



Device Management

SL1 version 8.12.0

Table of Contents

Introduction to Devices	12
What is a Device?	13
What is a Device Record?	13
What is a Device Class?	14
What is a Device Category?	14
What is Discovery?	15
What is a Credential?	15
What is a Virtual Device?	16
What are Component Devices?	16
What is a Dynamic Application?	17
What is an SL1 Agent?	17
What is Virtualization?	18
What is an Asset Record?	18
Overview of Data Collection	20
What Is Collection?	21
What Kind of Data Can SL1 Collect?	21
What Kind of Data can the SL1 Agent Collect?	23
What is Device Availability?	24
What is Device Latency?	24
Monitoring Policies	25
Using the Devices Page	26
Viewing Devices	27
Viewing Additional Data about a Device	28
Aligning a Device with a Different Organization	29
Adding Devices with Discovery	29
What is Discovery?	29
What are Credentials?	30
Prerequisites for Discovering Devices on the Devices Page	31
Adding Devices Using Universal or Guided Discovery	31
Adding Devices Using Unguided Discovery	36
Working with Discovery Sessions	43
Using the Device Investigator	44
Adding Metrics to the Investigator Tab	47
The Info Drop-Down	49
Comparing Devices on the Investigator Tab	50
Using Device Tools	51
Combining Charts on the Investigator Tab	52
Running a Device Report	53
Overview of the Device Investigator Tabs	54
The Settings Tab	54
The Collections Tab	56
The Configs Tab	57
The Events Tab	58
The Interfaces Tab	58
The Journals Tab	60
The Map Tab	60
The Monitors Tab	61
The Notes Tab	61
The Ports Tab	62
The Processes Tab	63

The Redirects Tab	63
The Relationships Tab	64
The Schedules Tab	65
The Services Tab	65
The Software Tab	66
The Thresholds Tab	67
The Tickets Tab	67
Assigning Icons to Devices and Device Classes	68
Working with Device Categories	71
Using the Device Manager Page	74
Viewing the List of All Devices	75
Device Manager Preferences	77
Filtering the List of Devices	78
Special Characters	80
Using the Advanced Filter with the List of Devices	83
Generating a Report for Multiple Devices	85
Generating a Report for a Single Device	87
Viewing the List of Component Devices	89
Viewing Children Devices	92
Filtering the List of Component Devices	93
Using the Advanced Filter with the List of Component Devices	94
Bulk Actions in the Device Management Page	95
Bulk Actions for Component Devices	97
Bulk Merging and Unmerging of Devices	98
Performing a Bulk Device Merge	99
Performing a Bulk Device Unmerge	102
Viewing Details in the Device Reports Panel	104
What is the Device Reports panel?	105
Device Dashboards in the Device Summary Page	108
The Default Device Summary Page	110
Read-Only Information	112
Vitals	113
Tickets and Events	114
Elements	115
Monitors	116
System Component Utilization	116
Hourly Interface Usage	117
Shortcut Keys for Device Reports panel	117
Viewing Performance Graphs	119
Features of the Performance Tab	120
Viewing System Vitals for a Device	122
Viewing Availability Reports for a Device	124
Viewing Latency Reports for a Device	127
Viewing a Report on CPU Usage for a Device	130
Viewing a Report on Physical Memory Usage for a Device	132
Viewing a Report on Virtual Memory Usage for a Device	134
Viewing a Report on File System Usage for a Device	136
Viewing Reports on Network Interfaces	140
Default Reports for Network Interfaces	141
Network Utilization Report	143
Network Bandwidth Usage Report	144
Network Bandwidth Usage Report (Stacked)	145

