community string for read-only access to SNMP information on the device. The community string is a password that allows SL1 to gather SNMP information from the device. If this device has been aligned with a credential to which you do not have access, this field will display the value *Restricted Credential*. If you align the device with a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.
- ***SNMP Write***. The community string for read-and-write access to SNMP information on the device. The community string is a password that allows SL1 to gather SNMP information from the device and send SNMP information to the device. If this device has been aligned with a credential to which you do not have access, this field will display the value *Restricted Credential*. If you align the device with a different credential, the entry for *Restricted Credential* will be removed from the list in this field; you will not be able to re-align the device with the *Restricted Credential*.

NOTE: Devices that do not support SNMP ("pingable" devices) display the value *None* in both the ***SNMP Read*** field and the ***SNMP Write*** field.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***SNMP Read*** field and the ***SNMP Write*** field. For details, see the ***Discovery and Credentials*** manual.

- ***Availability Port***. Specifies the protocol and specific port SL1 should monitor to determine if the device is available. The list of ports will contain all the ports discovered by SL1 and the options *ICMP* and *SL1 agent*. For the *ICMP* option, SL1 performs a ping request. The data collected from this port or ping request will be used in device availability reports. The *SL1 agent* option allows you to specify that the platform should use information collected by the agent to determine port availability. The agent must be installed on the device to use this option.
    - If you select *ICMP* as the protocol, you can use the ***ICMP Availability Thresholds*** in the *Device Thresholds* page to further define how SL1 will test the device's availability.

NOTE: Component Devices use a Dynamic Application collection object to measure availability. For details, see the description of the ***Component Identifier*** field in the **Collection Objects** page. For details, see the manual ***Monitoring Device Infrastructure Health***.

- ***Run Availability Policy*** ( ). When you select this icon, SL1 immediately checks the availability of the device, using the port and protocol specified in the ***Availability Port*** fields. SL1 displays a **Session Logs** modal page that displays a detailed description of each step of the availability policy. This information is helpful when troubleshooting availability problems with a device.

- ***Latency Port***. Specifies the protocol and specific port SL1 should monitor to determine latency for the device. The list of ports will contain all the ports discovered by SL1 and the option *ICMP*, for which SL1 performs a ping request. The data collected from this port or ping request will be used in device latency reports.

    - If you select *ICMP* as the protocol, you can use the ***ICMP Availability Thresholds*** in the *Device Thresholds* page to further define how SL1 will test the device's latency.

- ***Avail + Latency Alert***. Specifies how SL1 should respond when the device fails an availability check, when the device fails a latency check, and when the device fails both. These options allow you to create separate events when SNMP fails on a device and when a device is not up and running. Choices are:

    - *Enabled*. SL1 will create the following events:

        - ***If the device fails the availability check***, generates the event "Device Failed Availability Check: UDP - SNMP".
        - ***If the device fails the latency check***, generates the event "Network Latency Exceeded Threshold: No Response".
        - ***If the device fails both the availability check and the latency check***, generates the event "Device Failed Availability and Latency checks".

    - *Disabled*. SL1 will create the following events:

        - ***If the device fails the availability check***, generates the event "Device Failed Availability Check: UDP - SNMP".
        - ***If the device fails the latency check***, generates the event "Network Latency Exceeded Threshold: No Response".
        - ***If the device fails both the availability check and the latency check***, generates the event "Device Failed Availability Check: UDP - SNMP". The event "Network Latency Exceeded Threshold: No Response" is suppressed under the availability event.

- ***User Maintenance***. Specifies whether the device will be put into "user maintenance" mode. By default, when a device is in "user maintenance", SL1 will not generate events about the device.

    You can choose to enable or disable polling during "user maintenance" mode. If polling is enabled during "user maintenance", SL1 will collect information from the device but will generate only events of severity less than the severity specified in the system-wide ***Maintenance Minimum Severity*** setting. For more information about the ***Maintenance Minimum Severity*** setting, see the *Device Maintenance* section.

    "User maintenance mode" is not scheduled. That is, a user must manually enable "user maintenance" to put a device into this mode and a user must manually disable "user maintenance" to turn off this mode for a device. "User maintenance mode" overrides scheduled maintenance for a device. Choices are:

    - *Enabled*. Device will be set to "user maintenance" mode.
    - *Disabled*. Device will not be set to "user maintenance" mode.

- ***User Maintenance Collection***. Specifies whether SL1 should poll the device during the "user maintenance". During normal operation, SL1 polls each device as specified by each device's policies and aligned Dynamic Applications. Choices are:
    - *Enabled*. During "user maintenance" mode, SL1 will continue to poll the device.
    - *Disabled*. During "user maintenance" mode, SL1 will not poll the device.
- ***Collection State***. Specifies if device will be monitored by SL1. To edit this field, select one of the following from the drop-down list:
    - *Enabled*. Device will be monitored by SL1.
    - *Disabled*. Device will not be monitored by SL1.
- ***Collection Poller***. Specifies which Collector Group will perform discovery and gather data from the device. The drop-down list contains a list of available collector groups. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups). For details on Collector Groups, see the ***System Administration*** manual.
- ***Coll. Type***. Specifies how SL1 should perform collection. The choices are:
    - *Standard*. SL1 will perform discovery of each device based on the device's IP address. This method is appropriate for devices using standard DNS.
    - *DHCP*. SL1 will perform a DNS lookup for the device each time SL1 retrieves information from the device. This allows SL1 to get the latest IP address for the device.
- ***Critical Ping***. Frequency with which SL1 should ping the device in addition to the five minute availability poll. If the device does not respond, SL1 creates an event. The choices are:
    - *Disabled*. SL1 will not ping the device in addition to the five minute availability poll.
    - *Intervals from every 120 seconds - every 5 seconds*.

NOTE: SL1 does not use this ping data to create device-availability reports. SL1 will continue to collect device availability data only every five minutes, as specified in the process "Data Collection:Availability" (in the **Process Manager** page). For more details on critical ping, see the manual ***Monitoring Device Infrastructure Health***.

NOTE: Because high-frequency data pull occurs every 15 seconds, you might experience up to 15 seconds of latency between an unavailable alert and that alert appearing in the Database Server if you set ***Critical Ping*** to *5 seconds*.

NOTE: You might experience some performance issues if you have a large number of devices using Internal Collections Dynamic Applications to monitor Critical Availability on a brief polling interval.

- ***Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. The selected device dashboard will appear by default in the **Device Summary** page for this device. This field is optional.
- ***Event Mask***. Events that occur on a single device within the selected time-interval are grouped together. This allows related events that occur in quick succession on a single device to be rolled-up and posted together, under one event description. Select a time-span from the drop-down list:
    - *Disabled*. SL1 will not group events.
    - *Group in blocks at intervals from every 30 seconds - every 1 month*

  By default, when events are masked, the **Events page** displays all events that occur on the device within the specified time-span under a single event, the one with the highest severity. The magnifying-glass icon ( ) appears to the left of the event. When you click on the magnifying-glass icon, the **Suppression Group** modal page is displayed. This page displays details about all events that are masked under the displayed event.

NOTE: If an event has ***Occurrence Count*** and ***Occurrence Time*** set in its **Event Policy Editor** page, SL1 will use the very first logged occurrence of the event to calculate the ***Event Mask***, even if that first occurrence did not appear in the **Events page** (due to the ***Occurrence Count*** and ***Occurrence Time*** fields).

For example, suppose an event, *event_x*, has an ***Occurrence Count*** of "3" and an ***Occurrence Time*** of "10 minutes". This means that the event must occur on the same device at least three times within 10 minutes before the event appears in the**Events page**. Suppose the event, *event_X*, occurs on *device_A* at 15:51, 15:52, and 15:53. The event will appear in the **Events page** with a timestamp of "15:53", an age of "2 minutes" and a count of "3".

Suppose **device_A** includes an ***Event Mask*** of "Group in blocks every 5 minutes". To calculate how to group *event_x*, the ***Event Mask*** will use the timestamp of the first occurrence, 15:51, even though the event did not appear in the **Events page** at that time. The ***Event Mask*** will also use the time of the first occurrence, 15:51, to calculate the "Age/Elapsed" value for the event in the **Suppression Group** modal page.

Preferences

- ***Auto-Clear Events***. Auto Clear automatically removes an event from the Event Monitor if a specified succeeding event occurs. For example, suppose the event "Device not responding to ping" occurs. If the next polling session produces the event "Device now responding normally to ping", the Auto Clear feature could clear the event. If you do not want events to be cleared automatically, uncheck this field. For this specific device, this field overrides the global auto-clear settings in the**Event Policy Editor** page (Events > Event Manager > create or edit).
- ***Accept All Logs***. This checkbox specifies whether or not you want to keep and save all logs for this device. If you want to retain only logs associated with events, uncheck this field.
- ***Daily Port Scans***. This checkbox specifies whether or not you want SL1 to perform a daily scan of the device for open ports. Select this field to enable daily port scans.

- ***Auto-Update***. This checkbox specifies whether or not you want SL1 to perform a nightly discovery of the device and update records with changes to the device. Check this box to enable nightly updates. If this field is unchecked, SL1 will not perform nightly discovery. Changes to the device, including newly opened ports, will not be recorded by SL1.
- ***Scan All IPs***. If the device uses multiple IP Addresses, SL1 can scan for open ports on all IPs during nightly discovery. Check this box to enable scanning of all IP Addresses for open ports every night.
- ***Dynamic Discovery***. If selected, SL1 will automatically assign the appropriate Dynamic Applications to the device during nightly discovery.
- ***Preserve Hostname***. If selected, the name of the device in SL1 will remain the same, even if the name of the actual device is changed. If unselected, the name for the device will be updated if the name of the actual device is changed.
- ***Disable Asset Update***. If selected, SL1 will ***not*** automatically update the asset record associated with the device. For a single device, this checkbox overrides any settings defined in the **Asset Automation** page (System > Settings > Assets).

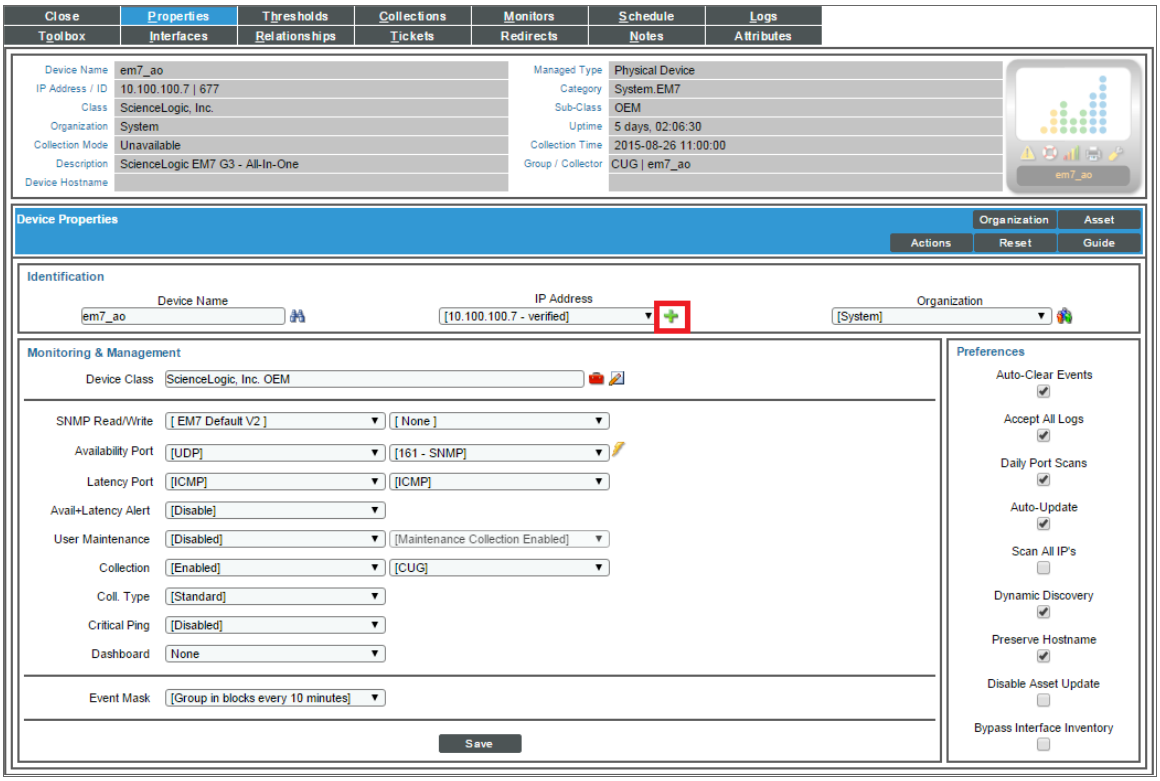
Adding an IP Address to a Device

If a device has multiple IP addresses, you can add those IP addresses in SL1. SL1 will continue to use the primary IP address for communication with the device. However, after you add an additional IP address to a device, you can change the primary IP address to the new IP address by selecting it in the ***IP Address*** field.

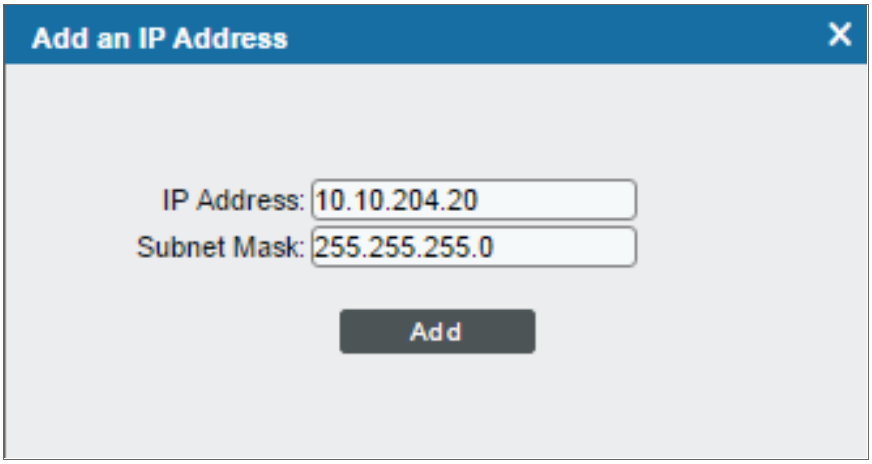
To define additional IP addresses for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to define additional IP address. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, find the ***IP Address*** field.

4. To the right of the ***IP Address*** field, click on the plus-sign icon ( ):



5. Alternately, you can also select the **[Actions]** menu and choose ***Add IP Address***.
6. The **Add IP Address** modal page appears. The **Add IP Address** modal page allows you to define an additional IP address for the device.



7. The **Add IP Address** modal page allows you to define an additional IP address for the device. SL1 will continue to use the Admin Primary IP address for communication with the device. However, SL1 will also

collect data about the additional IP address(es).To associate an additional IP address with the device, supply values in the following fields:

- ***IP Address***. Supply the IP address, in standard dotted-decimal format.
- ***Subnet Mask***. Supply the subnet mask associated with the IP address. This field is optional.

8. Select the **[Add]** button.
9. In the **Device Properties** page, you will now see the additional IP address in the ***IP Address*** field. During auto-discovery, SL1 will verify that this IP address exists on the device and will append the label "verified" to the value in the ***IP Address*** field.

NOTE: After you manually rediscover the device or after SL1 runs nightly auto-discovery (whichever occurs first), the new IP address will appear in the **Network Browser** page.

Removing an IP Address from a Device

If you have added an IP address to a device using the steps in the section on *Associating an Additional IP Address with the Device*, you can also delete that IP address.

There are two exceptions to this ability:

- You cannot delete an IP address that is currently the *Admin Primary* IP address for the device.
- You cannot delete an IP address that is associated with a network interface.

To delete an IP address:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device from which you want to delete an IP address. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, find the ***IP Address*** field.
4. To the right of the ***IP Address*** field, select the bomb icon ( ). The **Remove IP Address** modal page displays:

5. Select the checkbox for the IP address you want to delete.
6. Select the **[Remove]** button. The IP address is deleted.

> **NOTE:** The **Remove IP Address** modal page will display checkboxes only for IP addresses that you can delete. If an IP address appears in the **Remove IP Address** modal page without a checkbox, you cannot delete that IP address.

If an IP address that you want to delete appears in the **Remove IP Address** modal page as *Selected*, it is currently the *Admin Primary* IP address and you must select a new Admin Primary IP before you can delete the IP address. To select a new Admin Primary IP address:

1. In the ***IP address*** drop-down list in the **Device Properties** page, select a new Admin Primary IP address.
2. Select the **[Save]** button.
3. You can now delete the previous Admin Primary IP address.

Managing Device IPs

There are three types of IP addresses that can be associated with a device:

- ***Admin Primary***. This is the IP address that SL1 uses to communicate with a device. This IP address is always a primary address and cannot be demoted to a secondary address. You can change the Admin Primary address by changing the value in the ***IP Address*** field in the **Device Properties** page.
- ***Primary***. One or more IP addresses that SL1 uses to match incoming log messages (traps and syslog messages) with a device. When you select an IP address in the **Select Primary IP Addresses** modal page, that IP address becomes a primary. You can also unselect an IP address in the**Select Primary IP Addresses** modal page. When you unselect an IP address, that IP address becomes a secondary.
- ***Secondary***. SL1 gathers information about this IP address, but does not use this IP address to match incoming messages (traps and syslog messages) with a device.

A ***Message Collection Server*** accepts inbound, asynchronous messages from monitored devices and applications in your network. For example, Message Collectors accept all SNMP traps, SNMP informants, and syslog messages. A SL1 system can include one or more Message Collectors.

- A single Message Collector can be aligned with multiple Collector Groups.

> **NOTE:** If you are using a combination Data Collector and Message Collector, this combination appliance should be assigned only to its own dedicated Collector Group and that Collector Group should not include other Data Collectors or Message Collectors.

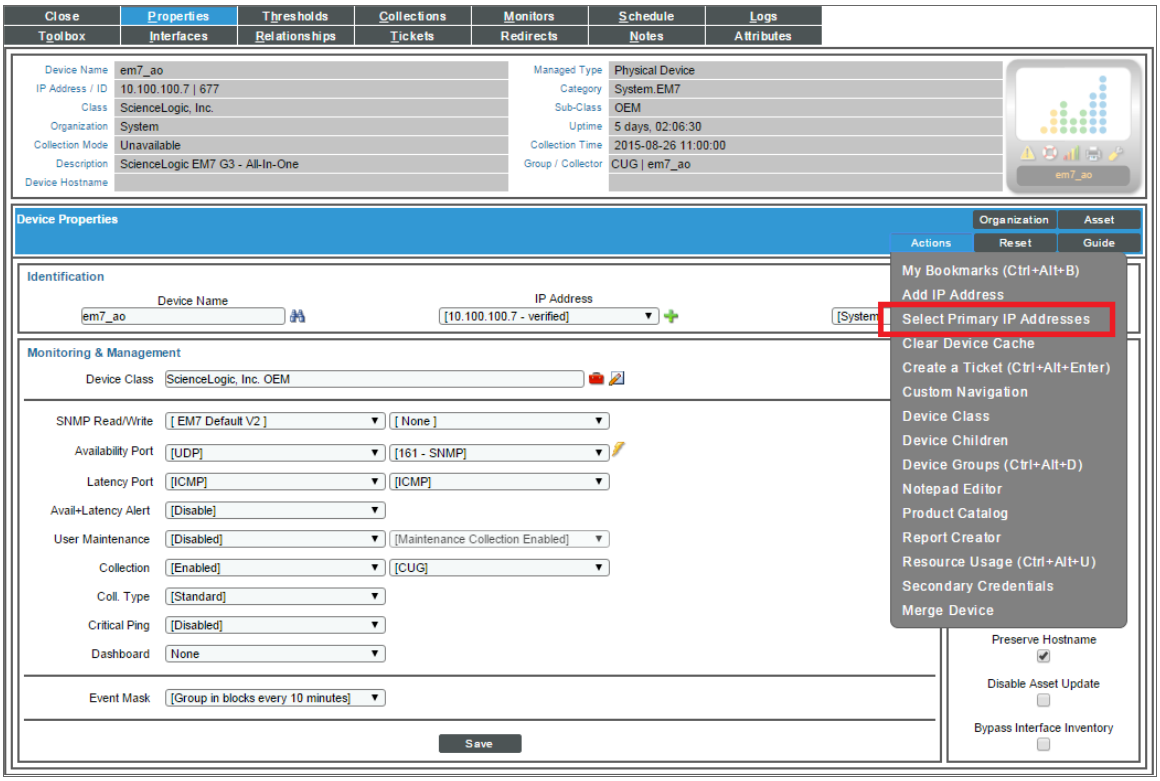
- Although SL1 will not allow duplicate IP addresses within a single Collector Group, SL1 does allow duplicate IP addresses if each device is aligned with a different Collector Group.

- If a single Message Collector is aligned with multiple Collector Groups, the single Message Collector might be aligned with two or more devices (each in a separate Collector Group) that use the same primary IP address or the same secondary IP address. If this happens, SL1 will generate an event. To fix this situation, you can go to the **Select Primary IP Addresses** modal page for one of the devices and change the primary IP address in question. You can demote the primary and promote a secondary IP address for the device. This will fix the problem with duplicate IPs and allow the Message Collector to align messages with the device.

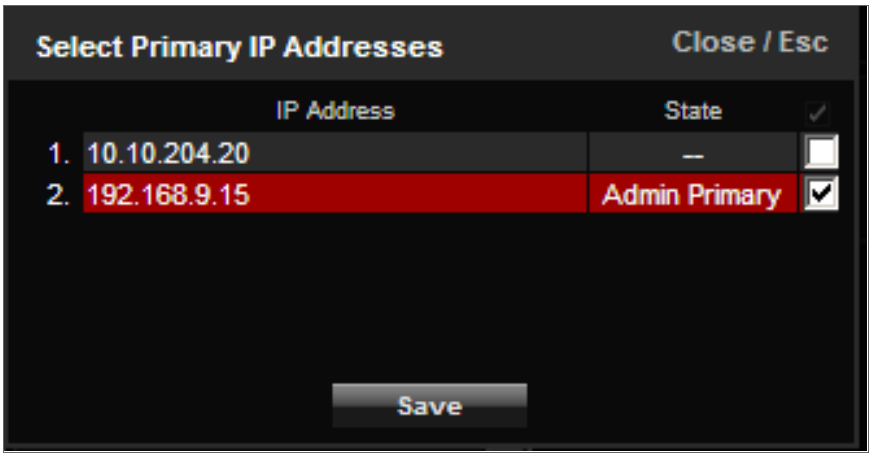
NOTE: For All-In-One Appliances, the function provided by a Message Collector is built in to the All-In-One Appliance. All-In-One systems contain only one built-in Collector Group.

The **Select Primary IP Addresses** modal page allows you to view a list of IP addresses for the device and define one or more of those IP addresses as "primary" or "secondary". To change an IP address to Primary or Secondary, perform the following:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to manage the IP addresses. Select its wrench icon ( ).
3. In the **Device Properties** page for the device, select the **[Actions]** menu. Choose *Select Primary IP Address*.



4. The **Select Primary IP Addresses** modal page appears. There are three types of IP addresses that can be associated with a device:



- ***Admin Primary***. This is the IP address that SL1 uses to communicate with a device. This IP address is always the admin primary address and cannot be demoted to a secondary address.
- ***Primary***. One or more IP addresses that SL1 uses to match incoming messages (traps and syslog messages) with a device. When you select an IP address in the Select Primary IP Addresses modal page, that IP address becomes a primary. You can also unselect an IP address in the Select Primary IP Addresses modal. When you unselect an IP address, that IP address becomes a secondary.
- ***Secondary***. SL1 gathers information about this IP address, but does not use this IP address to match incoming messages (traps and syslog messages) with a device.

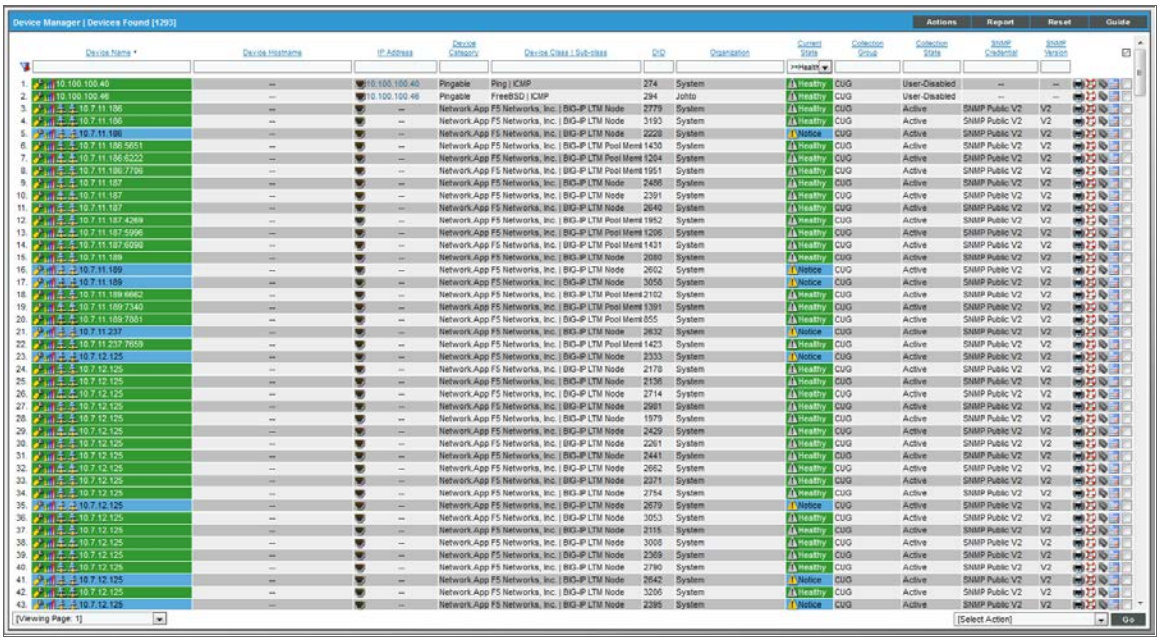
NOTE: Within a Collector Group, multiple devices cannot use the same primary IP address. In some circumstances, an IP address appears in the **Select Primary IP Addresses** modal page for the current device but does not have a corresponding checkbox. This means that the IP address is currently used as a primary IP on another device in the same Collector Group. SL1 will not allow you to promote this IP address to a primary IP address on the current device.

5. Select the **[Save]** button to save the changes to the device.

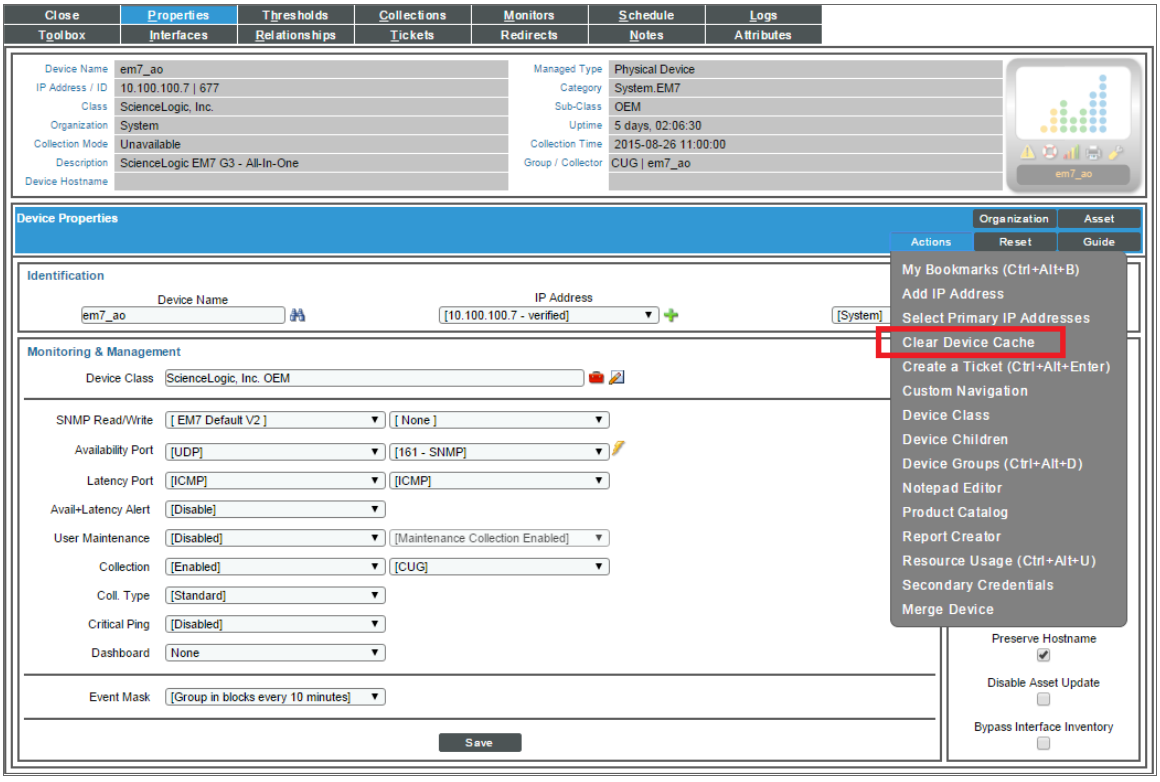
Clearing the Device Cache

Between HTTP requests, SL1 caches data in memory. For diagnostic purposes, you might want to clear the cached data about a specific device. To do this:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device whose data you want to clear from the cache. Select its wrench icon ( ).



3. In the **Device Properties** page for the device, select the **[Actions]** menu. Select ***Clear Device Cache***.



4. Data about the device will be cleared from the cache.

Aligning a Secondary Credential

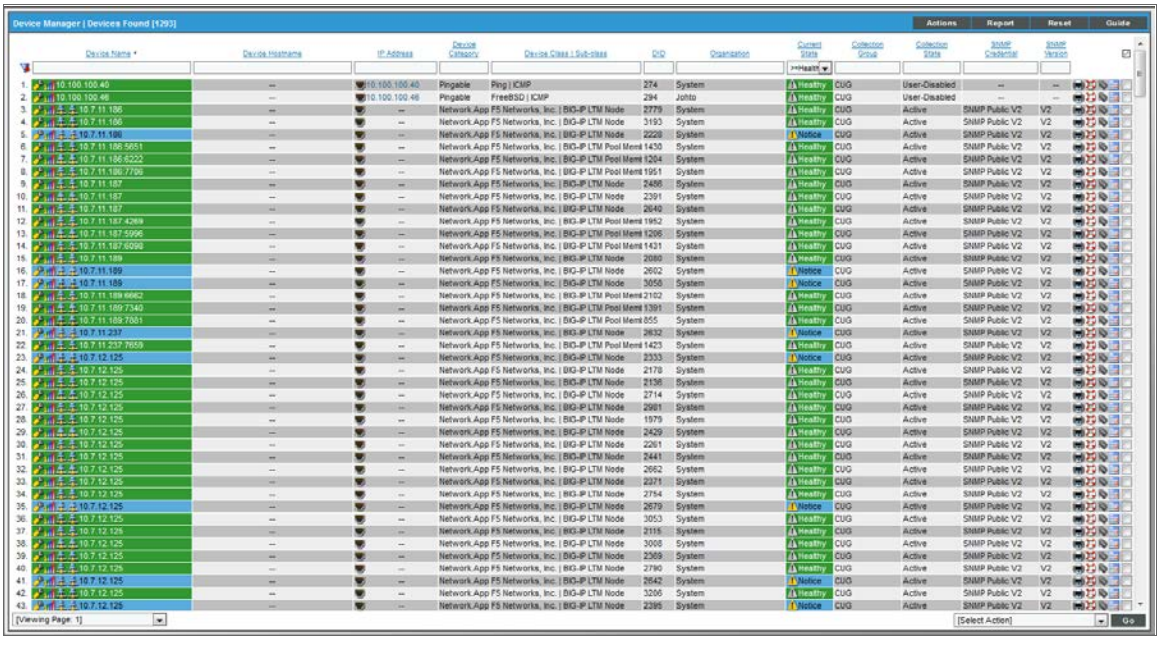
During initial discovery of a device, SL1 uses a specified SNMP credential. If you specified that SL1 should discover non-SNMP devices, SL1 will use ICMP and nmap to gather information about a device. After SL1 finds devices, discovery can use a second list of specified credentials to access database data, SOAP data, XML data or data that is monitored with a Snippet Dynamic Application.

After initial discovery, you can add additional credentials to a device. For example, if more than one SNMP agent is running on the device, each agent can now be associated with its own credential. If SL1 will be monitoring multiple applications on the device, each application can now be associated with its own credential. During the next discovery session, SL1 will use the appropriate credential for each agent or application on the device.

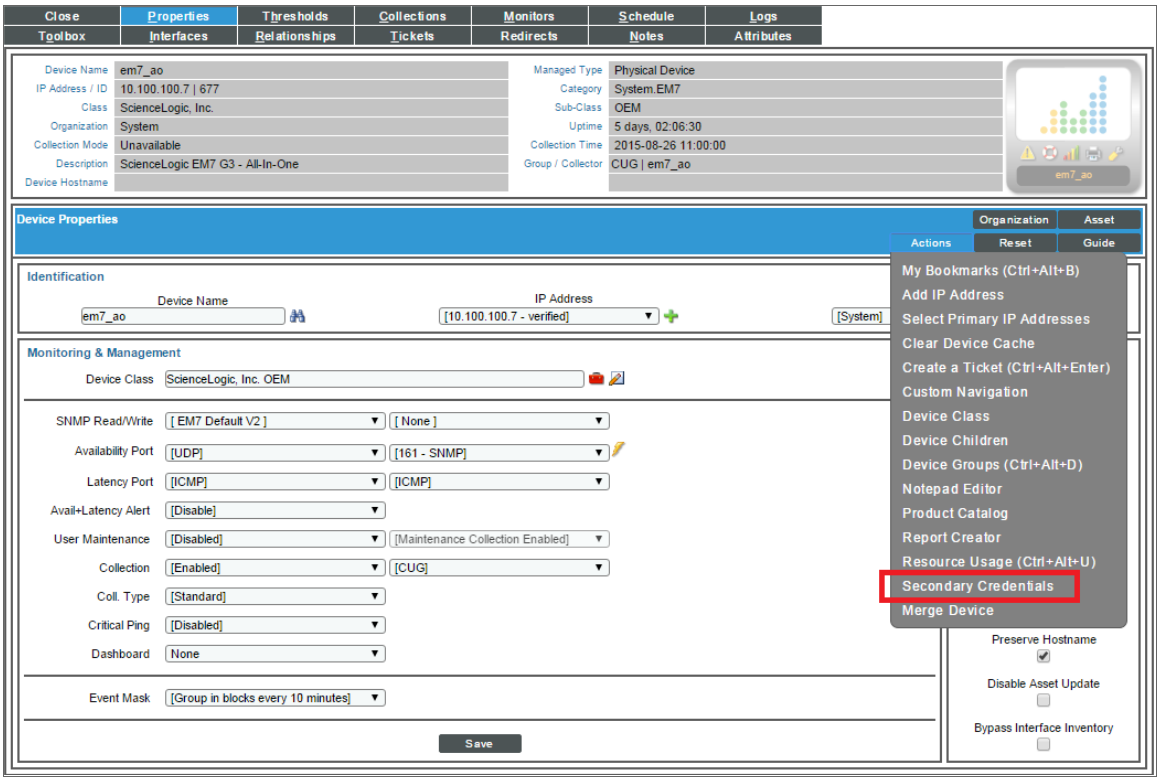
NOTE: When performing a nightly discovery on a device or when performing a manual discovery on a device, SL1 uses the credentials in this order: 1) Each credential manually aligned with each Dynamic Application in the **Dynamic Application Collections** page, in the **Device Administration** panel; 2) Secondary credentials defined in the **Device Properties** page, in the **Device Administration** panel; 3) The SNMP Read/Write string defined in the **Device Properties** page, in the **Device Administration** panel; 4) The credential used in the initial discovery session for the device.

To associate one or more additional credentials with a device:

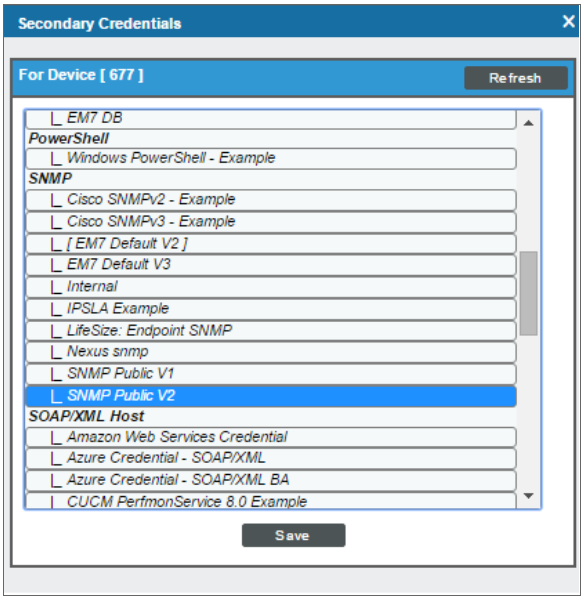
1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to define additional credentials. Select the wrench icon ( ) for the device.



3. In the **Device Properties** page, select the **[Actions]** menu and choose ***Secondary Credentials.***



4. The **Secondary Credentials** modal page appears. The **Secondary Credentials** modal page displays a list of all credentials defined in SL1.



NOTE: When defining primary and secondary credentials for a device, you will see only the credentials aligned to organizations you are a member of. If a primary or secondary credential has already been defined on the device, and is aligned to an organization you are not a member of, the credential will be restricted. To learn more about credentials and organizations, see the manual ***Discovery and Credentials***.

- ***To add a credential***, highlight an entry in the list of credentials.
- ***To select multiple credentials***, hold down the **<CTRL>** key and select the entries by left-clicking.
- ***To remove all secondary credentials from a device***, select the ***Remove All/None*** option.

5. Select the **[Save]** button.

Adding the Device to a Device Group

A ***device group*** is a group of multiple devices. Device groups allow you to configure and edit multiple devices simultaneously. You can view a list of existing device groups, edit a device group, or define a new device group in the **Device Group Editor** page (Devices > Device Groups).

Device configuration templates allow you to save a device configuration and apply it to one or more devices, and re-use the same configuration over and over again. A device template contains pre-defined settings for all the fields in the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page. Device templates can also apply policies for interface monitoring, port monitoring, web-content monitoring, service monitoring, and process monitoring and align devices with Dynamic Applications. You can view and define device templates in the **Configuration Templates** (Devices > Templates) page.

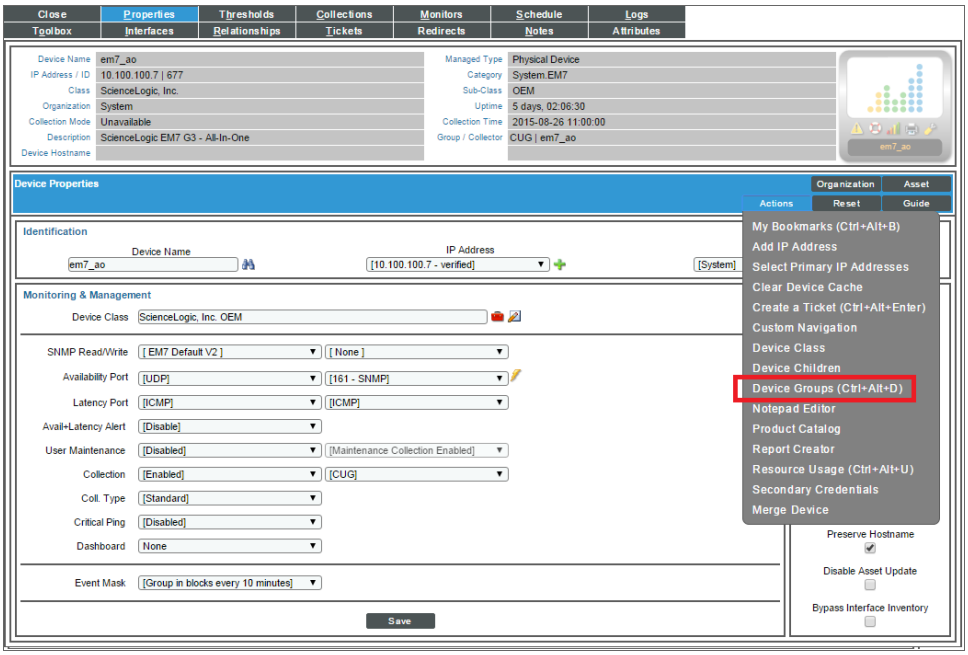
You can apply device configuration templates to a device group and automate the initial configuration of multiple devices. You can also use device groups and device configuration templates to modify the configuration of multiple devices.

For details on device groups and device templates, see the manual ***Device Groups and Device Templates***.

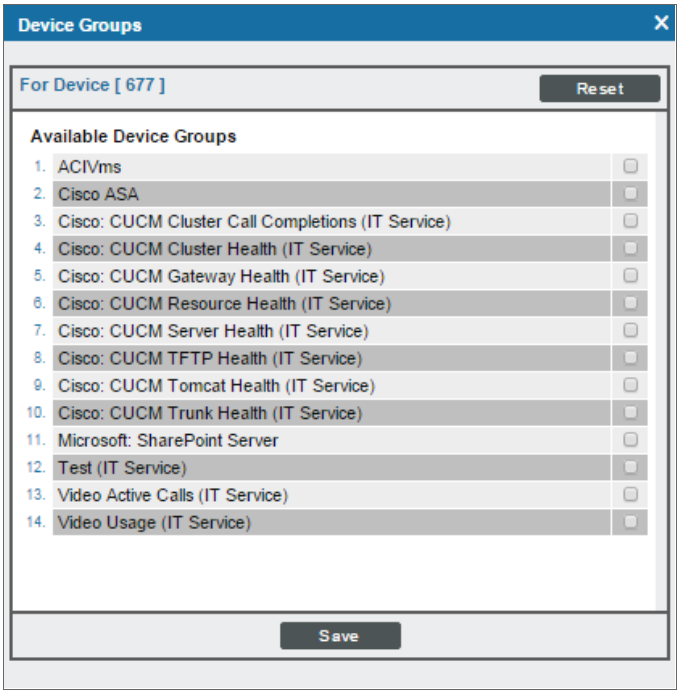
To add a device to an existing device group:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device that you want to add to a device group. Select the wrench icon ( ) for the device.

3. In the **Device Properties** page, select the **[Actions]** menu and choose ***Device Groups***.



4. The **Device Groups** modal page appears. The **Device Groups** modal page allows you to assign a device to a device group or remove a device from a device group.



- ***To add the device to a device group***, in the **Available Device Groups** pane, select one or more device groups. After selecting the **[Save]** button, the device group will appear in the **Member Device Groups** pane.
- ***To remove the device from a device group***, in the **Member Device Groups** pane, select one or more device groups. After selecting the **[Save]** button, the device group will appear in the **Available Device Groups** pane.

5. Select the **[Save]** button.
6. To remove the device from a device group, in the **Member Device Groups** pane, select one or more device groups.
7. Select the **[Save]** button.

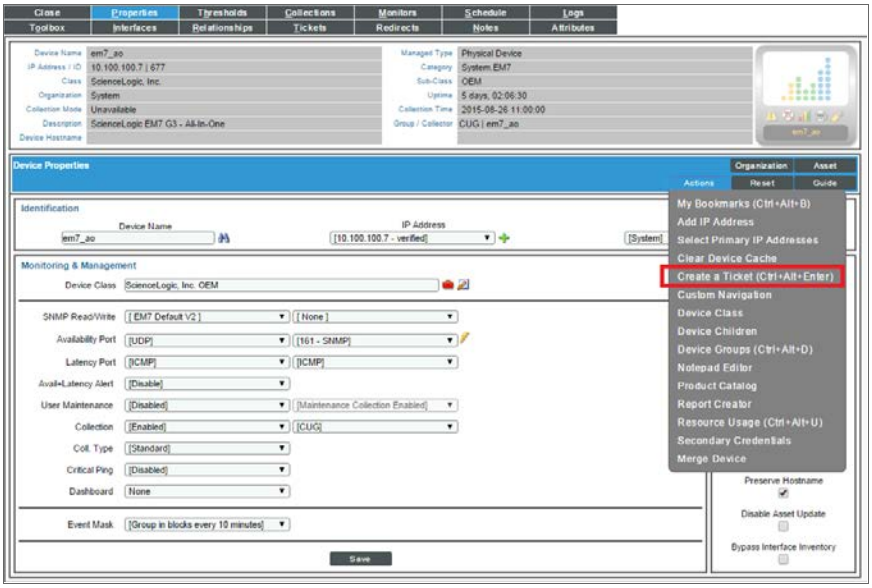
Creating a Ticket About the Device

A ticket is a request for work. Tickets allow you to monitor work tasks associated with your network. You can create a ticket about a device. The ticket can describe a problem with the device or a maintenance task for the device.

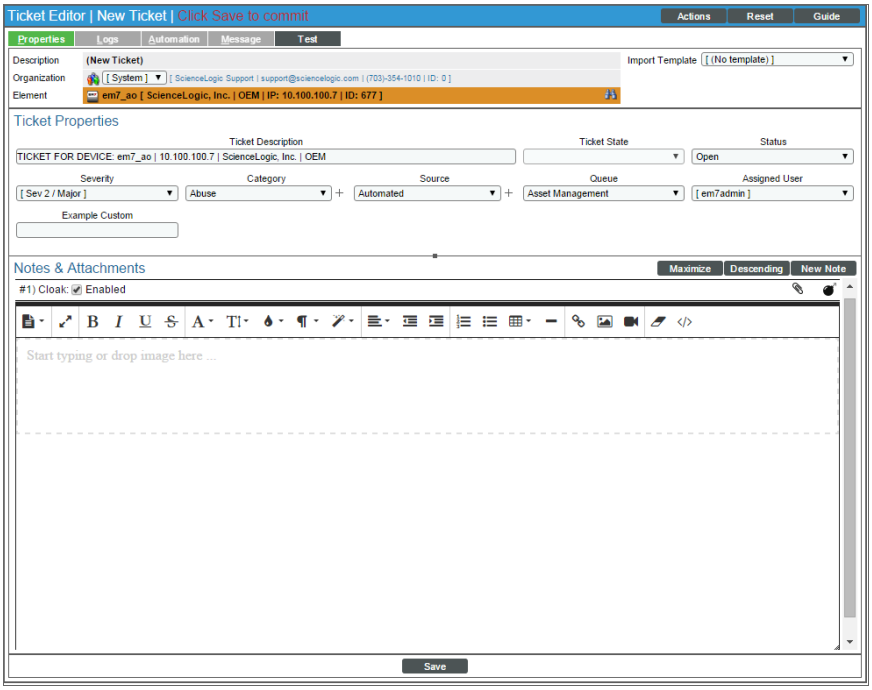
For details on tickets and ticketing, see the manual ***Ticketing***.

To create a ticket for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device about which you want to create a ticket. Click the wrench icon ( ) for the device.
3. In the **Device Properties** page, click the **[Actions]** menu and select ***Create a Ticket***.



4. The **Ticket Editor** page appears. In this page, you can define the basic parameters for a ticket. Notice that the ***Description*** field and ***Element*** field are automatically populated with the device name.



5. Click the **[Save]** button to save the ticket.

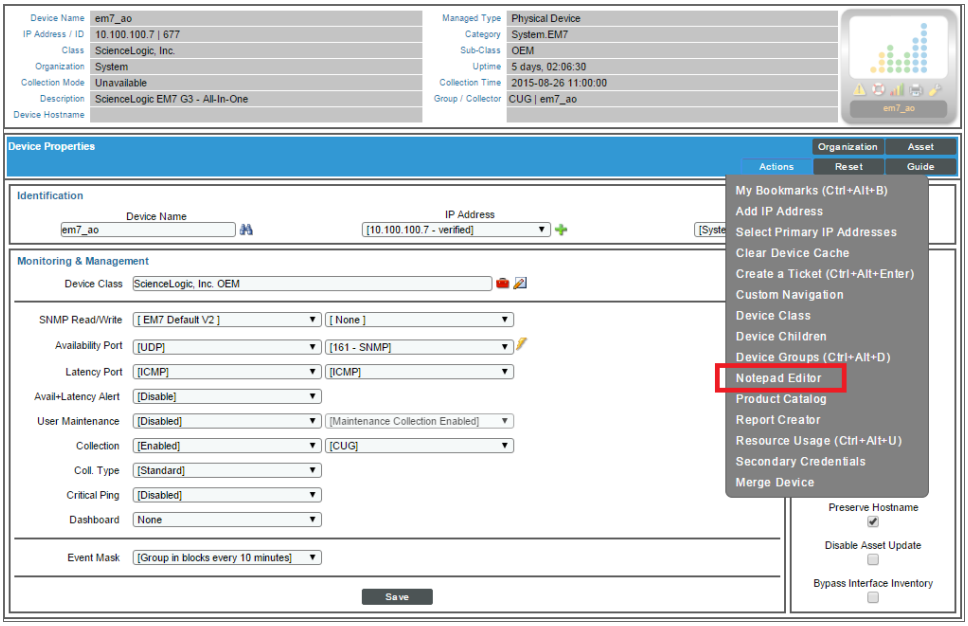
Adding a Note to a Device

You can add notes about a device to the device administration panel. The note will appear in the **Notes & Attachments** page (the **[Notes]** tab in the **Device Administration** panel). Each note you add to the device can include formatted text, links, images, videos, and attachments.

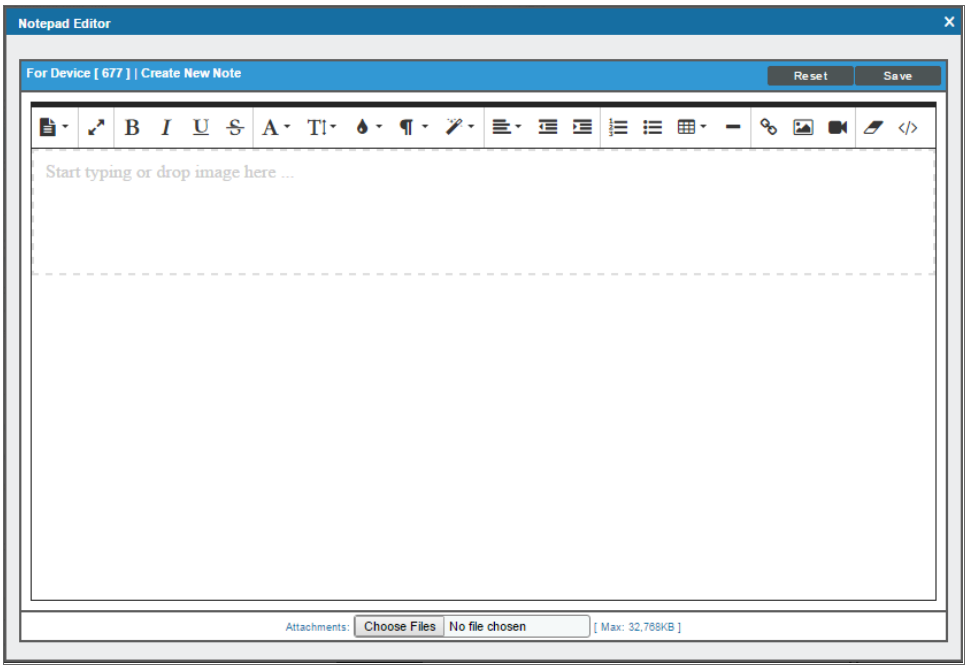
To add a note to a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device that you want to add a note to. Click the wrench icon ( ) for the device.