Network Error Report	146
Network Error Report (Percent)	147
CBQoS Reports for Network Interfaces	149
Class Map Overview	151
Match Statements Overview	152
Policing Overview	153
Queueing Overview	154
Set Overview	155
Traffic Shaping Overview	156
WRED Overview	159
Viewing Reports about DNS Servers and DNS Records for a Device	161
Viewing Reports on an Email Round-Trip Monitoring Policy	163
Viewing Reports on an SOAP or XML Transaction Policy	165
Viewing Availability Reports for a Single System Process on a Device	171
Viewing Port Availability Reports for a Single Device	174
Viewing Reports for a Web Content Policy	175
Viewing Availability Reports for a Single Windows Service on a Device	182
Viewing Configuration & Journal Data	185
Configuration Dynamic Applications	186
Selecting Data to View	187
Viewing Data	187
Generating a Report of the Data	188
Viewing Historical Data	188
Editing the Application	189
Journal Dynamic Applications	190
Selecting Data to View	190
Viewing Data	191
Searching & Filtering the List of Data	191
Special Characters	193
Generating a Report of the Data	196
Editing the Application	197
Network Interfaces	198
Class-Based Quality of Service (CBQoS)	199
Viewing All Interfaces Discovered by the ScienceLogic Platform	199
Viewing Interfaces for a Single Device	203
Generating a Report for Multiple Network Interfaces	207
Generating a Report for a Single Network Interface	209
Monitoring Interfaces	211
Defining a Detailed Monitoring Policy for a Single Interface	211
Defining Monitoring Settings for Multiple Interfaces	217
Defining Thresholds for an Interface	222
Viewing the List of Discovered CBQoS Objects	226
Filtering the List of Quality of Service (QoS) Objects	228
Editing Thresholds for a Quality of Service (QoS) Object	229
Viewing Reports About Interfaces and Bandwidth	232
Global Settings that Affect Interfaces	232
Behavior Settings	233
Interface Threshold Defaults	234
Quality of Service Threshold Defaults	242
Monitoring Networks	247
IPv4 Networks	248
Viewing the List of IPv4 Networks	249

Browsing a Network	251
Viewing Used and Unused IP Addresses in a Network	251
Viewing Devices Aligned with a Network	252
Viewing Interfaces Aligned with a Network	252
Viewing a Map of a Network	252
Generating a Report for a Network	253
Defining a New Network	254
Merging One or More Networks	255
Synchronizing One or More Networks	256
Editing a Network's Properties	257
Performing Dynamic Discovery for a Network	257
Creating a Ticket About a Network	258
Deleting One or More IPv4 Networks	259
Hardware and Software	260
Viewing the List of All Discovered Hardware Components	261
Filtering the List of Hardware Components	262
Generating a Report for Multiple Hardware Components on Multiple Devices	263
Hiding a File System	264
Changing Thresholds for One or More File Systems	266
Viewing the List of All Discovered Software Titles	266
Filtering the List of Software Titles	267
Viewing a List of Software Titles for a Single Device	268
Filtering the List of Software	270
Generating a Report on All Software on All Devices	270
Generating an Exclusion Report for a Single Software Title	273
Device Logs	275
Viewing Logs for a Device	275
Viewing Events Associated with a Log Entry	277
Creating an Event Policy from a Log Entry	278
Viewing Logs for All Devices	279
Device Relationships	280
Viewing the List of Device Relationships	281
Filtering the List of Device Relationships	284
Viewing the Relationships for a Single Device	285
The Device View Page	287
Event Correlation	288
Defining Device Relationships	289
Device Categories that Don't Support Parent-Child Devices	290
Events that May Not Be Displayed in the Events Page	291
Defining Event Correlation	291
Layer-2 Topology Collection	294
CDP Topology Collection	295
LLDP Topology Collection	296
Layer-3 Topology Collection	298
SSL Certificates	300
Monitoring SSL Certificates	300
System Settings that Affect SSL Certificates in the ScienceLogic Platform	301
Viewing the List of SSL Certificates	302
Filtering the List of SSL Certificates	304
Device Processes	305
Viewing the List of Device Processes	306
Filtering the List of Device Processes	308

Viewing a List of System Processes on a Single Device	309
Generating a Report on Multiple System Processes	311
Generating an Exclusion Report for a Single System Process	313
Viewing the System Process Monitoring Policies	315
Filtering the List of System Process Monitoring Policies	315
Defining a Monitoring Policy for a System Process	316
Editing a Monitoring Policy for a System Process	319
Executing a System Process Monitoring Policy	320
Example Policy for System Process	321
Viewing Reports for a System Process Policy	321
Deleting a System Process Monitoring Policy	321
Windows Services	323
Viewing the List of Windows Services	324
Filtering the List of Windows Services	326
Viewing a List of Windows Services on a Single Device	326
Generating a Report on Multiple Windows Services	330
Generating an Exclusion Report for a Single Windows Service	332
Viewing the Windows Service Monitoring Policies	333
Filtering the List of Windows Service Monitoring Policies	334
Defining a Policy to Monitor Windows Services	335
Optional Settings in the ScienceLogic Platform	335
Required Configuration	336
Required Configuration on External Device	337
Defining the Policy	338
Executing a Monitoring Policy for a Windows Service	340
Editing a Monitoring Policy for a Windows Service	340
Example Policy for Windows Service	342
Viewing Reports about Windows Services	342
Deleting a Windows Service Policy	342
TCP Ports	344
What is a Port?	345
Port Security	345
Port Availability	345
Viewing a List of All Open Ports on All Devices	346
Filtering the List of IP Ports	347
Viewing a List of All Open Ports on a Single Device	348
System Settings for Monitoring Port Availability	350
Viewing the TCP/IP Port Monitoring Policies	351
Filtering the List of TCP/IP Port Monitoring Policies	352
Defining a Monitoring Policy for Port Availability	352
Editing a Monitoring Policy for a TCP/IP Port	354
Executing a TCP-IP Port Monitoring Policy	355
Example Policy for TCP/IP Port Availability	356
Viewing Reports for a Port-Availability Policy	356
Deleting a TCP/IP Port Monitoring Policy	356
Monitoring Domain Servers and DNS Records	358
Monitoring Domain Names	358
Viewing the List of Domain Name Monitoring Policies	360
Filtering the List of Domain-Name Monitoring Policies	360
Defining a Monitoring Policy for a Domain Name	361
Editing a Monitoring Policy for a Domain Name	363
Example Policy for Domain Name	364

Executing the Domain-Name Monitoring Policy	365
Viewing Reports for a Domain-Name Monitoring Policy	365
Deleting a Domain-Name Policy	365
Monitoring Email Round-Trips	367
Monitoring Email	367
Viewing the Email Round-Trip Monitoring Policies	369
Filtering the List of Email Round-Trip Monitoring Policies	369
Defining an Email Round-Trip Monitoring Policy	370
Required System Settings in the ScienceLogic Platform	371
Required Configuration on the External Email Client	372
Defining the Policy	373
Editing an Email Round-Trip Monitoring Policy	375
Example Email Round-Trip Monitoring Policy	376
How the ScienceLogic Platform Collects and Calculates Round-Trip Time	376
Viewing Reports on an Email Round-Trip Monitoring Policy	377
Deleting an Email Round-Trip Monitoring Policy	377
Events for Email Round-Trip Policies	378
Monitoring SOAP and XML Transactions	379
Monitoring SOAP or XML Transactions	380
Viewing the SOAP/XML Transaction Monitoring Policies	381
Filtering the List of SOAP/XSL Transaction Policies	382
Defining a SOAP/XML Transaction Policy	382
Editing a SOAP/XML Transaction Policy	385
Executing a SOAP/XML Transaction Policy	387
Example SOAP/XML Transaction Policy	387
Viewing Reports on a SOAP/XML Transaction Policy	388
Viewing Raw Data from a SOAP/XML Policy	388
Deleting a SOAP/XML Policy	388
Monitoring Web Content	390
Monitoring Web Content	390
Viewing the Web Content Monitoring Policies	391
Filtering the List of Web Content Monitoring Policies	392
Defining a Web Content Policy	393
Executing the Web Content Monitoring Policy	398
Editing a Web Content Policy	398
Example Web Content Policy	399
Viewing Reports on a Web Content Policy	400
Viewing ASCII Page Content	400
Viewing the Monitored Website	401
Deleting a Web Content Monitoring Policy	402
Managing a Single Device with the Device Administration Panel	403
What is the Device Administration Panel?	404
Actions Menu	407
Device Properties	410
Viewing Read-Only Information About the Device	411
Editing Device Settings	412
Identification	413
Monitoring & Management	413
Preferences	417
Adding an IP Address to a Device	418
Removing an IP Address from a Device	420
Managing Device IP Addresses	421