3. In the **Device Properties** page, click the **[Actions]** menu and select ***Notepad Editor***.



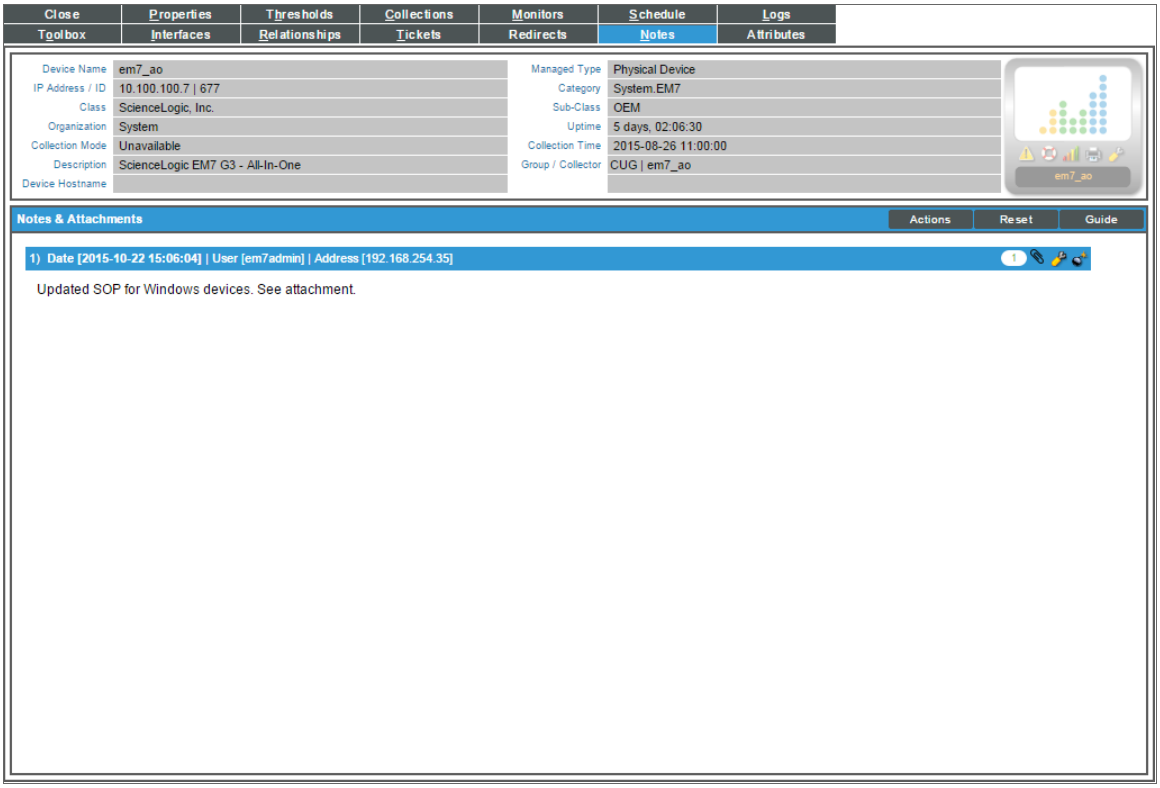
4. The **Notepad Editor** modal page appears. In this page, you can enter and format text, include images and links in the message, and include an attachment. Click the **[Save]** button to save the note.



5. The **Notepad Editor** modal page allows you to enter notes or comments about the device.

    - You can format the text and include links, images, and videos in the note.
    - You can also include a document template (System > Customize > Document Templates) in the field.

6. The note will appear in the **[Notes]** tab, in the **Notes & Attachments** page.



7. The **Notes & Attachments** page displays all the notes about the device that were created with the **Notepad Editor** modal page. In the **Notes & Attachments** page, each entry includes the username, date and time, and text of the comment. You can perform the following on each note entry:

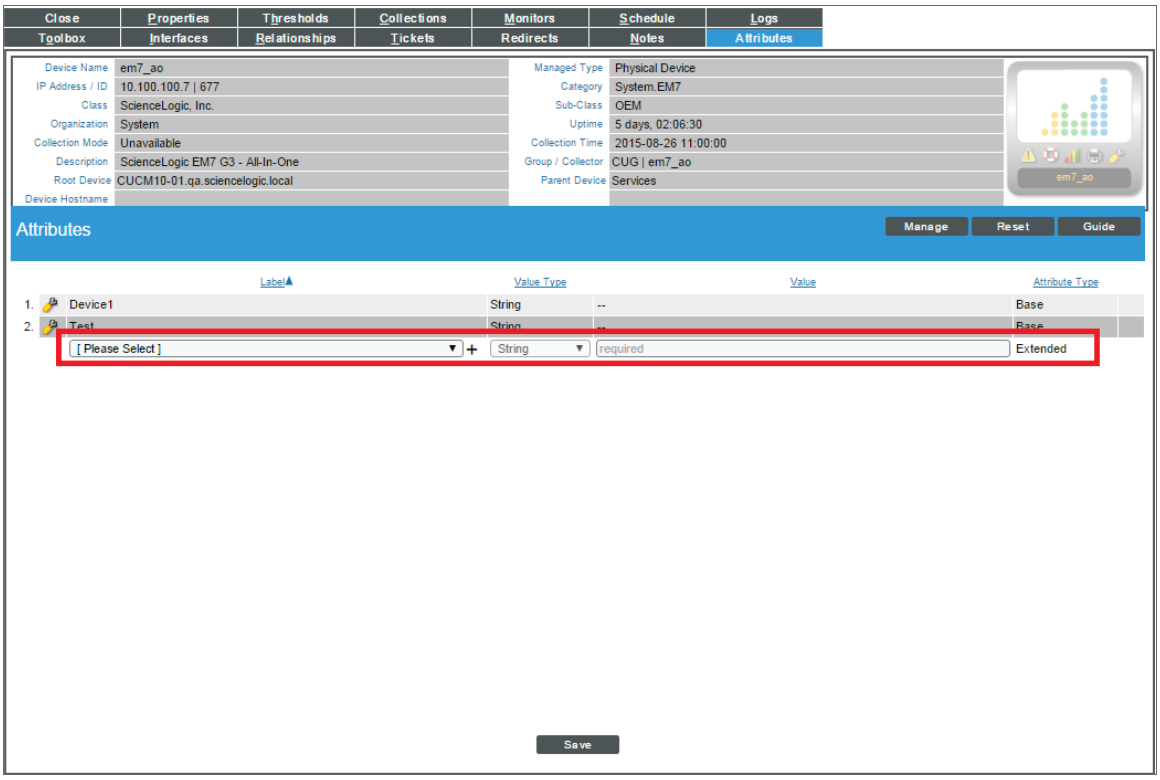
    - ***To view a note's attachment***, click the paperclip icon ( ).
    - ***To edit the content of a note***, click the wrench icon ( ). The **Notepad Editor** modal page appears. You can update the note; format the text; insert content from a saved template; and add an attachment, image, or video to the note. Click the **[Save]**button to save your changes.
    - ***To delete a note***, click its bomb icon ( ).

Aligning Custom Attributes with a Device

You can align custom attributes with a device, assign values to those custom attributes (for the selected device only), and create new extended custom attributes for a device on the **Attributes** page (the **Attributes** tab in the **Device Administration** panel).

To align custom attributes with a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device that you want to align with a custom attribute. Click its wrench icon ( ).
3. Click the **[Attributes]** tab.
4. In the **Attributes** page, go to the ***Please Select*** field in the bottom-most row.



5. Select the custom attribute that you want to align with the device.
6. Supply a value in the ***Value*** field.

NOTE: To align an extended custom attribute with a device, you must supply a value. You cannot align an extended custom attribute to a device and leave the value as "null."

NOTE: Base custom attributes for devices are automatically aligned with each device in your SL1 System. If the base custom attribute does not include a value for this device, the ***Value*** column will display "--" (dash dash). To assign a value to an "empty" base custom attribute: Find the base custom attribute that you want to edit, select its wrench icon ( ), and supply a value in the ***Value*** field.

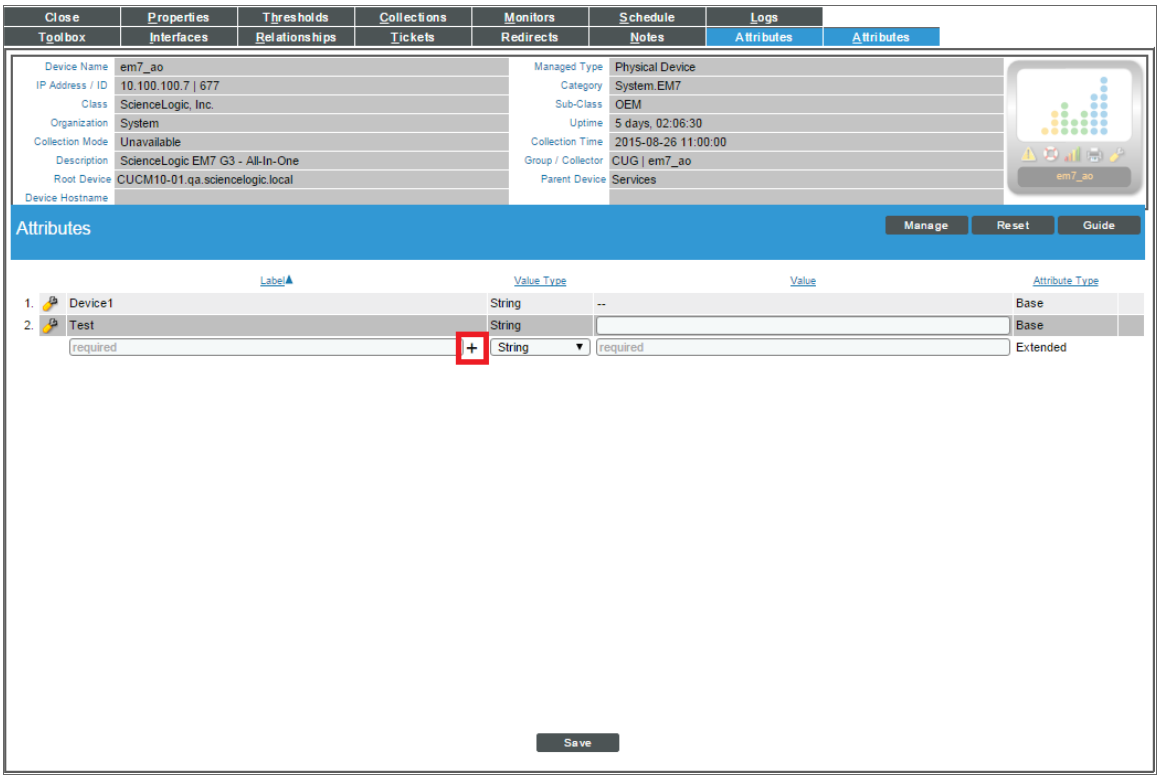
7. Click the **[Save]** button.

Creating a New Extended Custom Attribute

You can create a new extended custom attribute from the **Attributes** page. The custom attribute is then aligned with the current device and available to be used by any device in your SL1 System. To create a new extended custom attribute:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to create a new custom attribute. Click its wrench icon ( ).
3. Click the **[Attributes]** tab.

4. In the **Attributes** page, click the plus icon (+) in the bottom-most row, then supply a value in the following fields:



- ***Label***. User-defined name for the custom attribute. This value appears in the user interface. If the value in this field does not comply with XML rules for names, SL1 will convert the value to a name that complies with XML rules and store the converted value as the ***Internal Field Name*** for the custom attribute.

NOTE: Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character or an extending character. If a value in the ***Internal Field Name*** column does not conform to XML standards, SL1 will replace non-valid characters with an underscore plus the hexadecimal value of the illegal character plus an underscore. So "serial number" would be replaced with "serial_X20_ number".

- ***Value Type***. Specifies the type of value that will be saved in the custom attribute. Choices are:
  - *String*. Non-numeric value
  - *Integer*. Numeric value
- ***Value***. Value that will be assigned to the custom attribute for this device.

5. Click the **[Save]** button.

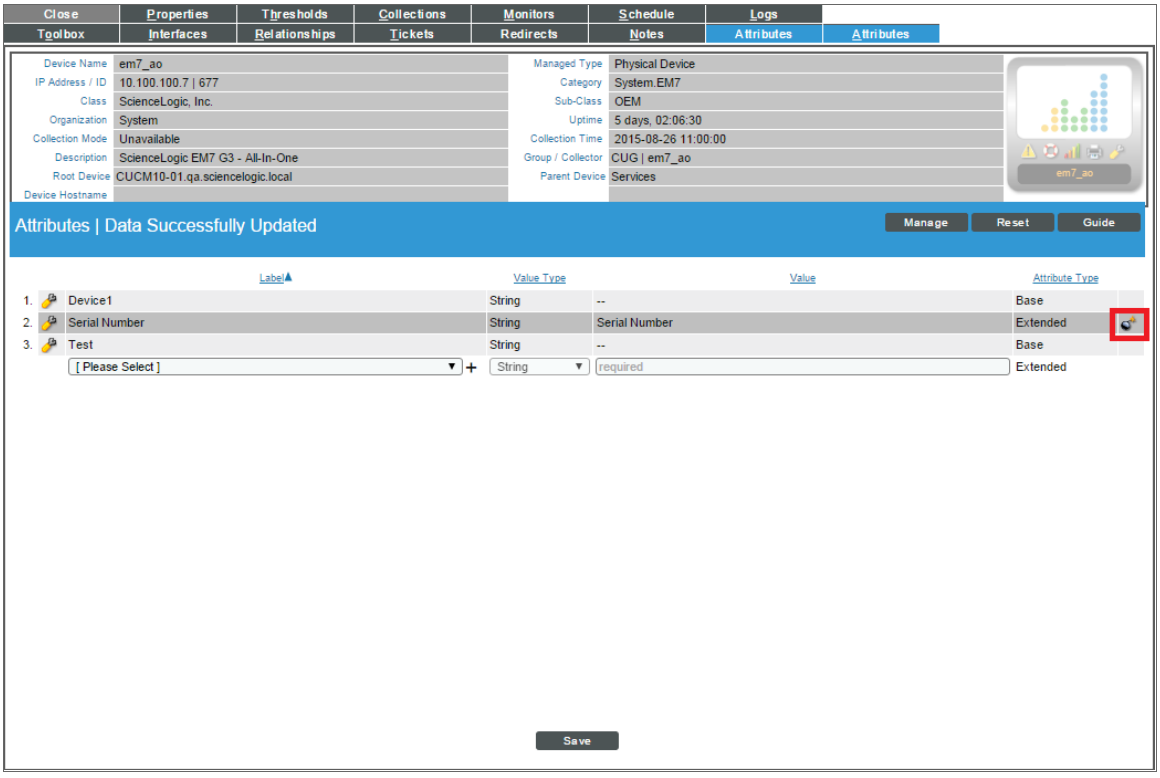
Deleting an Extended Custom Attribute from a Device

You can delete an extended custom attribute from a device. When you delete the custom attribute, you remove the value from the custom attribute and unalign the custom attribute with the device.

> **NOTE:** You cannot delete a base custom attribute from the **Attributes** page. To delete a base custom attribute, you must go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes).

To delete an extended custom attribute from a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to delete a custom attribute. Click its wrench icon ( ).
3. Click the **[Attributes]** tab.
4. In the **Attributes** page, find the extended custom attribute you want to delete. Click its bomb icon ( ).



5. A message appears asking you to confirm that you want to delete the value and unalign the custom attribute from the device.
6. Click the **[OK]** button.

Associating a Product SKU with the Device

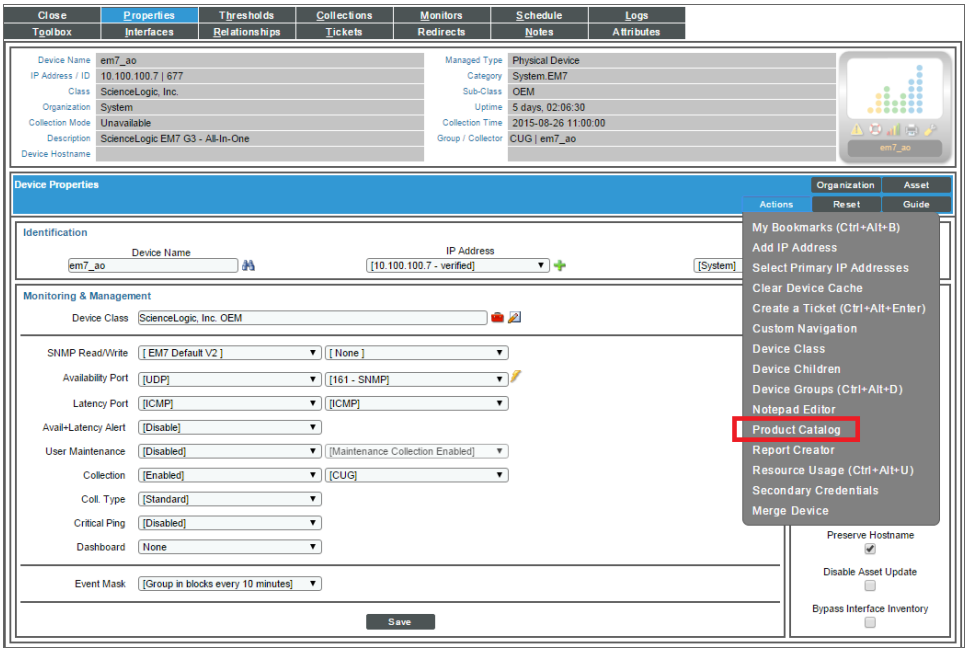
A product SKU describes a billable product or service and can be used later to create a billing policy. For details on creating and editing product SKUs, see the **Product Catalog** page (Registry > Business Services > Product Catalog). For information on billing policies, see the **Bandwidth Billing Policies** page (Registry > Business Services > Bandwidth Billing).

You can associate a product SKU with a device and then use a bandwidth billing policy to generate a bill that includes the device.

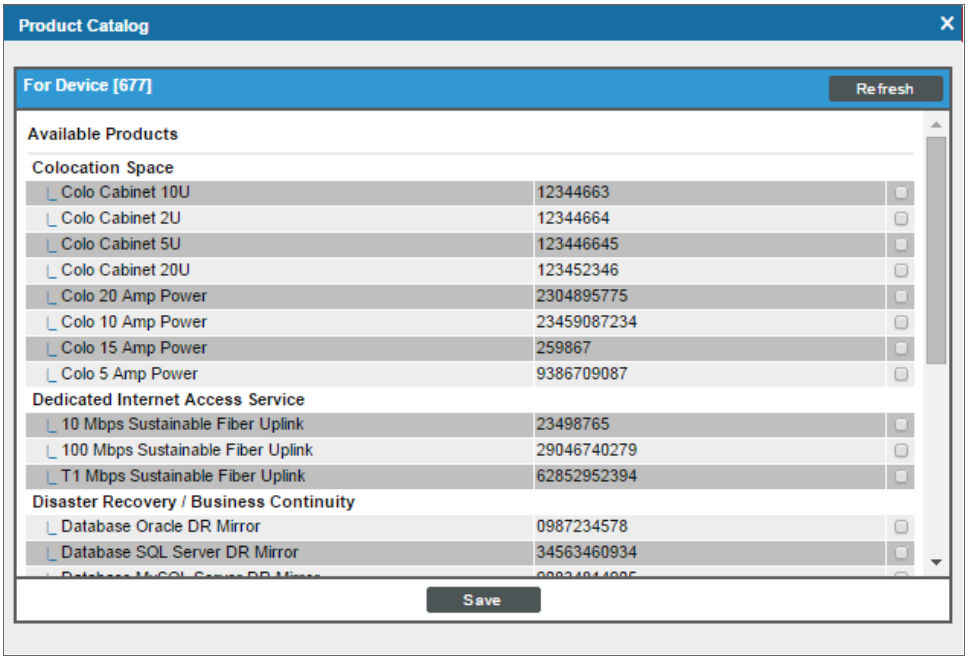
For details on product SKUs and bandwidth billing policies, see the manual ***Business Services***.

To associate a product SKU with a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device that you want to add a note to. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, select the **[Actions]** menu and choose ***Product Catalog***.



4. The **Product Catalog** modal page appears. In this page, you can associate one or more product SKUs with the device.



- ***To associate a product SKU with the device***, in the **Available Products** pane, select one or more product SKUs.
- ***To disassociate a product SKU with a device***, in the **Active Product Subscriptions** pane, select one or more product SKUs.

5. Select the **[Save]** button.

Merging Devices

If your SL1 system includes a physical device and a component device, you can merge those device records into a single record for easier monitoring. Merging consolidates the devices and their data—device fields, values, graphs, behaviors, and other user interface elements—providing you with a single set of data for the device. Additionally, merged devices consume only a single device license.

Merging does not remove, replace, or add any data; merging simply groups data together. When you merge a physical device and a component device, the device record for the component device no longer displays in the user interface, while the device record for the physical device displays in user interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the record for the physical device.

Merged devices can be unmerged back into individual device records, if needed.

NOTE: You can merge only two individual devices together into a single merged device. To do so, you must have user permissions that allow merging and unmerging on both devices.

NOTE: When you merge devices, active events associated with the component device will be set to "cleared." The cleared events will not be associated with the physical device. If the devices are unmerged, the cleared events cannot be moved back to the component device.

CAUTION: Merging devices also merges the log data from each device. The log data cannot later be unmerged.

SL1 enables you to either merge one pair of devices at a time, as described in the *Merging Individual Devices* section, or multiple pairs of devices at one time, as described in the *Performing a Bulk Device Merge* section. For information about unmerging devices, see the *Unmerging Individual Devices* section or the *Performing a Bulk Device Unmerge* section.

Merging Individual Devices

If you have a small number of physical and component devices that you want to merge, you can merge each device pair individually.

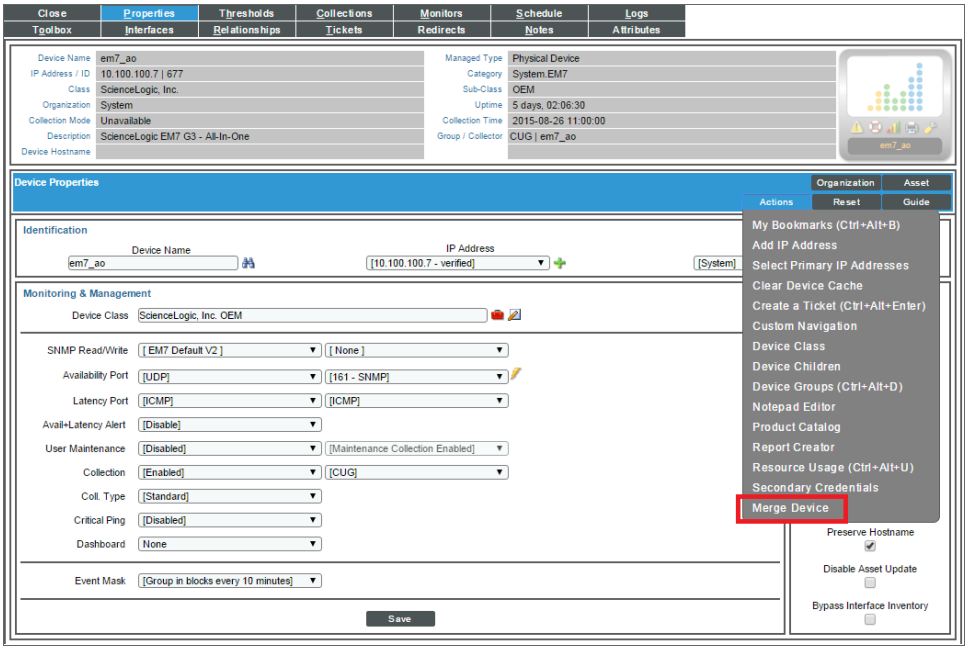
NOTE: If you have a large number of devices you want to merge, it might be more efficient to use the Bulk Merge feature, which is described in the *Performing a Bulk Device Merge* section.

NOTE: For clarity, the following instructions describe how to merge a physical device from the **Device Manager** page with a selected component device, but the process is the same when merging a component device from the **Device Manager** page with a selected physical device.

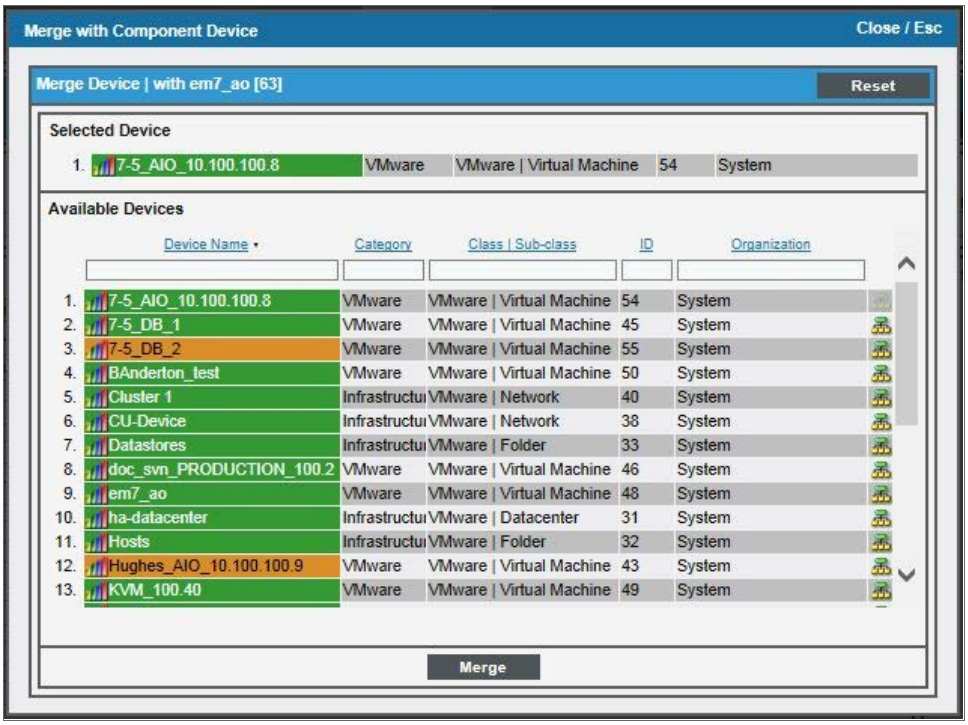
To merge individual devices:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Click the wrench icon ( ) for the physical device that you want to merge with a component device.

3. On the **Device Properties** page, click the **[Actions]** menu and then select *Merge Device*.



4. A list of component devices that are available for merging with the physical device displays. Click the merge icon ( ) for the component device you want to merge with the physical device. Information for the component device then displays in the **Selected Device** panel.



5. Click the **[Merge]** button. A pop-up message appears that asks you to confirm the merge.

6. Click the **[OK]** button.

> **NOTE:** To view an updated list of devices that includes your merged devices, click the **[Reset]** button on the **Device Manager** page.

Unmerging Individual Devices

You can unmerge any pair of physical device and component device that are currently merged. When you unmerge devices, SL1 does not delete any devices or device data; the devices are simply separated into two separate device records.

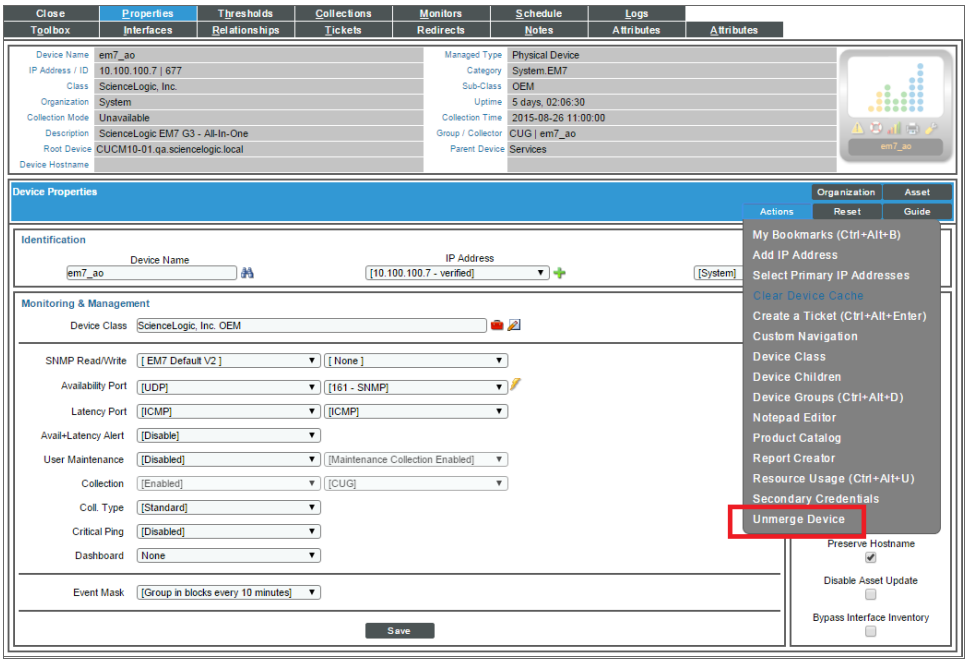
> **NOTE:** If you have a large number of devices you want to unmerge, it might be more efficient to use the Bulk Unmerge feature, which is described in the *Performing a Bulk Device Unmerge* section.

> **CAUTION:** The log data associated with the devices cannot be unmerged. After the devices are unmerged, all log data that was generated before the devices were unmerged is associated with the physical device record.

To unmerge individual devices:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Select the wrench icon ( ) for the device that you want to unmerge.

3. On the **Device Properties** page, select the **[Actions]** menu and then choose ***Unmerge Device***.



4. A modal window displays that asks you to confirm the unmerging. Select the **[Unmerge]** button.

NOTE: To view an updated list of devices that includes your unmerged devices, select the **[Reset]** button on the **Device Manager** page.

Performing Administrative Tasks for One or More Devices

The **Device Manager** page (Devices > Device Manager) contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once.

To apply an action to multiple devices:

1. In the **Device Manager** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the red checkbox ( ) at the top of the page.
2. In the ***Select Action*** drop-down list, select one of the following actions:

    - ***Delete Devices***. Deletes all selected devices from SL1. Tickets associated with the device are unlinked from the device, but are not deleted.
    - ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device templates to all selected devices. You can also make one-time changes to the template, that will be applied only to the selected devices.
    - ***Clear Device Logs***. Deletes data from the device's log files.
    - ***Create Asset Record***. Automatically creates an asset record for the device. SL1 automatically populates as many fields as possible, using retrieved data.
    - ***Schedule Maintenance***. Leads to the **Maintenance Schedule** page. In this page, you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, SL1 will not generate events about the selected devices. You can choose to enable or enable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate events for the devices.
    - ***Find Collection Label Duplicates***. Leads to the **Duplicates** page. In this page, you can view a list of devices where the Collection Labels have more than possible presentation object aligned. From this page, you can manually align a single presentation object with a Collection Label for a device.
    - ***Change Collection State***. Changes the status of the device in SL1. The choices are:

        - *Active*. SL1 polls the device on a regular basis and updates the data displayed in SL1.
        - *Disabled*. SL1 does not poll the device. Data displayed in SL1 is not updated.

- ***Change Maintenance Mode***. These options allow you to enable User-Initiated-Maintenance and disable both User-Initiated-Maintenance and scheduled Maintenance.

  When a device is in User-Initiated-Maintenance, by default SL1 will not generate events about the device. If you want to allow events during User-Initiated-Maintenance, you can specify which events to allow in the **Behavior Settings** (System > Settings > Behavior) page. You can choose to enable or disable polling. If polling is enabled during User-Initiated-Maintenance, SL1 will collect information from the device but will generate only the events you specified in the **Behavior Settings** page. By default, SL1 will not generate any events. User-Initiated-Maintenance mode is not scheduled. That is, a user must manually enable User-Initiated-Maintenance to turn off this mode for a device. User-Initiated-Maintenance Mode overrides scheduled maintenance for a device. Choices are:

  - *Enabled with Collection*. One or more devices are set to User-Initiated-Maintenance mode. During User-Initiated-Maintenance mode, SL1 will continue to poll the device.
  - *Enabled without Collection*. One or more devices are set to User-Initiated-Maintenance mode. During User-Initiated-Maintenance mode, SL1 will not poll the device.
  - *Disabled*. User-Initiated-Maintenance mode is disabled for each selected device.

- ***Change Collector Group***. Changes the collector group used to collect data from the device. Choose from the list of all collector groups in SL1. When you select one of the collector groups, each selected device will be polled by the collectors in the collector group. For All-In-One Appliances, you can select only the built-in Collector Group and any virtual Collector Groups.
- ***Move To Organization***. Associates a device with an organization. The list of choices will include all organizations in SL1.
- ***Align SNMP Read Credential***. This option applies the selected credential to all selected devices. The selected devices will use the selected credential as their primary credential. Secondary credentials will remain unchanged. Choose from a list of SNMP Read credentials (defined in System > Manage > Credentials). The list will include only credentials that you are allowed to use.
- ***Add to Device Group***. This option aligns the selected devices with the selected device group. The selected devices will then appear in **Device Group Views** and will inherit the properties of the device group, including scheduling, access, and visibility.
- ***Align to Device Dashboard***. This option aligns the selected devices with the selected device dashboard. The selected device dashboard will appear as the default view in the **Device Summary** page.

3. Select the **[Go]** button.
4. The selected action is applied to each selected device.

Shortcut Keys for Device Administration panel

When you edit a device (select its wrench icon ( ), you enter the **Device Administration** panel.

When you enter the **Device Administration** panel, you can use the following shortcut keys to navigate the tabbed pages and the entries in the **[Actions]** menu.

Page or Tab	Shortcut Keys
Administer Bookmarks page	Ctrl + Alt + B
Dynamic Application Collectionspage	Ctrl + Alt +C
Device Groups page	Ctrl + Alt + D
Guides page	Ctrl + Alt + G
Device Thresholds page	Ctrl + Alt + H
Device Interfaces page	Ctrl + Alt + I ("eye")
Device Logs & Messages page	Ctrl + Alt + L
Monitoring Policies page	Ctrl + Alt + M
Notes & Attachments page	Ctrl + Alt + N
Device Toolbox page	Ctrl + Alt + O ("oh")
Device Properties page	Ctrl + Alt + P
Maintenance Schedule page	Ctrl + Alt + S
Ticket History page	Ctrl + Alt + T
Resource Usage page	Ctrl + Alt + U
Exit Device Administration panel	Ctrl + Alt + X
Device Properties page	Ctrl + Alt + . ("period")
Ticket Editor page	Ctrl + Alt + <Enter>

Chapter 6

Device Toolbox

Overview

This chapter describes the **Device Toolbox** page.

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

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

This chapter includes the following topics:

What is the Device Toolbox? *164*

Accessing the Device Toolbox page *164*

Viewing the Session Logs *167*

What is the Device Toolbox?

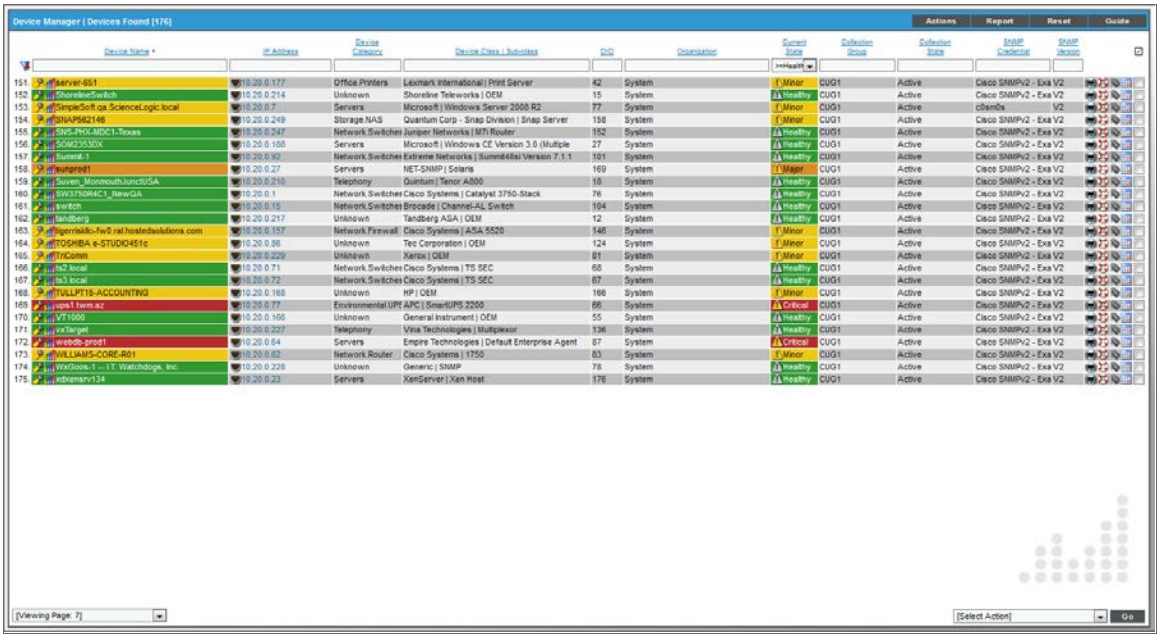
The **Device Toolbox** page allows you to access common network tools. The list of tools available depends upon the type of device and the configuration of the device.

The **Device Toolbox** page allows you to run diagnostics on a device and access devices without leaving the user interface session.

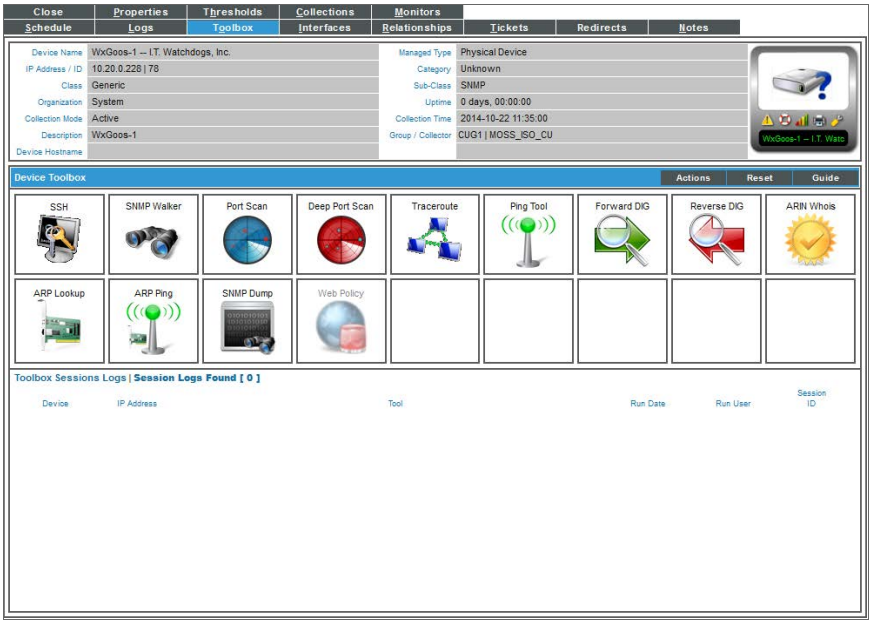
Accessing the Device Toolbox page

To access the **Device Toolbox** page:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to access the **Device Toolbox** page. Select its wrench icon ( ).



3. In the **Device Administration** panel, select the Toolbox tab.



4. Depending on the device, the **Device Toolbox** page can display one or more of the following buttons. These tools run on the Data Collector that is currently monitoring the device unless otherwise noted:
    - ***FTP***. Opens a new browser window and attempts to make an FTP connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 21) is detected as open by SL1.
    - ***SSH***. Opens an SSH session on the device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 22) is detected as open by SL1.

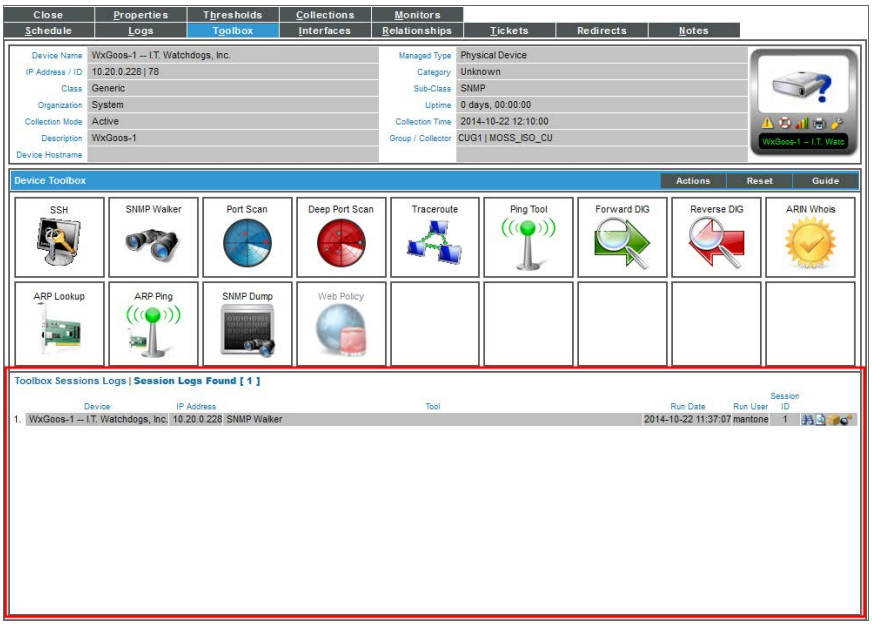
      NOTE: The SSH tool is not available for SL1 systems that are configured as military unique systems.

    - ***Telnet***. Opens a browser session or terminal session using the IP address of the current device and prompts you for the telnet username and password. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 23) is detected as open by SL1.
    - ***Terminal***. Opens the **Terminal Services Client Web Connection** modal page, where you can enter the login information for the terminal services session. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 3389) is detected as open by SL1.
    - ***Web***. Opens a new browser window and attempts to make an http connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector.
    - ***Secure Web***. Opens a new browser window and attempts to make an HTTPS connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 443) is detected as open by SL1.
    - ***SNMP Walker***. Opens the SNMP Walker modal page, where you can perform an SNMP walk on the device. If the device has an IPv6 address, SL1 will use the appropriate IPv6 SNMP command.
    - ***Port Scan***. Leads to the **Port Scan** modal page, where you can view a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Leads to the **Deep Port Scan** modal page, where you can view a list of all open ports and view as much detail about each open port as the deep port scanner can retrieve.
    - ***Traceroute***. Leads to the **Traceroute** modal page, where you can view the network route between SL1 and the device. If the device has an IPv6 address, SL1 will use the appropriate IPv6 traceroute command.
    - ***Ping Tool***. Leads to the **Ping_Tool** modal page, where you can view the statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, SL1 will use the appropriate IPv6 ping command.
    - ***Forward DIG***. Leads to the **Forward DIG** modal page, where you can view the output from the DIG utility. This tool automatically finds all available DNS information about the domain associated with the current device.

- ***Reverse DIG***. Leads to the **Reverse DIG** modal page, where you can view the output from the reverse DIG utility. The reverse DIG tool retrieves the domain name that is associated with the device's IP.
- ***ARIN Whois***. Leads to the **ARIN Whois** modal page, where you can view the output from the Whois utility. The Whois utility displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
- ***ARP Lookup***. Leads to the **ARP Lookup** modal page, where you can view the results from the ARP Lookup tool. The ARP Lookup tool displays a list IP addresses for the device and the resolved Ethernet or Token Ring physical addresses (MAC addresses) for each IP address.
- ***ARP Ping***. Leads to the **ARP Ping** modal page, where you can view the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it operates using ARP instead of ICMP. The ARP Ping tool can be used only on the local network.
- ***SNMP Dump***. Leads to the **SNMP Dump** modal page, where you can view the results of the SNMP Dump. The SNMP Dump tool retrieves each OID and its corresponding value from the device.
- ***Web Policy***. Leads to the **Web Policy** modal page, where you can manually run a web-content policy on the device. This tool is initiated from the user's machine and does not run on the collector. This tool appears only if a Web Content Monitoring Policy has been configured for the device.

Viewing the Session Logs

After you run a tool in the Device Toolbox, information about the session appears the **Toolbox Sessions Logs** pane (at the bottom of the page).



For each session, you can view the following:

- ***Device***. Device associated with the session.

- ***IP Address***. IP address that was polled by the session.
- ***Tool***. Tool that was run.
- ***Run Date***. Date the session occurred.
- ***Run User***. User who initiated the session.
- ***Session ID***. Unique numeric identifier automatically assigned to the session by SL1.

From the **Toolbox Sessions Logs** pane, you can also:

- View an SNMP Walk Session ( ).
- View raw data from the session ( ).
- Export raw data from the session to a file on the local computer ( ).
- Delete a session from the **Toolbox Sessions Logs** pane ( ).

Chapter 7

Managing Device Classes and Device Categories

Overview

This chapter describes how to manage device classes and device categories in SL1.

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

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

This chapter includes the following topics:

Device Classes 170
Generic | SNMP 171
Non-SNMP 171
Component 171
Agent-Only Device Classes 171
Viewing the List of Device Classes 172
Filtering the List of Device Classes 174
Special Characters 175
Creating Device Classes 177
Creating a New Device Class of Type "SNMP-Enabled" 177
Editing an SNMP-Enabled Device Class 181
Creating a New Device Class for a Device with Device Class "Generic | SNMP" 181

Creating a New Device Class for Devices That Do Not Support SNMP *184*
Applying the New Device Class *189*
Maintaining the New Device Class During Auto-Discovery *190*
Editing a Device Class That is Not SNMP-Enabled *190*
Creating a Device Class of Type "Component" *191*
Editing a Device Class of Type "Component" *193*
Legacy Device Classes of Type "ICMP" *193*
Managing Device Classes *194*
Manually Changing the Device Class for a Device *194*
Changing the Icon for a Device Class *196*
Aligning One or More Device Classes with a Device Dashboard *196*
Deleting One or More Device Classes *197*
Device Categories *198*
Viewing the List of Device Categories *198*
"Pingable" Device Category *199*
Creating a New Device Category *199*
Editing a Device Category *201*
Deleting a Device Category *201*
Aligning One or More Device Categories with a Device Dashboard *202*

Device Classes

In SL1, each device is associated with a device class. Typically, a ***device class*** maps to a make/model pair. When possible, SL1 automatically assigns each discovered device to a device class. Device classes determine:

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

SL1 includes already-defined device classes for the most popular hardware. The **Device Class Editor** page (System > Customize > Device Classes) allows advanced administrators to define new or legacy device classes in SL1 and to customize properties of existing device classes.

Most TCP/IP-compliant devices have an internally-defined class ID, called the System Object ID and abbreviated to SysObjectID. This SysObjectID is an SNMP OID defined by the manufacturer. Each manufacturer specifies a SysObjectID for each different hardware model. In SL1, each SNMP device class is associated with a SysObjectID. During initial discovery, SL1 searches each device for the SysObjectID and assigns each device to the appropriate device class.

SL1 also includes device classes for devices that do not support SNMP. These device classes are associated with values returned by nmap. SL1 runs nmap against each device during discovery.

Generic | SNMP

SL1 includes a default device class for devices that include a SysObjectID but for which SL1 does not have an aligned device class. This device class is ***Generic | SNMP***.

For each device with a device class of ***Generic | SNMP***, you can use SL1 to view the SysObjectID for the device and then define a new device class using that SysObjectID.

Non-SNMP

SL1 also includes device classes for devices that do not support SNMP. Devices that do not support SNMP are sometimes referred to as "pingable". Devices that have a device category of "pingable" are devices that meet one of the following criteria:

- Device does not support SNMP.
- SNMP has been disabled on the device.
- Wrong credential was provided during discovery and "Discover Non-SNMP" was enabled for the discovery session.

SL1 can use nmap to match a "pingable" device to an appropriate "pingable" device class.

Component

SL1 includes device classes for component devices. SL1 discovers management systems and the component devices they manage. SL1 uses Dynamic Applications to retrieve data from a management system and discover each component device managed by that management system. Device classes for components are aligned with the Dynamic Applications that discover component devices.

Agent-Only Device Classes

SL1 includes device classes for devices that are monitored by the SL1 agent and are not monitored via SNMP.

During initial discovery, the agent returns operating system type and version information to SL1.

Based on this information, SL1 assigns one of the following device classes to a device monitored only by an agent:

- Microsoft Windows Workstation
- Microsoft Windows Cluster Point
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 Domain Controller
- Microsoft Windows Server 2008 R2 Domain Controller

- Microsoft Windows 8.1 Workstation
- Microsoft Windows 8 Workstation
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 Workstation
- Microsoft Windows Server 2012 R2 Domain Controller
- Microsoft Windows 10 Workstation
- Linux Ubuntu 16.04
- Linux Ubuntu 14.04
- Linux Ubuntu 12.04
- Linux Debian 8
- Linux Debian 7
- Linux Debian 6
- Linux Red Hat Enterprise Linux 7
- Linux Red Hat Enterprise Linux 6
- Linux Red Hat Enterprise Linux 5
- Linux Oracle Linux 7
- Linux Oracle Linux 6
- Linux Oracle Linux 5
- Linux CentOS 7
- Linux CentOS 6

NOTE: If a device is monitored by an agent and via SNMP, the device class assigned by SNMP discovery will take precedence.

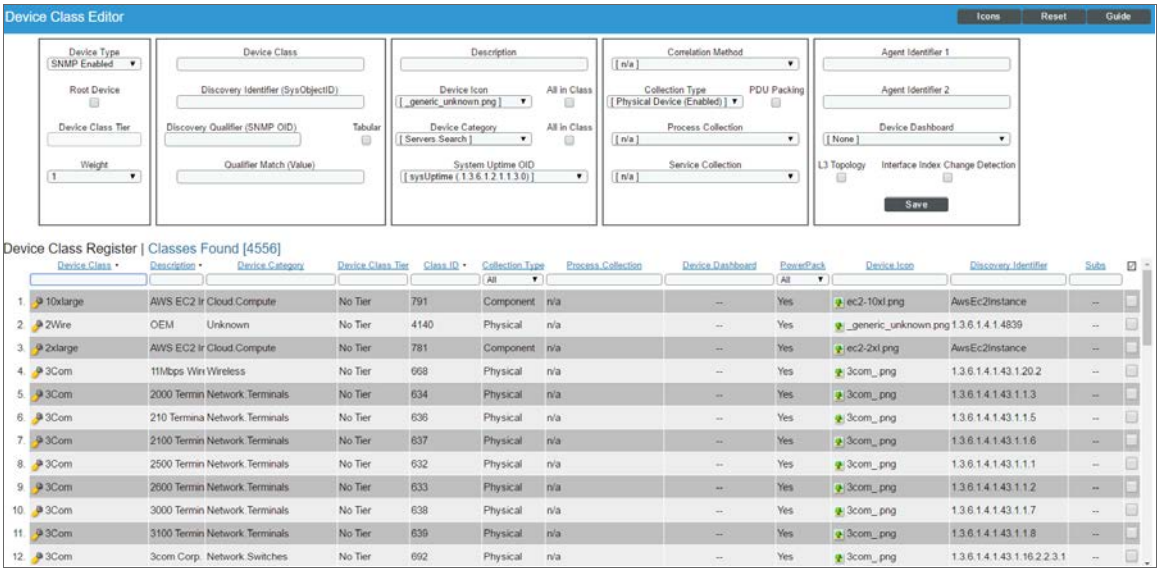
Viewing the List of Device Classes

The **Device Class** page displays a list of existing device classes in the **Device Class Register** pane.

To view the list of device classes:

1. Log in to SL1.

2. Go to the **Device Class** page (System > Customize > Device Classes).



3. For each device class, the **Device Class Register** pane displays:

TIP: To sort the list of device classes, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again.

- ***Device Class Name***. Name of the device class.
- ***Description***. Description of the device class. If the device class is for an entire manufacturer, rather than for a specific product, the description will contain the value "OEM".

NOTE: If you see a device class of ***Ping | ICMP*** or a device with a device category of ***pingable***, this means that the device does not support SNMP, that SNMP has been disabled on the device, or that the wrong SNMP credential was provided during discovery.

NOTE: If you see a device class of ***Generic | SNMP***, this means that SL1 discovered a SysObjectID for the device, but SL1 does not include a device class that aligns with that SysObjectID.

- ***Device Category***. The device category. A device category is a way to categorize devices by primary function. SL1 uses device categories to group related devices in reports and views.The list of device categories is defined in the **Device Category Editor** page (System > Customize > Device Categories).

- ***Device Class Tier***. A read-only field that displays the device tier for subscription billing. The device class tier allows you to calculate the "cost" (according to your license) of each device. By default, this field displays "Standard Device". If you are using a subscription model for billing, this field will display the license tier for the device class.

NOTE: If you create a custom device class, please contact ScienceLogic Customer Support to define the device class tier for the new device class.

- ***Class ID***. Unique numeric ID, automatically assigned to the device class by SL1.
- ***Collection Type***. Device type. Can be either "physical" or "virtual".
- ***Process Collection***. Specifies the application that maintains process information for the device. SL1 will poll this application for information on the system processes. Choices are:
  - *n/a*. Don't monitor processes.
  - *Host Resource*. MIB that provides information on processes.
  - *HP/UX*. Specifies that HP agents will provide information on processes.
  - *Solaris (prior to Solaris 10)*. Specifies that Solaris agents will provide information on processes.
  - *Extended User Information*. Specifies that ScienceLogic's custom extension to net-SNMP will provide process information. Users must have installed the extension before selecting this option.
- ***Device Dashboard***. This field displays the device dashboard associated with the device class.
- ***PowerPack***. This field specifies whether or not this device class is included in a PowerPack.
- ***Device Icon***. The icon associated with the device class. To view the icon, select the picture icon ( ).
- ***Discovery Identifier***. An SNMP OID defined by the manufacturer. Usually, a hardware manufacturer specifies a SysObjectID for each different hardware model.
- ***Subs***. Specifies if one or more devices are aligned with the device class. If so, the devices icon ( ) appears in this column. Selecting the devices column leads to the **Subscribers** modal page, where you can view a list of devices that are aligned with the device class.

Filtering the List of Device Classes

You can filter the list on the Device Class Editor page by one or more parameters. Only device classes that meet all the filter criteria will be displayed in the Device Class Editor page.

For each filter except *Collection Type*, enter text into the desired filter-while-you-type field. The **Device Class Editor** page searches for device classes that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list is dynamically updated as you type. Text matches are not case-sensitive.

You can also use ***special characters*** to filter each parameter.

Filter by one or more of the following parameters:

- ***Device Class***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching device class name.
- ***Description***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching description name.
- ***Device Category***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching device category name.
- ***Device Class Tier***. You can enter text to match, including special characters, and the Device Class Editor page will display only devices that have a matching device class tier.
- ***Class ID***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching class ID.
- ***Collection Type*** Specifies the device class's collection type. Only those devices that match all the previously selected fields and have the specified collection type will be displayed. The choices are:
    - *All*. Include device classes that have a Collection Type of physical and virtual.
    - *Physical*. Include only device classes that have a Collection Type of physical.
    - *Virtual*. Include only device classes that have a Collection Type of virtual.
- ***Device Dashboard***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching device dashboard.
- ***Process Collection***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching process collection type.
- ***PowerPack***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching PowerPack value.
- ***Device Icon***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching device icon name.
- ***Discovery Identifier***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching discovery identifier.
- ***Subs***. You can enter text to match, including special characters, and the **Device Class Editor** page will display only devices that have a matching subs value.

Special Characters

When filtering a list in a registry page, you can include the following special characters to search each field except those that display date and time:

NOTE: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

- , (comma). Specifies an "or" operation. Works for string and numeric values. For example:

"dell, micro" would match all values that contain the string "dell" OR the string "micro".

- & (ampersand). Specifies an "and" operation. Works for string and numeric values. For example:

  "dell & micro" would match all values that contain both the string "dell" and the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

  "!dell" would match all values that do not contain the string "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

  "hel*er" would match "helpers" and "helicopter" but not "hello".

  "325*" would match "325", "32561", and "325000".

  "*000" will match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

  "l?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

  "135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502".

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

  "^sci" would match "scientific" and "sciencelogic", but not "conscious".

- $ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

  "ter$" would match the string "renter" but not the string "terrific".

NOTE: You can use both ^ and $ if you want to match an entire string. For example, "^tern$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

  "1-5 "would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

  "1-" matches 1 and greater, so it would match 1, 2, 6, 345, etc.

  "-5" matches 5 and less, so it would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

  ">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

  "<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

  "=>7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

  "=<12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

  "=-5 " would match "-5" instead of being evaluated as the "half open range" as described above.

Creating Device Classes

The following sections describe how to create new device classes for:

- *Devices that support SNMP*.
- *Devices with Device Class "Generic | SNMP"*.
- *Devices that do not support SNMP*.
- *Devices with a Device Class of "Component"*.

Creating a New Device Class of Type "SNMP-Enabled"

In the **Device Class Editor** page, you can define a new device class. SL1 can then use this device class during discovery and users can assign this device class to devices.

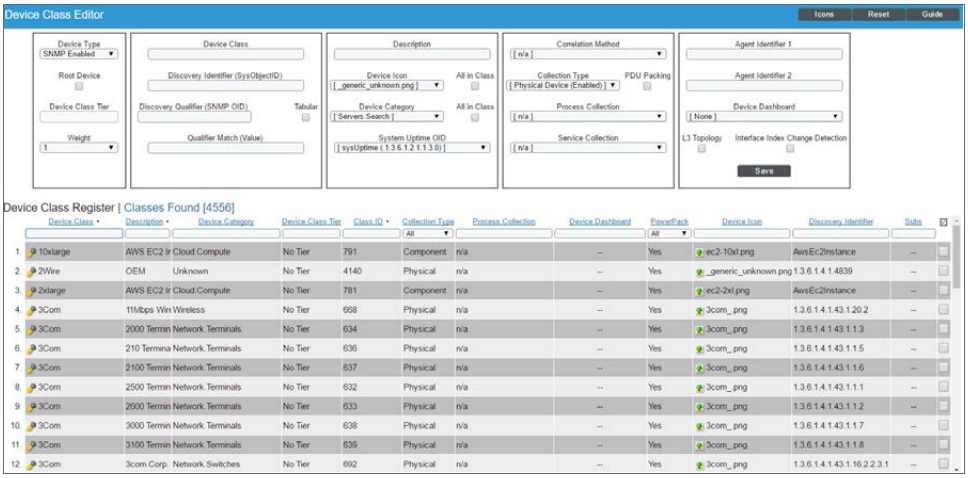
NOTE: You can use an existing device class as a template when defining a new device class. To do this, follow the steps in the Editing an *SNMP-Enabled Device Class* section, but supply a new name in the ***Device Class*** field and click **[Save As]** to save your changes.

NOTE: The ***Device Class Tier*** is a read-only field that is automatically populated by the subscription billing process. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class.

When you create a new device class of type ***SNMP Enabled***, you are defining a device class that uses the ***SNMP SysObjectID*** to identify member device.

To create a new device class of type ***SNMP Enabled***:

1. Go to the**Device Class Editor** page (System > Customize > Device Classes).
2. Click **[Reset]** to clear the fields in the **Device Class Editor** pane.
3. Select *SNMP Enabled* in the ***Device Type*** drop-down list. You can now define the value in the following fields:



- ***Root Device***. If selected, this checkbox specifies that this device can have children devices. Ensures that root devices are included in nightly re-discovery.
- ***Weight***. If two device-class definitions are similar, a device might meet the criteria for both device classes. In this case, the ***Weight*** field tells SL1 which device class to align with the device. The ***Weight*** field allows you to define both detailed, non-SNMP device-class definitions, as well as less detailed, catch-all device classes.

SL1 will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, SL1 will align the device with the device class that appears first in the alphabetical list of device classes.

For example, you could define a detailed device class with a weight of "1" and a similar but less detailed device class with a weight of "10". SL1 will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, SL1 will then try to assign the discovered device to the device class with a weight of "10".

- ***Device Class***. The name of the manufacturer who created the device and/or agent. Can be any combination of alphanumeric characters, up to 48 characters in length.
- ***Discovery Identifier (SysObjectID)***. The SNMP OID, in numeric form, that is returned when querying the device's sysObjectID. Can be up to 64 characters in length. Refer to the appropriate MIB file to determine this value.

NOTE: To view a list of OIDs associated with companies, organizations, and manufacturers, see http://www.iana.org/assignments/enterprise-numbers

- ***Discovery Qualifier (SNMP OID)***. Optional field. Secondary SNMP OID, in numeric form, used to further qualify device types. Can be up to 255 characters in length. If a device matches both the ***Discovery Identifier*** and responds to the ***Discovery Qualifier***, the device will be assigned to the device class.
- ***Tabular***. If you want to use a tabular value in the ***Discovery Qualifier*** field, select this checkbox. When you select this checkbox, SL1 will perform an SNMP walk of the ***Discovery Qualifier*** (as opposed to an SNMP "get" request) and then search for the value that matches the ***Qualifier Match*** field.
- ***Qualifier Match***. Optional field. String that must be present in returned value for the ***Discovery Qualifier*** OID. If a device matches the ***Discovery Identifier***, responds to the ***Discovery Qualifier***, and the response matches the ***Qualifier Match***, the device will be assigned to the device class. Can be up to 64 characters in length.
- ***Description***. The model name of the device. Can be any combination of alphanumeric characters, up to 48 characters in length. For ease-of-use, ScienceLogic recommends that you follow this convention: If you are creating a device class for an entire manufacturer, rather than for a specific product, enter "OEM" as the device description.
- ***Device Icon***. The icon used to display the device in the graphical interface. To view the available icons, click **[Icons]**. Select an icon from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device icon for all existing members of the device class.
- ***Device Category***. A logical categorization of device by primary function. This field allows SL1 to group related devices in reports and views. Select a value from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device category for all existing members of the device class.
- ***System Uptime OID***. Specifies the OID to monitor to determine system uptime. Choices are:

- *sysUpTime (.1.3.6.1.2.1.1.3.0)*. EM7 Default. From the System group of MIB RFC 1213. Returns uptime of the device's SNMP Agent. The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
- *hrSystemUptime (.1.3.6.1.2.1.25.1.1.0)*. From the HR-MIB. The amount of time since this host was last initialized.
- Any additional OIDs defined in the **System Uptime OIDs** page (System > Customize > Uptime OIDs).

- ***Correlation Method***. Used for special topological correlation. Allows SL1 to support event correlation and mapping for VMware and Microsoft hypervisors.
- ***Collection Type***. Specifies whether the device is a hardware-based device (physical) or a virtual device.
- ***PDU Packing***. If your managed network includes a large number of interfaces, and you want to monitor those interfaces, select this checkbox. PDU packing enables quicker collection of interface data.
- ***Process Collection***. Specifies how SL1 will retrieve process information for the device. SL1 will use this method to gather information on the system processes. Choices are:
  - *n/a*. Don't monitor processes.
  - *Host Resource*. Specifies that the Host Resources MIB will be used to collect information on processes.
  - *HP/UX*. Specifies that HP agents will provide information on processes.
  - *Solaris (prior to Solaris 10)*. Specifies that Solaris agents will provide information on processes.
  - *Extended User Information*. Specifies that ScienceLogic's custom extension to net-SNMP will provide process information. Users must have installed the extension before selecting this option.
- ***Service Collection***. Specifies how to collect information on Windows services. Choices are:
  - *n/a*. This is not a Windows device class.
  - *Windows Basic*. Use the Windows MIB to gather information about Windows services.
  - *WMI Informant*. Use the WMI Informant MIB to gather information about Windows services.
- ***Agent Identifier 1 and Agent Identifier 2***: These fields are used to align device classes to devices using the SL1 agent. Device classes exist for every possible combination of values returned by the agent; you do not need to enter or change values in these fields when creating or editing a device class.
- ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. For devices with this device class, the selected device dashboard will appear as an option in the **Device Summary** page. This field is optional.
- ***L3 Topology***. If selected, SL1 includes devices in this device class in the **Layer-3 Maps** page (Views > Topology Maps > Layer-3). SL1 uses traceroute from each Data Collector to each managed device to create Layer-3 maps.

- ***Interface Index Change Detection***. On some devices, the SNMP index of an interface can change when the interface goes down and then comes back up. If you select this checkbox, SL1 will use the combination of interface ID and ifPhysAddress to monitor interfaces on devices that use this device class and to align events with those interfaces.

4. Click **[Save]** to save the new device class or click **[Save As]** to save your changes under a new device class name.

Editing an SNMP-Enabled Device Class

In the **Device Class Editor** page, you can edit a device class for a device that supports SNMP.

When you ***select SNMP Enabled***, you are defining a device class that uses the ***SNMP SysObjectID*** to identify member devices.

To edit an existing device class:

1. Go to the**Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
4. The fields in the top pane will be populated with values from the selected device class. You can edit one or more of the fields described in the section *Creating a New Device Class for Devices That Support SNMP*.
5. Select the **[Save]** button to save your changes to the device class or select the **[Save As]** button to save your changes under a new device class name.

Creating a New Device Class for a Device with Device Class "Generic | SNMP"

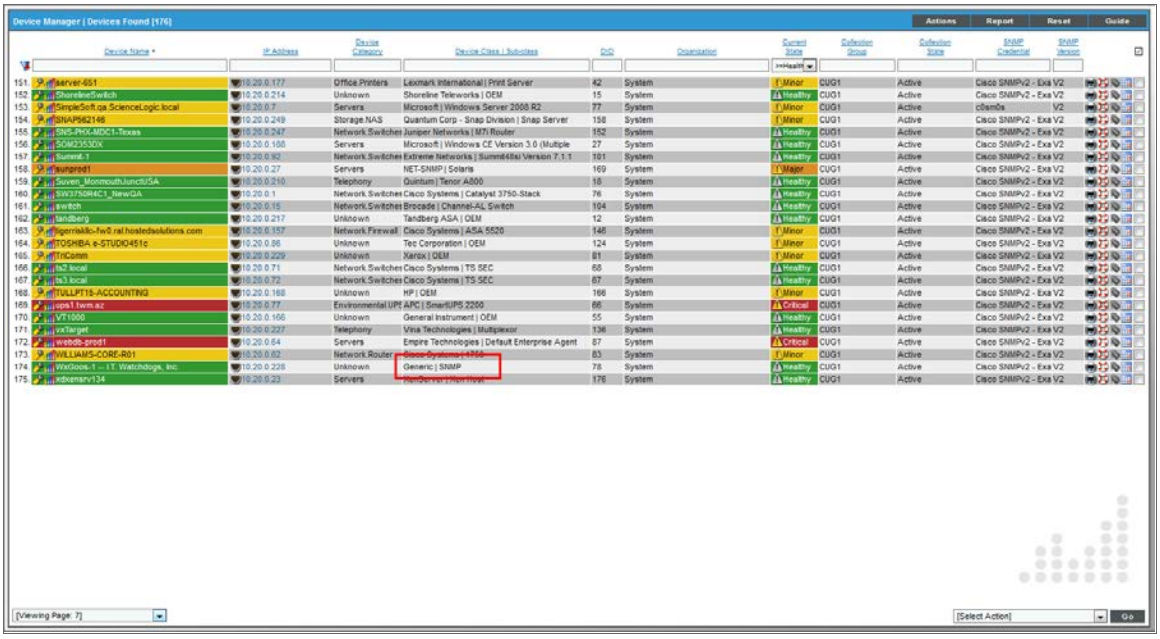
After discovery, SL1 might discover devices and assign those devices to the device class ***Generic | SNMP***. This means that SL1 was able to retrieve a SysObjectID value from the device, but SL1 does not include a Device Class for that SysObjectID.

NOTE: The ***Device Class Tier*** is a read-only field that is automatically populated by the subscription billing process. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class.

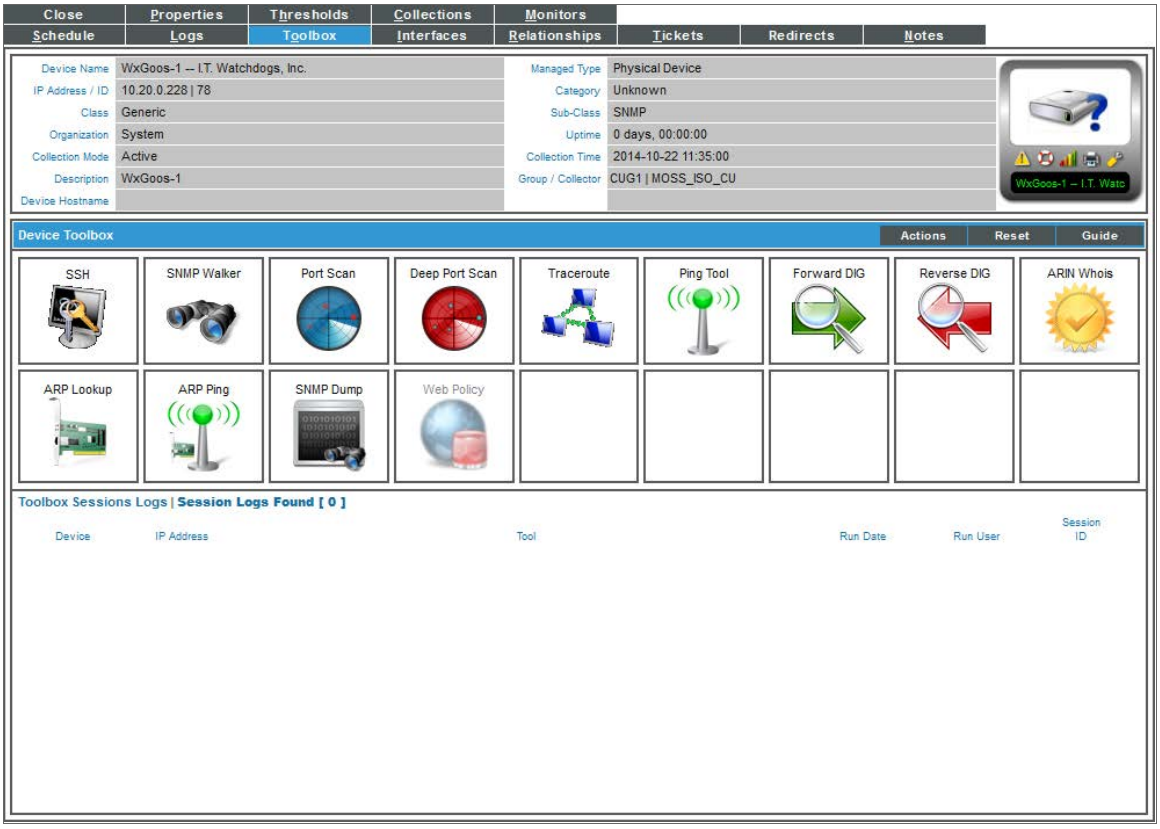
To create a new device class for a device with device class ***Generic | SNMP***, perform the following:

1. Go to the **Device Manager** page (Devices > Device Manager).

2. In the **Device Manager** page, find the device with the device class ***Generic | SNMP***. Select the wrench icon ( ) for the device.

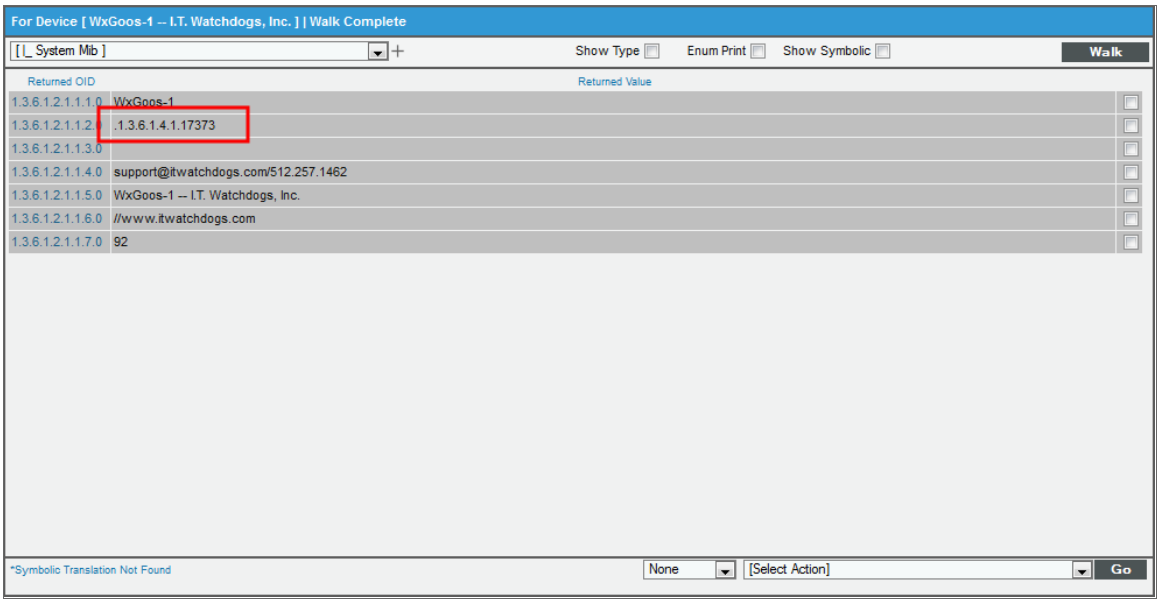


3. In the **Device Administration** panel, select the **[Toolbox]** tab.



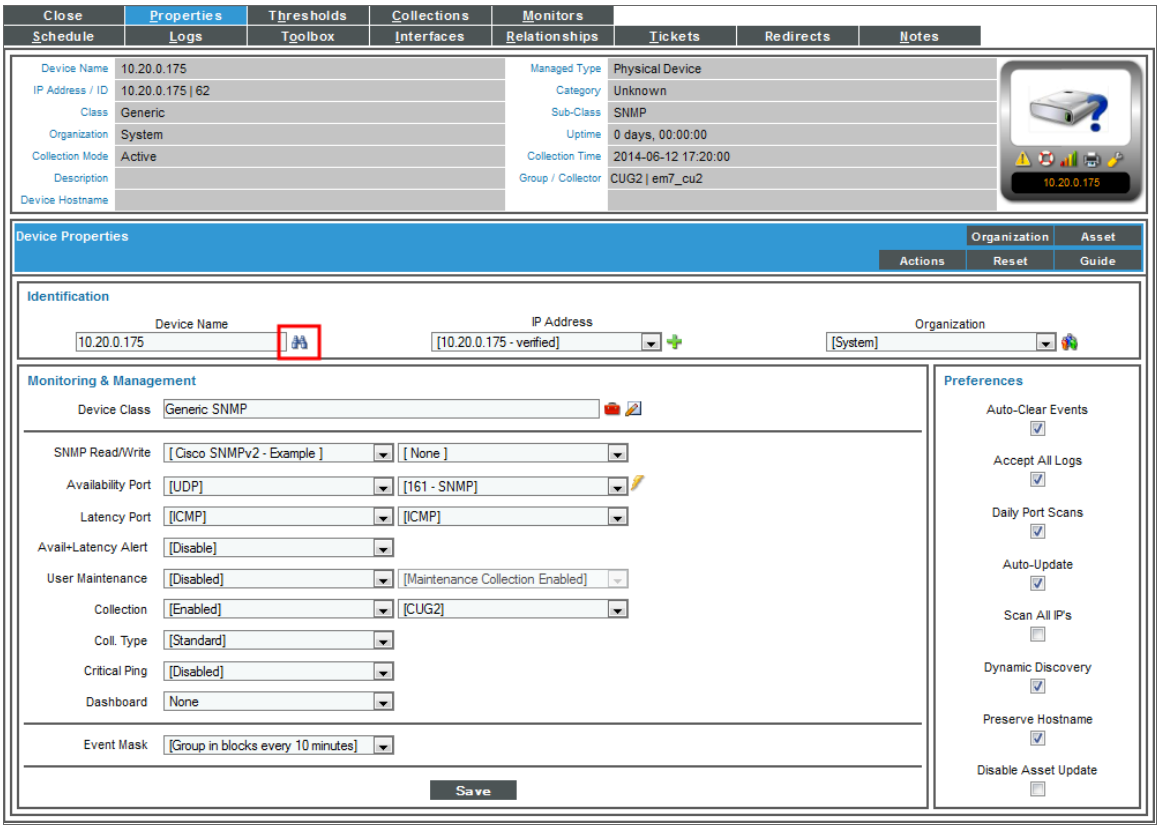
4. In the **Device Toolbox** page, select the icon for SNMP Walker.

5. In the **SNMP Walker** modal page, go to the drop-down menu in the upper left and select ***System MIB***. Then select the **[Walk]** button.



6. The second entry in the ***Returned Value*** column is the SysObjectID. In the example above, that value is ***1.3.6.1.4.1.303.3.3.7.3***. Copy this value and save it in a document or write down this value. You will need it to create a new device class.
7. Follow the directions in the section *Creating a New Device Class of type "SNMP-Enabled"*. In the ***Discovery Identifier*** field, enter the value of the SysObjectID from the SNMP Walker. Make sure there are no blank spaces before or after the SysObjectID value.
8. To assign the new device class to a device, follow the instructions in the section *Manually Changing the Device Class for a Device*.

9. Alternately, you can re-discover the device with the device class "Generic | SNMP". To re-discover the device, go to the **Device Manager** page (Devices > Device Manager). Find the device you want to rediscover. Select its wrench icon ( ). In the **Device Properties** page for the device, select the binoculars icon ( ).



10. After the device is re-discovered, it should now be aligned with the new device class.

Creating a New Device Class for Devices That Do Not Support SNMP

SL1 includes device classes for devices that are "pingable". By default, these devices are aligned with the device category of "pingable" and are placed in the device class "Ping | ICMP". To discover devices that have a device category of "pingable", you must select ***Discover Non-SNMP*** in the **Discovery Session Editor** page.

Devices with the device category of "pingable" are devices that meet one of the following criteria:

- Device does not support SNMP.
- SNMP has been disabled on the device.
- Either no SNMP credential was provided in the discovery session or an incorrect SNMP credential was provided in the discovery session.

In some cases, you might want to discover a "pingable" device and use XML requests, XSLT requests, WMI requests, SOAP transactions, Python snippets, or SQL queries to gather information from the device. You can do this through Dynamic Applications.

You might also want to create a more descriptive device class for these types of devices and assign a device category other than "pingable". SL1 can use the values returned by nmap (run during discovery) to match a "pingable" device to a descriptive device class.

NOTE: You can use an existing device class as a template when defining a new device class. To do this, follow the steps in the *Editing a Device Class That is Not SNMP-Enabled* section, but supply a new name in the ***Device Class*** field and click **[Save As]** to save your changes.

NOTE: The ***Device Class Tier*** is a read-only field that is automatically populated by the subscription billing process. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class.

When you create a new device class of type ***Pingable***, you are defining a device class that uses the ***XML values returned by nmap*** to identify member devices.

To create a new device class with a device category of "pingable":

1. To discover details about devices that do not support SNMP, during discovery (System > Manage > Classic Discovery), you should select an ***Initial Scan Level*** of *5. Deep Discovery* and select the checkbox for ***Discover Non-SNMP***. SL1 will run the following nmap command on each device during discovery:

   nmap -sS -O --host-timeout=12000ms "-p 21,22,23,25,80" -A --version-all -oX *full pathname of file in which to store XML outputIP address of device*

NOTE: Depending on your selections in the **Discovery Session Editor** page, SL1 might use the ***-sU*** or ***-sT*** option instead of ***-sS***. The value supplied to the ***host-timeout*** option will vary depending upon the list of ports specified in the **Discovery Session Editor**page. The list of ports supplied with the ***-p*** option will vary depending upon the list of ports specified in the **Discovery Session Editor**page. For more details on the nmap command, see the webpage http://nmap.org/book/man.html.

2. SL1 stores the output from the nmap command in an XML file. In the ***NMAP Report XPATH*** field (described later in this section), you specify a path in that XML file. That path will specify the location of a value in the XML file. SL1 will then examine the specified value and use the regular expression defined in the ***XPATH Match Regex*** field (described later in this section) to match devices to this device class.
3. To begin gathering information to include in the device class, find a device for which you want to create a "pingable" device class. If you have already discovered this device, it might currently have a device class of "Ping | ICMP".

4. You must now run nmap on the device. You can either log in directly to the device or log in to another device that can communicate with the device on which you want to run nmap. At the command prompt, enter the following:

   nmap -sS -O -oX *full pathname of file in which to XML output*-sV --version-all -A *IP address of device*

5. Navigate to the XML file where you stored the output from the nmap command. Examine the output and find an XML element or attribute that you can use to uniquely identify a device class for the device. Note the XPATH to the element or attribute.

NOTE: For information on XPATH syntax, see http://www.w3schools.com/xpath/xpath_syntax.asp

6. The device data in the XML report generally uses the following element structure:

   - Information about nmap, including scan level and debugging level.
   - Information about each discovered host, including start-time and end-time for the nmap and the IP address, MAC address, and hardware vendor.
   - Specific information about each port, including the service running on the port, some stored as attributes of the Port element, some stored as child elements of the Port element
   - Specific information about the operating system, include vendor and version number, stored as attributes of the OSClass element
   - Information about uptime for the device.
   - Information about traceroute to the discovered device and round-trip time to the discovered device.
   - Performance data for this session of nmap.

7. For example, suppose we want to create a device class for each device that runs an Apache web server. After running nmap on a device that is running Apache, we might see the following elements and attributes under **Host/Ports**:

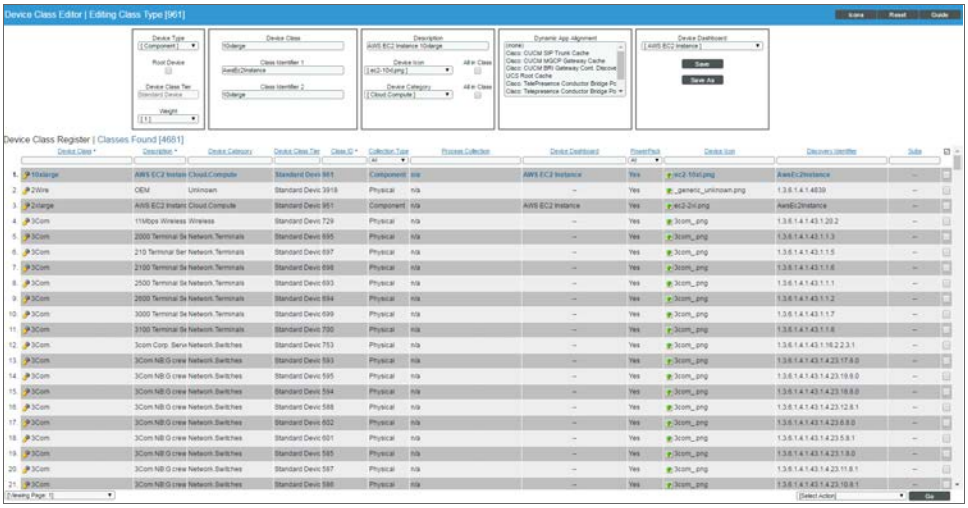
   <**port** protocol="tcp" portid="80">

   <state state="open" reason="syn-ack" reason_ttl="64"/>
   <**service** name="http" **product="Apache httpd"** version -"2.2.3", extraninfo="(CentOS)" method="probed" conf="10" />
   <script id="html-title" output="Apache HTTP Server Test Page powered by CentOS" />
   <script id="http-favicon" output="" />

   </port>

   The XPATH would be **/nmaprun/host/ports/port/service/@product**

8. Go to the **Device Class Editor** page (System > Customize > Device Classes) to create a new device class. Click the **[Reset]** button to clear any values from the **Device Class Editor** page. Supply a value in the following fields:



- ***Device Type***. Select *Pingable*.
- ***Root Device***. Specifies that this device can have children devices. Ensures that root devices are included in nightly re-discovery. Leave this box unchecked.
- ***Weight***. If two device-class definitions are similar, a device might meet the criteria for both device classes. In this case, the ***Weight*** field tells SL1 which device class to align with the device. The ***Weight*** field allows you to define both detailed, non-SNMP device-class definitions, as well as less detailed, catch-all device classes.

  SL1 will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, SL1 will align the device with the device class that appears first in the alphabetical list of device classes.

  For example, you could define a detailed device class with a weight of "1" and a similar but less detailed device class with a weight of "10". SL1 will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, SL1 will then try to assign the discovered device to the device class with a weight of "10".

- ***Device Class***. The name of the manufacturer who created the device and/or agent. Can be any combination of alphanumeric characters, up to 48 characters in length.

- ***NMAP Report XPATH***. Specifies how should parse the results of an nmap request (run during discovery) to determine whether the device should be aligned to this device class. If you select an ***Initial Scan Level*** of *5. Deep Discovery* for a discovery session, SL1 will run the following nmap command on each device during discovery. SL1 will include the -A option, to retrieve as much information as possible and match pingable devices with custom device classes.

    - In the ***NMAP Report Path*** field, enter the XPATH for the element or attribute you want to use to identify member devices. That path will specify the location of a value in the XML file. SL1 will then examine the specified value and use the regular expression defined in the ***XPATH Match Regex*** field to match devices to this device class.

  In SL1, the XPATH must always begin with **/nmaprun/host**. Using our example from step #7 above, we would provide an XPATh of:

  /nmaprun/host/ports/port/service/@product

NOTE: In the ***NMAP Report Path*** field, we included the entire path to the attribute we want to match, ***but intentionally did not filter on the attribute value***. That is, we specified **/nmaprun/host/ports/port/service/@product** instead of **/nmaprun/host/ports/port/service/@product='Apache httpd'**. When you include the value of the attribute in the XPATH, XPATH does not return the attribute value, but instead returns the entire element that includes the attribute. **Because the element is not a text string , SL1 cannot search the element using a regex.**

- ***XPATH Match Regex***. In this field, specify a regular expression you want to use when examining the value returned by nmap. The location of the value returned by nmap is defined in the ***NMAP Report XPATH*** field. SL1 will align a device to a device class if the nmap response includes a value at the path specified in the ***NMAP Report XPATH*** and the value at that location matches the regular expression in the ***XPATH Match Regex*** field.

  Using our example in step #7, we would provide the value **Apache httpd**.

- ***Description***. The model name of the device. Can be any combination of alpha-numeric characters, up to 48-characters in length. For ease-of-use, ScienceLogic recommends that you follow this convention: If you are creating a device class for an entire manufacturer, rather than for a specific product, enter "OEM" as the device description.
- ***Device Icon***. The icon used to display the device in the graphical interface. To view the available icons, click **[Icons]**. Select an icon from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device icon for all existing members of the device class.
- ***Device Category***. A logical categorization of device by primary function. This field allows to group related devices in reports and views. Select a value from drop-down list.
- ***All in class***. Selecting this checkbox updates the device category for all existing members of the device class.

- ***Collection Type***. Specifies whether the device is a hardware-based device (physical) or a virtual device.
- ***Weight***. If two device-class definitions are very similar, a device might meet the criteria for both device classes. In this case, the ***Weigh***t field tells which device class to align with the device. SL1 will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, SL1 will align the device with the device-class that appears first in the alphabetical list of device classes.

  The ***Weight*** field allows you to define detailed non-SNMP device-class definitions and still have catch-all device-classes with less-specific criteria.

  For example, you could define a detailed device class with a weight of "1" and a similar but less detailed catch-all device class with a weight of "10". SL1 will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, SL1 will then try to assign the discovered device to the device class with a weight of "10".

- ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. For devices with this device class, the selected device dashboard will appear as an option in the **Device Class Editor** page. This field is optional.

9. Click the **[Save]** button to save your changes to the device class or click the **[Save As]** button to save your changes under a new device-class name.

Applying the New Device Class

To apply a new "pingable" device class during discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery). If you are creating a new discovery session, click the **[Create]** button. If you are editing an existing discovery session, click its wrench icon ( ).
2. In the **Discovery Session Editor**page:

   - In the ***Initial Discovery Scan Level*** field, select *5. Deep Discovery*.

NOTE: You can also define ***Initial Discovery Scan Level*** in the **Behavior Settings** page (System > Settings > Behavior). Because this discovery level is very compute-intensive, you might want to avoid setting this discovery level globally and instead choose this discovery level ***only for specific discovery sessions***.

   - Select the ***Discover Non-SNMP*** checkbox.
   - Select the ***Model Device*** checkbox.

3. Click the **[Save]** button.
4. When you run the discovery session, SL1 will apply the new device class to discovered or re-discovered devices.

NOTE: You can also apply a new "pingable" device class ***during nightly auto-discovery***. You can define (nightly) ***Rediscovery Scan Level*** in the **Behavior Settings**page (System > Settings > Behavior) and select *5. Deep Discovery*. **However, because this auto-discovery level is very compute-intensive, you might not want to use this setting for global auto-discovery.**

Maintaining the New Device Class During Auto-Discovery

If you have applied a new "pingable" device class to a device, you should do the following to make sure that doesn't reset the device's device-class to "Ping | ICMP" during nightly auto-discovery.

NOTE:SL1 will reset a pingable device's device class to "Ping | ICMP" if Deep Discovery is not enabled for nightly auto-discovery. You can enable Deep Discovery for nightly auto-discovery in the **Behavior Settings**page (System > Settings > Behavior). Go to the field ***Rediscovery Scan Level***, and select *5. Deep Discovery*. However, because this auto-discovery level is very compute-intensive, you might not want to use this setting for global auto-discovery.

You can disable auto-discovery for each device that uses Deep Discovery. Instead of using nightly auto-discovery, you can create a scheduled discovery session that will update the device class. To do this:

1. Go to the **Device Properties** page (Devices> Device Manager > wrench icon).
2. Unselect the checkbox for ***Auto-Update***.
3. Click the **[Save]** button.
4. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery) and create a discovery session for this device (and each device that uses Deep Discovery and which you want to update regularly). When creating this discovery session:
    - In the ***Initial Discovery Scan Level*** field, select *5. Deep Discovery*.
    - Select the ***Discover Non-SNMP*** checkbox.
    - Select the ***Model Device*** checkbox.
5. Define the new discovery session as a scheduled discovery session, so you can periodically update the device's data.

Editing a Device Class That is Not SNMP-Enabled

In the **Device Class Editor** page, you can edit the parameters of an existing device class.

When you ***do not select SNMP Enabled***, you are defining a device class that does not use SNMP to identify member devices. Instead, the device class will use a value returned by nmap (run during discovery) to identify member devices.

NOTE: You can use an existing device class as a template for a new device class. To do this, follow the steps in this section, but supply a new name in the ***Device Class*** field and select the **[Save As]** button to save your changes.

To edit an existing Device Class:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class.
4. In the **Device Class Editor** page, you can edit the parameters of an existing device class. If you do not select *SNMP Enabled* in the ***Device Type*** drop-down list, you can edit the value in one or more of the fields described in the section *Creating a New Device Class for Devices That Do Not Support SNMP*.
5. Select the **[Save]** button to save you changes to the device class or select the **[Save As]** button to save your changes under a new
6. The newly selected device class is now associated with the device.

Creating a Device Class of Type "Component"

A device of type "component" is an entity that runs under the control of a management system running on a physical device. For example, SL1 can discover a VMWare ESX server (management system) and then discover the virtual machines (component devices) running on that ESX server.

SL1 uses Dynamic Applications to retrieve data from a management system and discover each component device managed by that management system. SL1 then uses that retrieved data to create a device for each component device.

Device classes for components are aligned with the Dynamic Applications that discover component devices. For example, we could have a device class of type component for "Cisco Systems | UCS Chassis". We could align the Dynamic Application for "UCS Chassis Discovery" with this device class. When SL1 runs the "UCS Chassis Discovery" Dynamic Application and discovers a component device, SL1 assigns each discovered component device to the device class "Cisco Systems | UCS Chassis".

When you create a new device class of type ***Component***, you are defining a device class that uses an aligned Dynamic Application to identify the member devices.

NOTE: The ***Device Class Tier*** is a read-only field that is automatically populated by the subscription billing process. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class.

To create a new device class of type ***Component***:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, click the pencil icon ( ).
2. Click **[Reset]** to clear any values from the **Device Class Editor** page.
3. Supply a value in each required field in the top pane:
   - ***Device Type***. Select *Component*.
   - ***Root Device***. Specifies that this device can have children devices. Ensures that root devices are included in re-discovery.
   - ***Weight***. If two device-class definitions are similar, a device might meet the criteria for both device classes. In this case, the ***Weight*** field tells SL1 which device class to align with the device. The ***Weight*** field allows you to define both detailed, non-SNMP device-class definitions, as well as less detailed, catch-all device classes.

     SL1 will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, SL1 will align the device with the device class that appears first in the alphabetical list of device classes.

     For example, you could define a detailed device class with a weight of "1" and a similar but less detailed device class with a weight of "10". SL1 will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, SL1 will then try to assign the discovered device to the device class with a weight of "10".
   - ***Device Class***. The name of the manufacturer who created the device and/or agent. Can be any combination of alphanumeric characters, up to 48 characters in length.
   - ***Description***. The model name of the device. Can be any combination of alphanumeric characters, up to 48 characters in length.
   - ***Device Icon***. The icon used to display the device in the graphical interface. To view the available icons, click **[Icons]**. Select an icon from the drop-down list.
   - ***All in class***. Selecting this checkbox updates the device icon for all existing members of the device class.
   - ***Device Category***. A logical categorization of device by primary function. This field allows SL1 to group related devices in reports and views. Select a value from the drop-down list.
   - ***All in class***. Selecting this checkbox updates the device category for all existing members of the device class.

- ***Dynamic App Alignment***. The Dynamic Application to align with this device class. This list will include all Dynamic Applications that have the ***Component Mapping*** checkbox selected in the **Dynamic Applications Properties Editor** page and are not currently being used by another device class. When you select a Dynamic Application, each component device discovered by that Dynamic Application will be assigned to the current device class.
- ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. For devices with this device class, the selected device dashboard will appear as an option in the **Device Summary** page. This field is optional.

4. Click **[Save]** to save you changes to the device class or click **[Save As]** to save your changes under a new device-class name.

Editing a Device Class of Type "Component"

To edit an existing Device Class of Type "Component":

1. Go to System > Customize > Device Classes, or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class.
4. You can edit the value in one or more of the fields. For details on each field, see the section on *Creating a New Device Class of Type "Component"*.
5. Select the **[Save]** button to save you changes to the device class or select the **[Save As]** button to save your changes under a new device-class name.

Legacy Device Classes of Type "ICMP"

SL1 includes legacy device classes of type ***SNMP Enabled*** for "pingable" devices (that is for devices that don't support SNMP). SL1 includes the following legacy, ***SNMP Enabled*** device classes for "pingable" devices:

- Cisco Systems | ICMP
- FreeBSD | ICMP
- Linux | ICMP
- Microsoft | ICMP
- Novell | ICMP
- Ping | ICMP
- Sun Microsystems | ICMP
- Tektronix, Inc. | ICMP

NOTE: Best practice is to define "pingable" devices as those that do not support SNMP. For "pingable" devices that do not support SNMP, ScienceLogic recommends you use the new "deep discovery" feature and then create device classes of type "pingable".

Managing Device Classes

The following sections describe:

- *Manually changing the device class for a device*.
- *Changing the icon for a device class*.
- *Deleting one or more device classes*.

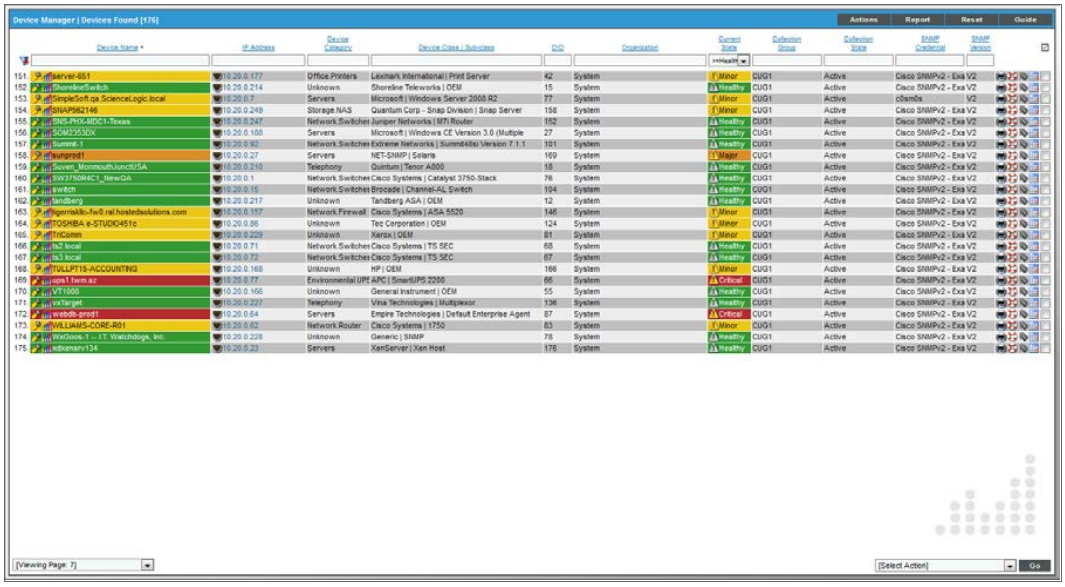
Manually Changing the Device Class for a Device

During discovery, SL1 automatically assigns a device class to each discovered device. For example, SL1 assigns the device class "Ping" to devices that do not support SNMP. You might want to manually change the device class for such a device after discovery.

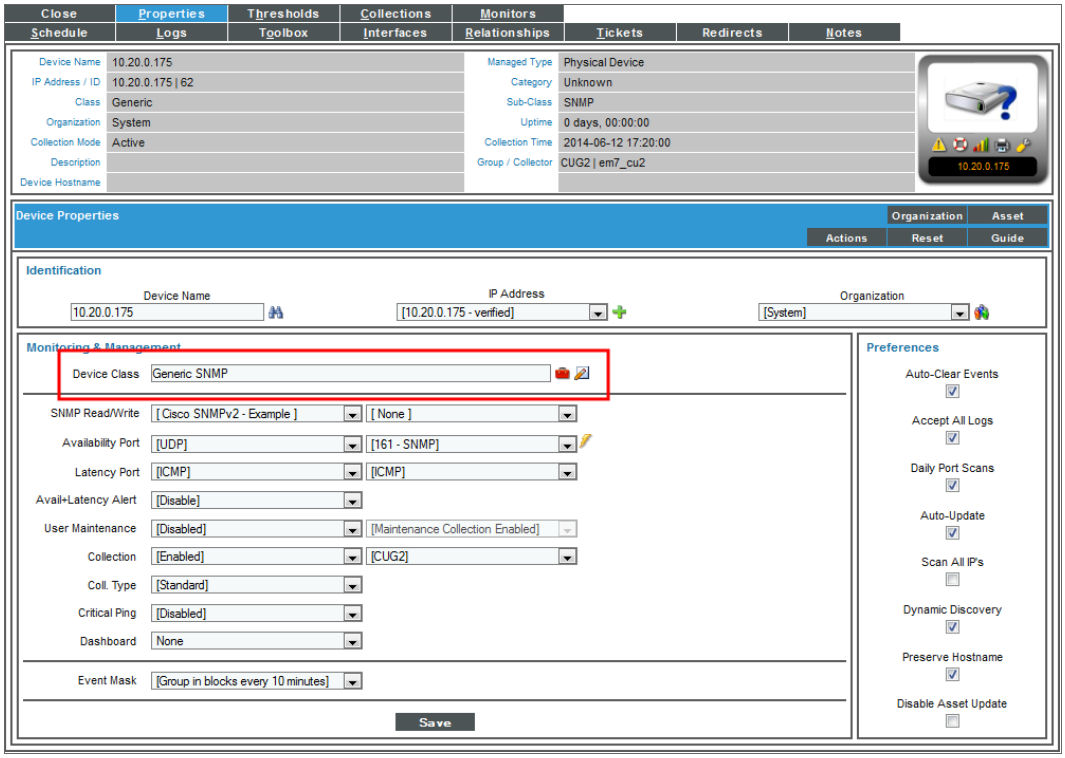
In the **Device Properties** page, you can assign a different device class to the device.