Clearing the Device Cache	423
Aligning a Secondary Credential	425
Adding the Device to a Device Group	427
Creating a Ticket About the Device	429
Adding a Note to a Device	431
Aligning Custom Attributes with a Device	434
Creating a New Extended Custom Attribute	435
Deleting an Extended Custom Attribute from a Device	437
Associating a Product SKU with the Device	438
Merging Devices	439
Merging Individual Devices	440
Unmerging Individual Devices	442
Performing Administrative Tasks for One or More Devices	444
Shortcut Keys for Device Administration panel	445
Managing Device Classes and Device Categories	447
Device Classes	448
Generic SNMP	448
Non-SNMP	449
Component	449
Agent-Only Device Classes	449
Viewing the List of Device Classes	450
Filtering the List of Device Classes	452
Creating Device Classes	453
Creating a New Device Class of Type "SNMP-Enabled"	454
Editing an SNMP-Enabled Device Class	457
Creating a New Device Class for a Device with Device Class "Generic SNMP"	457
Creating a New Device Class for Devices That Do Not Support SNMP	461
Applying the New Device Class	466
Maintaining the New Device Class During Auto-Discovery	467
Editing a Device Class That is Not SNMP-Enabled	467
Creating a Device Class of Type "Component"	468
Editing a Device Class of Type "Component"	470
Legacy Device Classes of Type "ICMP"	470
Managing Device Classes	471
Manually Changing the Device Class for a Device	471
Changing the Icon for a Device Class	473
Deleting One or More Device Classes	473
Aligning One or More Device Classes with a Device Dashboard	474
Device Categories	474
Viewing the List of Device Categories	475
"Pingable" Device Category	476
Creating a New Device Category	476
Editing a Device Category	477
Deleting a Device Category	478
Aligning One or More Device Categories with a Device Dashboard	479
Monitoring Device Availability and Device Latency	480
Availability	480
Configuring Availability Monitoring on a Device	481
Defining Availability Thresholds	483
Configuring Availability for Component Devices	483
Latency	486
Configuring Latency Monitoring on a Device	486

Defining Latency Thresholds	488
Viewing Reports on Device Availability and Device Latency	488
Device Toolbox	489
What is the Device Toolbox?	489
Accessing the Device Toolbox page	489
Viewing the Session Logs	492
Device Maintenance	494
What is Scheduled Maintenance?	495
What is User Maintenance?	496
The Maintenance Minimum Severity Setting	497
Enabling and Disabling User Maintenance for a Single Device	497
Enabling and Disabling User Maintenance for a One or More Devices	499
Scheduling Maintenance for a Single Device	500
Viewing the Schedule Manager	500
Defining a Scheduled or Recurring Device Maintenance Window for a Single Device	501
Scheduling Maintenance for One or More Devices	504
Enabling or Disabling Scheduled Maintenance for One or More Devices	505
Deleting Scheduled Maintenance for One or More Devices	506
Managing Dynamic Applications	507
Overview	507
Viewing the List of Dynamic Applications	508
Searching and Filtering the List of Dynamic Applications	512
Special Characters	513
Viewing the Dynamic Applications Associated with a Device	517
Viewing the Status of a Dynamic Application	519
Found	519
Collect	519
How the ScienceLogic Platform Manages Collect Status	520
Stopping Collection	520
Starting Collection	521
Collection Objects that are Excluded from Maintenance	521
Status of Objects for Deviation	521
Manually Associating a Dynamic Application with a Device	522
Editing the Credential Associated with a Dynamic Application	523
Performing Other Administrative Tasks for an Aligned Dynamic Application	524
Enabling or Disabling Objects	525
Restarting Automatic Maintenance of Collection Objects	526
Editing the Poll Frequency for a Dynamic Application on the Current Device	526
Stopping Data Collection for a Dynamic Application	526
Resetting Statistical Data for a Dynamic Application	527
Resetting Persistent Session Objects for a Dynamic Application	528
Testing Data Collection for a Dynamic Application	528
Removing Data Collected by a Dynamic Application	529
Bulk Un-Aligning Dynamic Applications	529
Setting Thresholds for Dynamic Applications	530
Dynamic Applications and Discovery	531
How Does the ScienceLogic Platform Align Dynamic Applications During Discovery?	532
Queuing Discovery from the Dynamic Applications Manager Page	533
Grouping Dynamic Application Data Using Collection Labels	534
What are Collection Labels and Collection Groups?	535
Viewing the List of Collection Labels	535
Filtering the List of Collection Labels	536

Special Characters	537
Creating a Collection Group	540
Creating a Collection Label	541
What is Normalization?	541
What are Duplicates and How Does the ScienceLogic Platform Manage Them?	544
What is Precedence?	545
Aligning a Presentation Object with a Collection Label	545
Viewing and Managing the List of Presentation Objects Aligned with a Collection Label	547
Viewing and Editing Duplicate Presentation Objects by Collection Label	551
Viewing and Managing the List of Devices Aligned with a Collection Label	553
Editing Duplicate Presentation Objects by Device	555
Editing Duplicate Presentation Objects for a Single Device	557
Editing a Collection Label	558
Deleting a Collection Label	559
Viewing Reports About Collection Labels on a Single Device	559
Viewing Dashboards About Collection Labels	560
Device Thresholds and Data Retention	561
Global Settings for Thresholds	562
Device Thresholds	566
Bulk Management with Device Groups and Device Templates	577
What is a Device Group?	578
What is a Device Template?	580
Virtual Devices	583
What is a Virtual Device?	583
Defining a Virtual Device	584
Directing Data to a Virtual Device	585
Redirecting Log Data to a Virtual Device	586
Aligning a Dynamic Application with a Virtual Device	588
Customizing the User Interface for a Device	590
Custom Navigation	590
Editing a Custom Navigation tab	593
Vanishing & Purging Devices	595
Setting Vanish and Purge Thresholds	596
Viewing the List of Vanished Devices	598
Filtering the List of Devices	600
Using the Advanced Filters	601
Manually Purge Selected Devices	603
Set One or More Devices to Never Purge	604
Device Dashboards	605
Viewing the List of Device Dashboards	606
Creating a Device Dashboard	608
Aligning Device Dashboards	609
Aligning a Device Dashboard with a Device	609
Aligning a Device Dashboard with a Device Class	610
Aligning a Device Dashboard with a Device Category	611
Aligning a Device Dashboard with a Dynamic Application	612
Editing a Device Dashboard	613
Deleting a Device Dashboard	613
Copying a Device Dashboard	614
Defining the Global Default for Device Dashboards	614
Unaligning a Device Dashboard	616
Moving Alignment for Device Dashboards	617

Using Custom Attributes	619
Viewing the List of Custom Attributes	620
Filtering the List of Custom Attributes	622
Viewing the List of Subscribers for a Custom Attribute	622
Creating Custom Attributes	624
Deleting One or More Custom Attributes	625
Custom Attributes in the ScienceLogic API	626
Using a Dynamic Application to Create and/or Populate Custom Attributes	626
Using Custom Attributes to Define Device Groups	629
Viewing Custom Attributes in the Custom Table Widget	630

Chapter



1

Introduction to Devices

Overview

This manual describes how SL1 collects data from monitored devices, and how SL1 displays that data in the user interface. This manual also describes how to configure settings and monitoring policies that control how data is collected from devices.