To assign a different device class to the device:

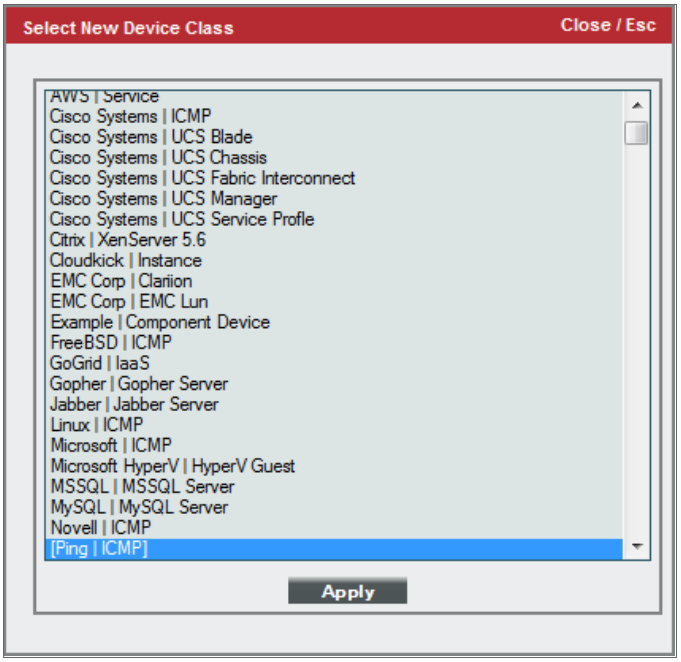
1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device you want to edit. Select its wrench icon ( ).



3. In the **Device Properties** page, find the *Device Class* field. Select the toolbox icon ( ).



4. In the **Select New Device Class** modal page, select a device class.



5. There are two other ways to align devices with the devices class:

    - You can re-run discovery for a single device. To re-discover a device, go to Devices > Device Manager. Find the device you want to re-discover. Select its wrench icon ( ). In the **Device Properties** page for the device, select the binoculars icon ( ). After the device is re-discovered, it will be aligned with the appropriate device class. You can repeat this process for each device you want to align with the new or edited device class.
    - If you re-run one or more discovery sessions (System > Manage > Classic Discovery), SL1 will automatically apply the new or edited device class to those devices that match the criteria. Remember that to discover details about device of type "pingable", you must select the checkbox ***Discovery Non-SNMP***. Optionally, to retrieve details about "pingable" devices, in the field ***Initial Scan Level***, you can also select *5. Deep Discovery*.

Changing the Icon for a Device Class

You can select a new icon for a device class or import your own image as an icon. To do this:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class. To edit the icon associated with the selected device class, edit the value of the ***Device Icon*** field. The icon you select will be associated with the device class.

    - To view the list of icon names and icon images, select the **[Icon]** button in the upper right of the page.
    - The **Device Icon Browser** modal page displays a list of all icons for device class.
    - To import an image to use as an icon, select the **[Import]** button. In the **Device Icon Browser** modal page, you can import a .png image for use as an icon in SL1.

4. Select the **[Save]** button to save the changes to the device class.

Aligning One or More Device Classes with a Device Dashboard

From the **Device Class Editor** page, you can align one or more device classes with a device dashboard. You can manually align a device dashboard with a device class. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the device class will appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

1. To align a device dashboard with one or more device classes:
2. Go to the **Device Class Editor** page (System > Customize > Device Classes).
3. In the **Device Class Register** pane at the bottom of the page, find the device class(es) you want to align. Select its checkbox ( ).
4. In the ***Select Action*** drop-down in the lower right, select a device dashboard in the *Align Device Dashboard* section. Select the **[Go]** button.
5. Each selected device class is now aligned with the selected device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the device class will appear as the default view in the **Device Summary** page.

Deleting One or More Device Classes

From the **Device Class Editor** page, you can delete one or more device classes.

NOTE: Before you delete a device class, you should assign any member devices to another device class. If you delete a device class that is associated with a device, that device will now display "Unknown - Missing" for device class. During the next discovery session, SL1 will try to find the appropriate device class for the device.

To delete one or more device classes:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class(es) you want to delete. Select its checkbox.
3. In the ***Select Action*** drop-down in the lower right, select *DELETE Device Classes*. Select the **[Go]** button.
4. Each selected device class is deleted from SL1.
5. If the device class includes devices, after deletion, those devices will have a device class of "unknown". While the device has a device class of "unknown", polling associated with existing device policies might fail. During the next discovery session, SL1 will rediscover those devices and try to assign a device class to another device class. For example, if you delete the device class for Microsoft Servers, during nightly discovery, SL1 would assign those devices to the device class for Microsoft OEM.

Device Categories

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

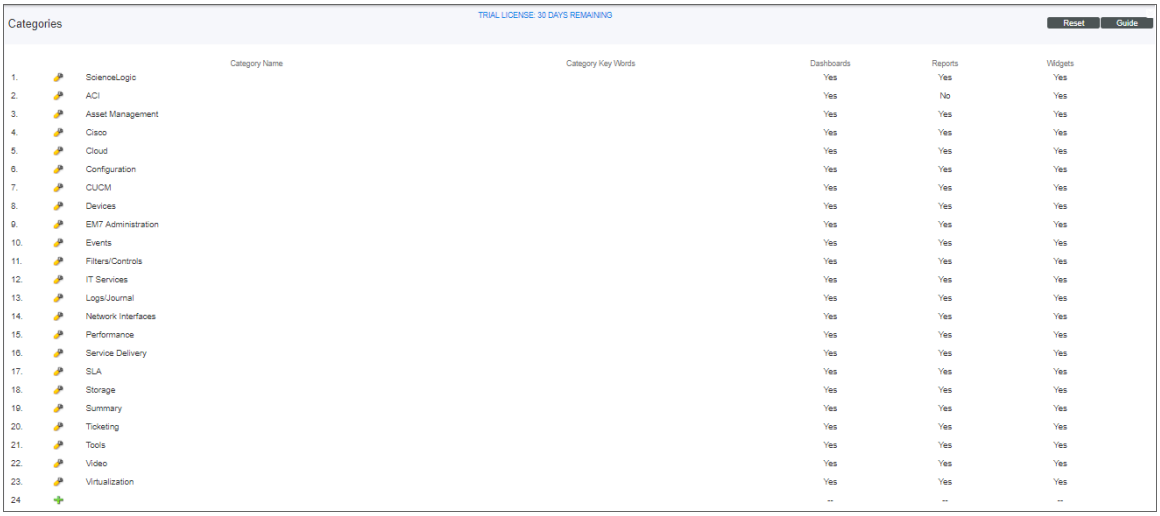
Device categories are paired with device classes to organize and describe discovered devices. Device class usually describes the manufacturer. Device category describes the function of the hardware. Each device class can include a device category.

NOTE: "Reserved" device categories are those device categories required by SL1. These device categories cannot be edited or deleted. If a device category does not display the bomb icon ( ), the device category is a reserved device category and cannot be deleted.

Viewing the List of Device Categories

The **Categories** page displays a list of all existing device categories. To view this page:

1. Log in to SL1.
2. Go to the **Device Category Editor** page (System > Customize > Categories).



3. For each device category, the **Categories** page displays the following:

TIP: To sort the list of device categories, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Edit Date*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- ***Category Name***. The name of the device category.
- ***Map Icon***. Pathname of the image used as an icon for the device category.
- ***Device Dashboard***. This field displays the device dashboard associated with the device category.
- ***ID***. A unique numeric identifier for the device category, automatically assigned by SL1.
- ***Edit User***. User who created or last edited the device category.
- ***Edit Date***. Date and time the device category was created or last edited.

"Pingable" Device Category

Devices that have a device category of "pingable" are devices that meet one of the following:

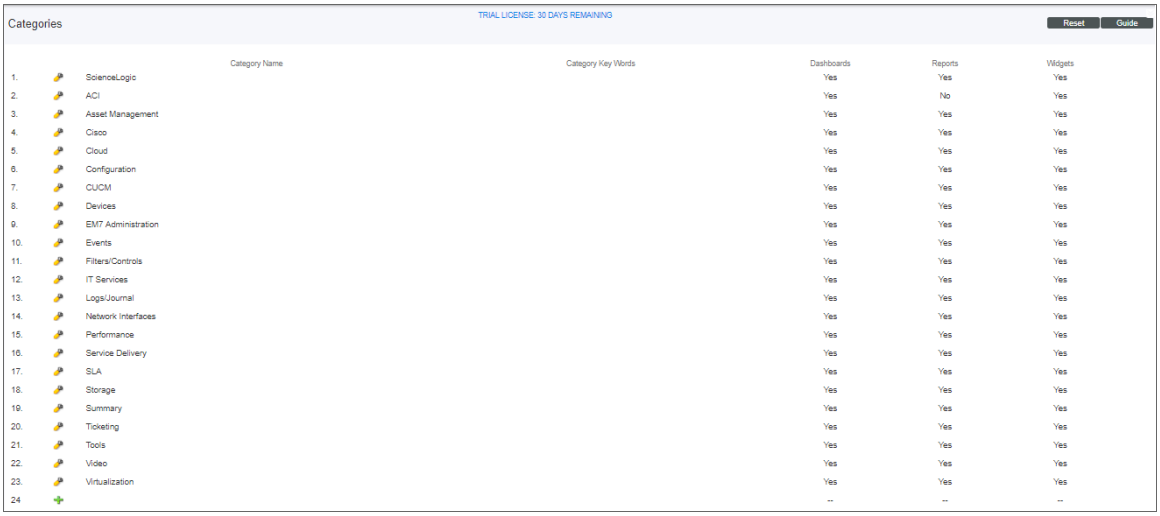
- Device does not support SNMP.
- SNMP has been disabled on the device.
- Wrong credential was provided during discovery and "Discover Non-SNMP" was enabled for the discovery session.

Creating a New Device Category

From the **Categories** page, you can create a new device category. To do this:

1. Go to the **Device Category Editor** page (System > Customize > Categories).

2. In the **Categories** page, select the **[Reset]** button to clear any values from the fields in the editor pane.



	Category Name	Category Key Words	Dashboards	Reports	Widgets
1.	ScienceLogic		Yes	Yes	Yes
2.	ACI		Yes	No	Yes
3.	Asset Management		Yes	Yes	Yes
4.	Cisco		Yes	Yes	Yes
5.	Cloud		Yes	Yes	Yes
6.	Configuration		Yes	Yes	Yes
7.	CUCM		Yes	Yes	Yes
8.	Devices		Yes	Yes	Yes
9.	EM7 Administration		Yes	Yes	Yes
10.	Events		Yes	Yes	Yes
11.	Filters/Controls		Yes	Yes	Yes
12.	IT Services		Yes	Yes	Yes
13.	Logs/Journal		Yes	Yes	Yes
14.	Network Interfaces		Yes	Yes	Yes
15.	Performance		Yes	Yes	Yes
16.	Service Delivery		Yes	Yes	Yes
17.	SLA		Yes	Yes	Yes
18.	Storage		Yes	Yes	Yes
19.	Summary		Yes	Yes	Yes
20.	Ticketing		Yes	Yes	Yes
21.	Tools		Yes	Yes	Yes
22.	Video		Yes	Yes	Yes
23.	Virtualization		Yes	Yes	Yes
24			--	--	--

3. In the editor pane (top of the page), supply values in each of the following fields:

   - ***Category Name***. Enter a name for the new device category. This name can be any combination of alphanumeric characters, up to 32 characters in length. SL1 naming convention is to create names using the following prefixes:

     - *Environmental* for environmental-monitoring devices.
     - *Network* for networking hardware like routers, switches, and firewalls.
     - *Office* for office equipment.
     - *Server* for server hardware.
     - *System* for networked hardware like servers and network stores.
     - *Telephony* for telephone hardware.
     - *Wireless* for wireless network hardware.

   However, you are not required to follow this convention.

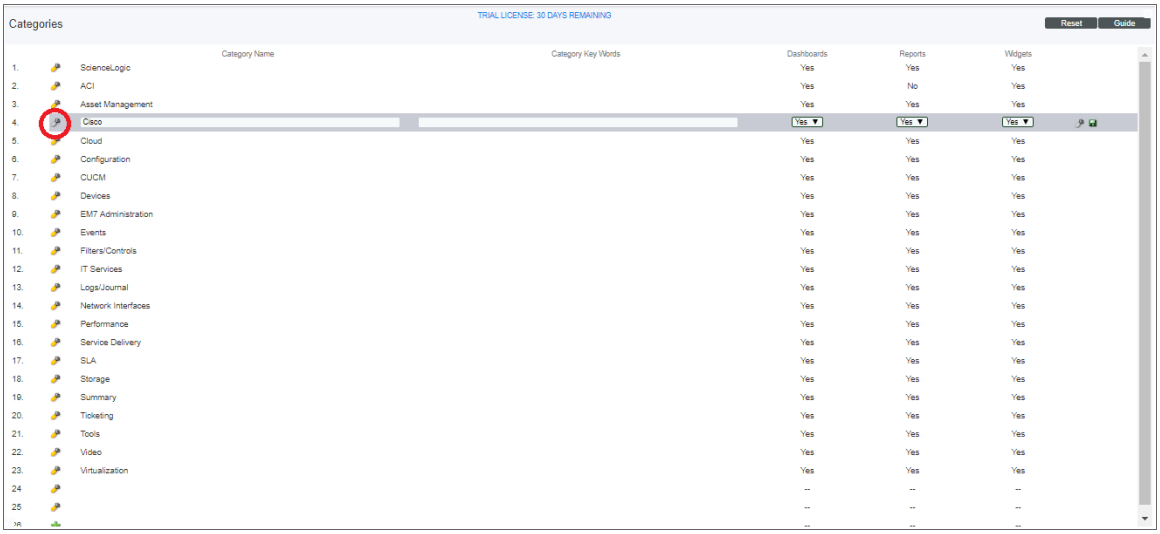
   - ***Map Icon***. Select an icon to be associated with this device category. You can select from a list of all possible icons for device categories. The selected icon will be used to represent members of the device category in the network maps in Views and maps.
   - ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. For devices with this device category, the selected device dashboard will appear as an option in the **Device Summary** page. This field is optional.

4. Select the **[Save]** button.
5. The new device category should now appear in the list of device categories in this page and appear in the ***Device Category*** drop-down list in the **Device Class Editor** page.

Editing a Device Category

In the **Categories** page, you can edit the parameters of an existing device category. To do this:

1. Go to the **Categories** page (System > Customize > Categories).
2. In the **Categories** page, in the register pane at the bottom of the page, find the device category you want to edit. Select its wrench icon ( ).



3. The fields in the top pane will be populated with values from the selected device category. You can edit the value in one or more of the fields.
4. For a description of each field, see the previous section on *Creating a New Device Category*.

Deleting a Device Category

From the **Categories** page, you can edit an existing device category.

> CAUTION: Do not delete device categories that are being used by managed devices. If you delete a device category to which devices have been assigned, you risk losing data from the device.

To delete a device category:

1. Go to the **Categories** page (System > Customize > Categories).
2. In the **Categories** page, find the device category you want to delete. Select its bomb icon ( ).
3. The device category is deleted from SL1.

Aligning One or More Device Categories with a Device Dashboard

From the **Categories** page, you can align one or more device categories with a device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page, or a device dashboard defined in the **Device Class Editor** page, the device dashboard associated with the device category will appear as the default view in the **Device Summary** page.

> **NOTE**: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with one or more device categories:

1. Go to the **Categories** page (System > Customize > Categories).
2. In the **Device Category Register** pane at the bottom of the page, find the device categories you want to align. Select their checkboxes (☑).
3. In the ***Select Action*** drop-down list in the lower right, select a device dashboard under the *Align Device Dashboard* section. Select the **[Go]** button.
4. Each selected device category is now aligned with the selected device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page, or a device dashboard defined in the **Device Class Editor** page, the device dashboard associated with the device category will appear as the default view in the **Device Summary** page.

Chapter 8

Device Maintenance

Overview

This chapter describes the ways in which you can maintain devices in SL1.

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

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

This chapter includes the following topics:

What is Scheduled Maintenance? *204*

What is User Maintenance? *205*

The Maintenance Minimum Severity Setting *205*

Enabling and Disabling User Maintenance for a Single Device *205*

Enabling and Disabling User Maintenance for One or More Devices *208*

Scheduling Maintenance for a Single Device *209*

Viewing the Schedule Manager *209*

Defining a Scheduled or Recurring Device Maintenance Window for a Single Device *210*

Scheduling Maintenance for One or More Devices *213*

Enabling or Disabling Scheduled Maintenance for One or More Devices *214*

Deleting Scheduled Maintenance for One or More Devices *215*

What is Scheduled Maintenance?

Scheduled Maintenance is a date and time when a device is put into "maintenance mode". During maintenance mode, for the selected devices SL1 will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate applicable events for the devices.

SL1 includes tools that allow you to view, edit, and define scheduled maintenance for one or more devices. The **Schedule Manager** page allows you to schedule one-time and recurring maintenance tasks and downtime for a device. You can use the scheduled maintenance to:

- Specify recurring downtime for routine maintenance (for example, a weekly database backup that occurs every Tuesday at 3 AM).
- Specify one-time downtime (for example, when upgrading software or hardware).

When a device is in maintenance, SL1 will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled during maintenance, SL1 will collect information from the device but will not generate applicable events for the device.

You can specify a "patch window" within the larger maintenance period. The "patch window" allows SL1 to limit the suppression events to a small time-frame within the larger maintenance window. For example:

Suppose you have to patch a server that is monitored by SL1. Suppose you know you will perform this task sometime between midnight and 6:00 AM. Suppose you know that the actual patch process will require only 15 minutes of downtime for the server. In SL1, you would define a maintenance window of 24:00 - 6:00 and a patch window of 15 minutes.

1. At 24:00, SL1 generates an event saying that the server is going into maintenance mode. Because you have defined a patch window, SL1 continues to monitor this server as normal.
2. At 3:00, you apply the patch to the server. The server reboots, and SL1 generates an event saying that the server is offline. This first event within the larger maintenance window triggers the start of the patch maintenance window.
3. SL1 suppresses the event that triggered the patch maintenance window and instead generates an event "Patch Maintenance Window Opened".
4. For the next 15 minutes, SL1 will suppress all events for the device.
5. At 3:15, SL1 will generate an event for "Patch Maintenance Window Closed". This event clears the previous event "Patch Maintenance Window Opened".
6. SL1 will now generate events for the device, even though the maintenance window extends until 6:00.

NOTE: If the patch was applied at 5:50, the server was rebooted, and SL1 generated an event saying that the server is offline, events would be suppressed only until the end of the maintenance window, 6:00, even though the patch window is 15 minutes.

What is User Maintenance?

User maintenance is an option that allows a user to manually put a device in to "maintenance mode". During maintenance mode, for the selected devices SL1 will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate applicable events for the devices.

User maintenance mode is not scheduled. That is, a user must manually enable user maintenance to put a device into this mode and a user must manually disable user maintenance to turn off this mode for a device. User maintenance mode overrides scheduled maintenance for a device.

User maintenance can be enabled and disabled in the user interface or through the API. For information about using the API, see the ***ScienceLogic API*** manual.

The Maintenance Minimum Severity Setting

The global ***Maintenance Minimum Severity*** setting specifies the minimum severity required for an event to be suppressed during device maintenance and user maintenance. The default value is *Healthy*, which causes all events to be suppressed. To change this setting:

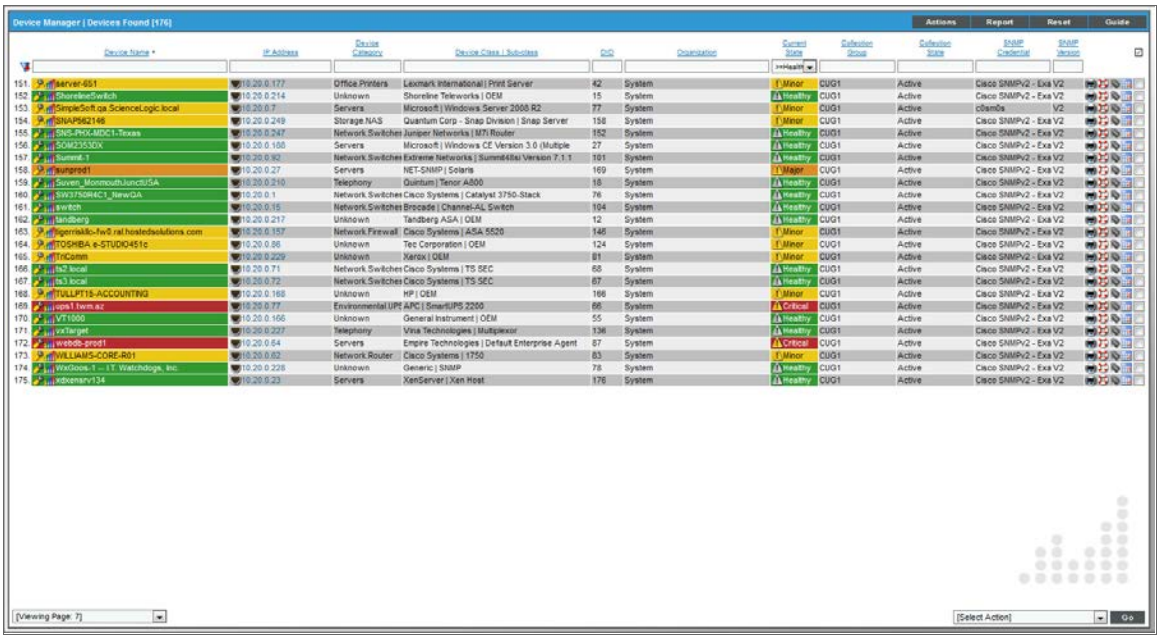
1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. In the **Behavior Settings** page, select a value in the ***Maintenance Minimum Severity*** drop-down list. The choices are *Healthy*, *Notice*, *Minor*, *Major*, or *Critical*.
3. Select the **[Save]** button. Events with a severity lower than the severity you chose will now be generated for all devices in scheduled maintenance mode and user maintenance mode.

Enabling and Disabling User Maintenance for a Single Device

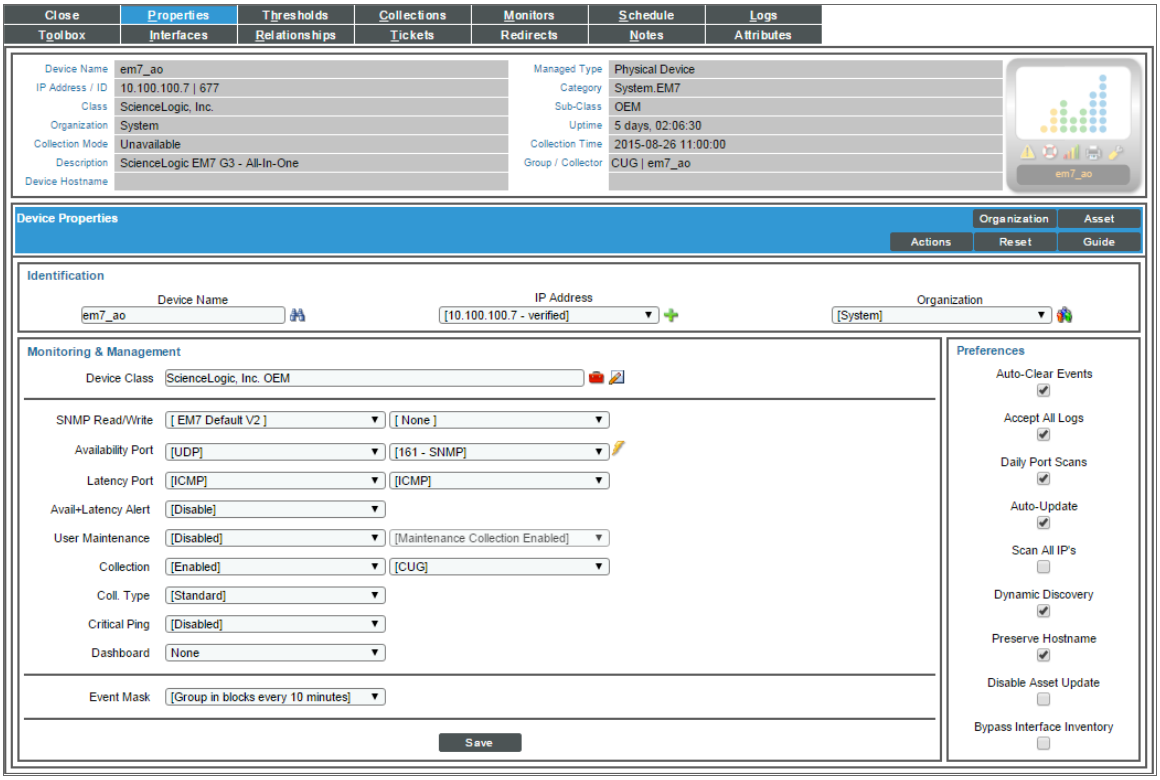
You can enable and disable user maintenance mode in the **Device Properties** page.

To enable or disable user maintenance mode for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).



2. In the **Device Manager** page, find the device for which you want to enable or disable user maintenance. Select its wrench icon ( ). The **Device Properties** page is displayed:



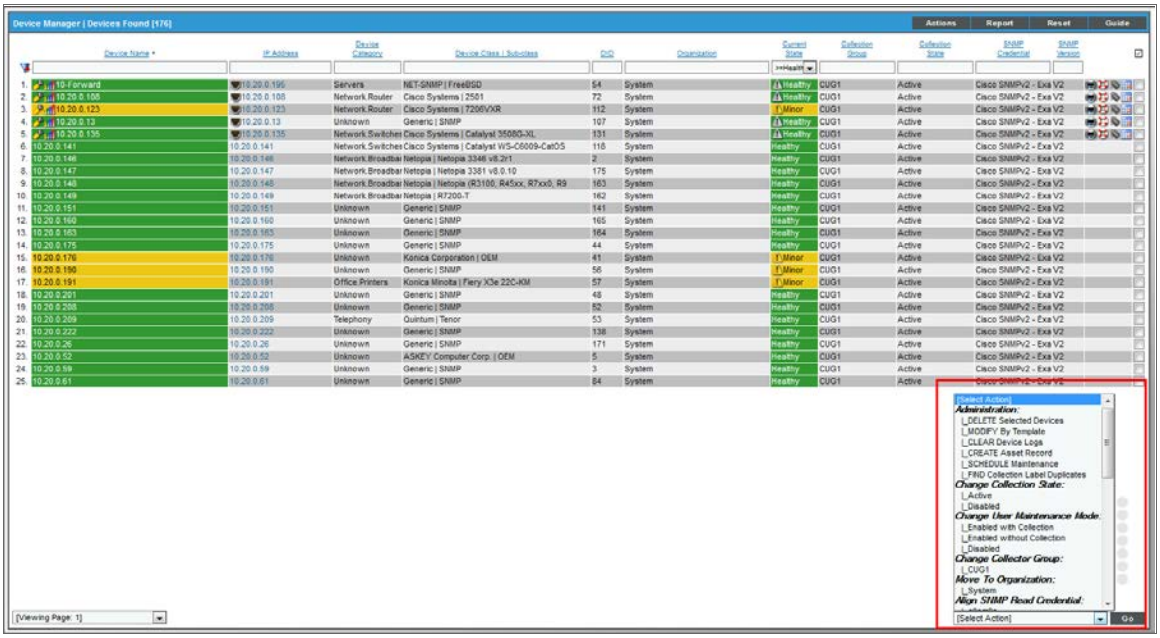
3. In the **Device Properties** page, edit the following fields:
   - ***User Maintenance***. Specifies whether the device is in user maintenance mode. During maintenance mode, for the selected devices SL1 will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, SL1 will collect information from the selected devices but will not generate applicable events for the devices. Choices are:
     - *Enabled*. Device will be put in user maintenance mode. The device will remain in this state until you or another user disables user maintenance mode.
     - *Disabled*. User maintenance mode will be disabled for this device.
   - ***User Maintenance Collection***. The drop-down list to the right of the ***User Maintenance*** field specifies whether SL1 will poll the device during user maintenance mode. Choices are:
     - *Enabled*. The device will be polled during user maintenance mode.
     - *Disabled*. The device will not be polled during user maintenance mode.
4. Select the **[Save]** button.

Enabling and Disabling User Maintenance for One or More Devices

The **Device Manager** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once. From the ***Select Action*** menu, you can enable or disable user maintenance mode for multiple devices, simultaneously.

To enable or disable user maintenance mode for multiple devices:

1. Go to the **Device Manager** page (Devices > Device Manager):



2. In the **Device Manager** page, select the checkbox for each device to which you want to apply the action. To select all checkboxes for all devices, select the red checkbox (☑) at the top of the page.
3. In the ***Select Action*** drop-down list, select one of the following:

   - *Change User Maintenance Mode: Enabled with Collection*. This option puts the selected devices into user maintenance mode with collection enabled. The devices will remain in this state until you or another user disables user maintenance mode.
   - *Change User Maintenance Mode: Enabled without Collection*. This option puts the selected devices into user maintenance mode with collection disabled. The devices will remain in this state until you or another user disables user maintenance mode.
   - *Change User Maintenance Mode: Disabled*. This option disables user maintenance mode for the selected devices.

4. Click the **[Go]** button.
5. The changes are applied to each selected device.

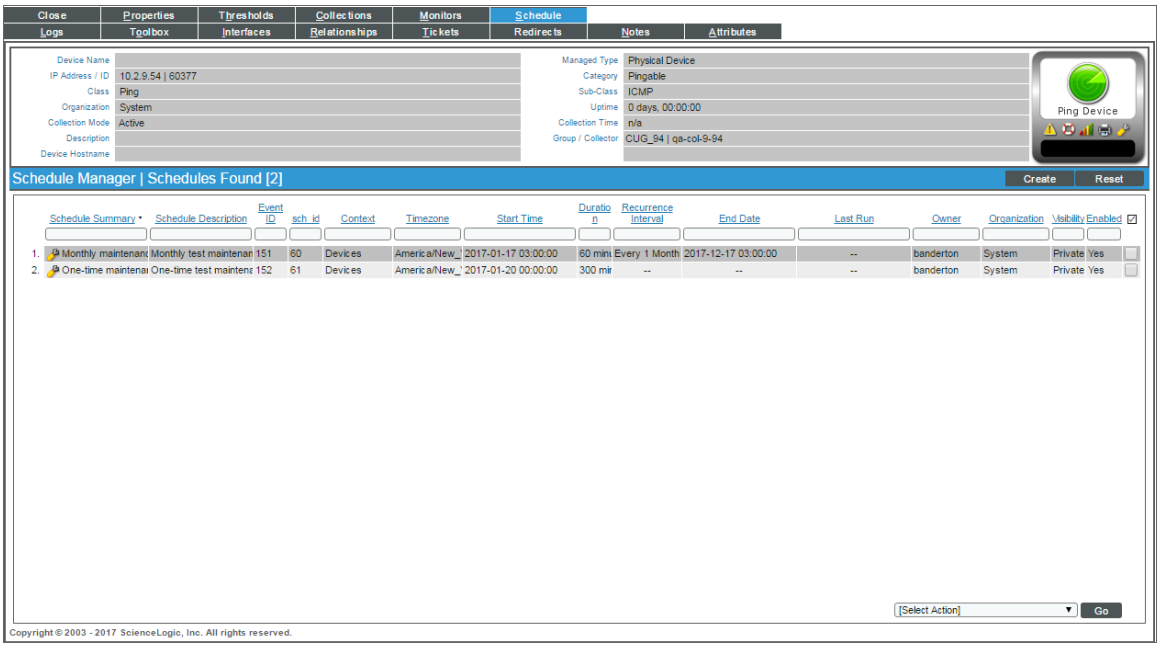
Scheduling Maintenance for a Single Device

In the **Schedule Manager** page (in the **Device Administration** panel), you can schedule maintenance and downtime for a device.

NOTE: You can also view and manage all scheduled processes from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). For more information, see the ***System Administration*** manual.

Viewing the Schedule Manager

The **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule) displays the following information about each scheduled or recurring device maintenance window:



- ***Schedule Summary***. Displays the name assigned to the scheduled process.
- ***Schedule Description***. Displays a description of the scheduled process.
- ***Event ID***. Displays a unique, numeric ID for the scheduled process. SL1 automatically created this ID for each scheduled process.
- ***sch id***. Displays a unique, numeric ID for the schedule. SL1 automatically created this ID for each schedule.
- ***Context***. Displays the area of SL1 upon which the schedule works.

- ***Timezone***. Displays the time zone associated with the scheduled process.
- ***Start Time***. Displays the date and time at which the scheduled process will begin.
- ***Duration***. Displays the duration, in minutes, which the scheduled process occurs.
- ***Recurrence Interval***. If applicable, displays the interval at which the scheduled process recurs.
- ***End Date***. If applicable, displays the date and time on which the scheduled process will recur.
- ***Last Run***. If applicable, displays the date and time the scheduled process most recently ran.
- ***Owner***. Displays the username of the owner of the scheduled process.
- ***Organization***. Displays the organization to which the scheduled process is assigned.
- ***Visibility***. Displays the visibility level for the scheduled process. Possible values are "Private", "Organization", or "World".
- ***Enabled***. Specifies if the scheduled process is enabled. Possible values are "Yes" or "No".

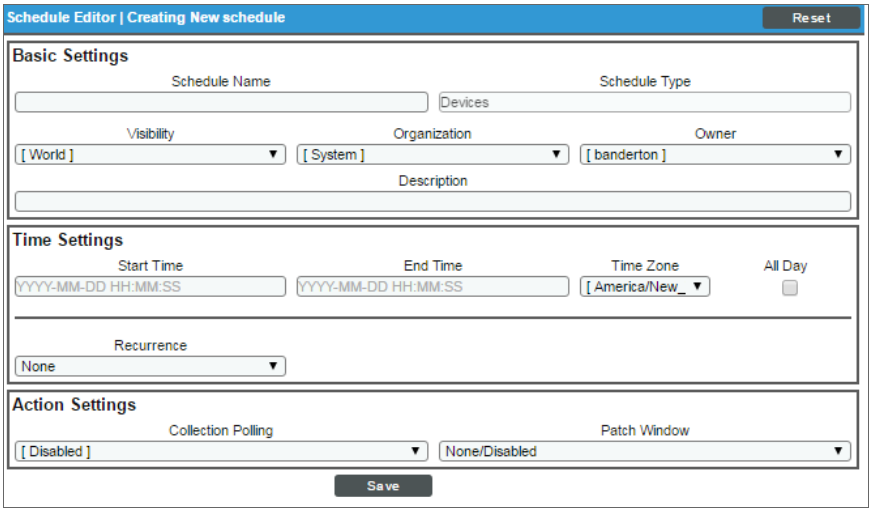
To edit a scheduled or recurring device maintenance window, click its wrench icon ( ) and update the settings as needed on the **Schedule Editor** modal page. (For more information, see the section *Defining a Scheduled or Recurring Device Maintenance Window for a Single Device*.)

Defining a Scheduled or Recurring Device Maintenance Window for a Single Device

You can schedule a device maintenance window in SL1 from the **Schedule Manager** page. SL1 will automatically set the status of the device to "maintenance" at the scheduled time.

To define a scheduled or recurring device maintenance window:

1. Go to the **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule).
2. Click **[Create]**. The **Schedule Editor** modal page appears.
3. On the **Schedule Editor** modal page, enter values in the following fields:



Basic Settings

- ***Schedule Name***. Type a name for the scheduled process.
- ***Schedule Type***. Indicates the scheduled process type (such as Tickets, Reports, or Devices).
- ***Visibility***. Select the visibility for the scheduled process. You can select one of the following:
  - *Private*. The scheduled process is visible only to the owner selected in the ***Owner*** field.
  - *Organization*. The scheduled process is visible only to the organization selected in the ***Organization*** field.
  - *World*. The scheduled process is visible to all users.
- ***Organization***. Select the organization to which you want to assign the scheduled process.
- ***Owner***. Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
- ***Description***. Type a description of the scheduled process.

Time Settings

- ***Start Time***. Click in the field and select the date and time you want the scheduled process to start.
- ***End Time***. Click in the field and select the date and time you want the scheduled process to end.
- ***Time Zone***. Select the region or time zone for the scheduled start time.

NOTE: If you want SL1 to automatically adjust for daylight savings time (if applicable), then you must select a named region (such as *America/New York*) in the ***Time Zone*** field. If you select a specific time zone (such as *EST*) or a specific time offset (such as *GMT-5*), then SL1 will not automatically adjust for daylight savings time.

- ***All Day***. Select this checkbox if the scheduled process occurs all day rather than during a specific period of time. If you do so, the ***End Time*** field becomes disabled.
- ***Recurrence***. Select whether you want the scheduled process to occur once or on a recurring basis. You can select one of the following:
  - *None*. The scheduled process occurs only once.
  - *By Interval*. The scheduled process recurs at a specific interval.

If you select *By Interval*, the following additional fields appear:

- ***Interval***. In the first field, enter a number representing the frequency of the scheduled process, then select the time interval in the second field. Choices are *Minutes*, *Hours*, *Days*, *Weeks*, or *Months*. For example:
  - If you specify "6 Hours", then the scheduled process recurs every six hours from the time listed in the ***Start Time*** field.

- If you specify "10 Days", then the scheduled process recurs every 10 days from the date listed in the ***Start Time*** field.
- If you specify "2 Weeks", then the scheduled process recurs every two weeks, on the same day of the week as the ***Start Time***.
- If you specify "3 Months" the ticket recurs every three months, on the same day of the month as the ***Start Time***.

- ***Recur Until***. Specifies when the scheduled process stops recurring. You can select one of the following:
  - *No Limit*. The scheduled process recurs indefinitely until it is disabled.
  - *Specified Date*. The scheduled process recurs until a specific date and time. If you select *Specified Date*, you must select a date and time in the ***Last Recurrence*** field.
- ***Last Recurrence***. Click in the field and select the date and time you want the scheduled process to stop recurring.

Action Settings

- ***Collection Polling***. Specifies whether SL1 should perform collection on the device during the scheduled maintenance. Choices are:
  - *Enabled*. During scheduled maintenance, SL1 will collect data from the device, but no events will be triggered for the device.
  - *Disabled*. During scheduled maintenance, SL1 will not collect data from the device. No events will be triggered for the device.
- ***Patch Window***. You can specify a "patch window" within the larger maintenance period. The "patch window" allows SL1 to limit the suppression of events to a small time-frame within the larger maintenance window. Your choices are:
  - *None*
  - Between *5 minutes and 60 minutes*, in five-minute intervals.

  For example:

  Suppose you have to apply a patch to a server that is monitored by SL1. Suppose you know you will perform this task sometime between midnight and 6:00 AM. Suppose you know that the actual patch process requires only 15 minutes of downtime for the server. In SL1, you would define a maintenance window of 24:00 - 6:00 and a patch window of 15 minutes. In this scenario:

1. At 24:00, SL1 generates an event saying that the server is going into maintenance mode. Because you have defined a patch window, SL1 continues to monitor this server as normal.
2. At 3:00, you apply the patch to the server. The server reboots, and SL1 generates an event saying that the server is offline. The first event that both matches or exceeds the ***Patch Maintenance Minimum Severity*** in the **Behavior Settings** page (System > Settings > Behavior) and occurs within the larger maintenance window triggers the start of the patch window.

3. SL1 suppresses the event that triggered the patch maintenance window and instead generates an event "Patch Maintenance Window Opened".
4. For the next 15 minutes, SL1 will suppress all events for the device.
5. At 3:15, SL1 will generate an event for "Patch Maintenance Window Closed". This event clears the previous event "Patch Maintenance Window Opened".
6. SL1 will now generate events for the device, even though the maintenance window extends until 6:00.

NOTE: If the patch was applied at 5:50, the server was rebooted, and SL1 generated an event saying that the server is offline, events would be suppressed only until the end of the maintenance window, 6:00, even though the patch window is 15 minutes.

4. Click **[Save]**.

Scheduling Maintenance for One or More Devices

The **Device Manager** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once. From the ***Select Action*** menu, you can schedule maintenance for multiple devices, simultaneously.

To schedule maintenance for multiple devices:

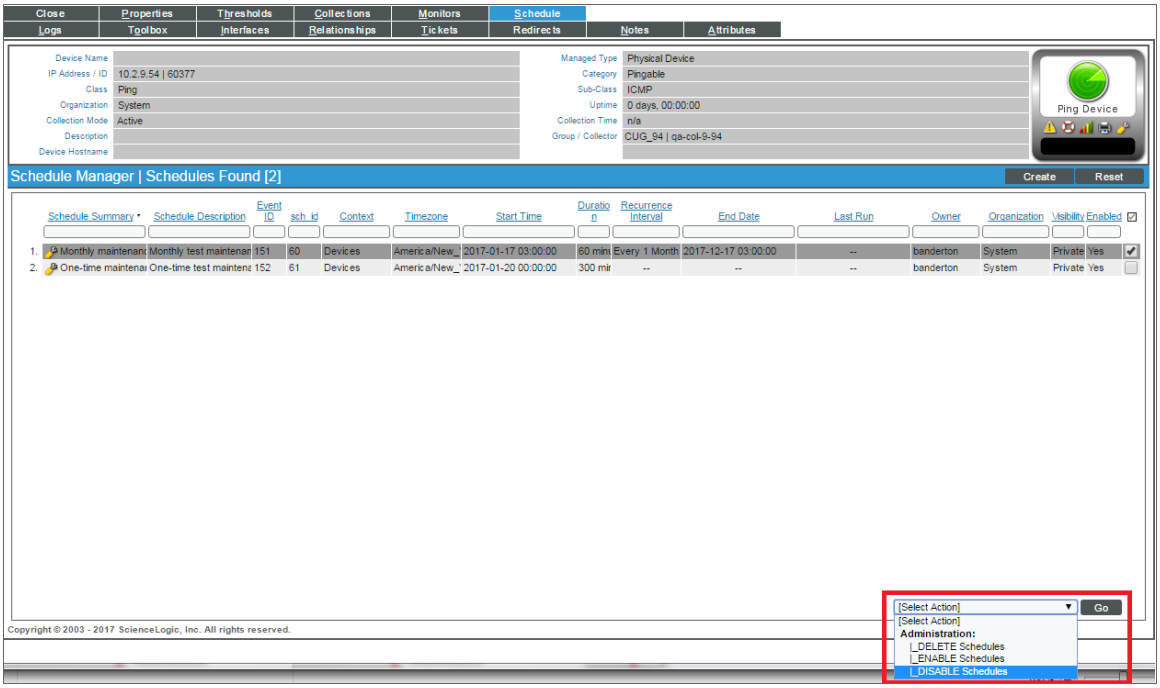
1. Go to the **Device Manager** page (Devices > Device Manager):

2. In the **Device Manager** page, select the checkbox for each device for which you want to schedule maintenance. To select all checkboxes for all devices, select the red checkbox ( ) at the top of the page.
3. In the ***Select Action*** drop-down list, select *Schedule Maintenance*, and then click **[Go]**. The **Schedule Editor** modal page appears.
4. To schedule maintenance for the selected devices, follow the steps described in the section *Defining a Scheduled or Recurring Device Maintenance Window for a Single Device*. The values you supply in the **Schedule Editor** modal page are applied to each selected device.

Enabling or Disabling Scheduled Maintenance for One or More Devices

You can enable or disable one or more scheduled or recurring device maintenance windows from the **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule). To do this:

1. Go to the **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule).



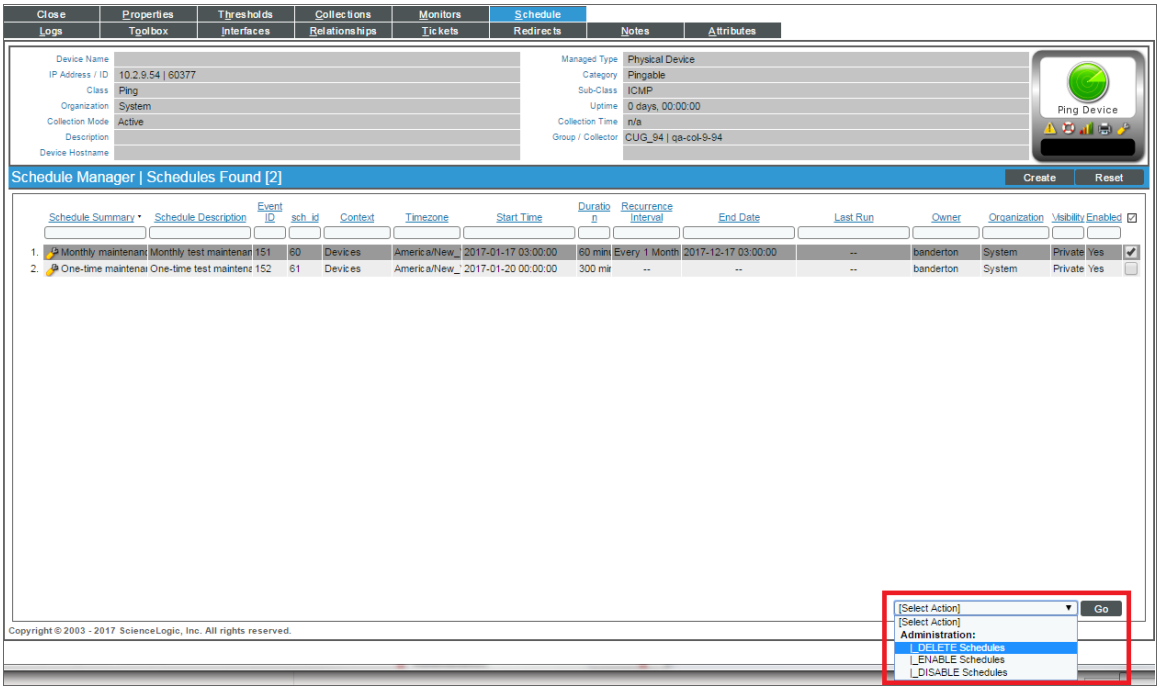
2. Select the checkbox icon for each scheduled process you want to enable or disable.
3. Click the ***Select Action*** menu and choose *Enable Schedules* or *Disable Schedules*.
4. Click the **[Go]** button.

Deleting Scheduled Maintenance for One or More Devices

You can delete one or more scheduled or recurring device maintenance windows from the **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule).

To delete maintenance windows:

1. Go to the **Schedule Manager** page (Devices > Device Manager > wrench icon > Schedule).



2. Select the checkbox icon for each scheduled process you want to delete.
3. Click the ***Select Action*** menu and choose *Delete Schedules*.
4. Click the **[Go]** button.

Chapter 9

Managing Dynamic Applications

Overview

This chapter describes how to manage the Dynamic Applications aligned to a device.

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

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

This chapter includes the following topics:

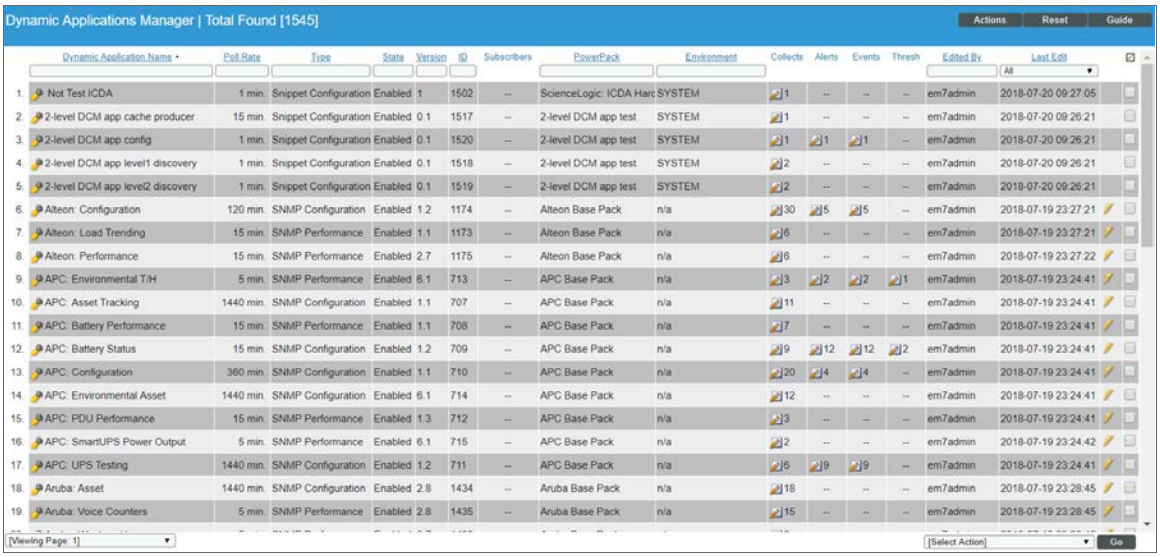
Viewing the List of Dynamic Applications 217
Searching and Filtering the List of Dynamic Applications 221
Special Characters 223
Viewing the Dynamic Applications Associated with a Device 226
Viewing the Status of a Dynamic Application 228
Found 229
Collect 229
How SL1 Manages Collect Status 230
Stopping Collection 230
Starting Collection 230
Collection Objects that are Excluded from Maintenance 231
Status of Objects for Deviation 231
Manually Associating a Dynamic Application with a Device 231

Editing the Credential Associated with a Dynamic Application 233
Performing Other Administrative Tasks for an Aligned Dynamic Application 234
Enabling or Disabling Objects 235
Restarting Automatic Maintenance of Collection Objects 235
Editing the Poll Frequency for a Dynamic Application on the Current Device 236
Stopping Data Collection for a Dynamic Application 236
Resetting Statistical Data for a Dynamic Application 237
Resetting Persistent Session Objects for a Dynamic Application 238
Testing Data Collection for a Dynamic Application 238
Removing Data Collected by a Dynamic Application 239
Bulk Un-Aligning Dynamic Applications 239
Setting Thresholds for Dynamic Applications 240
Dynamic Applications and Discovery 241
How Does SL1 Align Dynamic Applications During Discovery? 242
Queuing Discovery from the Dynamic Applications Manager Page 243

Viewing the List of Dynamic Applications

The **Dynamic Applications Manager** page (System > Manage > Dynamic Applications) displays a list of all existing Dynamic Applications. For each Dynamic Application, the page displays the following:

TIP: To sort the list of Dynamic Applications, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Last Edit*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.



NOTE: By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

- ***Dynamic Application Name***. Name of the Dynamic Application, as defined in the **Dynamic Applications Properties Editor** page.
- ***Poll Rate***. Frequency, in minutes, at which SL1 will poll all devices that use this Dynamic Application.

NOTE: The ***Poll Rate*** column displays the default poll frequency for the Dynamic Application, as defined in the **Dynamic Applications Properties Editor** page. You can define a ***custom*** poll frequency for one or more devices in a device template. The poll frequency defined in the device template overrides the poll frequency defined for the Dynamic Application. Devices to which the device template is applied will use the poll frequency defined in the device template.

- ***Type***. Type of Dynamic Application. The choices are:
    - *Bulk Snippet Configuration*. A *single instance of the Dynamic Application* uses custom-written Python code to collect static configuration data from *multiple devices*. This is useful for systems that include a large number of component devices. For details on creating bulk snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.
    - *Bulk Snippet Performance*. A *single instance of the Dynamic Application* uses custom-written Python code to collect trendable performance data from *multiple devices*. This is useful for systems that include a large number of component devices. For details on creating bulk snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.

- *Database Configuration*. The Dynamic Application retrieves configuration data from a database application. The Dynamic Application uses SQL queries. The queried device returns table data. For details on creating database Dynamic Applications, see the ***DatabaseDynamic Application Development*** manual.
- *Database Performance*. The Dynamic Application retrieves trendable performance data from a database application. The Dynamic Application uses SQL queries. The queried device returns table data. For details on creating database Dynamic Applications, see the ***DatabaseDynamic Application Development*** manual.
- *Internal Collection Inventory*. The Internal Collection Inventory Dynamic Application (ICDA) retrieves configuration data about filesystems and interface. For filesystem, an ICDA Inventory can retrieve data such as storage size, filesystem type, and storage used. These ICDAs can also collect configuration data about interfaces, such as physical address, operational status, and IP addresses. For details on creating ICDAs, see the ***Internal Collection Dynamic Application Development*** manual.
- *Internal Collection Performance*. The Internal Collection Performance Dynamic Application (ICDA) retrieves data about availability and latency, device information (system description, system uptime, system locale), filesystem performance, and interface performance. For details on creating ICDAs, see the ***Internal Collection Dynamic Application Development*** manual.
- *IT Service*. A special type of Dynamic Application that SL1 uses to monitor IT Services. When you create and edit an IT Service in the **IT Service Editor** page, SL1 will automatically create and maintain a Dynamic Application for that IT Service. Dynamic Applications for IT Services will appear in the **Dynamic Applications Manager** page. However, if you want to edit the settings for an IT Service, you should not edit the Dynamic Application for that IT Service. Instead, use the **IT Service Editor** page to edit IT Services. For details on creating IT Service policies, see the manual ***IT Services***.
- *PowerShell Configuration*. The Dynamic Application uses PowerShell commands to collect static configuration data from a Windows device. For details on creating PowerShell Dynamic Applications, see the manual ***Dynamic Application Development - WMI and PowerShell***. For information on configuring SL1 and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *PowerShell Performance*. The Dynamic Application uses PowerShell commands to collect trendable performance data from a Windows device. For details on creating PowerShell Dynamic Applications, see the manual ***Dynamic Application Development - WMI and PowerShell***. For information on configuring SL1 and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *Snippet Configuration*. The Dynamic Application uses custom-written Python code to collect configuration data from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.
- *Snippet Journal*. The Dynamic Application uses custom-written Python code to collect data formatted as log entries from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.
- *Snippet Performance*. The Dynamic Application uses custom-written Python code to collect trendable performance data from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.

- *SNMP Configuration*. The Dynamic Application uses SNMP to retrieve static, configuration data from devices or applications. For details on creating SNMP Dynamic Applications, see the ***SNMP Dynamic Application Development*** manual.
- *SNMP Performance*. The Dynamic Application uses SNMP to retrieve trendable performance data from devices or applications. For details on creating SNMP Dynamic Applications, see the ***SNMP Dynamic Application Development*** manual.
- *SOAP Configuration*. The Dynamic Application uses XML and SOAP to retrieve static configuration data from a SOAP server. The queried device returns XML data. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** manual.
- *SOAP Performance*. The Dynamic Application uses XML and SOAP to retrieve trendable performance data from a SOAP server. The queried device returns XML data. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP. and XSLT Dynamic Application Development*** manual.
- *WMI Configuration*. The Dynamic Application retrieves configuration information from either WMI or WBEM running on a managed device. WMI Dynamic Applications use a query format to request data from a managed device. WBEM Dynamic Applications use wbemcli and HTTP to request data from a managed device. For details on creating WMI Dynamic Applications, see the manual ***Dynamic Application Development - WMI and PowerShell***. For information on configuring SL1 and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *WMI Performance*. The Dynamic Application retrieves trendable performance data from either WMI or WBEM running on a managed device. WMI Dynamic Applications use a query format to request data from a managed device. WBEM Dynamic Applications use wbemcli and HTTP to request data from a managed device.
- *XML Configuration*. The Dynamic Application uses HTTP GET queries. The queried device returns static configuration data in XML format. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** manual.
- *XML Performance*. The Dynamic Application uses HTTP GET queries. The queried device returns trendable performance data in XML format. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** manual.
- *XSLT Configuration*. The Dynamic Application uses XML and SOAP to retrieve static configuration data from a SOAP server. The requests used to retrieve data are generated by performing an XSLT transformation on an XML document that contains data already collected by the Dynamic Application. The queried device returns XML data, which must be changed to a specific format by performing a second XSLT transformation. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** manual.
- *XSLT Performance*. The Dynamic Application uses XML and SOAP to retrieve trendable performance data from a SOAP server. The requests used to retrieve data are generated by performing an XSLT transformation on an XML document that contains data already collected by the Dynamic Application. The queried device returns XML data, which must be changed to a specific format by performing a second XSLT transformation. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** manual.

- ***State***. Specifies whether the Dynamic Application is *Enabled* or *Disabled*.
- ***Version***. Version number to assign to the Dynamic Application. You can customize this value and increment it according to your change-management policies.
- ***ID***. Unique application ID, assigned by SL1.
- ***Subscribers***. Number of devices that use the Dynamic Application. Clicking on the icon leads to the **Application Subscribers** modal page, where you can view the list of devices and access other pages for each subscriber device. You can also access this page by selecting the wrench icon ( ) for a Dynamic Application and selecting the **[Subscribers]** tab.
- ***PowerPack***. Specifies whether or not the Dynamic Application is included in a PowerPack.
- ***Environment***. The execution environment to which the Dynamic Application is aligned, if it is a snippet or internal collection Dynamic Application. If it is not a snippet or internal collection Dynamic Application, then this column displays "n/a".
- ***Collects***. Number of objects included in the Dynamic Application. Clicking on the icon ( ) leads to the **Collection Objects** page, where you can view the list of collection objects and edit their properties.
- ***Alerts***. Number of custom alerts defined for the Dynamic Application. Clicking on the icon ( ) leads to the **Alert Objects** page, where you can view and edit each alert defined for the Dynamic Application.
- ***Events***. Number of events associated with the Dynamic Application. Clicking on the icon ( ) leads to the **Event Policy Manager** page, where you can view information about each event definition associated with the Dynamic Application definition and edit each event definition.
- ***Thresh***. Number of threshold objects defined for the Dynamic Application. Clicking on the icon ( ) leads to the **Threshold Objects** page, where you can view and edit information about each threshold object defined for the Dynamic Application.
- ***Edited By***. Username of the person who created or last edited the Dynamic Application.
- ***Last Edit***. Date that the Dynamic Application was created or last edited.

Searching and Filtering the List of Dynamic Applications

The Filter-While-You-Type fields appear as a row of blank fields at the top of the list. These fields allow you to filter the items that appear in the list.

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. SL1 will search for entries that match the text, including partial matches. Text matches are not case-sensitive, and you can use special characters in each text field.

By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

You can filter by one or more of the following parameters. Only items that meet all of the filter criteria are displayed on the page.

- ***Dynamic Application Name***. You can enter text to match, including *special characters*, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching name.

- ***Poll Rate***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching polling rate.
- ***Type***. You can enter text to match, including ***special characters***, , and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching type.
- ***State***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching state.
- ***Version***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching version number.
- ***ID***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching ID number.
- ***Subscribers***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching number of subscribers.
- ***PowerPack***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching PowerPack.
- ***Environment***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching execution environment.
- ***Collects***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching number of collection objects.
- ***Alerts***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching number of alerts.
- ***Events***. You can enter text to match,including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching number of event policies.
- ***Thresh***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that have a matching number of thresholds.
- ***Edited By***. You can enter text to match, including ***special characters***, and the Dynamic Applications Manager page will display only Dynamic Applications that were created or edited by a a matching user-name.
- ***Last Edited***. Only those Dynamic Applications that match all the previously selected fields and have the specified "last edited" date will be displayed. The choices are:
    - *All*. Display all Dynamic Applications that match the other filters.
    - *Last Minute*. Display only Dynamic Applications that have been modified within the last minute.
    - *Last Hour*. Display only Dynamic Applications that have been modified within the last hour.
    - *Last Day*. Display only Dynamic Applications that have been modified within the last day.
    - *Last Week*. Display only Dynamic Applications that have been modified within the last week.
    - *Last Month*. Display only Dynamic Applications that have been modified within the last month.
    - *Last Year*. Display only Dynamic Applications that have been modified within the last year.

Special Characters

You can include the following special characters to filter by each column except those that display date and time:

NOTE: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:

  "dell, micro" matches all values that contain the string "dell" OR the string "micro".

- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:

  "dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

  "!dell" matches all values that do not contain the string "dell".

  "!^micro" would match all values that do not start with "micro".

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!^" would match null values.

  "!$" would match null values.

  "!*" would match null values.

  "happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

  "hel*er" would match "helpers" and "helicopter" but not "hello".

  "325*" would match "325", "32561", and "325000".

  "*000" would match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

  "l?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

  "135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502"

String

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

  "^sci" would match "scientific" and "sciencelogic", but not "conscious".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!^micro" would match all values that do not start with "micro".

  "!^$" would match all values that are not null.

  "!^" would match null values.

- $ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

  "ter$" would match the string "renter" but not the string "terrific".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!$" would match null values.

NOTE: You can use both ^ and $ if you want to match an entire string and only that string. For example, "^tern$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

Numeric

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

  "1-5 "would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

  "1-" matches 1 and greater. So would match 1, 2, 6, 345, etc.

  "-5" matches 5 and less. So would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

  ">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

  "<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

  "=>7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

  "=<12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

  "=-5 " would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contains the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!0$". Matches only text that does not end with "0".
- "!^silo$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!^". Matches null values, typically represented as "--" in most pages.
- "!$". Matches null values, typically represented as "--" in most pages.

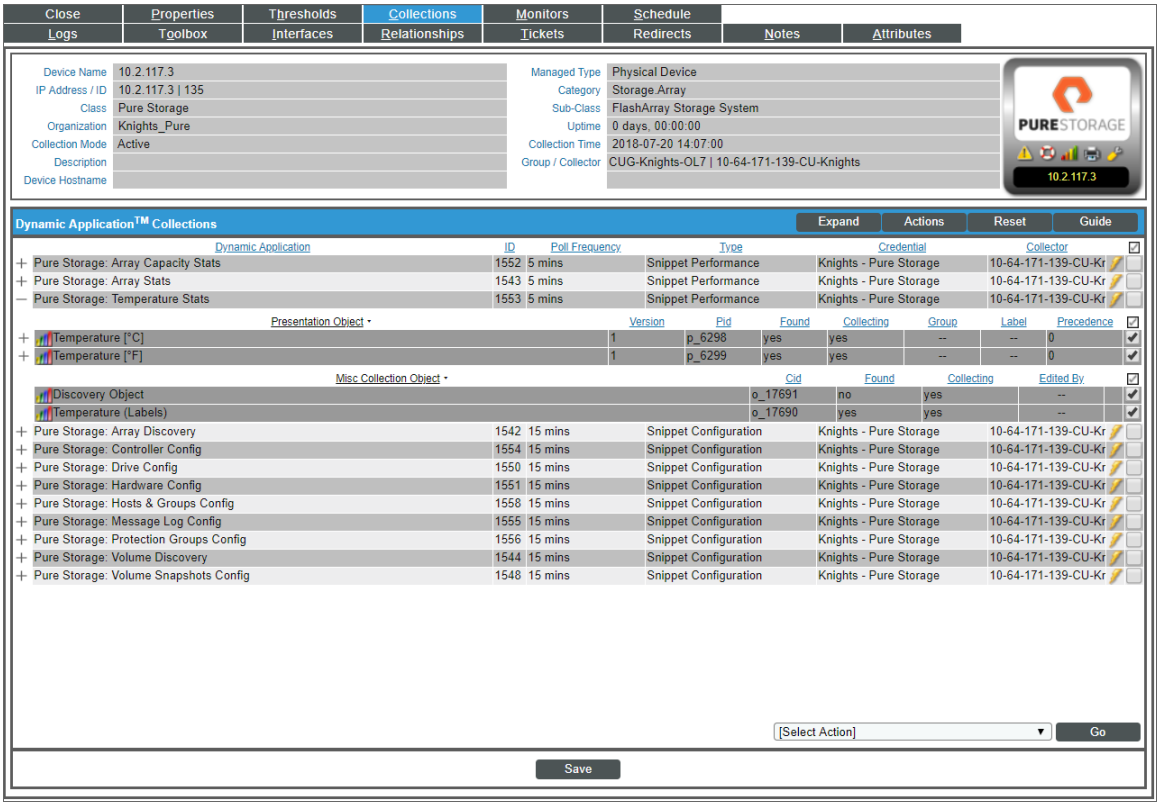
- "!^$". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*l*o$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- "!^s*i*l*o$". Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol' and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- " !silo ". Matches text that does not contain "silo".
- " !^silo$ ". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.
- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n*SAN$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

Viewing the Dynamic Applications Associated with a Device

To view the Dynamic Applications associated with a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to view Dynamic Applications. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Collections]** tab.

4. The **Dynamic Application Collections** page displays a list of all Dynamic Applications aligned with the current device. For each Dynamic Application, the **Dynamic Application Collections** page displays the following read-only information:



- ***Plus Sign*** (+). Clicking on this icon displays a list of all Presentation Objects included in Dynamic Applications of type "Performance" and "Journal" or a list of all Collection Objects included in Dynamic Applications of type "Configuration". You can click on the plus sign next to each Presentation Object to see all the Collection Objects included in the Presentation Object.
- ***Minus Sign*** (—). Collapses a Dynamic Application and hides the display of Presentation Objects and Collection Objects.
- ***Dynamic Application***. Name of the Dynamic Application.
- ***ID***. Numeric ID for the Dynamic Application.
- ***Poll Frequency***. Frequency at which SL1 will query the device to retrieve the data specified in the Dynamic Application. Each Dynamic Application includes a default frequency. From this page (**Dynamic Application Collections**), you can change the poll frequency for a Dynamic Application on the current device. This edited poll frequency will override the default frequency for the Dynamic Application and the poll frequency defined for a Dynamic Application in one or more device templates.

- ***Type***. The protocol used by the Dynamic Application (Database [SQL], Internal Collection Inventory or Internal Collection Performance (ICDA), Snippet [Python], SNMP, SOAP, WMI, XML, or XSLT) and the type of data collected by the Dynamic Application (Configuration, Performance, or Journal).
- ***Credential***. Name of the credential that SL1 uses to access the device and retrieve the data specified in the Dynamic Application.

NOTE: Cache-consuming Dynamic Applications do not require a credential. If you aligned a cache-consuming Dynamic Application in the **Dynamic Application Alignment** modal page, the ***Credential*** field displays *N/A* and is grayed out. You do not have to select a credential in the **Dynamic Application Alignment** modal page.

- ***Collector***. Name of the specific Data Collector used to collect data from the Dynamic Application.

NOTE: Based on the Dynamic Application's ***Collector Affinity*** settings, the Dynamic Application might be assigned to a different Data Collector than the Data Collector that is assigned to the device in the Device Properties page (Devices> Device Manager > wrench icon). In the **Dynamic Application Collections** page, hover your mouse over the ***Collector*** name for any of the Collection Objects to view a tooltip that explains why the Dynamic Application is assigned to its particular Data Collector.

- ***Run Dynamic Application*** ( ). Performs a test run of data collection for the selected Dynamic Application on the current device.

NOTE: If a device is currently unavailable, the lightning-bolt icon ( ) will be grayed out for each Dynamic Application aligned with the device.

- ***Checkbox*** (☑). Apply an action from the ***Select Action*** field to this instance of the Dynamic Application.

Viewing the Status of a Dynamic Application

For each device, SL1 maintains the collection status for each collection object in each Dynamic Application aligned with that device. The **Dynamic Application Collections** page displays the status of each collection object for a device as represented by two values: ***Found*** and ***Collect***. The **Dynamic Application Collections** page also displays the ***Found*** and ***Collect*** values for each presentation object, which are derived from the status of each collection object used by the presentation object.

Found

The ***Found*** status for a collection object has two possible values:

- *Yes*. Data has been successfully collected from this device for this object. ***Found*** is set to *Yes* the first time data is successfully collected from this device for this object.
- *No*. Data has never been successfully collected from this device for this object. *No* is the initial value of ***Found*** for every object when a Dynamic Application is initially aligned with a device.

The ***Found*** status for a presentation object also has two possible values (*Yes* and *No*).

- ***If the presentation object uses only one collection object***, the presentation object always has the same default ***Found*** and default ***Collect*** values as that collection object.
- ***If a presentation object uses multiple collection objects***, the default ***Found*** value for the presentation object will be *Yes* only if all the collection objects used by the presentation object have a ***Found*** value of *Yes*.

After ***Found*** is set to *Yes* for an object, SL1 will never automatically change the value of ***Found*** for this object.

The value of ***Found*** is used by SL1 to determine whether icons, tabs, and Navbar links that lead to the **[Performance]** or **[Configs]** page where the collection object is used should be active.

Collect

The ***Collect*** status for a collection object has two possible values:

- *Yes*. SL1 will attempt to collect data for this object when collection for this Dynamic Application occurs. *Yes* is the initial value for ***Collect*** for every object when a Dynamic Application is initially aligned with a device.
- *No*. SL1 will not attempt to collect data for this object when collection for this Dynamic Application occurs. SL1 might set ***Collect*** to *No* automatically if no data has been collected.
- If a collection object has a ***Collect*** value of *No*, all presentation objects that use that collection object will also have a ***Collect*** value of *No*.

The ***Collect*** status for a presentation object also has two possible values (*Yes* and *No*).

- ***If the presentation object uses only one collection object***, the presentation object always has the same default ***Found*** and default ***Collect*** values as that collection object.
- ***If a presentation object uses multiple collection objects***, the default ***Collect*** value for the presentation object will be *Yes* only if ***all*** the collection objects used by the presentation object have a ***Collect*** value of *Yes*. If one or more collection objects used by the presentation object have a ***Collect*** value of *No*, the presentation object will also have a default ***Collect*** value of *No*.
- The ***Collect*** status for a presentation object has no effect upon its collection objects. If you manually change the ***Collect*** status for a presentation object, the ***Collect*** status for the collection objects used by the presentation object will not change.

NOTE: Before determining which collection objects defined in a Dynamic Application will be collected, SL1 determines whether the Dynamic Application itself should be collected. Dynamic Applications are not collected for devices that are unavailable (because of a failed availability check) or have collection disabled (either manually by a user or because of maintenance scheduled in SL1) regardless of the ***Collect*** value of the objects.

How SL1 Manages Collect Status

Stopping Collection

One of the ScienceLogic hourly maintenance tasks checks the last collection time for every collection object being collected from every device. If the last collection time for an object on a device is more than 24 hours ago, collection is stopped for that collection object on that device. SL1 will set the ***Collect*** status of that object to *No*.

NOTE: If a device is in maintenance mode, is unavailable, or has been manually disabled by a user, SL1 will not automatically set the ***Collect*** status of objects to *No*. SL1 will automatically set the ***Collect*** status of objects to *No* only if the device is up and running, but SL1 still cannot collect the object.

When SL1 sets the ***Collect*** status of that object to *No*, SL1 generates an event. The event will include the name of the device, the name of the Dynamic Application, the name of the collection object, and the collection object IDs. By default, this event is of severity "notice".

NOTE: For Dynamic Applications that have the ***Component Mapping*** checkbox selected in the **Dynamic Applications Properties Editor** page, SL1 will never automatically set the ***Collect*** status to *No* for any of the collection objects in the Dynamic Application.

NOTE: For Dynamic Applications that have the ***Caching*** fields set to either *Cache Results* or *Consume cached results* in the **Dynamic Applications Properties Editor** page, SL1 will never automatically set the **Collect** status to *No* for any of the collection objects in the Dynamic Application.

Starting Collection

For each object that has the ***Collect*** status of *No*, SL1 will attempt to re-collect the object once a day. If re-collection is successful, SL1 will automatically set the ***Collect*** value for that object to *Yes*.

NOTE: If a user manually sets the ***Collect*** status of a collection object or presentation object to *No*, SL1 will **not** attempt to re-collect the object once a day and will **not** set the ***Collect*** status to *Yes*.

Collection Objects that are Excluded from Maintenance

The ***Collect*** status of the following collection objects is never changed automatically:

- Collection objects in Dynamic Applications that have the ***Component Mapping*** checkbox checked in the **Dynamic Applications Properties Editor** page.
- Collection objects in Dynamic Applications that have the ***Caching*** fields set to either *Cache Results* or *Consume cached results*, in the **Dynamic Applications Properties Editor** page.
- Collection objects that have the ***Disable Object Maintenance*** setting enabled.
- Collection objects that have a ***Collect*** status defined by a user, i.e. collection objects that were manually enabled or disabled by a user.

Status of Objects for Deviation

SL1 allows you to examine the value of an object and trigger an alert if that value falls outside the range of "normal" values for that object at the hour of the day on that day of the week. The deviation function allows you to define such alerts.

To use the deviation function, you must configure SL1 to store and calculate the mean values and standard deviation for an object. You do this by selecting the ***Enable Deviation Alerting*** field in the **Collection Objects** page. You then specify the minimum and maximum number of weeks to collect deviation data for the object. SL1 must have already collected at least the minimum number of weeks' worth of values for an object before SL1 can evaluate alert formulas that use the deviation function. To use the deviation function, you must specify a minimum value of at least two weeks.

If a Dynamic Application in the **Dynamic Application Collections** page contains one or more alerts that use the deviation function, the **Dynamic Application Collections** page displays the status of the collection objects.

For example, suppose an alert in a Dynamic Application will apply the deviation function to object "o_123". Suppose that you specified that SL1 must collect at least two weeks' worth of deviation data for this object. Suppose that SL1 contains only one weeks' worth of values for object "o_123". In this case, the **Dynamic Application Collections** page will display the following message:

```
Note: object 123 not ready for deviation alerting.
```

When SL1 contains at least two weeks worth of values for object "o_123", the **Dynamic Application Collections** page will display the following message:

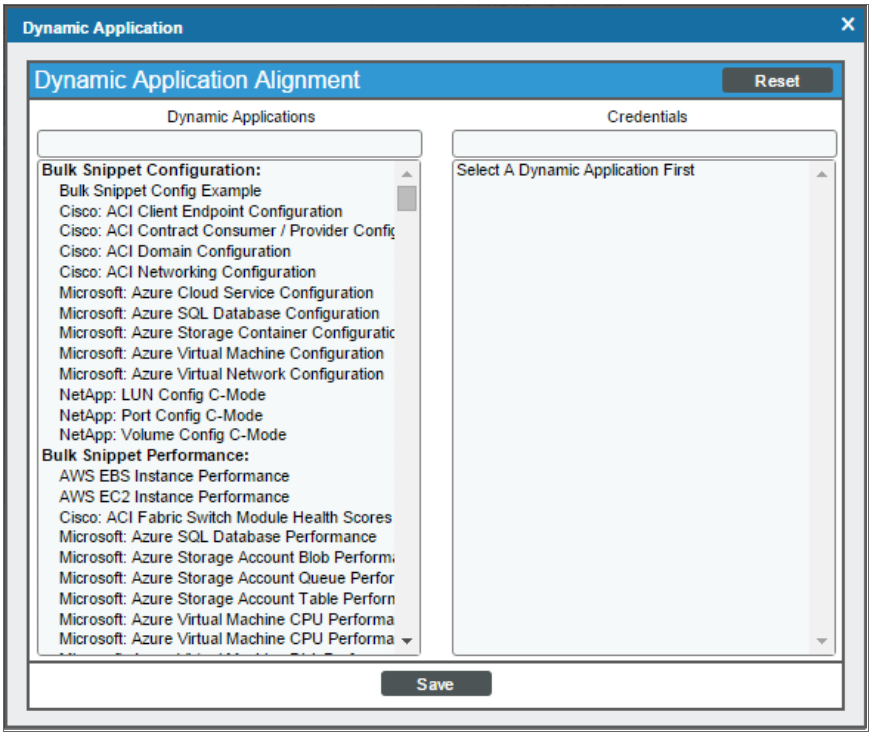
```
All objects ready for deviation alerting.
```

Manually Associating a Dynamic Application with a Device

From the **Dynamic Application Collections** page, you can manually associate a new Dynamic Application with a device.

To manually associate a Dynamic Application with a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device you want to associate with a Dynamic Application. Click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Actions]** menu and select *Add Dynamic Application*.
5. The **Dynamic Application Alignment** modal page appears. To align a Dynamic Application with a device in this page:



- Select the Dynamic Application you want to align with the device in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
- After selecting a Dynamic Application, you must select a credential. Select a credential in the ***Credentials*** field. You can filter the list of credentials using the search field above the ***Credentials*** field.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

NOTE: Cache-consuming Dynamic Applications **do not** require a credential. If you selected a cache-consuming Dynamic Application in the **Dynamic Application Alignment** modal page, the ***Credential*** field displays *N/A* and is grayed out. You do not have to select a credential in the **Dynamic Application Alignment** modal page.

6. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
7. SL1 will associate the Dynamic Application with the device and immediately attempt to collect the data specified in the Dynamic Application using the selected credential.
8. After the first, immediate collection, SL1 will collect the data at the frequency defined in the ***Polling Frequency*** field in the **Application Configuration Editor** page for the Dynamic Application.

Editing the Credential Associated with a Dynamic Application

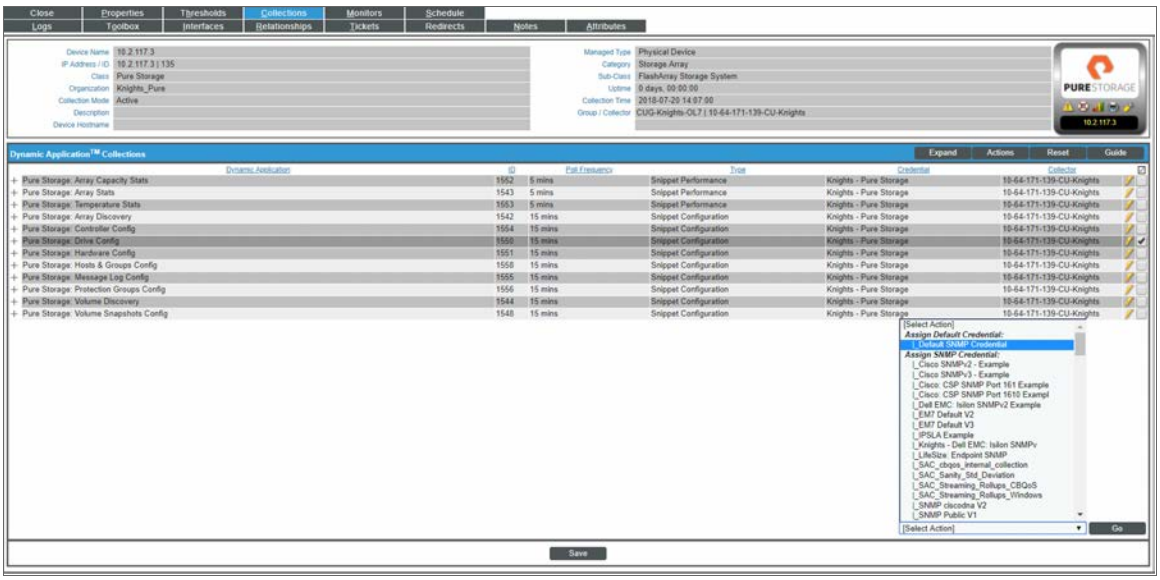
From the **Dynamic Application Collections** page, you can change the credential associated with a Dynamic Application. This credential will be used by SL1 for this specific Dynamic Application associated with this specific device . For all other devices, SL1 will use the default credential associated with the device, or will use the credential defined in the **Dynamic Application Collections** page for each device.

NOTE: Cache-consuming Dynamic Applications do not require a credential. If you aligned a cache-consuming Dynamic Application with this device (you do this in the **Dynamic Application Alignment** modal page), the ***Credential*** field displays *N/A* and is grayed out.

To change the credential associated with a Dynamic Application for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to define a credential. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, find the Dynamic Application for which you want to change the credential. Select its checkbox ( ). To apply a credential to multiple Dynamic Applications, select the checkbox for each Dynamic Application.

5. From the ***Select Action*** drop-down list, select the credential from the list of all credentials that you are allowed to use, and then select the **[Go]** button.



NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Select Action*** drop-down list.

NOTE: If this Dynamic Application has already been aligned with a credential to which you do not have access, the ***Credential*** column will display the value *Restricted Credential*. If you align the device with a different credential, you will not be able to re-align the device with the *Restricted Credential*.

6. You should see your change reflected in the ***Credential*** column in the **Dynamic Application Collections** page.

Performing Other Administrative Tasks for an Aligned Dynamic Application

You can perform the following other administrative tasks for an aligned Dynamic Application in the **Dynamic Application Collections** page:

- Enable or disable one or more collection objects or presentation objects.
- Stop data collection for the whole Dynamic Application.
- Reset the statistical data that has been stored for standard deviation alerting.
- Reset persistent session objects that have been collected and stored for a Dynamic Application.

- Test collection for a Dynamic Application.
- Remove all data collected using the Dynamic Application and optionally unalign the Dynamic Application from the device.

To perform one of these tasks:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to perform an administrative task. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, find the Dynamic Application for which you want to perform an administrative task. The following sections describe how to perform each task.

Enabling or Disabling Objects

From the **Dynamic Application Collections** page, you can customize the collection performed by the Dynamic Application for the current device. This customization will be used by SL1 only for this specific device. For all other devices, SL1 will use the default list of objects from the Dynamic Application's definition or will use the list of objects defined in the **Dynamic Application Collections** page for that device.

NOTE: If a collection object has a ***Collect*** value of *No*, all presentation objects that use that collection object will also have a ***Collect*** value of *No*.

To enable or disable collection for one or more objects in a Dynamic Application:

- ***To disable collection for one or more collection objects***, unselect the checkbox for each object for which you want to disable collection.
- For each unselected object, the ***Collect*** column should now display *No*.
- ***To enable collection for one or more collection objects***, select the checkbox for each object for which you want to enable collection.
- For each selected object, the ***Collect*** column should now display *Yes*.
- Select the **[Save]** button.

NOTE: If a user **manually** sets the ***Collect*** status of a collection object or presentation object to *No*, SL1 will **not** attempt to re-collect the object once a day and will **not** automatically set the ***Collect*** status to *Yes*.

Restarting Automatic Maintenance of Collection Objects

If a user **manually** sets the ***Collect*** status of a collection object or presentation object, SL1 will **not** automatically change the ***Collect*** status of that object as described in the *How the ScienceLogic Platform Manages Collect Status* section.

If you want SL1 to restart automatic maintenance of the objects in a Dynamic Application, perform the following steps:

1. In the **Dynamic Application Collections** page, select the checkbox (☑) for the Dynamic Application for which you want to restart automatic collection maintenance. To restart automatic collection maintenance for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the ***Select Action*** drop-down list, select *Restore System Control of Collection State* and then select the **[Go]** button.
3. Automatic collection maintenance for all objects in the Dynamic Application will now occur. The ***Collect*** status of the objects in the Dynamic Application will not change immediately.

Editing the Poll Frequency for a Dynamic Application on the Current Device

Poll Frequency is the frequency at which SL1 will query the device to retrieve the data specified in the Dynamic Application. Each Dynamic Application includes a default frequency.

From the **Dynamic Application Collections** page, you can change the poll frequency for a Dynamic Application on the current device. For the current device, the edited poll frequency will override:

- the default frequency for the Dynamic Application.
- the poll frequency defined for a Dynamic Application in one or more device templates.

To edit the poll frequency for a Dynamic Application on the current device:

1. In the **Dynamic Application Collections** page, select the checkbox (☑) for the Dynamic Application for which you want to change the poll frequency. To change the poll frequency for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the ***Select Action*** drop-down list, select *Poll Frequency* from the list of poll frequencies and then select the **[Go]** button.
3. You should see your change reflected in the ***Poll Frequency*** column in the **Dynamic Application Collections** page.

Stopping Data Collection for a Dynamic Application

You can stop data collection for a Dynamic Application on the current device. This will affect collection only for this specific device. For all other subscriber devices, SL1 will continue to use this Dynamic Application to collect data.

To stop data collection for a Dynamic Application on this device:

1. Select the checkbox (☑) of each Dynamic Application for which you want to stop data collection.
2. From the ***Select Action*** drop-down list, select the following:

    - ***Disable All Collection Objects***. For all collection objects in the selected Dynamic Application(s), the ***Collect*** value will be set to *No*.

3. Select the **[Go]** button.

> **NOTE**: If a user manually sets the ***Collect*** status of a collection object or presentation object to *No*, SL1 will not attempt to re-collect the object once a day and will not set the ***Collect*** status to *Yes*.

Resetting Statistical Data for a Dynamic Application

SL1 allows you to examine the value of an object and trigger an alert if that value falls outside the range of "normal" values for that object at that hour of the day on that day of the week. The deviation function allows you to define such alerts.

To use the deviation function, you must configure SL1 to store and calculate the mean values and standard deviation for an object. You do this by selecting the ***Enable Deviation Alerting*** field in the **Collection Objects** page. You then specify the minimum and maximum number of weeks to collect deviation data for the object. SL1 must have already collected at least the minimum number of weeks' worth of values for an object before SL1 will evaluate alert formulas that use the deviation function. To use the deviation function, you must specify a minimum value of at least two weeks.

In some cases, you might want to delete all the collected statistics for an object and start over. This is useful if known circumstances change the value of an object, and you no longer want to use the old data to calculate the "normal" ranges. You can do this by "resetting" the statistical data for an object.

For example, suppose you were monitoring bandwidth usage with a standard deviation alert. Suppose your company previously ran on a 09:00 to 17:00 work schedule. Suppose your company has recently added a nightshift to the schedule. In this circumstance, you might want to reset the statistical data to determine the new "normal" usage patterns.

When you reset the statistical data for an object, you are telling SL1 to ignore all previously collected values and to use only values from today onward. When you reset the statistical data for an object, the **Dynamic Application Collections** page will again display a message like:

```
Note: object 123 not ready for deviation alerting.
```

until enough data has been collected to again calculate standard deviation for the object. SL1 will again start collecting the minimum number of weeks of data for the object (as specified in the ***Enable Deviation Alerting*** field in the **Collection Objects** page) and calculating the "normal" ranges for those objects for each hour at each day of the week.

To delete all current statistical data for an object:

1. In the Dynamic Application, find the object for which you want to reset data.
2. In that Dynamic Application, find the object for which you want to reset data. Select its checkbox ( ).

3. From the ***Select Action*** drop-down list, select the following option:

    - *Reset Statistical Data*. Removes all previously collected statistical data for the selected object. SL1 will again start collecting the minimum number of weeks of data for the object (as specified in the ***Enable Deviation Alerting*** field in the **Collection Objects** page) and calculating the "normal" ranges for those objects for each hour at each day of the week.

4. Select the **[Go]** button.
5. The **Dynamic Application Collections** page will display a message like:

```
Note: object 123 not ready for deviation alerting.
```

Resetting Persistent Session Objects for a Dynamic Application

SOAP or XSLT Dynamic Applications can contain a collection object that stores a Session ID. The value for this collection object can be defined as a persistent value. If SL1 has already retrieved and stored a value in the collection object for the Session ID, SL1 will not collect a new value for the collection object until a SOAP fault occurs. You can force SL1 to re-collect a Session ID collection object by deleting the current persistent value.

To delete the current persistent value for a session object:

1. In the Dynamic Application, find the object for which you want to reset data. Select its checkbox (☑).
2. From the ***Select Action*** drop-down list, select the following option:

    - ***Reset Persistent Session Objects***. Removes the stored value for collection objects of type ***SOAP/XSLT Session ID***. ***SOAP/XSLT Session ID*** objects are persistent across collection periods; SL1 does not collect a ***SOAP/XSLT Session ID*** object if a collected value is available from a previous poll. After selecting this option, SL1 will delete the existing value for the object and collect a new value during the next collection.

3. Select the **[Go]** button.

Testing Data Collection for a Dynamic Application

On a single device, you can perform a test-run of collection with a single Dynamic Application. During this test run, SL1 displays details of each step of the collection process. This information can be very helpful for troubleshooting and debugging.

> **NOTE:** During a test run of a collection with a Dynamic Application, SL1 does not store the collected data or generate alerts. SL1 will continue to collect data and generate alerts using the selected Dynamic Application at the frequency defined in the Dynamic Application.

To execute a test run of collection with a single Dynamic Application:

1. Find the Dynamic Application for which you want to test collection and click its lightning bolt icon ( ).

NOTE: If a device is currently unavailable, the lightning bolt icon ( ) will be grayed out for each Dynamic Application aligned with the device.

2. SL1 displays a **Session Logs** modal page that includes details about each step of the collection process and diagnostic details about alerts in the Dynamic Application. This information can be helpful during troubleshooting.

Removing Data Collected by a Dynamic Application

You can remove the data retrieved with a Dynamic Application from the current device. You have two options for removing Dynamic Application data associated with a device:

- Remove all previously collected data, but continue to collect data at the specified polling frequency.
- Remove all normalized data, but retain all raw collected data and continue to collect data at the specified polling frequency.
- Remove all previously collected data and stop collecting data with this Dynamic Application. This unaligns the device from the Dynamic Application. The device will no longer be a subscriber to the Dynamic Application.

To remove Dynamic Application data associated with a device:

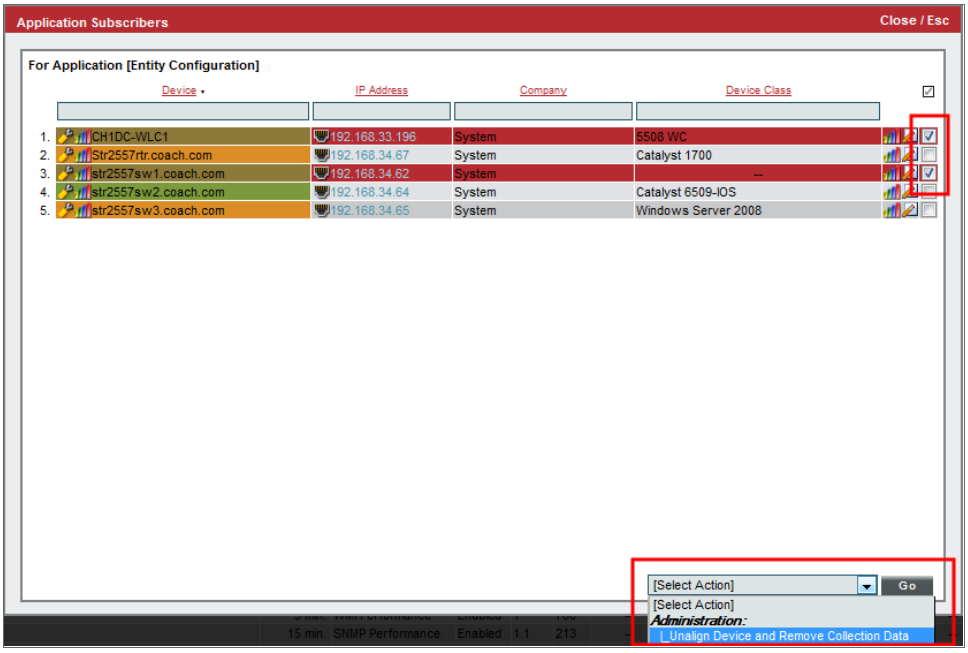
1. In the **Dynamic Application Collections** page, select the checkbox (☑) of the Dynamic Application for which you want to remove data. To remove data for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the ***Select Action*** drop-down list, select one of the following options:
    - ***Remove Data***. Removes all previously collected data, but data will continue to collect at the specified polling frequency.
    - ***Remove Normalized Data***. Removes all normalized data, but all raw collected data is retained and data will continue to collect at the specified polling frequency.
    - ***Stop Collection and Remove Data***. Removes all previously collected data and stops collection of data with this Dynamic Application. This "unaligns" the device from the Dynamic Application. The device is no longer considered a subscriber to the Dynamic Application. If you perform this option and later want to subscribe to this Dynamic Application again, you must re-align the device with the Dynamic Application.
3. Select the **[Go]** button.

Bulk Un-Aligning Dynamic Applications

The **Application Subscribers** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to un-align a Dynamic Application from one or more subscriber-devices.

To un-align a Dynamic Application from one or more devices:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. In the **Dynamic Applications Manager** page, find an application with a subscriber icon ( ) in the ***Subscribers*** column. Select the icon.
3. The **Application Subscribers** page appears.



4. In the **Application Subscribers** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the red checkbox ( ) at the top of the page.
5. In the ***Select Action*** drop-down list, select one of the following actions.
   - ***Unalign Device and Remove Collection Data***. This option unaligns the device from the Dynamic Application and deletes all data collected by the Dynamic Application from the device. The device is no longer considered a subscriber to the Dynamic Application. If you perform this option and later want to subscribe to this Dynamic Application again, you must re-align the device with the Dynamic Application.
6. Select the **[Go]** button to apply the action to all selected devices.

Setting Thresholds for Dynamic Applications

If a Dynamic Application includes one or more ***thresholds***, you can change the threshold value on a per-device basis. To change a Dynamic Application threshold for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to define a threshold. Select its wrench icon

( ).

3. In the **Device Administration** panel, select the **[Thresholds]** tab.

4. The **Device Thresholds** page displays a list of thresholds defined for each Dynamic Application that is aligned to the device. To change a threshold, move the slider for that threshold or enter a value in the number field for that threshold:

5. After changing one or more thresholds, select the **[Save]** button to save your changes.

NOTE: Changing a threshold in the **Device Thresholds** page affects only the current device. The threshold values defined in the Dynamic Application remain unchanged.

Dynamic Applications and Discovery

Discovery is the ScienceLogic tool that automatically discovers devices in your network. You supply the discovery tool with a range or list of IP addresses, and the discovery tool determines if a device exists at each IP address. The discovery tool also determines which (if any) Dynamic Applications to align with the device. If the discovery tool finds Dynamic Applications to align with the device, the discovery tool triggers collection for each aligned Dynamic Application.

To learn more about discovery, see the ***Discovery and Credentials*** manual.

How Does SL1 Align Dynamic Applications During Discovery?

Most Dynamic Applications include a discovery object. A discovery object enables SL1 to determine which devices to align with a Dynamic Application.

During discovery, SL1:

1. Searches the list of Dynamic Applications.
2. If a Dynamic Application includes a discovery object, SL1 adds that Dynamic Application to the list of Dynamic Applications to try to align during discovery.
3. For each Dynamic Application that includes a discovery object, SL1 checks the current discovery session for an appropriate credential. For example, for each database Dynamic Application, SL1 would look for one or more database credentials that have been selected for the discovery session.
4. For each discovered device, both those that support SNMP and those that don't, discovery tries to determine which Dynamic Applications to align. For each discovered device, SL1 tries to align each Dynamic Application in the list of Dynamic Applications to try during discovery. For each Dynamic Application in the list, SL1 tries to connect to each device with each of the appropriate credentials (until SL1 finds a working credential) and then tries to find the discovery object. If SL1 is able to connect to a device with one of the credentials and can then retrieve the discovery object, SL1 will align the Dynamic Application with the device.

NOTE: SL1 also includes more sophisticated logic that allows you to define multiple discovery objects, validate the value of the discovery object, and to align the Dynamic Application if a discovery object is not available. However, the most common use of a discovery object is as described above (discovery object exists).

5. If discovery aligns a Dynamic Application with a device, immediately after discovery completes SL1 will start the first collection from that device using the aligned Dynamic Application. This step is not performed for Dynamic Applications that meet all of the following three criteria:
    - Has a collection frequency of 1 minute, 2 minutes, 3 minutes or 5 minutes.
    - Does not have component mapping enabled (does not discover component devices).
    - Is aligned with a component device.

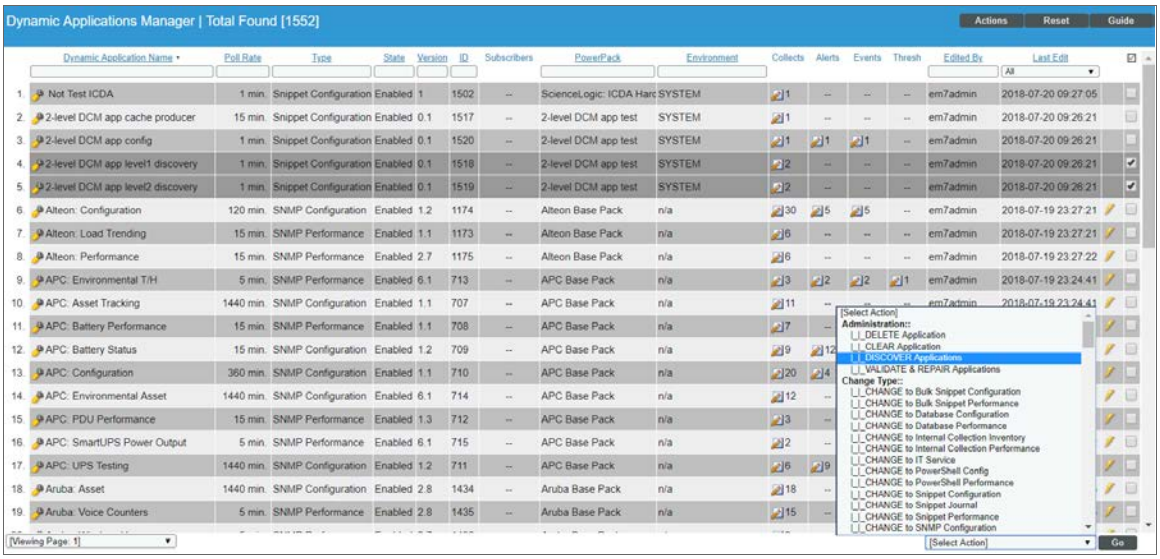
NOTE: During discovery, SL1 tries each SNMP credential specified in the discovery session on each discovered device, to determine if SL1 can collect SNMP details from the device. Later in the discovery session, during alignment of Dynamic Applications, discovery again tries each SNMP credential specified in the discovery session. If one of the SNMP credentials times out three times ***without any response***, discovery will stop trying to use that SNMP credential to align SNMP Dynamic Applications. Note that "no response" means that a device did not respond at all. Note that if a device reports that "no OID was found" or "the end of the OID tree was reached", these are considered a legitimate response and would not cause SL1 to abandon the credential.

Queuing Discovery from the Dynamic Applications Manager Page

From the **Dynamic Applications Manager** page, you can manually run the Dynamic Application alignment portion of discovery for all devices in the system using one or more selected Dynamic Applications.

To manually queue discovery from the **Dynamic Applications Manager** page:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. In the **Dynamic Applications Manager** page, select the checkbox for each Dynamic Application you want to use for discovery.
3. In the ***Select Action*** drop-down list, select *Discover Applications*. Select the **[Go]** button.



4. You can also run the Dynamic Application alignment portion of discovery for all devices in the system using a single Dynamic Application. To do this, select the lightning bolt icon ( ) for that Dynamic Application.

Chapter 10

Device Thresholds and Data Retention

Overview

SL1 allows users to define performance thresholds for devices. When these thresholds are exceeded, SL1 generates an ***event***. Events are messages that are triggered when a specific condition is met. For example, an event can signal that a CPU is at maximum capacity or that a device's hard drives are getting too full.

These events have messages like:

- CPU usage exceeded threshold
- Physical Memory usage exceeded threshold
- Virtual Memory usage exceeded threshold
- File system usage exceeded (critical) threshold
- File system usage exceeded (major) threshold
- Bandwidth usage exceeded threshold

These events notify users when hardware is starting to reach its limits. This allows users to fix the problem before a catastrophic hardware or software failure occurs.

Users can define hardware thresholds in two ways:

1. Users can define global hardware thresholds in the **Global Threshold Settings** page (System > Settings > Thresholds), in the **Operating System Thresholds** pane. These global thresholds apply to all hardware discovered by SL1.
2. For a single device, users can override the global hardware thresholds in the **Global Threshold Settings** page (System > Settings > Thresholds). Users can do this in the **Device Thresholds** page.

This chapter describes how to define both types of hardware thresholds.

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

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

This chapter includes the following topics:

Global Settings for Thresholds *245*
Device Thresholds *250*

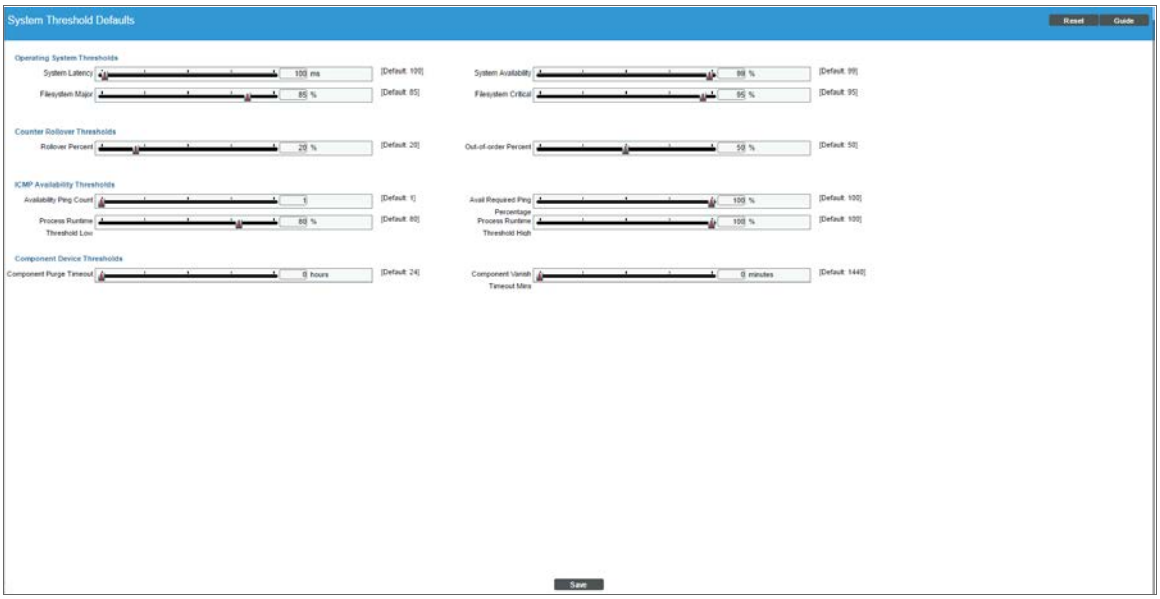
Global Settings for Thresholds

The **System Threshold Defaults** page (System > Settings > Thresholds > System) allows you to define global thresholds for system latency, file system usage, counter rollovers, ICMP availability, and number of component devices.