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:

<i>What is a Device?</i>	13
<i>What is a Device Record?</i>	13
<i>What is a Device Class?</i>	14
<i>What is a Device Category?</i>	14
<i>What is Discovery?</i>	15
<i>What is a Credential?</i>	15
<i>What is a Virtual Device?</i>	16
<i>What are Component Devices?</i>	16
<i>What is a Dynamic Application?</i>	17
<i>What is an SL1 Agent?</i>	17
<i>What is Virtualization?</i>	18
<i>What is an Asset Record?</i>	18

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.

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* chapter.

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

Overview of Data Collection

Overview

This chapter describes the process of data collection as well as the types of data that SL1 can collect.

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:

<i>What Is Collection?</i>	21
<i>What Kind of Data Can SL1 Collect?</i>	21
<i>What Kind of Data can the SL1 Agent Collect?</i>	23
<i>What is Device Availability?</i>	24
<i>What is Device Latency?</i>	24
<i>Monitoring Policies</i>	25

What Is Collection?

Collection is the tool that retrieves policy-based information and Dynamic Application-based information from a device. After a device is discovered, you can define monitoring policies for that device in SL1. For example, if you define a policy to monitor a system process, the collection tool retrieves that information.

- Dynamic Applications use collection processes to collect data.
- Monitoring Policies for devices also trigger collection. These policies include:
 - Domain Name Policies
 - Email Round-Trip policies
 - SOAP/XML Transaction policies
 - System Process Policies
 - TCP/IP Port Policies
 - Web Content Policies
 - Windows Services Policies
- SL1 automatically collects the following about each managed device:
 - Device availability and device latency
 - Network topology
 - File system information, if available
 - A list of open ports
 - Bandwidth usage
- The SL1 agent automatically collects the following about each device on which it is installed:
 - Device availability
 - Device performance and configuration metrics
 - A list of open ports
 - Log information
 - System processes

What Kind of Data Can SL1 Collect?

- 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 Kind of Data can the SL1 Agent Collect?

An SL1 agent collects the following data:

- **Device Availability.** SL1 can determine the availability state of a device (available or unavailable) and generate trended availability graphs based on uptime data collected by the agent.
- **Host Performance Metrics.** Using a Dynamic Application, SL1 translates data provided by an SL1 agent to trend the following metrics:
 - Overall CPU Utilization
 - Per-Processor CPU Utilization
 - Disk Average Queue Length
 - Disk Utilization
 - Memory Utilization
 - Network Bytes Read
 - Network Bytes Written

You can view these metrics on the **Device Investigator** page and the **[Performance]** tab of the **Device Reports** panel for a specific device.

- **Host Configuration.** Using a Dynamic Application, SL1 collects the following configuration data based on data provided by the agent:
 - The number and speed of the installed CPUs
 - The overall and per-disk storage size
 - The amount of installed memory

You can view the collected configuration data on the **[Configs]** tab of the **Device Investigator** page and the **Device Reports** panel.

- **System Processes.** The agent collects a list of all processes running on the device. You can view the list of processes on the **[Processes]** tab of the **Device Reports** panel and the **[Processes]** tab of the **Device Investigator** page. Monitoring policies can be configured to trend and alert on process availability, process CPU usage, and process memory usage.
- **Open Ports.** The agent collects a list of open TCP and UDP ports on the device. You can view the list of open ports on the **[TCP/UDP Ports]** tab of the **Device Reports** panel and the **[Ports]** tab of the **Device Investigator** page. Monitoring policies can be configured to trend and alert on port availability.

- **Logs.** The agent can be configured to push logs that match specific criteria from a log file or the Windows Event Log to SL1. You can view logs collected by the agent on the **Device Investigator** page and the **Device Logs** page for a device and can be configured to trigger events.