These settings apply to all devices. However, you can override these system settings on a case-by-case basis. For example, you can define thresholds for a device's file systems in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds). The settings you define for the specific device override the settings in the **System Threshold Defaults** page.

To edit the global settings for system thresholds:

1. Go to the **System Threshold Defaults** page (System > Settings > Thresholds > System).



2. In the **System Threshold Defaults** page, you can drag sliders to change to value of each field or edit a field manually. You can edit the value for one or more of the following fields:

- ***Interface Inventory Timeout***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
    - During *initial discovery*, initiated from the Discovery Session Editor page (System > Manage > Classic Discovery > Create), SL1 uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.
    - During *re-discovery* (clicking the binocular icon ( ) in the Device Properties page), SL1 will use the value in this field if there no value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for the device.
    - During *nightly auto-discovery* (run automatically by SL1 every night, to update device information), SL1 uses the value in this field if no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for a device.
- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per device. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
    - During *initial discovery*, initiated from the **Discovery Session Editor** page (System > Manage > Classic Discovery > Create), SL1 uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.
    - During *re-discovery* (clicking the binocular icon ( ) in the Device Properties page), SL1 will use the value in this field if there is no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for the device.
    - During *nightly auto-discovery* (run automatically by SL1 every night, to update device information), SL1 uses the value in this field if no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for a device.
- ***System Latency***. During polling, the platform initially pings monitored devices. The value in this field is the maximum number of milliseconds for the device to respond to SL1's ping (round-trip time divided by 2). The default value is 100 ms. When the latency threshold is exceeded, SL1 generates an event for that device.
- ***System Availability***. During polling, SL1 monitors devices for availability. Availability means the device's ability to accept connections and data from the network. The value in this field is the percent availability required of each device. The default value is 99%. When a device falls below this level of availability, SL1 generates an event for that device.

  During polling, a device has two possible availability values:

    - 100%. Device is up and running.
    - 0%. Device is not accepting connections and data from the network.

NOTE: Component devices use a Dynamic Application collection object to measure availability. SL1 polls component devices for availability at the frequency defined in the Dynamic ApplicationFor details, see the chapter on *Monitoring Device Availability and Latency* in the ***Monitoring Device Infrastructure Health*** manual.

NOTE: The ***Ping & Poll Timeout (Msec)*** setting in the **Behavior Settings** page (System > Settings > Behavior) affects how SL1 monitors device availability. This field specifies the number of milliseconds the discovery tool and availability polls will wait for a response after pinging a device. After the specified number of milliseconds have elapsed, the poll will timeout.

- ***File System Major***. Threshold that will trigger a "low disk space" event. The default threshold is 85%. When a device has used more disk space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "major".
- ***File System Critical***. Threshold that will trigger a "low disk space" event. The default threshold is 95%. When a device has used more disk-space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "critical".

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), SL1 does not generate events for that file system.

- ***Rollover Percent***. For any collected data that uses a 32-bit counter, you can specify how SL1 determines that the counter has "rolled over", that is, has reached its maximum value, is reset to zero, and restarts counting. When this happens, the collected values go from the maximum value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
    - Maximum value has been exceeded and counter was reset to zero.
    - Retrieved value was manually reset to zero on the external device.
    - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.

NOTE: For 64-bit counters, when the counter values go from a higher value to a lower value, SL1 assumes that the counter has been manually reset or that the two values were collected out of order. SL1 does not assume that the counter has rolled over.

The ***Rollover Percent*** field allows you to specify a threshold that indicates that a 32-bit counter has reached its maximum value and restarted counting. The default value is 20%. When SL1 records a counter value that is lower than the previously collected value, the platform:

- Calculates the difference between the two counter values (the delta):

  2^{32} - Last Collected Value + Current Collected Value

- Examines the value of the ***Rollover Percent*** threshold. If the delta is less than the specified percentage of the maximum possible value (2^{32}), SL1 concludes that the 32-bit counter rolled over.
- For example, if you specified "25" in this field, SL1 would determine if the delta is less than 25% of the maximum possible value. If the delta is less than 25% of the maximum possible value, SL1 concludes that the 32-bit counter rolled over.
- When SL1 determines a counter has rolled over, SL1 uses the delta value when displaying the data point for this poll period.

NOTE: The ***Rollover Percent*** field applies only to 32-bit counters. If a 64-bit counter value goes from a higher value to a lower value, the change is treated as either a manual reset or an out-of-order collection.

- ***Out-of-order Percent***. For any collected data that uses a counter, you can specify how SL1 determines that data has been collected out of order. When this data is collected out of order, the collected values go from a higher value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
  - Maximum value has been exceeded and counter was reset to zero (for 32-bit counters only).
  - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
  - Retrieved value was manually reset to zero on the external device.

  The ***Out-of-order Percent*** field allows you to specify a threshold that indicates that data has been collected out of order. The default value is 50%. When SL1 records a counter value that is lower than the previously collected value and the platform has determined that the value is not a rollover, SL1:

  - Compares the current value to the last collected value:

    current value / last collected value

  - If the ratio of current value / last collected value is greater than the percent specified in the ***Out-of-order Percent*** field, SL1 concludes that the data was collected out of order.
  - When SL1 determines a data point has been collected out of order, SL1 uses the following value as the current value of the data point:

    last collected value - current collected value

NOTE: If a 32-bit counter value goes from the maximum value to a lower value, and the current collected value does not meet the criteria for a rollover AND the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 32-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

NOTE: If a 64-bit counter value goes from a higher value to a lower value, and the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 64-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

- ***Availability Ping Count***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices> Device Manager > wrench icon) for a device, this field specifies the number of packets that should be sent during each availability check. The default value is "1".
- ***Avail Required Ping Percentage***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices> Device Manager > wrench icon) for a device, this field specifies the percentage of packets that must be returned during an availability check for SL1 to consider the device available. The default value is "100%".
- ***Process Runtime Threshold Low***. Threshold that will trigger a "process time exceeded" event. The default threshold is 80%. When a process has used more than 80% of its allowed ***Run Length***, SL1 will generate a "process time exceeded threshold" event with a status of "minor".
- ***Process Runtime Threshold High***. Threshold that will trigger a "process time exceeded" event. The default threshold is 100%. When a process has used 100% of its allowed ***Run Length***, SL1 will generate a "process time exceeded threshold" event with a status of "major".

NOTE: ***Run Length*** is defined in the **Process Manager** page (System > Settings > Admin Processes).

- ***Component Purge Timeout***. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many hours to wait until purging the component device. When a device is purged, SL1 stops trying to collect data about the component device. The purged device will not appear in reports or views on in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. If you set this value to "0", component devices are never purged. You can override this threshold for a specific device in the **Device Thresholds** page for the device.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

- ***Component Vanish Timeout Mins***. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", SL1 stops trying to collect data about the

component device. The vanished device will not appear in reports or views. The vanished device will appear in the **Vanished Device Manager** page. If you set this value to "0", component devices are never set to "vanished". You can override this threshold for a specific device in the **Device Thresholds** page for the device.

3. Click the **[Save]** button to save changes in this page.

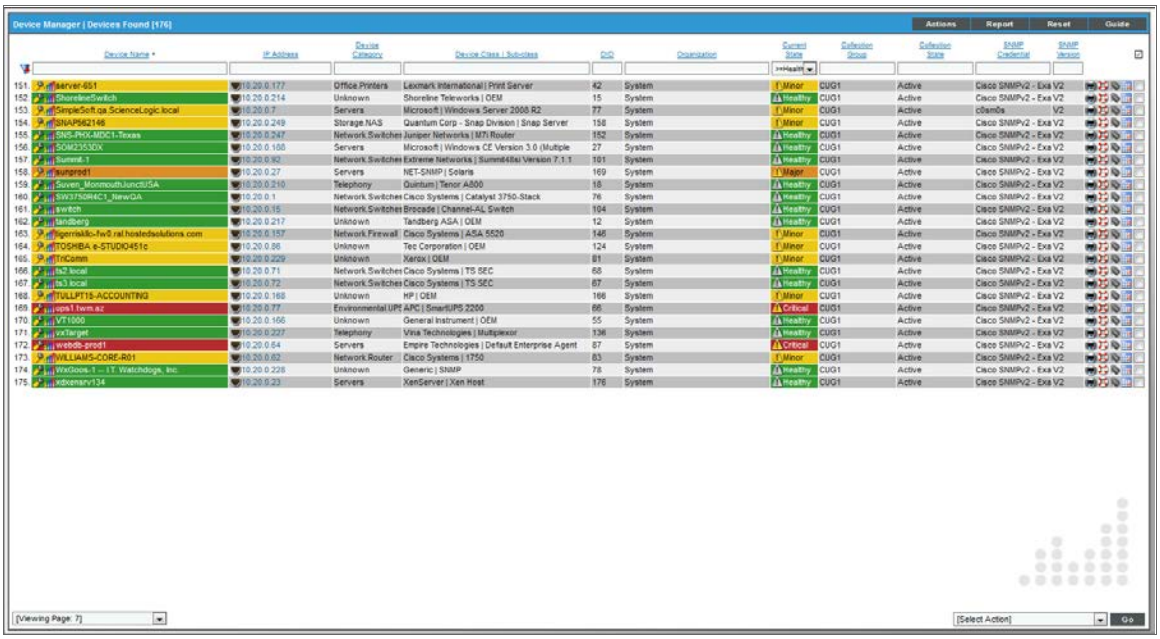
Device Thresholds

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

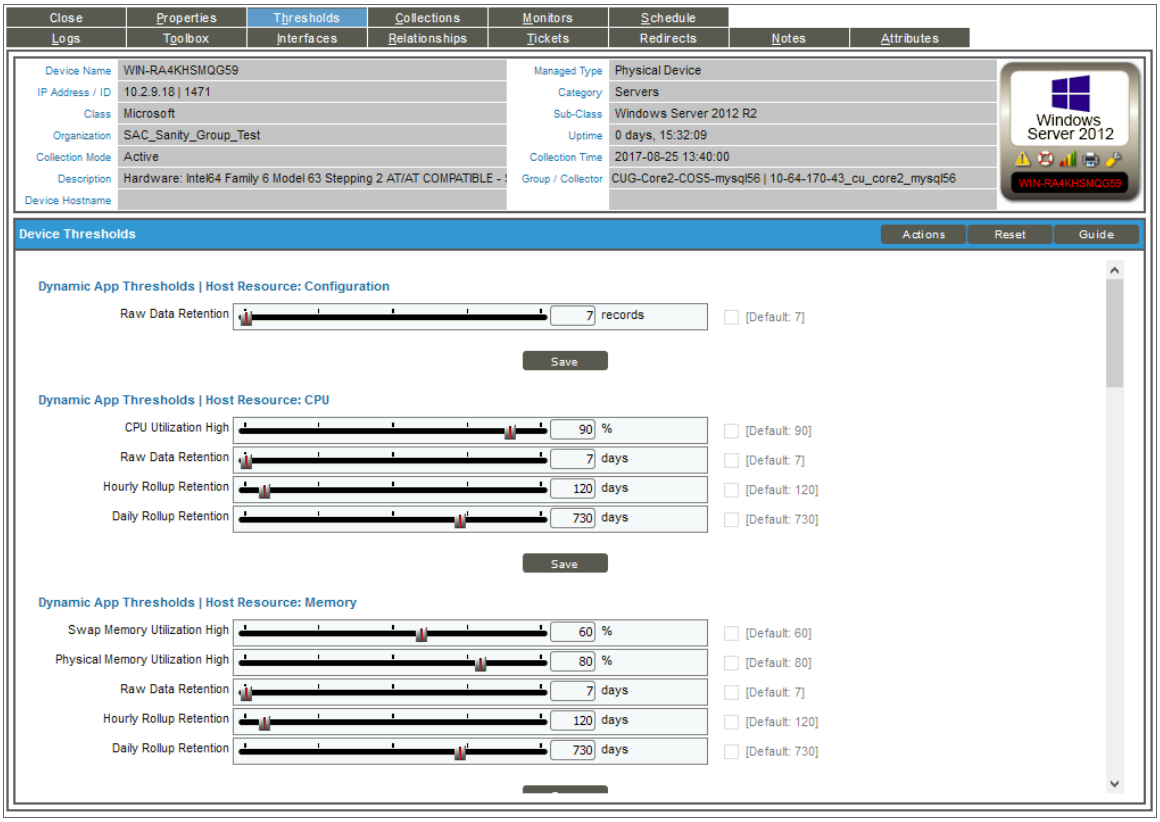
The thresholds defined for the device in the **Device Thresholds** page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds) and the **Data Retention Settings** page (System > Settings > Data Retention).

To define thresholds for a device:

1. Go to the **Device Manager** page Devices > Device Manager).
2. On the **Device Manager** page, find the device for which you want to define thresholds and click its wrench icon ( ).



3. In the **Device Administration** panel, click the **[Thresholds]** tab.



4. In the **Device Thresholds** page, you can define one or more of the following thresholds:

TIP: You might want to retain normalized data for longer periods of time and non-normalized data for shorter periods of time. This allows you to save space and still create historical reports.

- ***Dynamic Application Thresholds***. If the device is a subscriber for one or more Dynamic Applications, this page can include threshold objects from those Dynamic Applications. By default, each threshold object will have the default value as defined in its Dynamic Application. However, in the **Device Thresholds** page you can define a threshold value specifically for the current device. You can define a custom value for each threshold object, and SL1 will use that custom value when evaluating Dynamic Application alerts ***for this device***. The following data retention thresholds always appear for Dynamic Applications of type performance:

NOTE: To return a threshold to the default value as defined in its Dynamic Application, select the ***Restore Default*** checkbox.

  - *Raw Data Retention*. Number of days to retain raw performance data collected from the device using this Dynamic Application. Raw data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page (System > Settings > Data Retention).
  - *Hourly Rollup Performance Data*. Number of days to retain hourly normalized data for this Dynamic Application. Hourly normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page (System > Settings > Data Retention).
  - *Daily Rollup Performance Data*. Number of days to retain daily normalized data for this Dynamic Application. Daily normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page (System > Settings > Data Retention).

- ***Interface Inventory Thresholds***. When a device has a large number of interfaces, these settings prevent SL1 from consuming too many resources during *re-discovery* (clicking the binocular icon ( ) in the Device Properties page) and during *auto-discovery* (run automatically by SL1 every night, to update device information).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Interface Inventory Timeout*. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop scanning the device, will not update the device, and will continue with discovery. This setting is used during *re-discovery* (clicking the binoculars icon ( ) in the Device Properties page) and during *nightly auto-discovery* (run automatically by SL1 every night, to update device information). The default value is 600,000 ms (10 minutes).
  - *Maximum Allowed Interfaces*. Specifies the maximum number of interfaces per device. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not update the device, and will continue with discovery. This setting is used during *re-discovery* (clicking the binoculars icon ( ) in the Device Properties page) and during *nightly auto-discovery* (run automatically by SL1 every night, to update device information). The default value is 10,000.

- ***File System Thresholds***. For each file system on the device that has been detected by SL1, you can define two thresholds:

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Major*. Threshold that will trigger a "low disk space" event. The default threshold is 85%. When a device has used more disk space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "major". ***To disable this threshold for the current device***, set the threshold to 0% (zero percent). When you disable a threshold, SL1 does not generate an event for the threshold.
  - *Critical*. Threshold that will trigger a "low disk-space" event. The default threshold is 95%. When a device has used more disk space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "critical". ***To disable this threshold for the current device***, set the threshold to 0% (zero percent). When you disable a threshold, SL1 does not generate an event for the threshold.

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), SL1 does not monitor the thresholds on the file system and does not generate events for that file system.

- ***Operating System Thresholds***. You can define the following two thresholds for the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *System Latency*. Every five minutes, SL1 polls monitored devices to determine latency. The value in this field is the maximum number of milliseconds for the device to respond to SL1's poll (round-trip time divided by two). The default threshold value is 100ms. When the latency threshold is exceeded, SL1 generates an event ("network latency exceeded threshold") for that device. ***To disable this threshold for the current device***, set the threshold to 0 (zero) milliseconds. When you disable a threshold, SL1 does not generate an event for the threshold.
  - *System Availability*. Every five minutes, SL1 polls devices for availability. The default threshold value is 99%. Availability means the device's ability to accept connections and data from the network. The value in this field is the percent availability required of each device. When a device falls below this level of availability, SL1 generates an event for that device.

    For availability collection, a device has two possible availability values:

    - 100%. Device is up and running.
    - 0%. Device is not accepting connections and data from the network.

    However, you might see values other than 100 or 0 in an availability report. If a report contains any other percentage, it is an average of multiple readings. For example, if SL1 gathered five readings and during one of those readings a device was unavailable, the average would be 80% (100 + 100 + 100 + 100 + 0 = 400; 400/5 = 80).

NOTE: Component Devices use a Dynamic Application collection object to measure availability. SL1 polls component devices for availability at the frequency defined in the Dynamic Application. For details, see the description of the ***Component Identifier*** field in the **Collection Objects** page. For details, see the manual ***Monitoring Device Infrastructure Health***.

- ***Data Retention Thresholds***. These thresholds specify how long SL1 will store data collected from the device. The thresholds defined for the device on this page override the global thresholds defined in the **Data Retention Settings** page (System > Settings > Data Retention).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Device Logs Max*. Maximum number of records to store in the device log. The default value is 50,000 entries. When this number is exceeded, the oldest entries will be removed.

- *Device Logs Age*. Number of days to retain device logs. Log records that are older than the specified number of days are automatically removed. The default value is 90 days.
- *Bandwidth Data*. Number of days to retain bandwidth data and CBQoS data collected from each interface on a device . Bandwidth data that is older than the specified number of days is automatically removed. The default value is 270 days.
- *Daily Rollup Bandwidth Data*. Number of days to retain daily normalized data and daily normalized CBQoS data for each interface on the device. Daily normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Hourly Rollup Bandwidth Data*. Number of days to retain hourly normalized data and hourly normalized CBQoS data for each interface on a device. Hourly normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Raw Performance Data*. Number of days to retain performance data collected from the device. This setting applies to availability statistics, latency statistics, file system statistics, statistics generated by monitoring policies, and Performance Dynamic Applications for which a specific ***Raw Data Retention*** setting has not been defined. Performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Daily Rollup Performance Data*. Number of days to retain daily normalized performance data for the device. This setting applies to daily normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific ***Daily Rollup Retention*** setting has not been defined. Daily normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Hourly Rollup Performance Data*. Number of days to retain hourly normalized performance data for the device. This setting applies to hourly normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific ***Hourly Rollup Retention*** setting has not been defined. Hourly normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Raw Journal Data*. Number of days to retain raw collected data from Dynamic Applications of type "journal". The default value is defined in the **Data Retention Settings** page.
- *Crunched Journal Data*. Number of days to retain data that has been processed using the presentation objects in Dynamic Applications of type "journal". The default value is defined in the **Data Retention Settings** page.
- *Configuration Data*. Number of days to retain data from Dynamic Applications of type "configuration". The default value is defined in the **Data Retention Settings** page.

NOTE: In SL1, normalized data does not include polling sessions that were missed or skipped. So for normalized data, null values are not included when calculating maximum values, minimum values, or average values.

TIP: You might want to retain normalized data for longer periods of time and non-normalized data for shorter periods of time. This allows you to save space and still create historical reports.

- ***Counter Rollover Thresholds***. You can define the following two thresholds for the counters on the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Rollover Percent*. For any collected data that uses a 32-bit counter, you can specify how SL1 determines that the counter has "rolled over", that is, has reached its maximum value, is reset to zero, and restarts counting. When this happens, the collected values go from the maximum value to a lower value. However, there are multiple circumstances under which a 32-bit counter value can go from a higher value to a lower value:

NOTE: For 64-bit counters, when the counter values go from a higher value to a lower value, SL1 assumes that the counter has been manually reset or that the two values were collected out of order. SL1 does not assume that the counter has rolled over.

    - Maximum value has been exceeded and counter was reset to zero.
    - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
    - Retrieved value was manually reset to zero on the external device.

      The ***Rollover Percent*** field allows you to specify a threshold that indicates that a 32-bit counter has reached its maximum value and restarted counting. The default value is 20%. When SL1 records a counter value from a 32-bit counter that is lower than the previously collected value, SL1:

    - calculates the difference between the two counter values (the delta):

      ```
      maximum value (either 2^32) - Last Collected Value + Current
      Collected Value
      ```

    - Examines the value of the ***Rollover Percent*** threshold. If the delta is less than the specified percentage of the maximum possible value (either 2^{32}), SL1 concludes that the counter rolled over.
    - For example, if you specified "25" in this field, SL1 would determine if the delta is less than 25% of the maximum possible value. If the delta is less than 25% of the maximum possible value, SL1 concludes that the counter rolled over.

- When SL1 determines a 32-bit counter has rolled over, SL1 uses the delta value when displaying the data point for this poll period.

- *Out-of-order Percent*. For any collected data that uses a counter, you can specify how SL1 determines that data has been collected out of order. When this data is collected out of order, the collected values go from a higher value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value.
  - Maximum value has been exceeded and counter was reset to zero (for 32-bit counters only).
  - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
  - Retrieved value was manually reset to zero on the external device.

  The ***Out-of-order Percent*** field allows you to specify a threshold that indicates that data has been collected out of order. The default value is 50%. When SL1 records a counter value that is lower than the previously collected value and SL1 has determined that the value is not a rollover, SL1:

  - compares the current value to the last collected value:

    ```
    current value / last collected value
    ```

  - If the ratio of current value / last collected value is greater than the percent specified in the ***Out-of-order Percent*** field, SL1 concludes that the data was collected out of order.
  - When SL1 determines a data point has been collected out of order, SL1 uses the following value as the current value of the data point:

    ```
    last collected value - current collected value
    ```

NOTE: If a 32-bit counter value goes from the maximum value to a lower value, and the current collected value does not meet the criteria for a rollover AND the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 32-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

NOTE: If a 64-bit counter value goes from a higher value to a lower value, and the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 64-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

- ***ICMP Availability Thresholds***. You can define the following availability thresholds for the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Availability Ping Count*. If you selected *ICMP* in the ***Availability Port*** field in the **Device Properties** page, this field specifies the number of packets that should be sent during each availability check. If you selected *ICMP* in the ***Latency Port*** field in the **Device Properties** page, this field specifies the number of packets that should be sent during each latency check. The default value is "1".
  - *Avail Required Ping Percentage*. If you selected *ICMP* in the ***Availability Port*** field in the **Device Properties** page, this field specifies the percentage of packets that must be returned during an availability check for SL1 to consider the device available. The default value is "100%".
  - *Availability Packet Size*. If you selected *ICMP* in the ***Availability Port*** field in the **Device Properties** page, this field specifies the size of each packet, in bytes, that is sent during each availability check. If you selected *ICMP* in the ***Latency Port*** field in the **Device Properties** page, this field specifies the size of each packet, in bytes, that is sent during each latency check. The default value is "56 bytes".

- ***Component Device Thresholds***. You can define the following thresholds for component devices. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

NOTE: To return a threshold to the default value as defined in the **Global Threshold Settings** page (System > Settings > Thresholds), select the ***Restore Default*** checkbox.

  - *Component Vanish Timeout Mins*. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", SL1 stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear in the **Vanished Device Manager** page. If you set this value to "0", the component device is never set to "vanished". For the current device, this setting overrides the ***Component Vanish Timeout*** in the **Global Threshold Settings** page.
  - *Component Purge Timeout*. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many hours to wait until purging the component device. When a device is purged, SL1 stops trying to collect data from the component device. The purged device will not appear in reports or views on in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. If you set this value to "0", the component device is never purged. For the current device, this setting overrides the ***Component Purge Timeout*** in the **Global Threshold Settings** page.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

5. Click the **[Save]** button to save your changes.

Chapter 11

Bulk Management with Device Groups and Device Templates

Overview

This chapter provides an overview of the device groups and device template features. For more information on how to use and manage device groups and device templates, see the ***Device Groups & Device Templates*** manual.

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

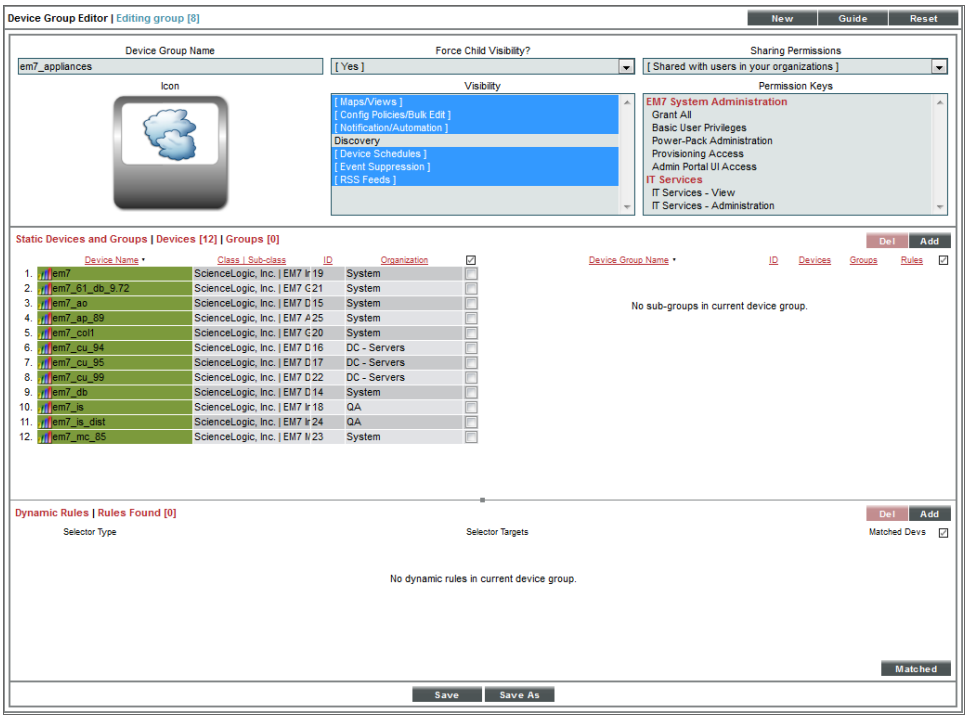
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

What is a Device Group? *260*
What is a Device Template? *262*

What is a Device Group?

A ***device group*** is a group of multiple devices.



Device groups allow you to:

- Use device configuration templates to perform initial configuration for multiple devices simultaneously.
- Use device configuration templates to make changes to the configuration for multiple devices simultaneously.
- InDevices > Device Groups, view each device group and the sub-groups and devices within each device group.
- Schedule maintenance and downtime for multiple devices simultaneously.
- Suppress events on multiple devices simultaneously.
- Include the device group in an automation policy. An automation policy allows you to trigger an automatic action if specified criteria are met on all the devices in the device group.

A device can belong to multiple device groups. For example, suppose SL1 discovered a server. Suppose this server hosts a corporate website that you want to monitor with a web-content policy. Suppose this server also hosts a MySQL database that you want to monitor with a Dynamic Application for MySQL. You could make this server a member of two device groups, one device group for web servers and another device group for MySQL databases. You could then use a device configuration template to apply a web-content policy to all devices in the device group for web servers and another device configuration template to apply a Dynamic Application for MySQL to all devices in the device group for MySQL servers.

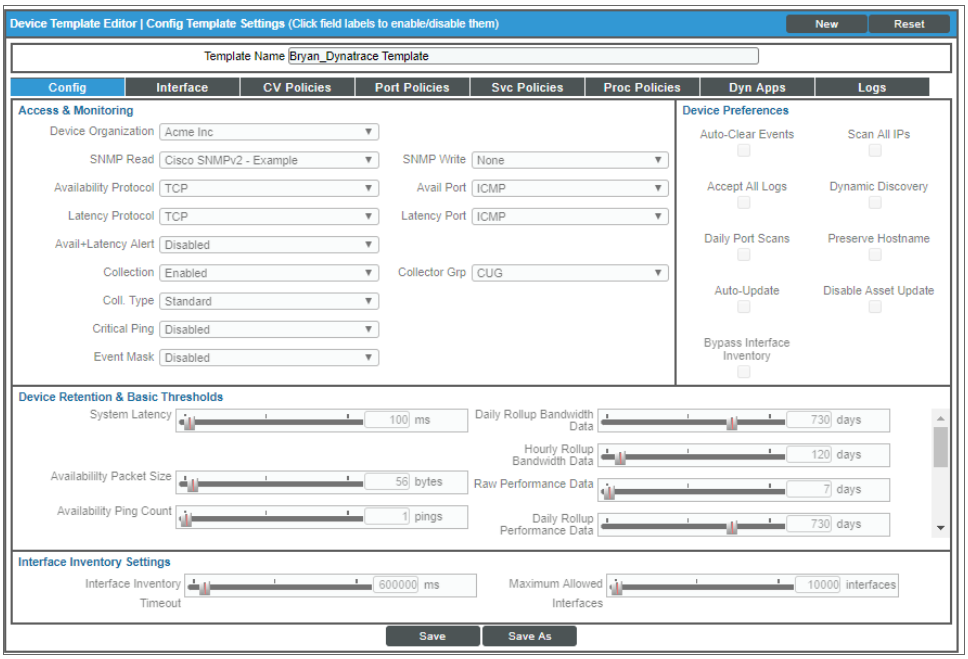
You can add devices to a device group either explicitly or dynamically.

- You can create ***static device groups***, where you explicitly assign one or more devices to a device group.
- You can create ***dynamic device groups***, where you define ***rules*** for the device group. Each device that meets the criteria in the rule is automatically included in the device group. For example, suppose that you define a rule that specifies "include all devices in the *System* organization, with an IP address that starts with '10.100.100' ". SL1 would automatically assign all devices from the *System* organization with an IP of "10.100.100.*" to the new device group. When a new device is added to the *System* organization with an IP that begins with "10.100.100.*", that device will also be included in the device group. If a device with an IP that starts with "10.100.100.*" is removed from the *System* organization, that device will also be removed from the device group.
- You can create a device group that includes both explicitly assigned devices and also includes a dynamic rule. This device group will include both the explicitly assigned devices and all devices that meet the criteria in the dynamic rule.

The IT Services feature in SL1 uses device groups to define an IT Service. An IT Service contains sets of rules that define the state of that IT Service based on the state of the devices within the device group. For example, if you created an IT Service that represents the state of your Email service, the associated device group might contain your DNS Servers, Exchange Servers, and Virtual Devices that are associated with Email Round-Trip Policies. To learn more about IT Services, see the ***IT Services*** manual.

What is a Device Template?

Device templates allow you to save a device configuration, apply it to one or more devices, and re-use the same configuration over and over again.



A device template contains the following tabs and settings:

- **[Config]** tab. Contains all the fields in the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Device Properties** page or the **Device Thresholds** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.
- **[Interface]** tab. Contains all the fields in the **Interface Properties** page that define how SL1 will monitor one or more network interfaces and the thresholds for those network interfaces. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Interface Properties** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.
- **[CV Policies]** tab. Specifies one or more web-content policies that can be applied to all devices that use the template. These web-content policies enable SL1 to monitor a website. SL1 will periodically check the website for specified content. If the content cannot be found on the website, SL1 will generate an event. When you apply a device template to a device, you do not have to manually define any web-content and availability policies in the **Monitoring Policies** page for the devices. All the devices that use the template will inherit the web-content policies from the device template; SL1 will automatically create these web-content policies for each device that uses the template.
- **[Port Policies]** tab. Specifies one or more TCP/IP Port policies that can be applied to all member devices. These TCP/IP Port policies tell SL1 to monitor a specified port for availability every five minutes. Availability refers to the port's ability to accept connections and data. When you apply a device template to a device group, you do not have to manually define any TCP/IP port policies in the **Monitoring Policies** page for the member devices. All the devices in the device group will inherit the TCP/IP port policies from the device template; SL1 will automatically create these port policies for each device that uses the template.
- **[Svc Policies]** tab. Specifies one or more Windows service policies that can be applied to devices that use the template. These Windows services policies tell SL1 to monitor the device and look for the specified service. You can define a service policy so that SL1 monitors whether or not the service is running and then performs an action (starts, pauses, or restarts the service, reboots or shuts down the device, triggers the execution of a remote script or program). When you apply a device template to devices, you do not have to manually define any Windows service policies in the **Monitoring Policies** page for those devices. All the devices that use the template will inherit the Windows service policies from the device template; SL1 will automatically create these Windows service policies for each device that uses the template.

NOTE: In addition to using a Windows Service policy, SL1 includes a PowerPack called "Windows Restart Automatic Services". This PowerPack includes a Dynamic Application that monitors Windows Services with a mode of "Automatic". This PowerPack also includes two events and a Run Book policy. If the Dynamic Application reports that a Windows Service with a mode of "Automatic" has stopped running, SL1 generates an event and the Run Book policy automatically restarts the Windows Service.

- **[Proc Policies]** tab. Specifies one or more Process policies that can be applied to devices that use the template. These Process policies tell SL1 to monitor the device and look for the process. You can define a process policy so that SL1 monitors whether or not the process is running and optionally, how much memory a process can use and how many instances of a process can run simultaneously. When you apply a device template to devices, you do not have to manually define any Process policies in the **Monitoring Policies** page for those devices. All the devices that use the device template will inherit the Process policies from the device template; SL1 will automatically create these process policies for each device that uses the template.

- **[Dynamic Apps]** tab. Specifies or more Dynamic Applications that can be aligned with devices that use the template. SL1 will use the specified Dynamic Applications to retrieve data from the devices that use the template. (Note that each device that uses the template might also be aligned with additional Dynamic Applications that have been aligned with the device in other ways: for example, from the automatic alignment that occurs during discovery.) When you apply a device template to devices, you do not manually have to align Dynamic Applications in the **Dynamic Application Collections** page for those devices. All devices that use the device template will be aligned with the Dynamic Applications specified in the device template.

    - If you select a Dynamic Application in a Device Template, and that Dynamic Application has associated thresholds, you can change one or more of those thresholds from the Device Template. The thresholds you specify in the Device Template will override the thresholds defined in the Dynamic Application. When you apply a device template to devices, you do not manually have to edit the Dynamic Application Thresholds in the **Device Thresholds** page for those devices. All devices that use the device template will inherit the Dynamic Application Thresholds specified in the device template.

NOTE: In a configuration template, you are not required to define all the fields in each tab. For example, you can choose to define only one or more fields in only one tab. When you apply the configuration template to devices, only those fields you defined in the template will be applied to the devices. For the remaining fields, the devices will retain their previous values or use the default values.

You can apply device templates to:

- One or more ***device groups***.
- One or more devices, selected from the **Device Manager** page.
- all the devices discovered by a specific discovery session.

You can also apply device templates to automate the initial configuration of multiple devices. If you change a device template, you can use it to automate the editing of the configuration of multiple devices.

Device templates are not dynamic. That is, when you update or change a device template, no changes are made to any devices that have used the template in the past.

You can make temporary changes to a device template, apply the template to a devices, and then exit the device template without saving the temporary changes. In this way, you can apply settings to a device group but not permanently save the settings in the device template.

NOTE: If you make changes to a device template or simply apply the device template a second time, SL1 will not create duplicate policies on the member devices. However, if you edit a device template and make a change to a policy, the policy will be updated on the member devices.

Chapter 12

Virtual Devices

Overview

This chapter describes how to create and use virtual devices in SL1.

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

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

This chapter includes the following topics:

What is a Virtual Device? 265
Defining a Virtual Device 266
Directing Data to a Virtual Device 267
Redirecting Log Data to a Virtual Device 268
Aligning a Dynamic Application with a Virtual Device 270

What is a Virtual Device?

A ***virtual device*** is a container for collected data. A virtual device can be used when you want to:

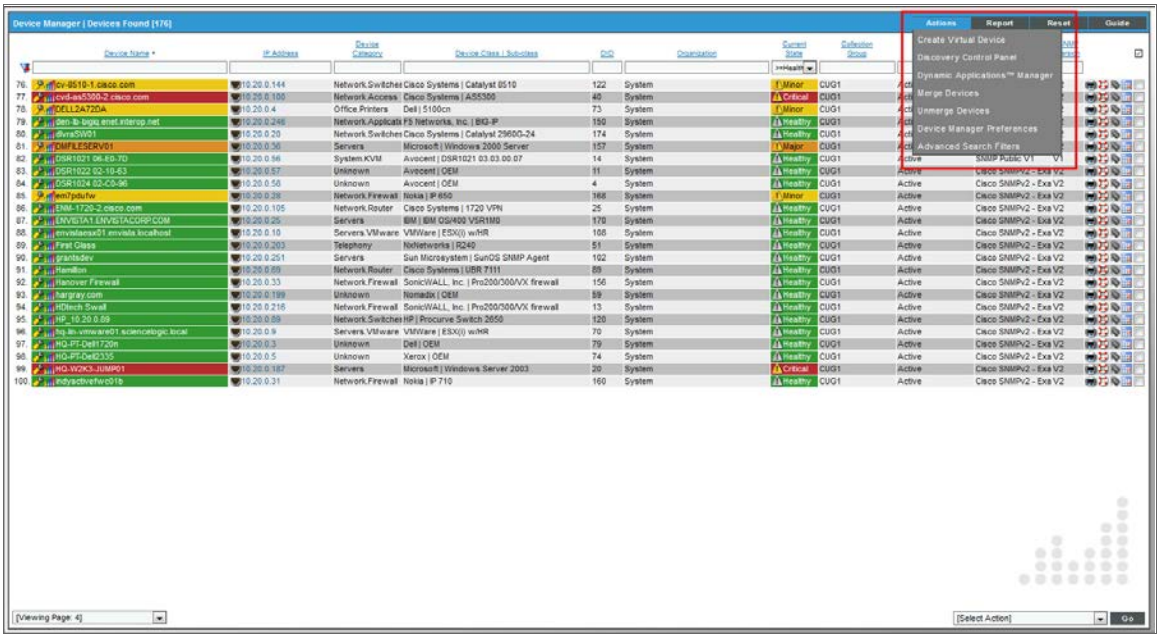
- Monitor a device or application that doesn't support TCP/IP, SNMP, or both. The device's data can be pushed to SL1 via another method (for example, email) and stored in a virtual device.

- Monitor multiple SNMP agents on a single device. In such a case, one of the SNMP agents (for example, a hardware agent) can be associated with the device and another SNMP agent (for example, an agent that monitors a software application) can be associated with a virtual device.
- Isolate and monitor specific parameters separately from their originating device. For example, you might want to monitor a database and keep its data separate from the hardware data you are collecting from the host device.

Defining a Virtual Device

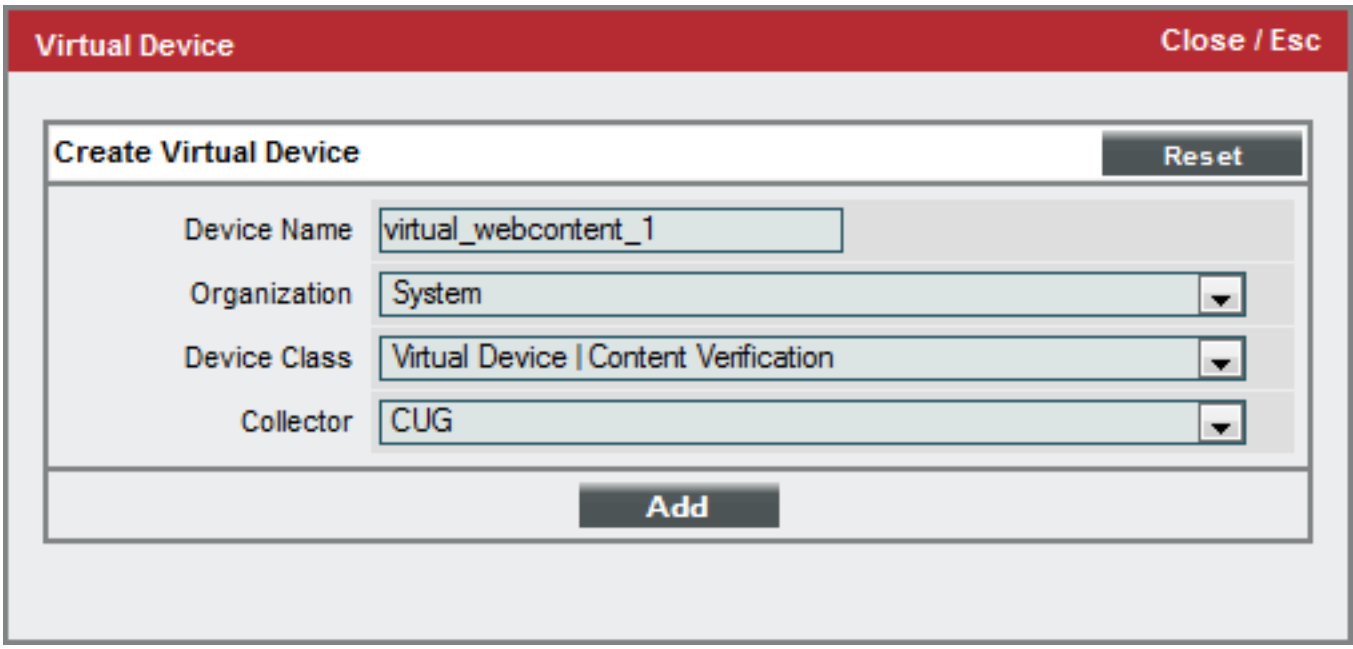
To create a virtual device, you must complete the following tasks:

1. Ensure that SL1 includes a device class for virtual devices. These device classes must have a device category of "virtual" and a collection type of "virtual". If SL1 does not include such a device class, you must ***define one*** in the **Device Class Editor** page (System > Customize > Device Classes).
2. Go to the **Device Manager** page (Devices > Device Manager).



3. From the **[Actions]** menu, select *Create Virtual Device*.

4. The **Create Virtual Device** modal page appears.



5. Supply a value in each of the following fields:

   - ***Device Name***. Name of the virtual device. Can be any combination of alphanumeric characters, up to 32 characters in length.
   - ***Organization***. Organization to associate with the virtual device. Select from the drop-down list of all organizations in SL1.
   - ***Device Class***. The device class to associate with the virtual device. Select from the drop-down list of device classes. Only device classes with a device category of "virtual" and a collection type of "virtual" appear in the list.
   - ***Collector***. Specifies which instance of SL1 will perform auto-discovery and gather data from the device. Can also specify a "virtual" poller. Select from the drop-down list of all collectors in SL1.

6. Select the **[Add]** button to save the new virtual device.
7. You must now define the data to store in the virtual device.

Directing Data to a Virtual Device

After defining a virtual device, you must tell SL1 which data to store in the virtual device.

- For data that is pushed to SL1, go to the **Redirect Policy Editor** page for the virtual device (Devices > Device Manager), find virtual device, select its wrench icon [ ], and then select the **[Redirects]** tab). Define the log data you want to collect and associate with the virtual device.

- For data that is collected via SNMP or TCP/IP, go to the **Dynamic Application Collections** page for the virtual device (Devices > Device Manager), find the virtual device, select its wrench icon [ ], and then select the **[Collections]** tab). Manually associate a Dynamic Application with the device. This ensures that data collected by the Dynamic Application is stored in the virtual device.

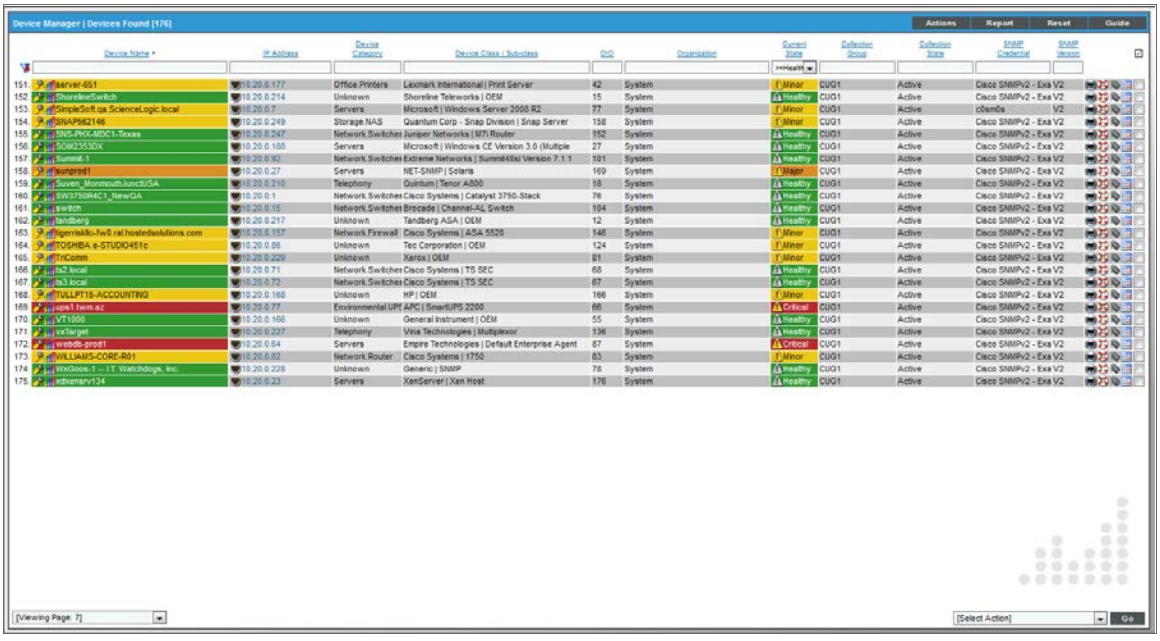
Redirecting Log Data to a Virtual Device

The **Redirect Policy Editor** is most useful for devices that don't support TCP/IP. For these devices, data can be pushed from the device to another device that does support TCP/IP. SL1 can then collect the data from the device that does support TCP/IP. You can create a virtual device in SL1 to represent the device that doesn't support TCP/IP. You can then move the data from the TCP/IP device that is monitored by SL1 to the virtual device in SL1. The **Redirect Policy Editor** page allows you to move data from the TCP/IP device to the virtual device. The **Redirect Policy Editor** page allows you to move log entries generated by inbound SNMP Trap, Syslog, or Email messages from the TCP/IP device to the virtual device.

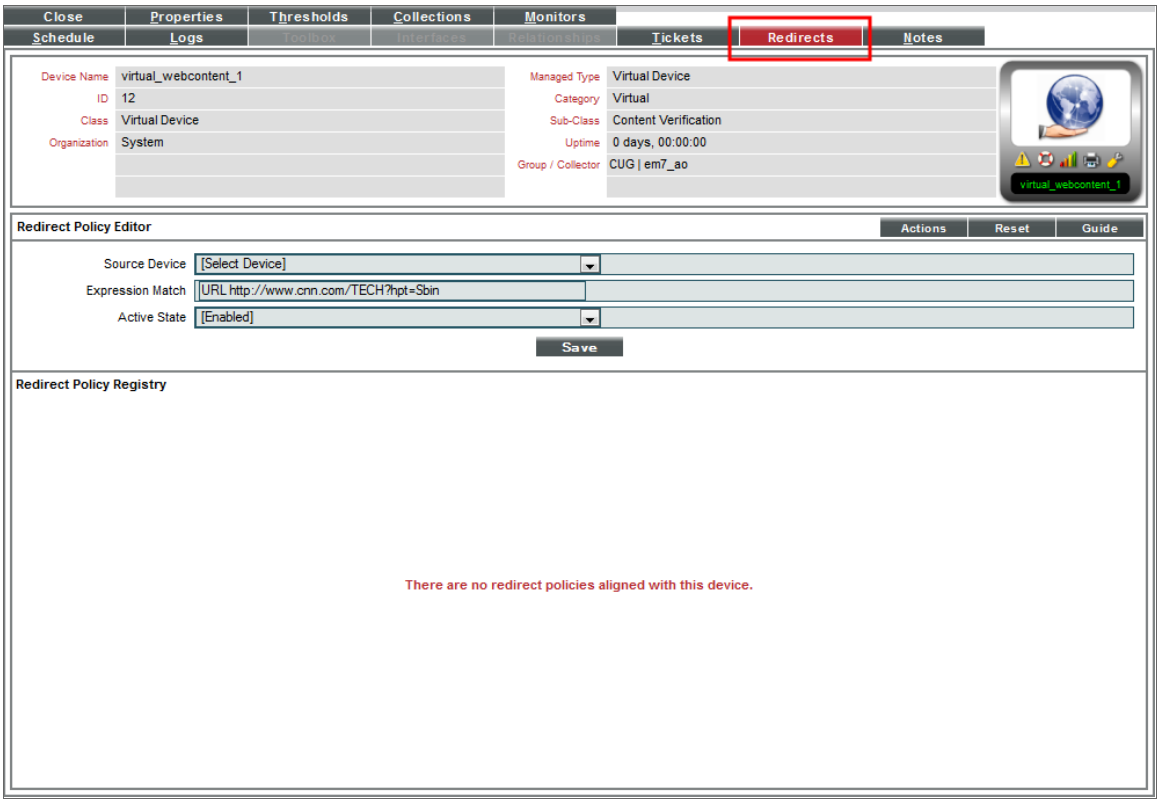
- Log entries that are redirected to a virtual device will no longer appear in the log files for the IP-based device.
- Log entries that are redirected to a virtual device are no longer associated with the IP address of the original device.
- Log entries with a ***Source*** of *Internal*, *Dynamic*, or *API* that match a redirect policy are not moved from the IP-based device to the current device.

To redirect data from a TCP/IP device to a virtual device:

1. Go to the **Device Manager** page Devices > Device Manager).
2. In the **Device Manager** page, find the virtual device to which you want to redirect data. Select its wrench icon ( ).



3. In the **Device Administration** panel, select the **[Redirects]** tab.



4. To move SNMP Trap, Syslog, or Email log messages from an IP-based device to the current device, provide values in each of the following fields:

   - ***Source Device***. This is the TCP/IP device from which you want to redirect log messages. Data from this device will be moved to the virtual device. Select from a drop-down list of all IP-based devices discovered by SL1.
   - ***Expression Match***. A regular expression used to locate the log entry to redirect. Can be any combination of alphanumeric and multi-byte characters, up to 64 characters in length. SL1's expression matching is case-sensitive. For details on the regular-expression syntax allowed by SL1, see http://www.python.org/doc/howto/ .
   - ***Active State***. Specifies whether or not SL1 will execute the redirection policy. The choices are:
     - *Enable*. SL1 will execute the redirection policy.
     - *Disable*. SL1 will not execute the redirection policy.

5. Select the **[Save]** button.
6. You can repeat Step 4 and Step 5 to redirect data to the virtual device from more than one device or from more than one type of log message.

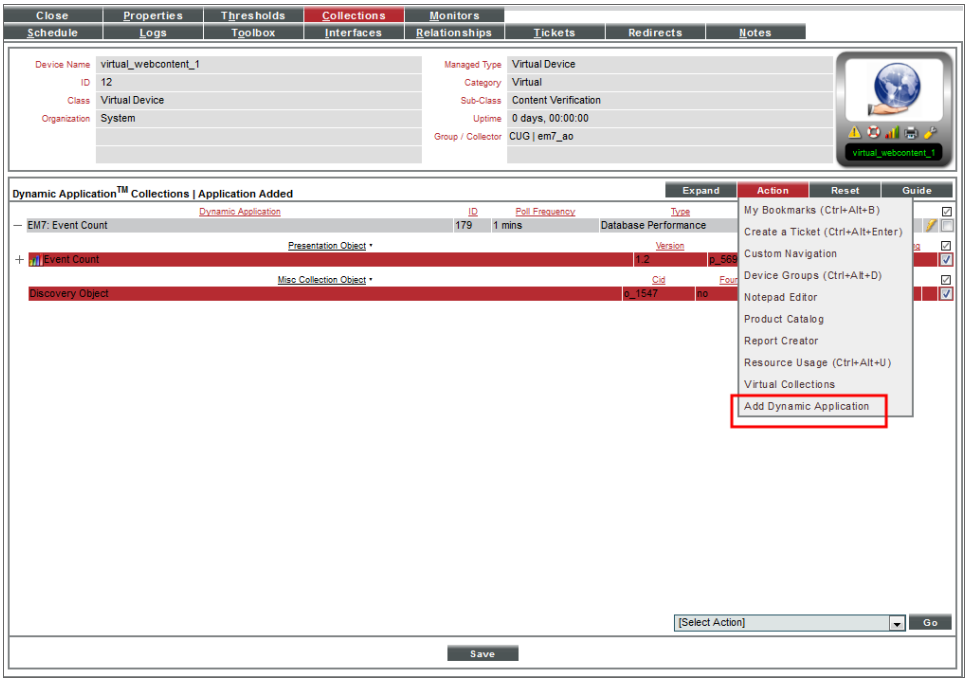
Aligning a Dynamic Application with a Virtual Device

For data that is collected via Dynamic Application, you can associate that data with a virtual device. The data collected by the Dynamic Application will be stored in the virtual device.

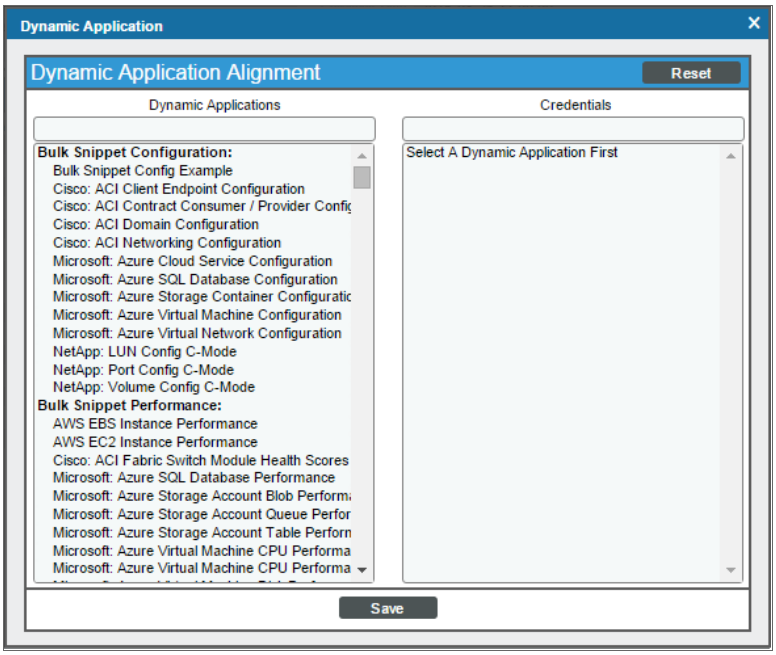
NOTE: You cannot align SNMP Dynamic Applications with a virtual device. You can align all other types of Dynamic Applications with a virtual device.

To manually associate a Dynamic Application with a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device you want to associate with a Dynamic Application. Click its wrench icon ( ).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Action]** menu and select *Add Dynamic Application*.



5. The **Dynamic Application Alignment** modal page appears.



6. To associate an additional Dynamic Application with the device, highlight it in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
7. After selection a Dynamic Application, you must select a credential. Select a credential in the ***Credentials*** field. You can filter the list of credentials using the search field above the ***Credentials*** field.

> **NOTE**: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

8. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
9. SL1 will associate the Dynamic Application with the device and immediately attempt to collect the data specified in the Dynamic Application using the selected credential.
10. After the first, immediate collection, SL1 will collect the data at the frequency defined in the ***Polling Frequency*** field in the **Application Configuration Editor** page for the Dynamic Application.

Chapter 13

Customizing the User Interface for a Device

Overview

This chapter describes how to define custom tabs in the **Device Administration** panel for a specific device.

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

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

This chapter includes the following topics:

Custom Navigation 272
Editing a Custom Navigation tab 274

Custom Navigation

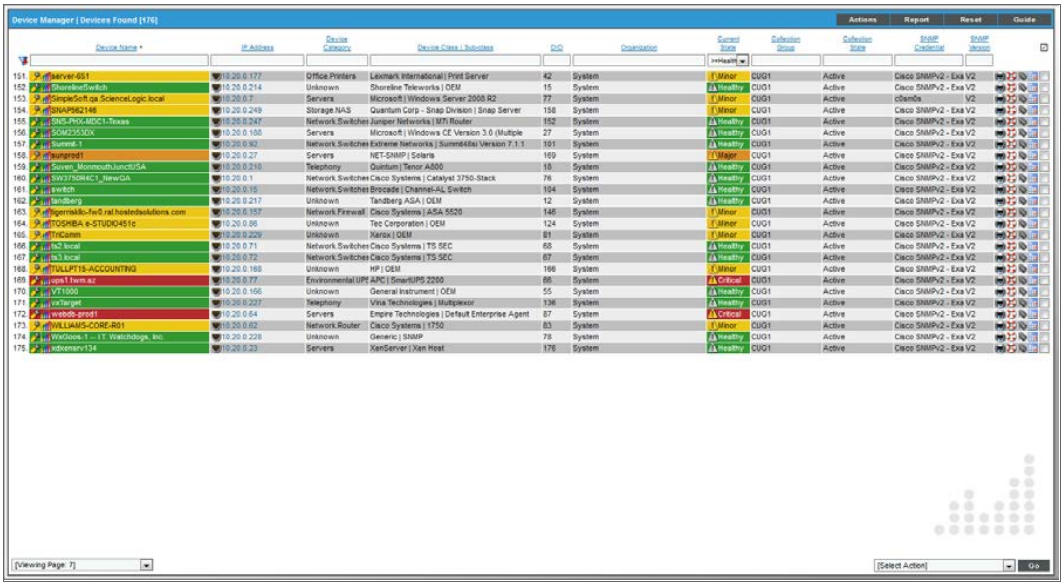
In the **Device Administration** panel you can access the **Custom Navigation** modal page.

The **Custom Navigation** modal page allows users to define custom tabs to include in the **Device Administration** panel for a specific device. Each custom tab includes one or more links. The links can be to internal pages in SL1 or external URLs and URIs.

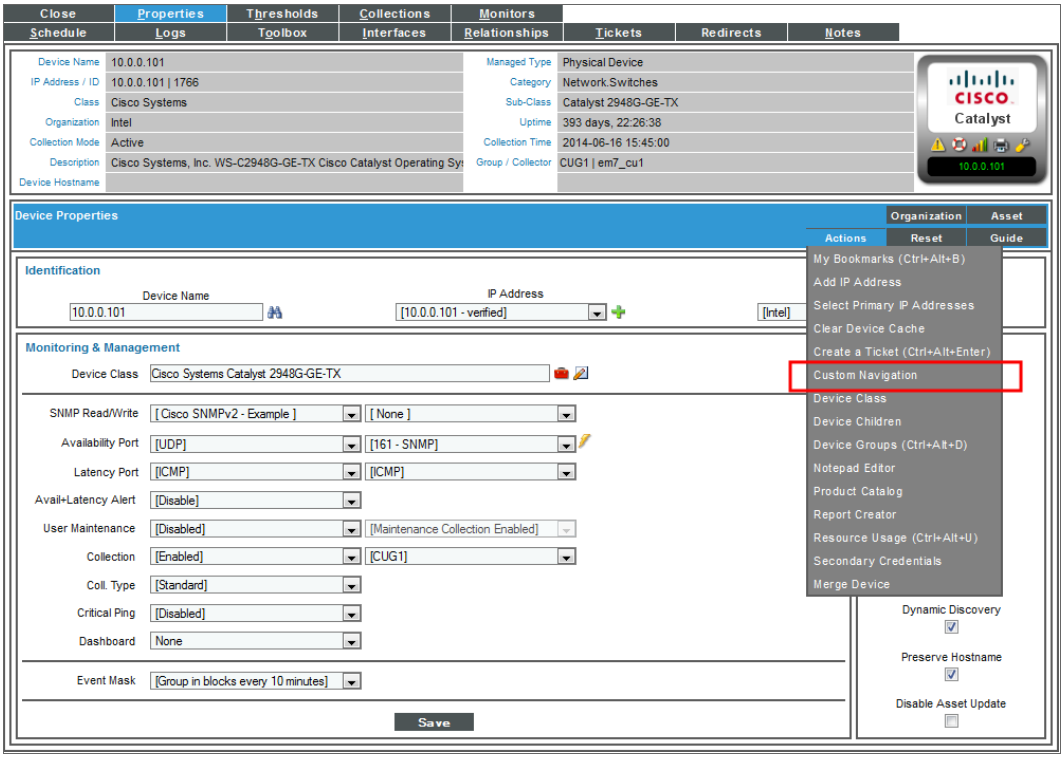
To define a custom tab for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).

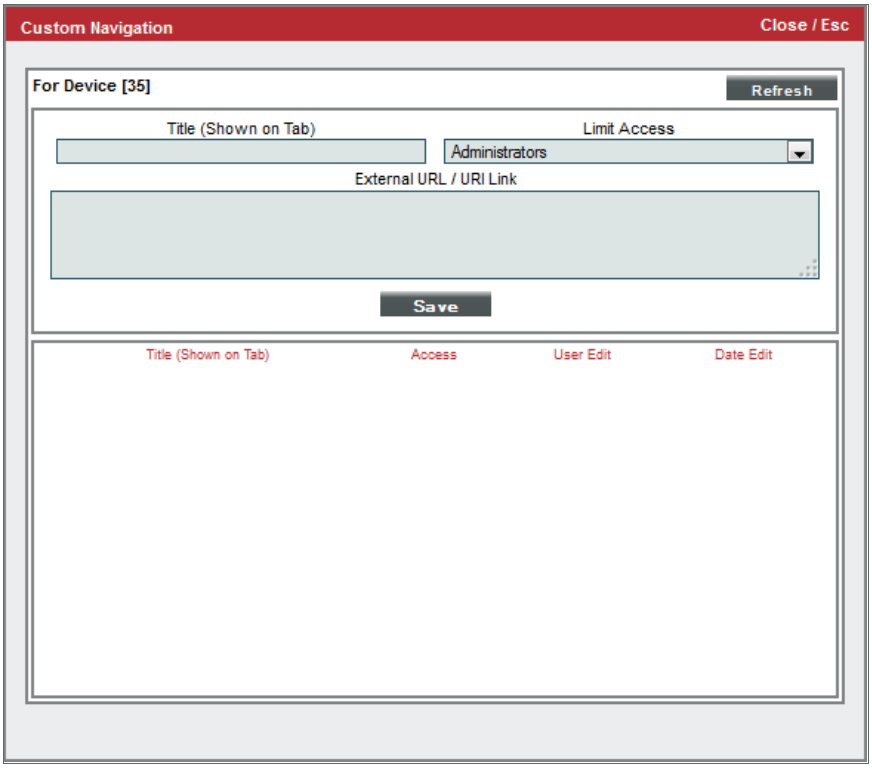
2. In the **Device Manager** page, find the device for which you want to create a custom tab. Select its wrench icon ( ).



3. In any page in the **Device Administration** panel, select the **[Actions]** menu and choose *Custom Navigation*.



4. The **Custom Navigation** modal page appears.



5. To create a custom tab in the **Device Administration** panel for the device, enter values in the following fields:

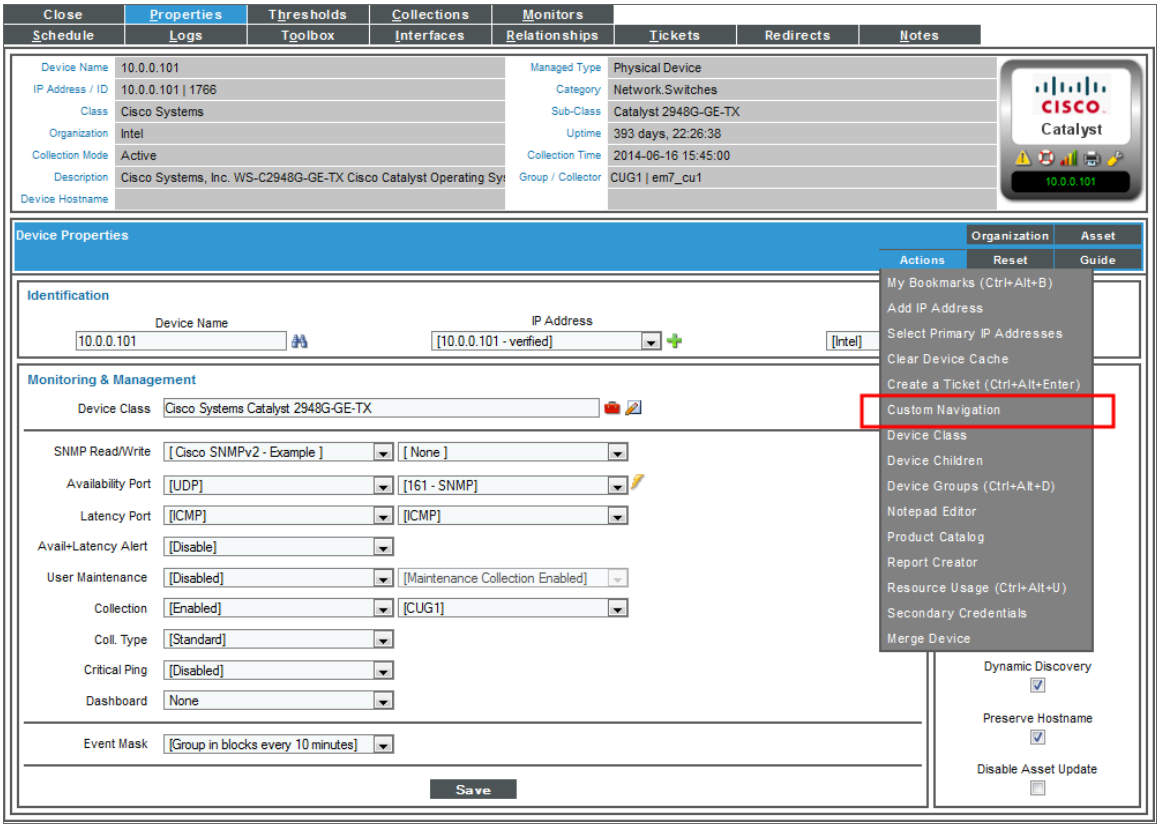
   - ***Title (Shown on Tab)***. Enter a name for the tab. This name will appear on a new tab in the Device Administration tools for this device.
   - ***Limit Access***. Users who will be allowed to access the custom tab, based on the type of user account. The choices are:
     - *Administrators*. Only users with account type "Administrator" are allowed to access this tab.
     - *Users*. Both users with account type "User" and users with account type "Administrator" are allowed to access this tab.
   - ***External URL / URI Link***. The URL of the page that is displayed when a user selects the tab. The page can be an internal page in SL1 or an external web page. This field can contain any combination of alphanumeric characters, with a maximum length of 128 characters. Forward slash (/), underscore (_), and question mark (?) are allowed.

Editing a Custom Navigation tab

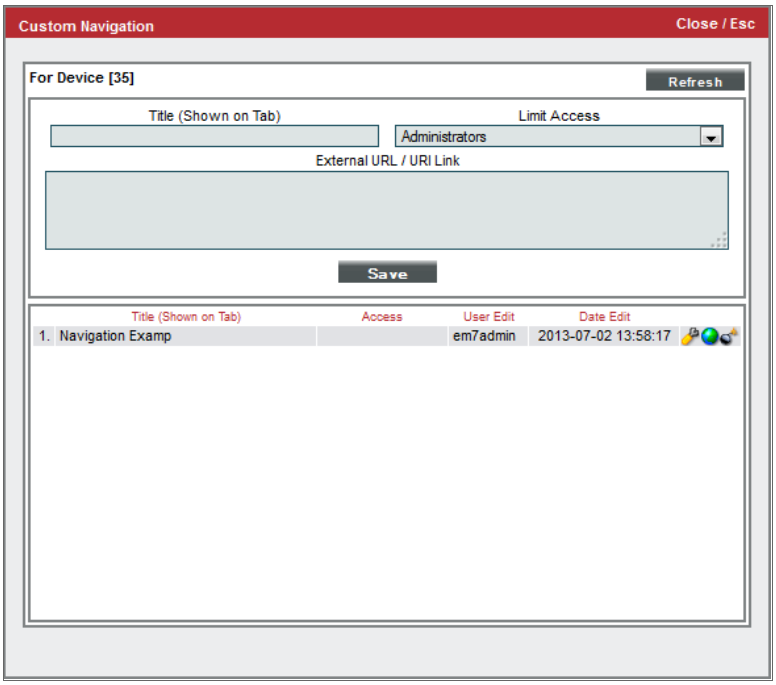
After you have defined one or more custom tabs in the **Device Administration** panel, each tab appears as an entry in the **Register** pane in the bottom of the **Custom Navigation** modal page.

To edit a custom tab:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to edit a custom tab. Select its wrench icon ( ).
3. In any page in the **Device Administration** panel, select the **[Actions]** menu and choose ***Custom Navigation***.



4. The **Custom Navigation** modal page appears:



5. Go to the **Register** pane. Find the custom tab you want to edit. Select its wrench icon ( ).
6. The fields in the top pane will be populated with values from the selected custom tab.
7. You can edit the values in one or more fields. Select the **[Save]** button to save your changes to the custom tab.
8. To delete the custom tab, go to the **Register** pane. Find the custom tab you want to edit. Select its bomb icon ( ).

NOTE: for details on creating a custom Navigation Tab for all devices, see the manual ***Customizing User Experience***.

Chapter 14

Vanishing & Purging Devices

Overview

If SL1 cannot retrieve information about a component device for the amount of time specified in the ***Component Vanish Timeout*** field (in either the **Global Threshold Settings** page, the **Device Thresholds** page for the component device, or the **Device Thresholds** page for a device higher in the component tree), SL1 sets the device to "vanished". When device is set to "vanished", SL1 stops trying to collect data about the component device. The vanished device will not appear in reports or views. The vanished device will appear only in the **Vanished Device Manager** page. When a device is set to "vanished", all children of that device are also set to "vanished".

NOTE: A vanished device automatically returns to a monitored state when the root device reports the device in the latest inventory of the component device discovery application.

After a device is vanished and SL1 cannot retrieve information about a component device for the amount of time specified in the ***Component Purge Timeout*** field (in either the **Global Threshold Settings** page, the **Device Thresholds** page for the component device, or the **Device Thresholds** page for a device higher in the component tree), SL1 purges the device. Purged devices are completely removed from SL1 and all associated data is deleted. When a device is purged, all children of that device are also purged.

The **Vanished Device Manager** page (Devices > Vanished Devices) displays a list of all component devices that have "vanished" from SL1.

NOTE: The vanishing and purging functions apply only to component devices and merged physical and component devices. Physical, IP-based devices and virtual devices that have not been merged with a component device are never vanished or purged.

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

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

This chapter includes the following topics:

Setting Vanish and Purge Thresholds 278
Viewing the List of Vanished Devices 279
Filtering the List of Devices 281
Using the Advanced Filters 282
Manually Purging Selected Devices 284
Setting One or More Devices to Never Purge 285

Setting Vanish and Purge Thresholds

Two threshold settings control the vanishing and purging behavior for component devices:

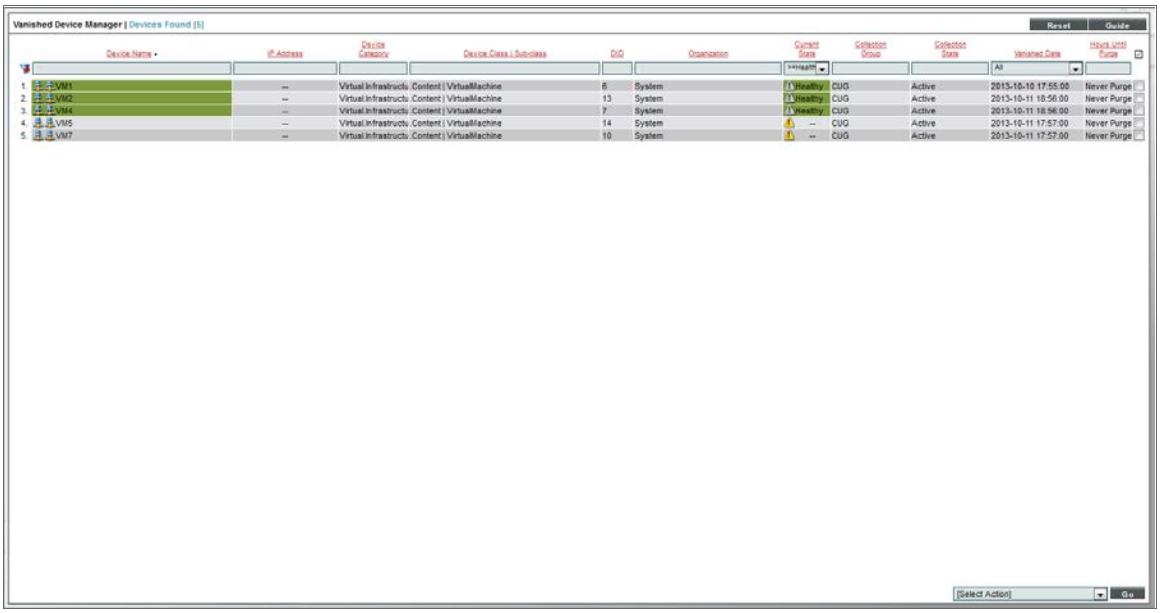
- ***Component Vanish Timeout***. If SL1 cannot retrieve information from a root device about a component device, this threshold specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", SL1 stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear in the *Vanished Device Manager* page. If this threshold is set to zero for a component device, the component device is never set to "vanished".
- ***Component Purge Timeout***. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many hours to wait until purging the component device. When a device is purged, SL1 stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from SL1. If this threshold is set to zero for a component device, the component device is never purged.

SL1 uses the following logic to determine the threshold value for a given component device when determining whether the component should be vanished or purged:

- If the threshold has been configured in the *Device Thresholds* page for the component device, that threshold value is used.
- If the threshold has not been configured in the *Device Thresholds* page for the component device but the threshold has been configured in the *Device Thresholds* page for an ancestor of the component device (i.e., a component device in the component tree between the root device and the component device), that threshold value is used. If multiple ancestors have the threshold configured in the *Device Thresholds* page, SL1 uses the threshold value for the component device that is closest to the root device (furthest up the tree).
- If the threshold has not been configured in the *Device Thresholds* page for the component device or an ancestor of the component device, the threshold value defined in the **Global Threshold Settings** page (System > Settings > Thresholds) is used.

Viewing the List of Vanished Devices

The **Vanished Device Manager** page (Devices > Vanished Devices) displays the following about each device:



TIP: To sort the list of devices, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again.

- ***Device Name***. Name of the device. For devices running SNMP or with DNS entries, the named device is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The IP address of the device.
- ***Device Category***. The ScienceLogic category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the Device Class/Sub-Class.
- ***Device Class/Sub-class***. The manufacturer (device class) and type of device (sub-class). The Device Class/Sub-Class is automatically assigned during discovery, at the same time as the as Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by SL1.
- ***Organization***. The organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. Condition can be one of the following:
    - *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 Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in the **Collector Group Management** page (System > Settings > Collector Groups) and specify one or more ScienceLogic Data Collectors. An ScienceLogic Data Collector is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).
- ***Collection State***. Collection state can be one of the following:
  - *Active*. SL1 is currently collecting data from the device.
  - *Disabled*. SL1 is not currently collecting data from the device.
  - *Unavailable*. The device is currently unavailable, so SL1 cannot collect data from the device at this time.
  - *Component Vanished*. The component device has vanished. SL1 cannot collect data from the device at this time.
- ***Vanished Date***. Date on which the device was set to "vanished". If SL1 cannot retrieve information from a root device about component device for the amount of time specified in the ***Component Vanish Timeout*** field (defined globally in the **Global Threshold Settings** page or for an individual device in the **Device Thresholds** page), SL1 sets the device to "vanished". When device is set to "vanished", SL1 stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear only in the **Vanished Device Manager** page.
- ***Hours Until Purge***. Based on the threshold ***Component Purge Timeout***, specifies the number of hours until the vanished device will be purged. When a device is purged, SL1 stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. You can define a global threshold for ***Component Purge Timeout*** in the **Global Threshold Settings** page. You can override the global threshold and define the ***Component Purge Timeout*** threshold for a single device in the device **Device Thresholds** page.

NOTE: To ensure that one or more devices are never purged, *you can set one or more devices to never purge*.

NOTE: To manually purge a device prior to the ***Hours to Purge*** time, *you can manually purge selected devices*.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

Filtering the List of Devices

You can filter the list on the **Custom Attribute Manager** page by one or more parameters. Only devices that meet all the filter criteria will be displayed in the **Custom Attribute Manager** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Web Content Monitoring**page searches for devices that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list is dynamically updated as you type. Text matches are not case-sensitive.

You can also use *special characters* to filter each parameter.

Filter by one or more of the following parameters:

- ***Device Name***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching device name.
- ***IP Address***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching IP address.
- ***Device Category***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching device category.
- ***Device Class***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching device class.
- ***DID***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching device ID.
- ***Organization***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching organization.
- ***Current State***. Specifies the device's current state. Only those devices that match all the previously selected fields and have the specified condition will be displayed. A device's condition is determined by its most severe, outstanding event. The choices are:
    - >=*Healthy*. Include devices with a condition of "Healthy" or greater. This will include all devices.
    - >=*Notice*. Include devices with a condition of "Notice" or greater. This means, include devices with a condition of "Notice", "Minor", "Major", and "Critical".
    - >=*Minor*. Include devices with a condition of "Minor" or greater. This means, include devices with a condition of "Minor", "Major", and "Critical".
    - >=*Major*. Include devices with a condition of "Major" or greater. This means, include devices with a condition of "Major" and "Critical".
    - >=*Critical*. Include devices with a condition of "Critical" or greater. This means, include devices with a condition of "Critical", because there is no "greater" condition.
- ***Collection Group***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching Collector Group.

- ***Collection State***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching Collection State.
- ***Vanished Date***. Date on which the device vanished. The **Vanished Device Manager** page will display only devices that match the specified vanish date. The choices are:
    - *All*. Display all tickets that match the other filters.
    - *Last Minute*. Display only tickets that have been created within the last minute.
    - *Last Hour*. Display only tickets that have been created within the last hour.
    - *Last Day*. Display only tickets that have been created within the last day.
    - *Last Week*. Display only tickets that have been created within the last week.
    - *Last Month*. Display only tickets that have been created within the last month.
    - *Last Year*. Display only tickets that have been created within the last year.
- ***Hours Until Purge***. You can enter text to match, including special characters, and the **Vanished Device Manager** page will display only devices that have a matching number of hours until the device is purged.

Using the Advanced Filters

In the **Vanished Device Manager** page, you can specify one or more parameters to filter the display of devices. Only devices that meet all the filter criteria will be displayed.

The Advanced Filter Tool allows you to make selections instead of manually typing in a string to filter on.

TIP: To select multiple entries in the Advanced Filter Tool, hold down the **<Ctrl>** key and left-click the entries.

- After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
- To reset each field and apply no filters, select the **[Reset]** button.

To access the Advanced Filter Tool:

1. Go to the **Vanished Device Manager** page.
2. Click on the funnel icon ( ).
3. The Advanced Filter Tool will display advanced filters for each column in the page.

NOTE: Unlike the "find while you type" feature, the Advanced Filter Tool is not applied to the list of devices until you select the **[Apply]** button.

4. In the Advanced Filter Tool, you can filter by one or more of the following filters:

- ***Device Name***. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters.The **Vanished Device Manager** page will display only devices that have a matching device name.
- ***IP Address***. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters.The **Vanished Device Manager** page will display only devices that have a matching IP address.
- ***Device Category***. Select from a list of device categories that have member devices. The **Vanished Device Manager** page will display only devices that have a matching device category. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters.
- ***Device Class | Sub-class***. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters.The **Vanished Device Manager** page will display only devices that have a matching device class or sub-class.
- ***DID***. In the ***From*** and ***To*** field, you can specify a range of device IDs. The **Vanished Device Manager** page will display only devices that fall within that range of device IDs.
- ***Organization***. Select from a list of organizations that have member devices. The **Vanished Device Manager** page will display only devices that have a matching organization. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters.
- ***Current State***. You can select from a list of device states. The **Vanished Device Manager** page will display only devices that have a matching state.
- ***Collection Group***. Select from a list of collection groups that have member devices. The **Vanished Device Manager** page will display only devices that have a matching collection group.
- ***Collection State***. You can select from a list of collection states. The **Vanished Device Manager** page will display only devices that have a matching state.
- ***Vanished Date***. In the ***From*** and ***To*** field, you can specify a range of vanished dates, in the format yyyy-mm-dd hh:mm:ss. The **Vanished Device Manager** page will display only device with a vanished date that falls within that range of date.
- ***Hour Until Purge***. In the ***Match Any*** fields, you can enter one or more text strings to match, including special characters. The **Vanished Device Manager** page will display only devices that have a matching number of hours until purge.

5. After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
6. To reset each field and apply no filters, select the **[Reset]** button.

TIP: You can perform an advanced filter and then perform a second advanced filter on the results of the first advanced filter. You can continue to modify and apply an advanced filter multiple times.

Manually Purging Selected Devices

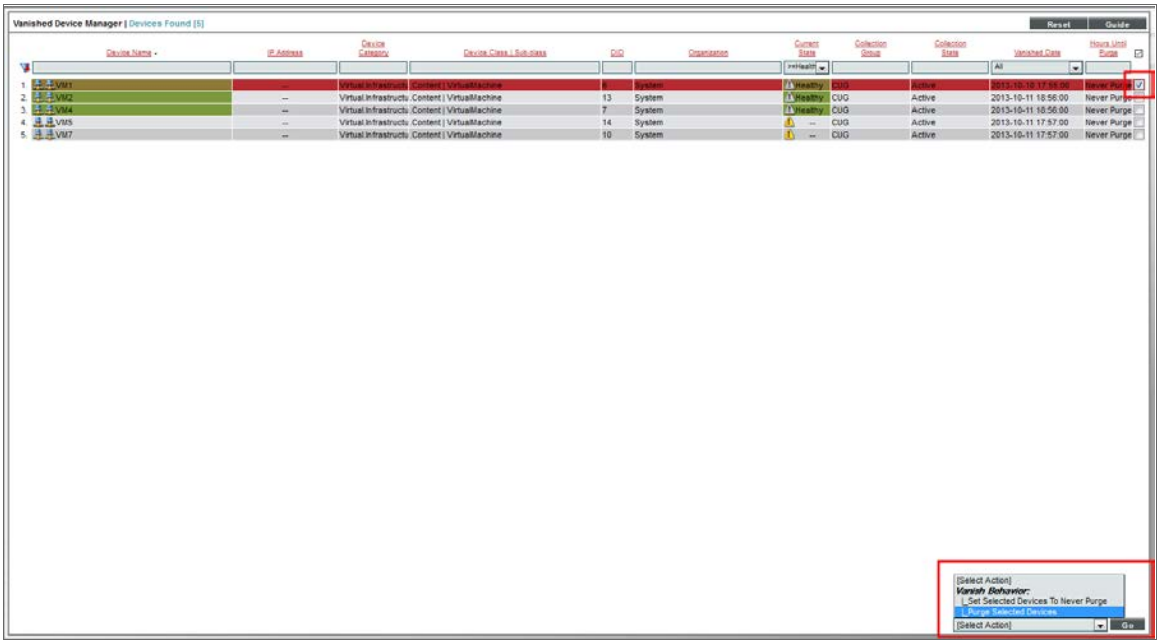
You can manually purge one or more devices in the **Vanished Device Manager** page.

When a device is purged, SL1 stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server.

NOTE: When a device is purged, all children of that device are also purged.

To purge one or more vanished devices:

1. In the **Vanished Device Manager** page (Devices > Vanished Devices), select the checkbox for each device you want to purge. To select all checkboxes for all devices, select the red checkbox ( ) at the top of the page.



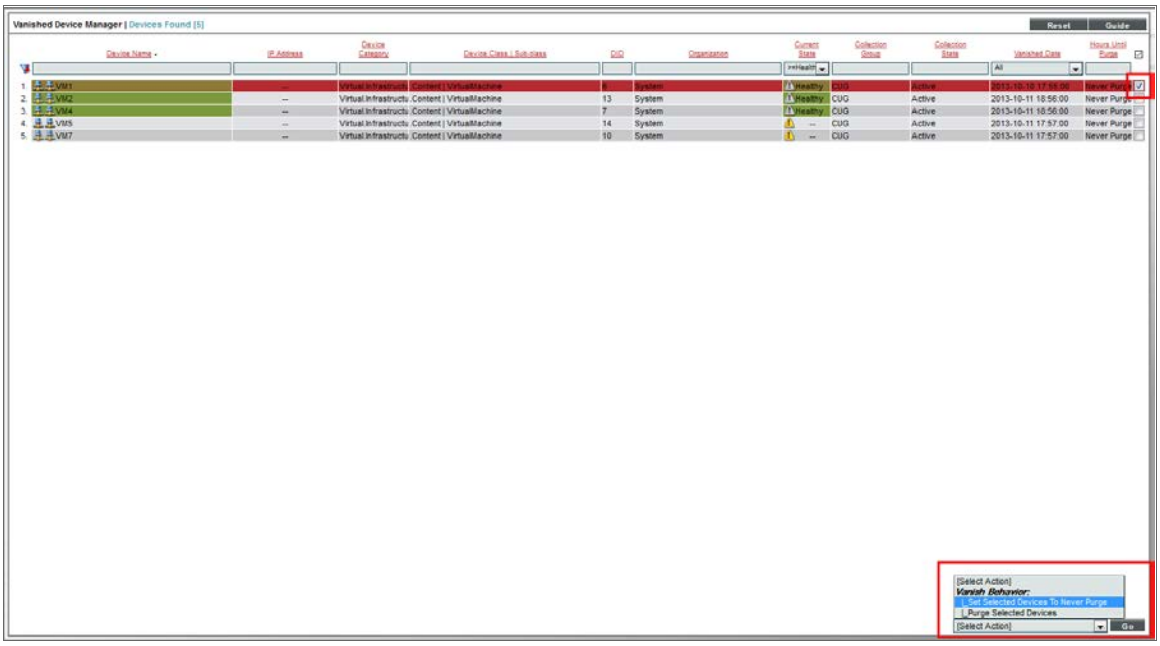
2. In the ***Select Action*** drop-down list, select *Purge Selected Devices*.
3. Select the **[Go]** button.

Setting One or More Devices to Never Purge

You can specify that a vanished device should never be purged. When you define this setting for a device, the device is never purged, regardless of the global threshold for ***Component Purge Timeout*** in the **Global Threshold Settings** page or the ***Component Purge Timeout*** threshold set for the device in the **Device Thresholds** page.

To set one or more vanished devices to never be purged:

1. In the **Vanished Device Manager** page (Devices > Vanished Devices), select the checkbox for each device you want to prevent from being purged. To select all checkboxes for all devices, select the select the red checkbox ( ) at the top of the page.



2. In the ***Select Action*** drop-down list, select *Set Selected Devices to Never Purge*.
3. Select the **[Go]** button.

Chapter 15

Device Dashboards

Overview

A dashboard is a page that displays graphical reports. Each report, called a widget, is displayed in its own pane. To define a graphical report, you select from a list of pre-defined widgets and then customize the selected widget by supplying values in the configuration fields. The customized widget then generates a graph, chart, table, or other information in a pane in the dashboard. For information on generating and viewing dashboards, see the ***Dashboards*** manual.

The **Device Summary** page, which appears when you select the graph icon ( ) for a device in the classic user interface for SL1, displays one or more dashboards similar to the dashboards available under the **[Dashboards]** tab.

Dashboards for the **Device Summary** page are always displayed with the context set to the device being viewed. Typically, the widgets on a device dashboard are configured to read the device context. As a result, the widgets display data for the device being viewed.

The **Device Dashboards** page (System > Customize > Device Dashboards) displays a list of dashboards that can be displayed for a device in the **Device Summary** page. From the **Device Dashboards** page, you can create, edit, delete, and align device dashboards.

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

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

This chapter includes the following topics:

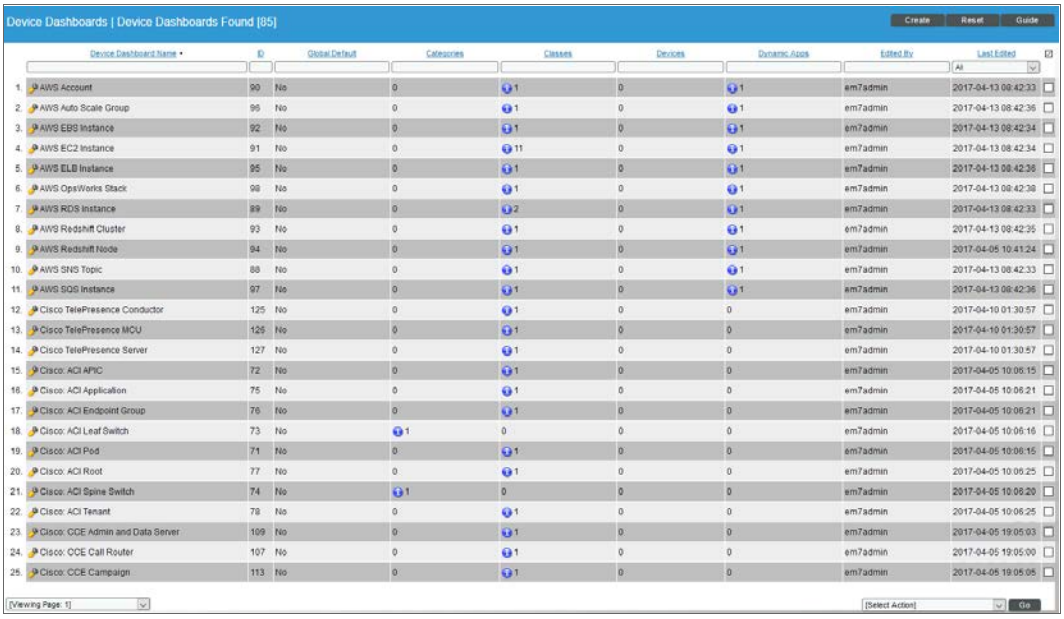
Viewing the List of Device Dashboards *287*
Creating a Device Dashboard *288*

Aligning Device Dashboards *289*
Aligning a Device Dashboard with a Device *290*
Aligning a Device Dashboard with a Device Class *291*
Aligning a Device Dashboard with a Device Category *292*
Aligning a Device Dashboard with a Dynamic Application *293*
Editing a Device Dashboard *294*
Deleting a Device Dashboard *294*
Copying a Device Dashboard *295*
Defining the Global Default for Device Dashboards *295*
Unaligning a Device Dashboard *297*
Moving Alignment for Device Dashboards *298*

Viewing the List of Device Dashboards

The **Device Dashboards** page displays a list of existing device dashboards. These dashboards include predefined device dashboards (which are installed with SL1 or can be installed with a PowerPack) and any user-defined device dashboards.

For each device dashboard, the **Device Dashboards** page displays:



TIP: To sort the list of dashboards, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Last Edited*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

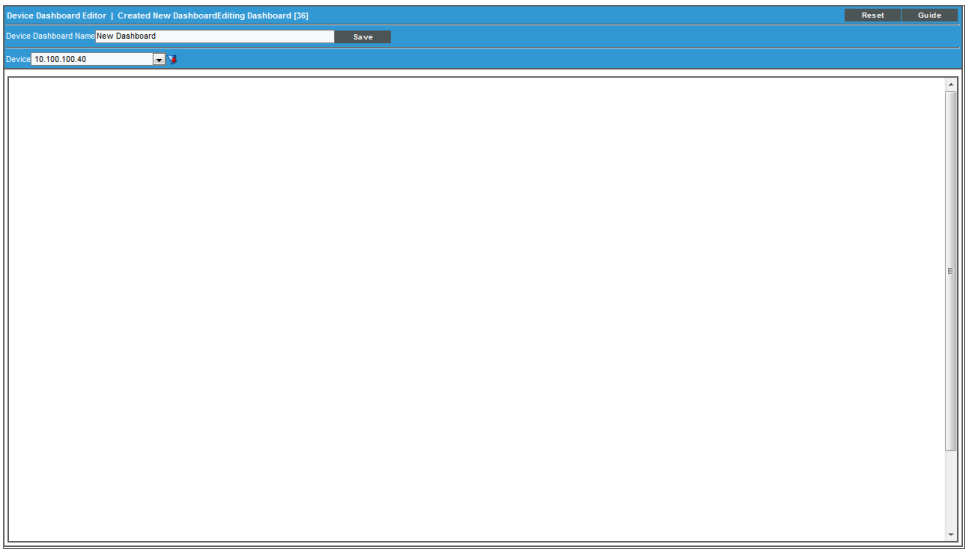
- ***Device Dashboard Name***. Name of the device dashboard.
- ***ID***. Unique ID that SL1 automatically assigned to each device dashboard.
- ***Global Default***. Specifies whether the device dashboard is the default device dashboard for all devices.
- ***Categories***. Specifies the number of device categories aligned with the device dashboard.
- ***Classes***. Specifies the number of device classes aligned with the device dashboard.
- ***Devices***. Specifies the number of devices that have been manually aligned with the device dashboard.
- ***Dynamic Apps***. Specifies the number of Dynamic Applications that are aligned with the device dashboard.
- ***Edited By***. ScienceLogic user who created or last edited the device dashboard.
- ***Last Edited***. Date and time the device dashboard was created or last edited.

NOTE: By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

Creating a Device Dashboard

To create a device dashboard:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, click the **[Create]** button.
3. The **Device Dashboard Editor** page appears. Supply values in the following fields:



- ***Device Dashboard Name***. Name of the device dashboard.
- ***Device***. Select a device to provide sample data while you create the dashboard. This device will not be permanently associated with the dashboard.
- ***Adding Widgets***. To add a widget, go to the big pane below the ***Device*** field. Left-click and drag with your mouse to draw a rectangle. This shape will determine the initial size and position of the widget in your dashboard. When the **Widget Configuration** page appears, configure the widget as you would for a dashboard.

NOTE: For maximum flexibility, when configuring a device-specific widget, ScienceLogic recommends that you select *Contextual Device (Auto)* in the ***Element*** field.

NOTE: For details on configuring widgets, see the manual ***Dashboards***.

4. The new device dashboard is automatically saved.

Aligning Device Dashboards

The device dashboard that is defined as the "Global Default" is the default dashboard that appears in the in the **Device Summary** page for each device.

SL1 decides what to display in the **Device Summary** page as follows:

- If the device is manually aligned with a device dashboard (in the **Device Properties** page), that dashboard is displayed in the **Device Summary** page for the device.

- If the device is not manually aligned with a device dashboard, the device dashboard that is aligned with the Device Class is displayed.
- If the device class is not aligned with a device dashboard, the device dashboard that is aligned with the Device Category is displayed.
- If the device category is not aligned with a device dashboard, the device dashboard that is defined as the "Global Default" is displayed.

NOTE: If the ***Prefer Global Device Summary Dashboard Over Category/Class*** checkbox is checked in the **Behavior Settings** page (System > Settings > Behavior) and a device is not manually aligned with a device dashboard, the dashboard that is defined as the "Global Default" is displayed.

NOTE: Although you can align a device dashboard with a Dynamic Application, the device dashboards that are aligned with Dynamic Applications are never displayed in the **Device Summary** page as the default display. However, from the **Device Summary** page, a user can select and view any device dashboards that are aligned with Dynamic Applications for the device.

Aligning a Device Dashboard with a Device

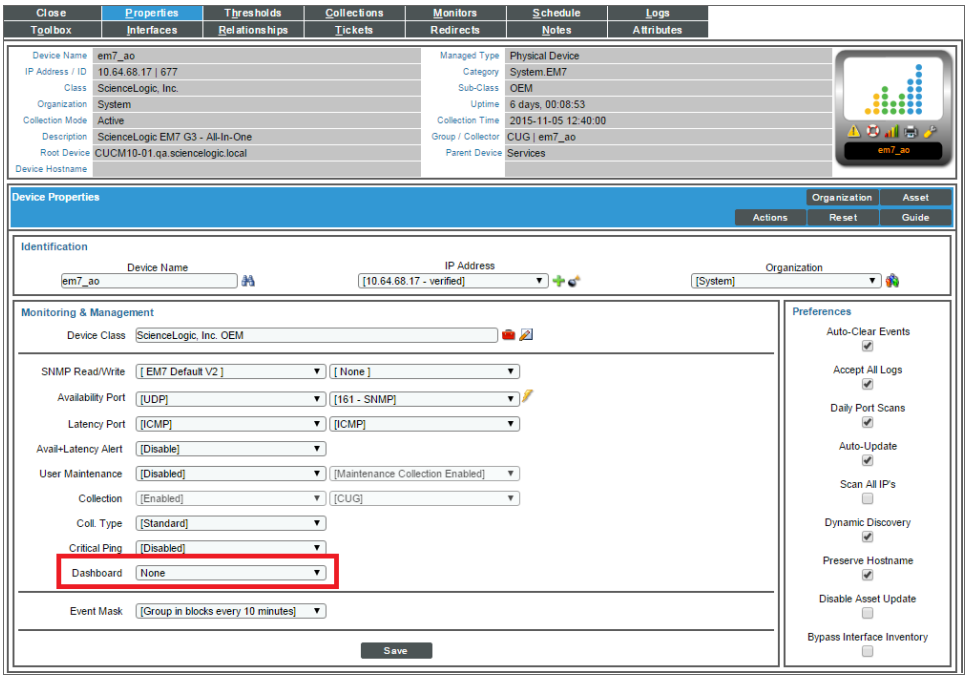
You can manually align a device dashboard with a device. The device dashboard will then appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Find the device you want to align with a device dashboard. Click the wrench icon ( ) for that device.

3. In the **Device Properties** page, edit the following field:



- ***Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. The selected device dashboard will appear by default in the **Device Summary** page for this device.

4. Click the **[Save]** button.

Aligning a Device Dashboard with a Device Class

You can manually align a device dashboard with a device class. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the Device Class will appear as the default view in the **Device Summary** page.

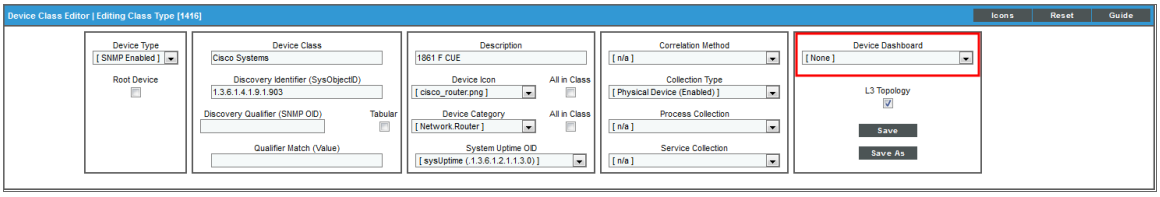
NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device class:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes).
2. In the **Device Class Register** pane, find the device class you want to align with a device dashboard. Click the wrench icon ( ) for that device class.

3. In the **Device Class Editor** page, edit the following field:

    - ***Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. The selected device dashboard will be associated with all devices that use this device class and will appear as an option in the **Device Summary** page.



4. Click the **[Save]** button.

NOTE: If a PowerPack updates one or more device classes, SL1 will not overwrite the alignment between device dashboards and any updated device classes.

Aligning a Device Dashboard with a Device Category

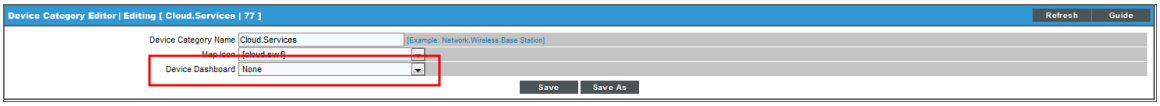
You can manually align a device dashboard with a device category. For devices that do not have a device dashboard defined in the **Device Properties** page or a device dashboard defined in the **Device Class Editor** page, the device dashboard associated with the Device Category will appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device category:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. In the **Register** pane, find the device category you want to align with a device dashboard. Click the wrench icon ( ) for that device category.
3. In the **Editor** pane, edit the following field:

    - ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. The selected device dashboard will be associated with all devices that use this device category and will appear as an option in the **Device Summary** page.



4. Click the **[Save]** button.

> **NOTE**: If a PowerPack updates one or more device categories, SL1 will not overwrite the alignment between device dashboards and any updated device categories.

Aligning a Device Dashboard with a Dynamic Application

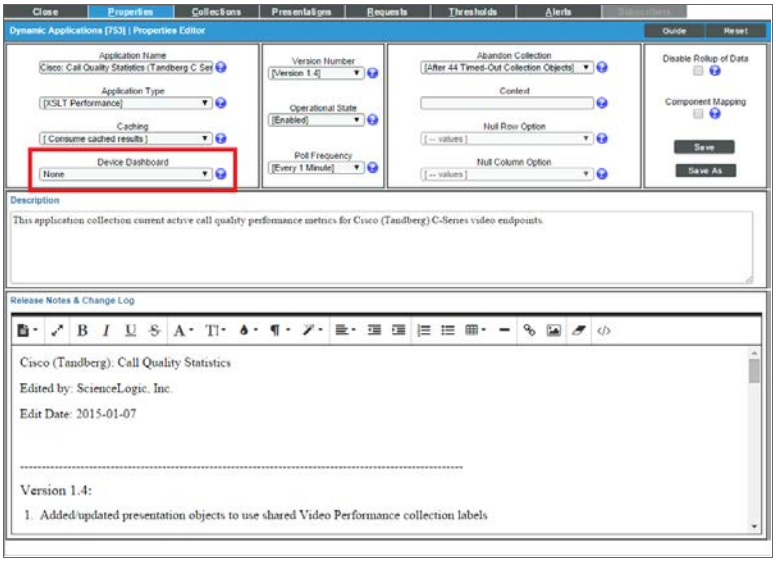
You can manually align a device dashboard with a Dynamic Application. For each device that subscribes to the Dynamic Application, the aligned device dashboard will appear as an option in the **Device Summary** page.

> **NOTE**: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To manually align a device dashboard with a Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the Dynamic Application you want to align with a device dashboard. Click the wrench icon ( ) for that Dynamic Application.
3. In the **Dynamic Applications Properties Editor** page, edit the following field:

    - ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in SL1. The selected device dashboard will be associated with all devices that subscribe to this Dynamic Application and will appear as an option in the **Device Summary** page.



4. Click the **[Save]** button.

NOTE: If a PowerPack updates one or more Dynamic Applications, SL1 will not overwrite the alignment between device dashboards and any updated Dynamic Applications.

Editing a Device Dashboard

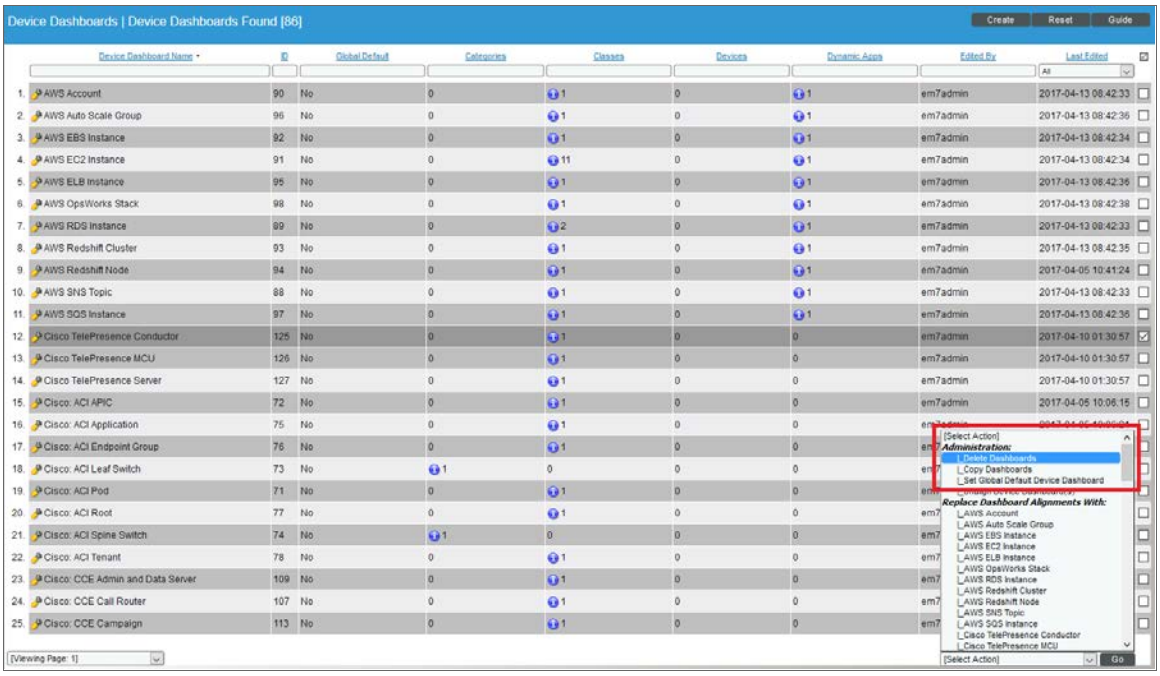
To edit a device dashboard:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, find the device dashboard you want to edit. Click its wrench icon ( ).
3. The **Device Dashboard Editor** page appears. Edit one or more fields and/or the dashboard widgets.
4. SL1 automatically saves your changes.

Deleting a Device Dashboard

To delete one or more device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for each dashboard you want to delete.
3. In the ***Select Action*** drop-down list, select *Delete Dashboards*.



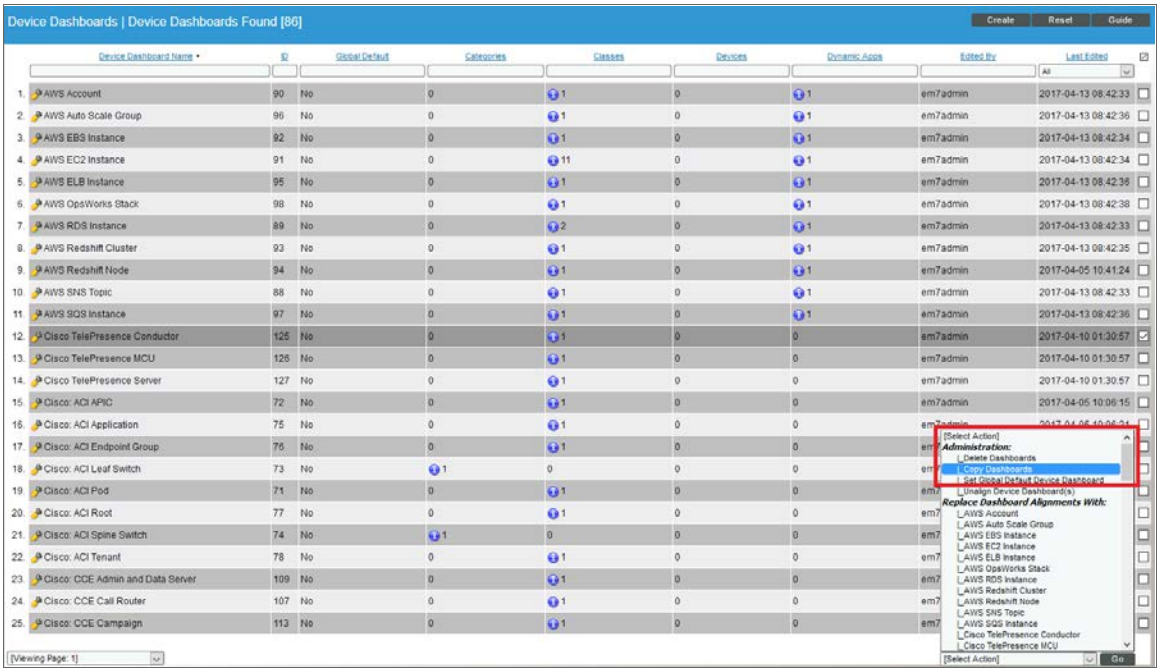
4. Click the **[Go]**button. The selected device dashboard(s) will no longer appear in this page or be accessible in the **Device Summary** page.

NOTE: You cannot delete a device dashboard that is defined as the Global Default.

Copying a Device Dashboard

To copy one or more device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for each dashboard you want to copy.
3. In the ***Select Action*** drop-down list, select *Copy Dashboards*.



4. Click the **[Go]** button. One or more new device dashboards will appear in this page with names that start with "Copy of".

Defining the Global Default for Device Dashboards

The device dashboard that is defined as the "Global Default" is the default dashboard that appears in the in the **Device Summary** page for each device.

SL1 decides what to display in the **Device Summary** page as follows:

- If the device is manually aligned with a device dashboard (in the **Device Properties** page), that dashboard is displayed in the **Device Summary** page for the device.
- If the device is not manually aligned with a device dashboard, the device dashboard that is aligned with the Device Class is displayed.
- If the device class is not aligned with a device dashboard, the device dashboard that is aligned with the Device Category is displayed.
- If the device category is not aligned with a device dashboard, the device dashboard that is defined as the "Global Default" is displayed.

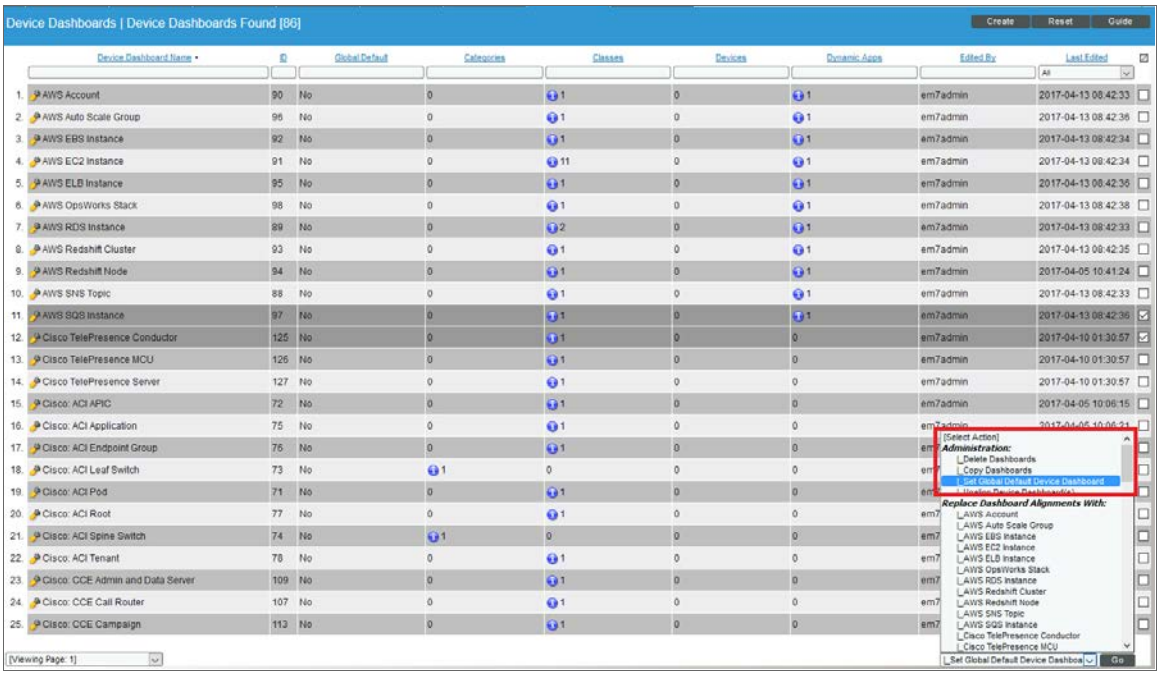
NOTE: If the ***Prefer Global Device Summary Dashboard Over Category/Class*** checkbox is checked in the **Behavior Settings** page (System > Settings > Behavior) and a device is not manually aligned with a device dashboard, the dashboard that is defined as the "Global Default" is displayed.

NOTE: Although you can align a device dashboard with a Dynamic Application, the device dashboards that are aligned with Dynamic Applications are never displayed in the **Device Summary** page as the default display. However, from the **Device Summary** page, a user can select and view any device dashboards that are aligned with Dynamic Applications for the device.

To define the Global Default for device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard you want to define as the Global Default.

3. In the ***Select Action*** drop-down list, select *Set Global Default Device Dashboard*.



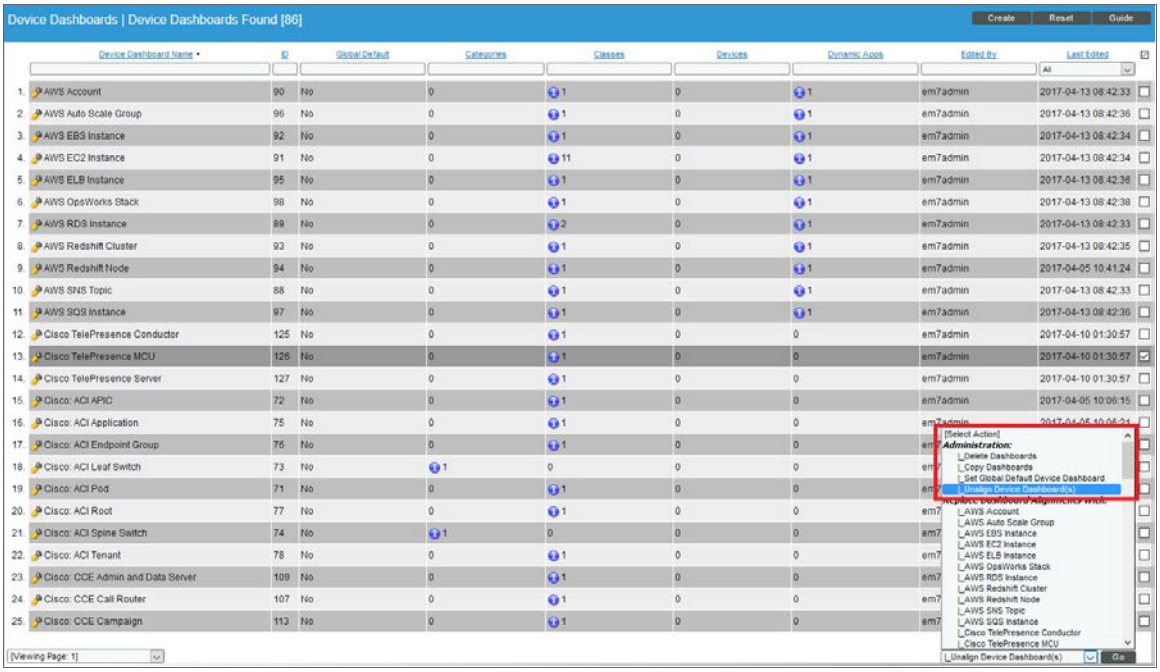
4. Click the **[Go]** button. In the***Global Default*** field for the selected device dashboard the value "Yes" will appear.

Unaligning a Device Dashboard

If you no longer want a device dashboard to appear as an option in the **Device Summary** page for any devices, you can remove all alignments for that device dashboard. To do this:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard you want to remove from the **Device Summary** page.

3. In the ***Select Action*** drop-down list, select *Unalign Device Dashboard(s)*.



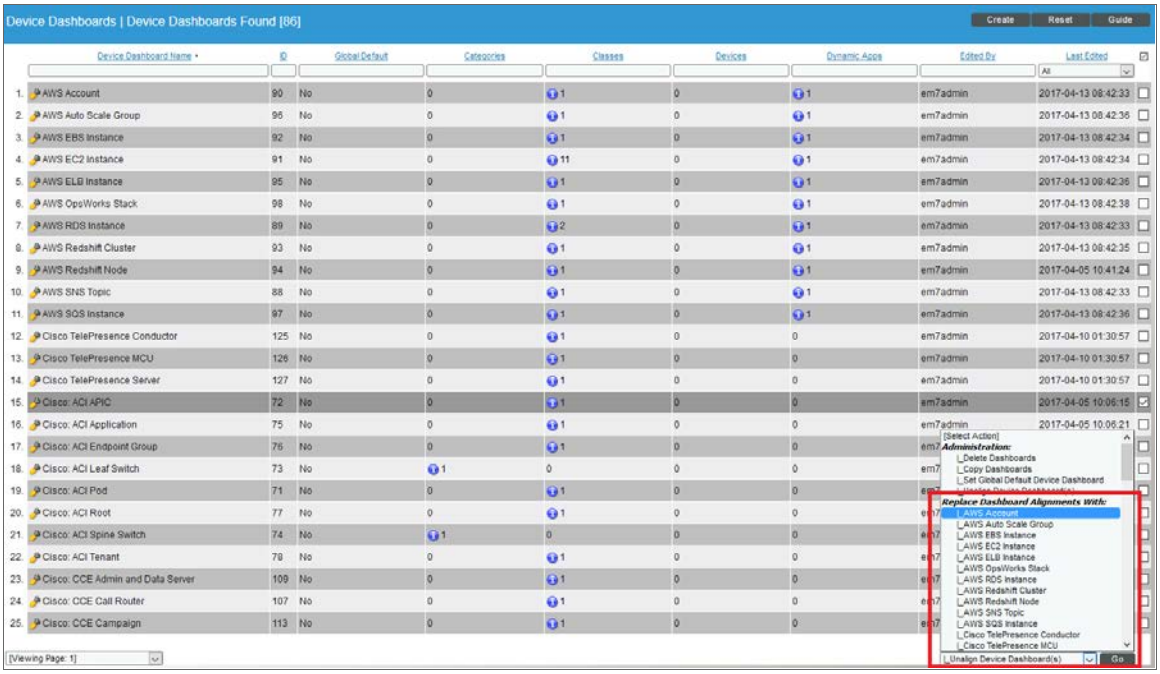
4. Click the **[Go]** button.
5. The selected dashboards are no longer aligned with Device Categories, Device Classes, Devices, or Dynamic Applications. The selected dashboards will no longer appear as an option in the **Device Summary** page for any devices.

Moving Alignment for Device Dashboards

You can specify that you want a device dashboard to "steal" all the alignments from another device dashboard. When you do this, the device dashboard that is stolen from will no longer have any alignment. To move alignments from one dashboard to another:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard that you want to "steal" alignments.

3. In the ***Select Action*** drop-down list, select *Replace Dashboard Alignments with* and then select the device dashboard that you want to "steal" alignments from.



4. Click the **[Go]** button.
5. The **Device Dashboards** page shows that the alignments have been removed from the device dashboard that you chose in the ***Select Action*** drop-down. In the **Device Dashboards** page, the device dashboard for which you selected the checkbox now displays all the alignments that it "stole" from the other device dashboard.

Chapter 16

Using Custom Attributes

Overview

This chapter describes how to use custom attributes.

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

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

This chapter includes the following topics:

Custom Attributes *301*

Viewing the List of Custom Attributes *301*

Filtering the List of Custom Attributes *304*

Viewing the List of Subscribers for a Custom Attribute *304*

Creating Custom Attributes *306*

Deleting One or More Custom Attributes *307*

Custom Attributes in the ScienceLogic API *307*

Using the ScienceLogic API to View, Create, and Edit Custom Attributes *308*

Using a Dynamic Application to Create and/or Populate Custom Attributes *308*

Using Custom Attributes to Define Device Groups *311*

Viewing Custom Attributes in the Custom Table Widget *312*

Custom Attributes

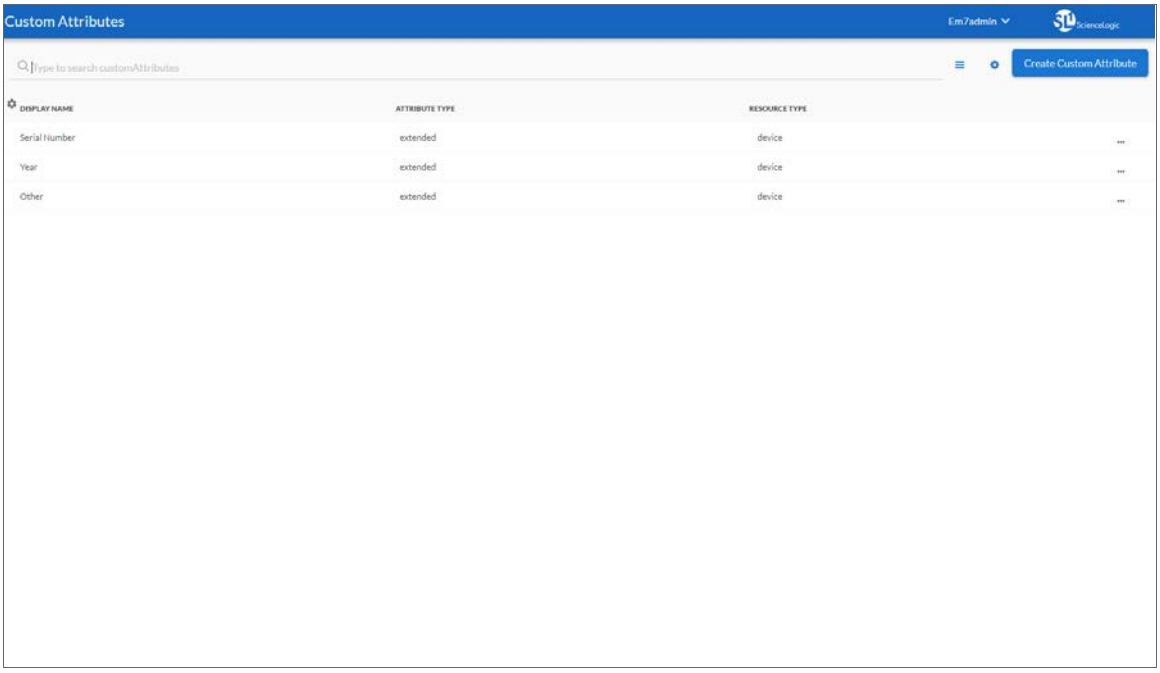
Custom Attributes are name-value pairs. You can use custom attributes to add custom descriptive fields to assets, devices, interfaces, themes, and vendors. In SL1, you can create and update custom attributes via the API, in configuration Dynamic Applications, and in the **Custom Attribute Manager** page. Custom attributes can be used to dynamically define device groups and can be viewed with the custom table widget.

There are two categories of custom attributes:

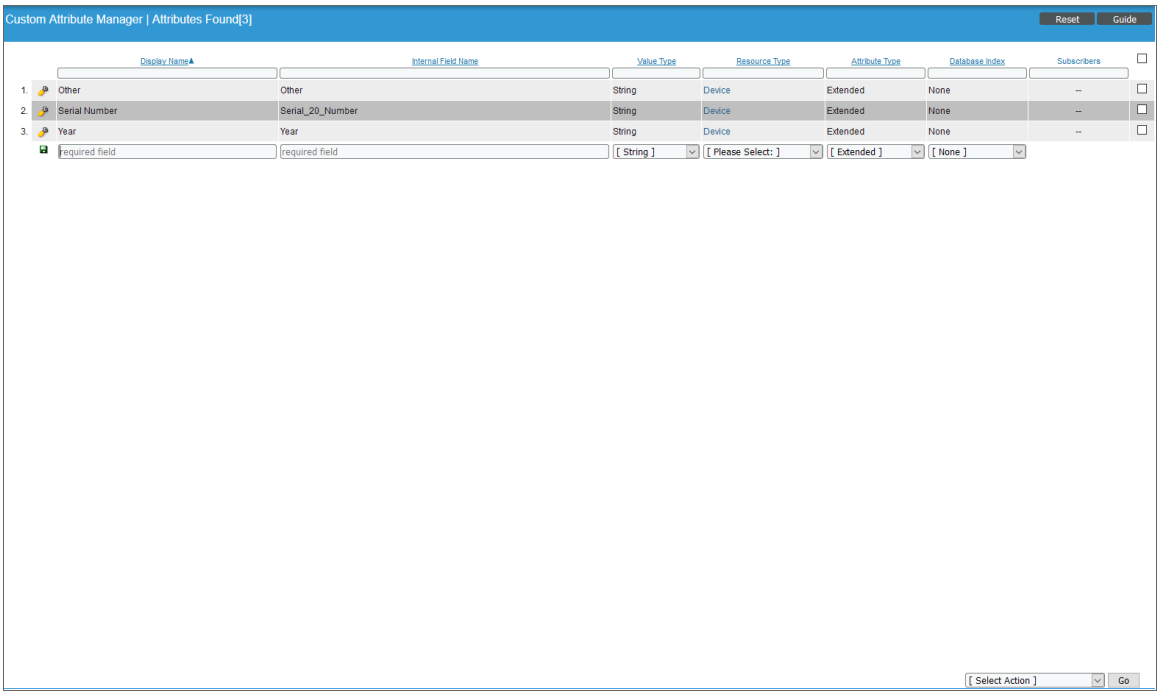
- **Base Custom Attributes**. These custom attributes are applied to each member of an element type. For example, a base attribute for devices would be applied to all devices.
- **Extended Custom Attributes**. These custom attributes are applied individually to one or more members of an element type. For example, you could apply the custom attribute cisco_ios_version only to those asset records for Cisco devices; you would not want to assign this custom attribute to all asset records.

Viewing the List of Custom Attributes

The **Custom Attribute Manager** page (Manage > Custom Attributes) displays a list of all the existing custom attributes created through the user interface:



The same information is available on the classic **Custom Attribute Manager** page (System > Manage > Custom Attributes):



For each custom attribute, the **Custom Attribute Manager** page displays the following information:

- ***Display Name***. Name for the custom attribute. This value appears in the user interface.
- ***Internal Field Name*** (classic only). Name for the custom attribute that complies with XML naming rules. If the value in the ***Display Name*** field does not comply with XML rules, SL1 will convert the value to a name that complies with XML rules.

NOTE: Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character, or an extending character. If a value in the ***Display Name*** column does not conform to XML standards, SL1 will replace non-valid characters with an underscore plus the hexadecimal value of the illegal character plus an underscore. So "serial number" would be replaced with "serial_X20_number".

- ***Value Type*** (classic only). Specifies the type of value that will be saved in the custom attribute. Choice are:
  - *String*. Non-numeric value
  - *Integer*. Numeric value
- ***Resource Type***. Specifies the ScienceLogic element that will use the custom attribute. Choices are:
  - *Asset*. Custom attribute will be associated with one or more asset records.
  - *Device*. Custom attribute will be associated with one or more devices.
  - *Interface*. Custom attribute will be associated with one or more network interfaces.

- *Theme*. Custom attribute will be associated with one or more user-interface themes.
- *Vendor*. Custom attribute will be associated with one or more vendor records.

- ***Attribute Type***. Specifies the behavior of the custom attribute. Choices are:
  - *Base*. A base custom attribute is automatically aligned to all members of the specified ***Resource Type***. For example, a base custom attribute for devices would be aligned with each and every device in your SL1 System.
  - *Extended*. An extended custom attribute is manually assigned only to some members of the ***Resource Type*** and should not be assigned to all members of the ***Resource Type***. For example, you could apply the custom attribute cisco_ios_version only to those asset records for Cisco devices; you would not want to assign this custom attribute to all asset records.

- ***Database Index*** (classic only). Specifies how the custom attribute is stored in the ScienceLogic database. Choices are:
  - *None*. Custom attribute is not indexed.

NOTE: Extended custom attributes allow only the value *None* in this field.

  - *Unique*. For base custom attributes, ensures that the value of each base custom attribute is unique within its ***Resource Type***.
  - *Index*. For base custom attributes, allows SL1 to efficiently search for custom attributes in the ScienceLogic database.

- ***Subscribers*** (classic only). Specifies the ***Resource Type*** and number of subscribers. Possible values in this field include:

NOTE: For base custom attributes, the value in the ***Subscribers*** column is always "- - " (dash dash).

  - *(Asset)*. Custom attribute is associated with one or more asset records. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Asset.
  - *(Device)*. Custom attribute is associated with one or more devices. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Device.
  - *(Interface)*. Custom attribute is associated with one or more network interfaces. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Interface.

- *(Theme)*. Custom attribute is associated with one or more user-interface themes. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Theme.
- *(Vendor)*. Custom attribute is associated with one or more vendor records. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Vendor.

Filtering the List of Custom Attributes

You can filter the list on the **Custom Attribute Manager** page by one or more parameters. Only attributes that meet all the filter criteria will be displayed in the **Custom Attribute Manager** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Custom Attribute Manager**page searches for attributes that match the text, including partial matches. By default, the cursor is placed in the left-most filter-while-you-type field. You can use the <Tab> key or your mouse to move your cursor through the fields. The list is dynamically updated as you type. Text matches are not case-sensitive.

You can also use *special characters* to filter each parameter.

Filter by one or more of the following parameters:

- ***Display Name***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching display name.
- ***Internal Field Name***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching internal field name.
- ***Value Type***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching value type.
- ***Resource Type***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching resource type.
- ***Attribute Type***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching attribute type
- ***Database Index***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching database index.
- ***Subscribers***. You can enter text to match, including special characters, and the **Custom Attribute Manager**page will display only custom attributes that have a matching number of subscribers.

Viewing the List of Subscribers for a Custom Attribute

To view a list of subscribers for a custom attribute:

1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes) .
2. Click the icon in the ***Subscribers*** column.
3. The **Custom Attribute Subscribers** modal page appears.

- For (*Asset*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
  - ***Make***. Make of the asset.
  - ***Model***. Model of the asset.
  - ***Device***. If applicable, name of the device associated with the asset record.
  - ***Asset Tag***. Asset tag associated with the asset.
  - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Device*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
  - ***DID***. Device ID for the device. SL1 automatically assigns this value to the device.
  - ***Device Name***. Name of the device.
  - ***IP Address***. If applicable, the IP address associated with the device.
  - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Interface*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
  - ***Device Name***. Name of the device associated with the interface.
  - ***IF Name***. Name of the interface.
  - ***IF Port***. Port number associated with the interface.
  - ***Alias.*** Alias associated with the interface.
  - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Theme*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
  - ***ID***. Unique ID associated with the theme. SL1 automatically assigns this value to the theme.
  - ***Theme Name***. Name of the theme.
  - ***HTML Header/Title***. HTML header associated with the theme.
  - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Vendor*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
  - ***ID***. Unique ID associated with the vendor. SL1 automatically assigns this value to the vendor.
  - ***Vendor Name***. Name of the vendor.
  - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.

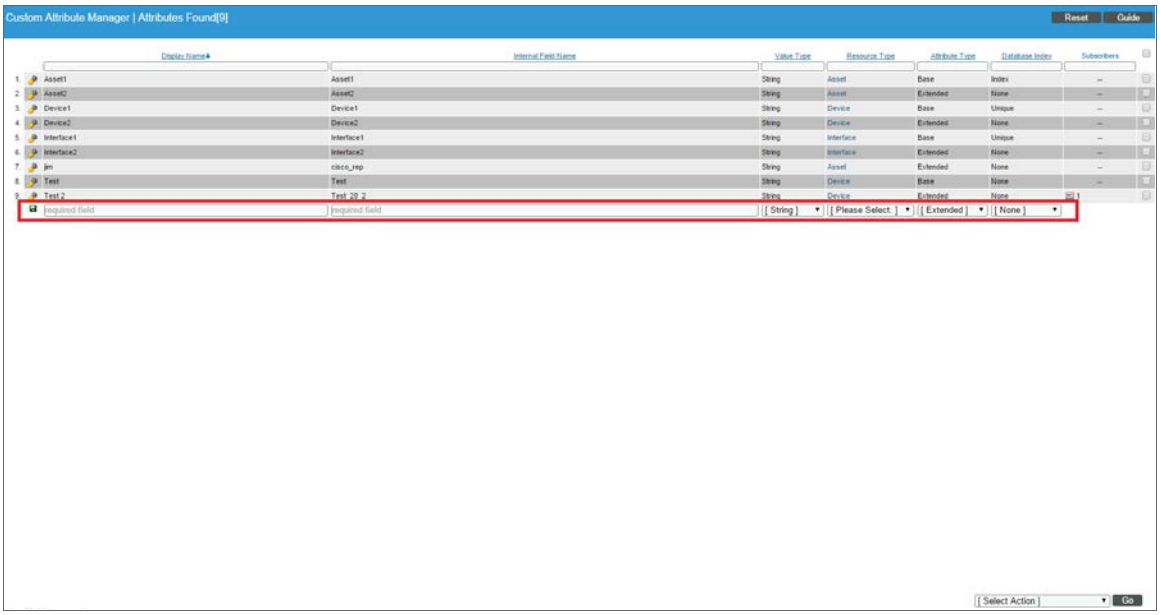
Creating Custom Attributes

You can create custom attributes on the **Custom Attribute Manager** page, via the ScienceLogic API, or by using a configuration Dynamic Application. The following rules apply to the creation of custom attributes:

- If you define a base custom attribute for devices on the **Custom Attribute Manager** page, that base custom attribute is aligned with each device in your system. The value of the base custom attribute will be null until you assign a value for each device.
- If you define an extended custom attribute for devices on the **Custom Attribute Manager** page, that extended custom attribute is not aligned with any devices.
- You can use the **Attributes** page in the **Device Administration** panel to assign a value or edit the value for each custom attribute aligned with a device. For more information, see the section on *Managing a Single Device with the Device Administration Panel*.
- You can use Dynamic Applications of type "configuration" to create custom attributes and/or assign values to custom attributes for devices. For details, see the section on *Using a Dynamic Application to Create and/or Populate Custom Attributes*.
- If you create a base custom attribute for asset records, network interfaces, themes, and vendor records, those custom attributes will appear in the ScienceLogic API for the specified entity. Initially, the value of the base attribute will be null. You cannot use the ScienceLogic user interface to assign a value to these base custom attribute. You must use the ScienceLogic API to assign values to these base custom attribute. For details, see the section on *Custom Attributes in the ScienceLogic API*.
- If you create an extended custom attribute for asset records, network interfaces, themes, and vendor records, those custom attributes can be aligned and populated using the ScienceLogic API. You cannot use the ScienceLogic user interface to assign a value to these extended custom attributes. You must use the ScienceLogic API to assign values to these extended custom attributes. For details, see the section on *Custom Attributes in the ScienceLogic API*.

To create a custom attribute from the **Custom Attribute Manager** page:

1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes).



2. In the bottom-most row, enter a value in each field.
3. Click the **Save** icon ( ).

Deleting One or More Custom Attributes

From the **Custom Attribute Manager** page, you can delete custom attributes from SL1. To do this:

1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes).
2. Select the checkbox ( ) for each custom attribute you want to delete.
3. Click the ***Select Action*** field in the lower-right and select *DELETE Custom Attributes*.
4. Click the **[Go]** button.

NOTE: SL1 will not allow you to delete an extended custom attribute that is aligned with one or more subscribers. If you try to delete an extended custom attribute that is aligned with one or more subscribers, SL1 will display the error message: "Error: Some attributes have entities aligned. Unalign entity from attribute before deleting." This message appears to the right of the page title.

Custom Attributes in the ScienceLogic API

The ScienceLogic API includes resources for adding custom attributes to the following resources:

- /asset
- /device
- The /interface sub-resource under /device resources
- /theme
- /vendor

When you define a custom attribute for a resource:

- For any instance of that resource (e.g., a specific device), you can perform a POST operation specifying a value for that attribute for that instance.
- If you configure the attribute as a base attribute, the attribute will appear in the list of fields for all instances of that resource. For example, if you define a custom attribute as a base attribute for the /device resource, the response to a GET request for any /device/*device_id* resource includes the custom attribute in the list of fields.
- If you configure the attribute as an extended attribute, the attribute will appear in the list of fields for instances of that resource only if a value has been specified for the attribute for that instance. For example, suppose you define a custom attribute as an extended attribute for the /device resource. The response to a GET request on the /device resource index with the extended_fetch option enabled will include the custom attribute only for devices that have a value for that custom attribute.
- GET requests for the resource index can include filter and sort criteria that use that custom attribute.

When you define a value for a custom attribute by performing a POST request to a resource, the value is available through the API and can be used in dynamic rules for device groups and viewed in the custom table widget.

Using the ScienceLogic API to View, Create, and Edit Custom Attributes

You can use the ScienceLogic API to view, edit, and create custom attributes. For details on viewing, creating, and editing custom attributes, see the manual ***Using the ScienceLogic API***.

Using a Dynamic Application to Create and/or Populate Custom Attributes

For details on creating aDynamic Application or creating collection objects, see the manual ***Dynamic Application Development***.

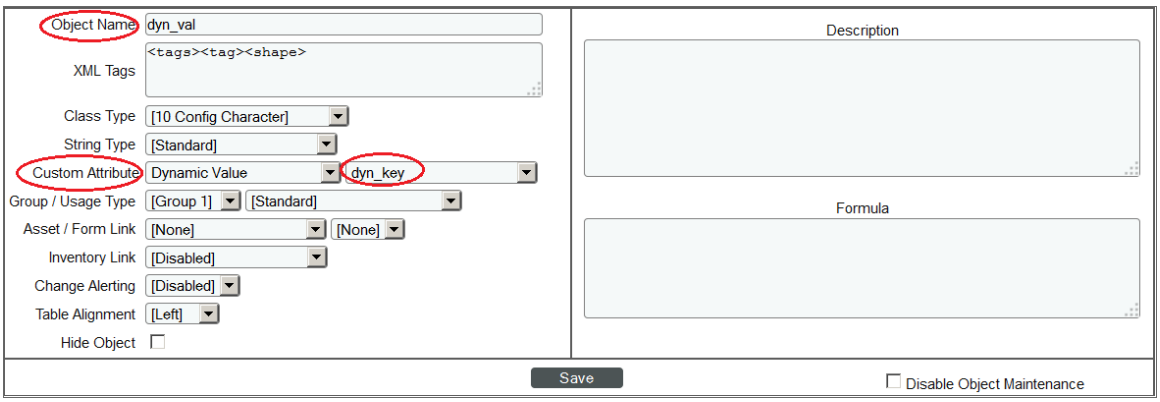
One of the ways you can create and/or populate a custom attribute for devices is through a Dynamic Application of type *configuration*.

In Dynamic Applications of archetype *configuration*, you can:

- Use a collection object to populate the value of an existing custom attribute.
- Use a pair of collection objects to create a custom attribute and provide a value for that custom attribute. You must define a collection object to define the name of the custom attribute; this causes the SL1 system to create a custom attribute with the name from the collection object. You must also define a second collection object to populate the value of the custom attribute.

NOTE: For details on creating and managing custom attributes, see the manual ***Using the ScienceLogic API***.

The following fields in the **Collection Objects** page allow you to use one or more collection objects to define and/or populate a custom attribute:



- ***Align to Custom Attribute***. Specify the custom attribute to associate with this collection object. The custom attribute will be populated with a value from a collection object. Choices are:
    - *None*. This collection object is not associated with a custom attribute.
    - *Static*. This collection object is associated with a specific custom attribute.
    - ***Static Name***. If you selected *Static* in the ***Custom Attribute*** field, the *Static Name* field appears. In this field, specify the name of the custom attribute that you want to populate with the value of the collection object. You can select from a list of existing custom attributes.
        - If the list does not include the custom attribute you want to align with the collection, select the plus-sign icon ( ). The icon clears the field and allows you to manually enter a value.
        - If you manually specify a custom attribute, SL1 will search for a custom attribute with a matching name and populate the custom attribute with the value of this collection object. If SL1 does not find a custom attribute with a matching name and therefore creates the custom attribute, the new custom attribute will be an extended custom attribute, for devices. The data type will be integer (for numeric values) or string (for all other value types).

- *Dynamic Name*. You can use a pair of collection objects to populate the name and value of a custom attribute. You must define each collection object separately. When you select *Dynamic Name* in the ***Custom Attribute*** field, the name of the custom attribute is populated with the value of the collection object. If SL1 does not find a custom attribute with a matching name, SL1 will create the custom attribute. If SL1 does not find a custom attribute with a matching name and therefore creates the custom attribute, the new custom attribute will be an extended custom attribute, for devices. The data type will be integer (for numeric values) or string (for all other value types).

NOTE: If you select *Dynamic Name* in the ***Custom Attribute*** field, you must create a second collection object that will populate the value of the custom attribute.

NOTE: Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character or an extending character. If a collected value for an attribute name does not conform to XML standards, SL1 will replace non-valid characters with an underscore + the hexadecimal value of the illegal character + an underscore. So "serial number" would be replaced with "serial_X20_number". The attribute label will use the original, non-converted value ("serial number").

- ***Dynamic Value***. The value of the custom attribute selected in the *Dynamic Name* field is populated with the value of the collection object.
- ***Dynamic Name***. If you selected *Dynamic Value* in the ***Custom Attribute*** field, the *Dynamic Name* field appears. Select from the list of collection objects that have a ***Custom Attribute*** value of *Dynamic Name*.

NOTE: The collection object assigned to the *Dynamic Value* is added to the same ***Group*** as the collection object assigned to the associated *Dynamic Name*. If the collection object for *Dynamic Name* is not assigned to a ***Group***, you will be prompted to select a ***Group*** for the both the collection object for *Dynamic Name* and the collection object for *Dynamic Value*.

NOTE: Each group can contain only one collection object that is assigned to a *Dynamic Value* and only one collection object that is assigned to a *Dynamic Name*. The group can contain other collection objects, but should not contain more than one collection object assigned to a *Dynamic Value* and not more than one collection object assigned to a *Dynamic Name*.

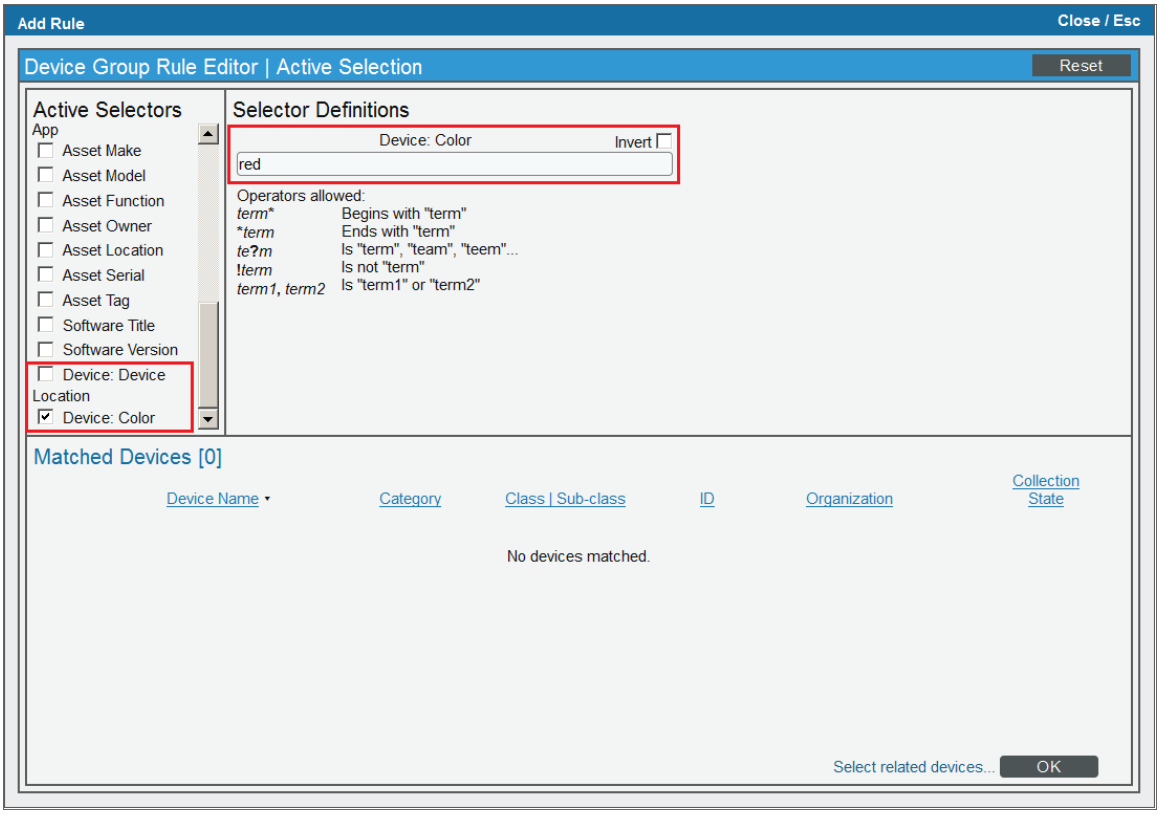
Using Custom Attributes to Define Device Groups

A device group is a group of multiple devices, grouped together for ease of management. You can use custom attributes to define membership in a device group. Only devices that have a specific value for a custom attribute will be included in the device group.

You can add devices to a device group either explicitly or dynamically.

- You can create ***static device groups***, where you explicitly assign one or more devices to a device group.
- You can create ***dynamic device groups***, where you define ***rules*** for the device group. Each device that meets the criteria in the rule is automatically included in the device group. For example, suppose that you define a rule that specifies "include all devices in the System organization, with an IP address that starts with '10.100.100' ". SL1 would automatically assign all devices from the *System* organization with an IP of "10.100.100.*" to the new device group. When a new device is added to the *System* organization with an IP that begins with "10.100.100.*", that device will also be included in the device group. If a device with an IP that starts with "10.100.100" is removed from the *System* organization, that device will also be removed from the device group.
- You can create a device group that includes both explicitly assigned devices and also includes a dynamic rule. This device group will include both the explicitly assigned devices and all devices that meet the criteria in the dynamic rule.

In the **Device Group Rule Editor** page, the ***Active Selectors*** field includes an entry for each custom attribute you have defined with the API or with a Dynamic Application. When you select a custom attribute, the ***Selector Definitions*** pane displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value for this custom attribute.



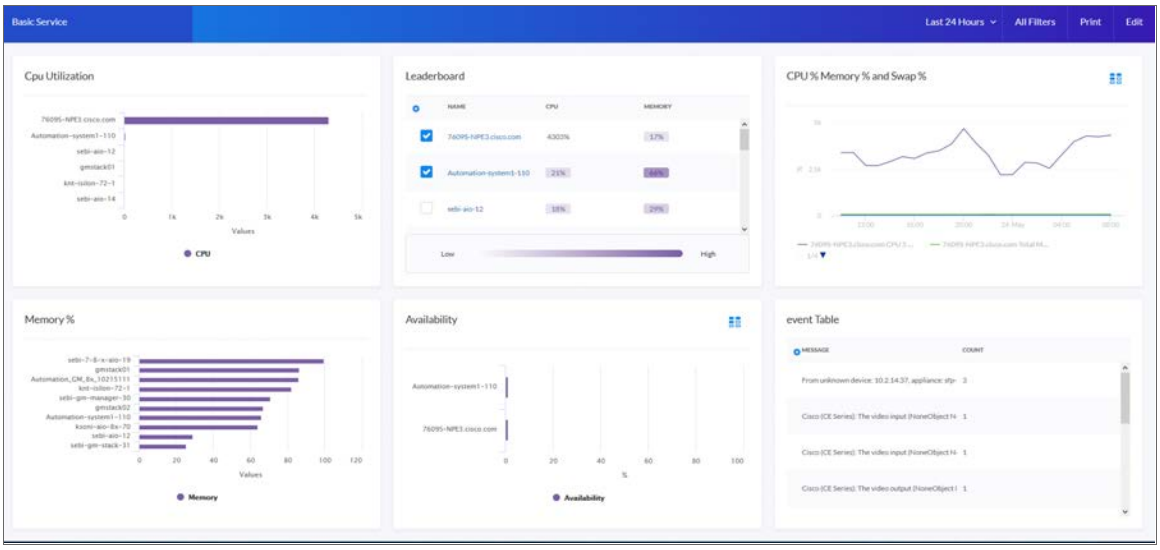
In the example above, we selected the custom attribute *Device:Color* and specified the value *red*. Our device group will include only devices that ihave the value *red* assigned to the *Device:Color* custom attribute.

For additional details on defining device groups and defining device group rules, see the manual ***Device Groups and Device Templates***.

Viewing Custom Attributes in the Custom Table Widget

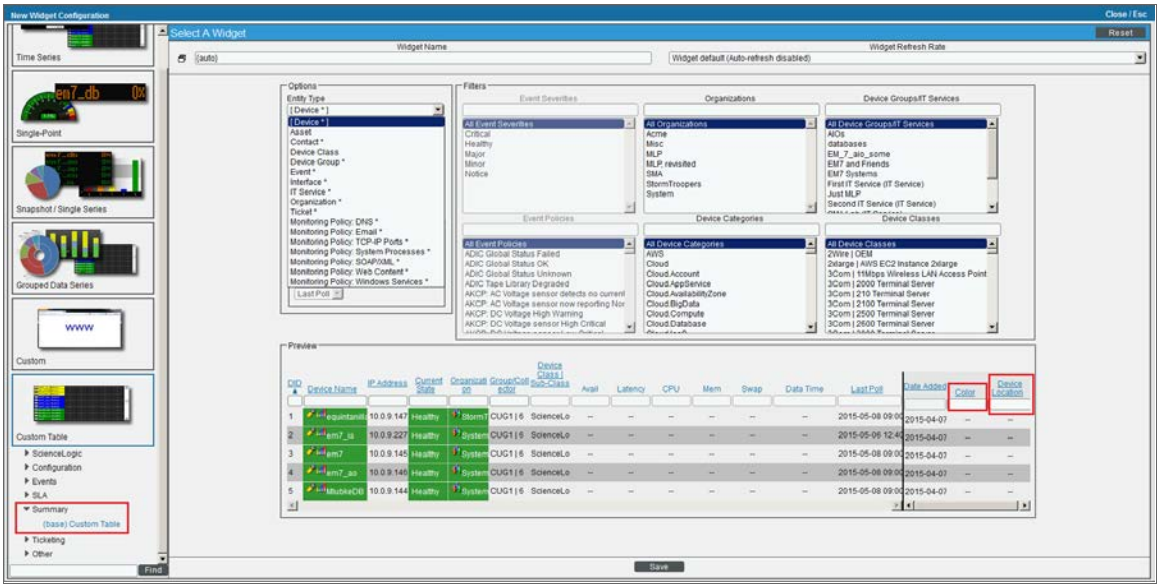
A dashboard is a page that displays one or more graphical reports, called widgets. SL1 includes pre-defined widgets that can be customized and displayed in the **Classic Dashboards** page. These widgets are displayed in their own pane, and display graphs, tables, and/or text.

To define an instance of 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.



The **Custom Table** widget displays multiple instances of an entity in a table. The **Custom Table** widget can be configured to display a list of devices, device classes, or device groups (and also other entities).

The generated table displays information about each entity in the list. You can configure which information is included in the table in the ***Layout Editor*** pane during configuration.



The **Layout Editor** panel displays the columns that will be displayed in the widget.

In the example above, *Color* and *Device Location* are custom attributes for devices.

If you selected *Device*,or *Asset*, or *Interface* in the ***Entity Type*** field of the Custom Table Widget, the Layout Editor will include columns for the custom attributes defined in your system for that entity type.

- By default, the columns for the custom attributes are excluded from the configuration.
- If an extended custom attribute is defined in your system but has not been assigned a value for any asset, device, or interface, it will not appear in the list of columns.

You can add or remove custom attributes from the layout of the widget using the following buttons:

- **<|>** You can move columns from left to right by clicking on the arrow characters at the top of each column and dragging the column left or right. Double-clicking on the arrow moves the column out of the display past a black bar to the right. All disabled columns can be seen to the right of the black bar. Double-clicking on the arrow again moves the column back into the display.

For additional details on configuring the Custom Table Widget, see the ***Dashboards*** manual.

© 2003 - 2020, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010