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

What is Device Availability?

Availability means a device's ability to accept connections and data from the network. 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.

By default, the method SL1 uses to monitor availability of the device is determined by the first method of discovery:

- If the agent is installed and creates a device record before the device is discovered as an SNMP or pingable device, availability is measured based on whether the agent is reporting data to SL1.
- If the device is discovered as an SNMP or pingable device before the agent is installed, availability is measured based on the method used to discover the device (SNMP, ICMP, or TCP).

If a device or interface becomes unavailable multiple times in a specified time frame, SL1 can generate an "availability flapping" event. By default, SL1 generates an event if a device becomes unavailable three times in an hour, or if an interface becomes unavailable three times in twenty-four hours.

To generate availability reports, SL1 must be configured to collect availability and latency data from devices. The following section describes how to configure SL1 to collect this data.

NOTE: Unlike for hardware-based devices, SL1 does not use an ICMP, TCP, or UDP to monitor availability for component devices. 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.

What is Device Latency?

Latency means the amount of time it takes SL1 to communicate with a device. Specifically, latency refers to the amount of time between when SL1 initiates communication with a device and when the device responds and allows communication. Latency is expressed in milliseconds (ms).

SL1 uses ports to monitor a device's latency. You specify which ports to use for device latency on the **[Settings]** tab of the **Device Investigator** page.

Monitoring Policies

For each device in SL1, you can define the following types of monitoring policies:

- **Domain Name policies.** Monitor the availability and lookup time for a specific domain-name server and a specific record on a domain-name server.
- **Email Round-Trip policies.** 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/XML Transaction policies.** Monitor 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.
- **System Process policies.** Monitor the device and look for the specified system process. You can define a process policy that also specifies:
 - How much memory a process can use.
 - How many instances of a process can run simultaneously.
 - Whether or not to generate an event if the process is running.
- **TCP/IP Port policies.** Monitor ports for availability every five 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 policies.** Monitor 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 Service policies.** Monitor the device and look for the specified service. You can define a service policy so that:
 - SL1 generates an event if the service is not running.
 - SL1 generates an event if the service is running.
 - SL1 starts, pauses, or restarts the service.
 - SL1 reboots or shuts down the device.
 - SL1 triggers the execution of a script (script must reside on the device).

You can define these policies either from the **Device Administration** panel of a device or from the pages in Registry > Monitors section.

Chapter

3



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 (.

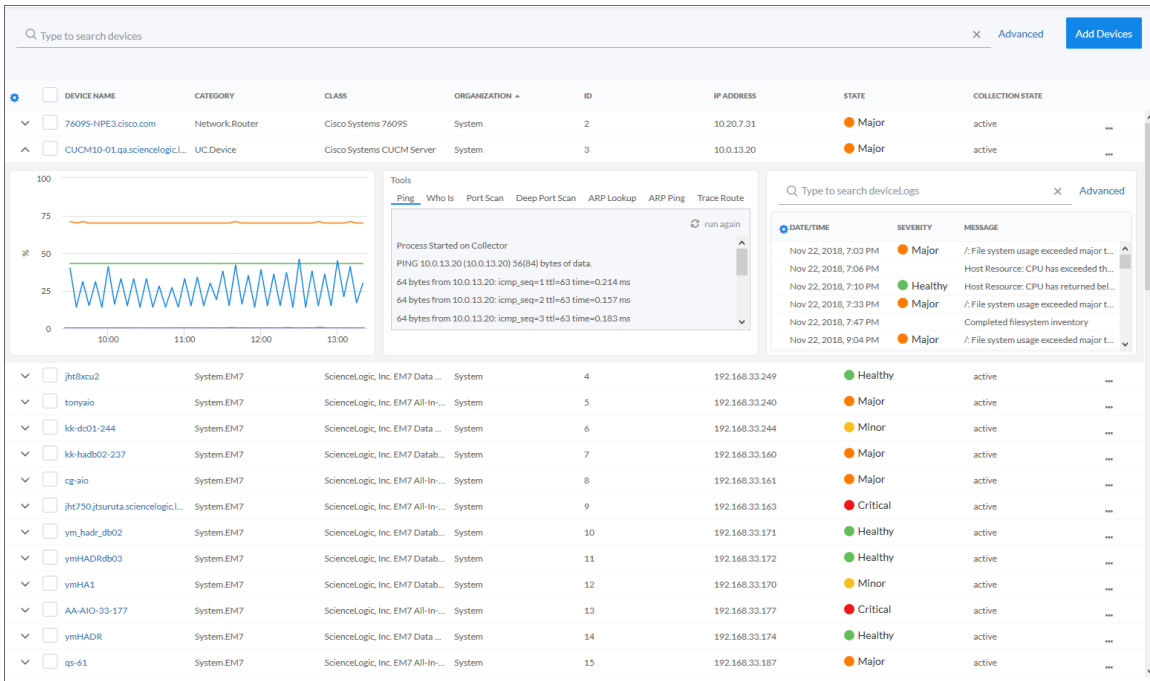
This chapter includes the following topics:

<i>Viewing Devices</i>	27
<i>Adding Devices with Discovery</i>	29
<i>Using the Device Investigator</i>	44
<i>Overview of the Device Investigator Tabs</i>	54
<i>Assigning Icons to Devices and Device Classes</i>	68
<i>Working with Device Categories</i>	71

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 ():




The screenshot displays the SL1 interface for viewing managed devices. At the top, there is a search bar with the text "Type to search devices" and an "Add Devices" button. Below the search bar is a table of devices with columns for Device Name, Category, Class, Organization, ID, IP Address, State, and Collection State. Two devices are visible: "76095-NPE3.cisco.com" (Network Router) and "CUCM10-01qa.sciencelogic.com" (UC Device), both in a "Major" state. Below the table, there are three panels: a ping graph showing a fluctuating line between 0 and 100; a "Tools" panel with options like Ping, Who Is, Port Scan, and ARP Lookup; and a "deviceLogs" panel with a search bar and a log table showing messages with dates, times, and severity levels (Major, Healthy, Minor, Critical).

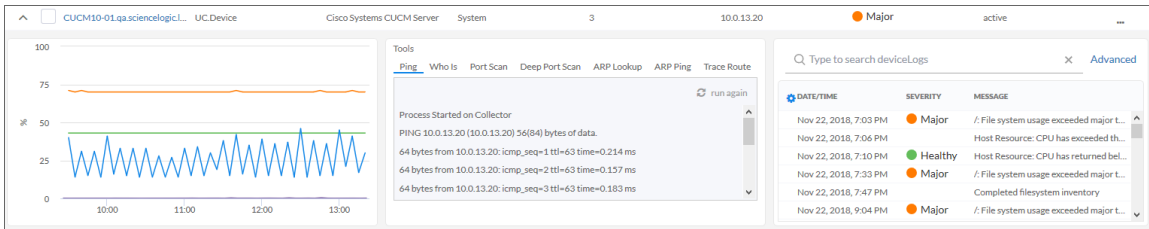
DEVICE NAME	CATEGORY	CLASS	ORGANIZATION	ID	IP ADDRESS	STATE	COLLECTION STATE
76095-NPE3.cisco.com	Network Router	Cisco Systems 76095	System	2	10.20.7.31	Major	active
CUCM10-01qa.sciencelogic.com	UC Device	Cisco Systems CUCM Server	System	3	10.0.13.20	Major	active

DATE/TIME	SEVERITY	MESSAGE
Nov 22, 2018, 7:03 PM	Major	/: File system usage exceeded major L...
Nov 22, 2018, 7:06 PM	Healthy	Host Resource: CPU has exceeded th...
Nov 22, 2018, 7:10 PM	Major	/: File system usage exceeded major L...
Nov 22, 2018, 7:33 PM	Major	/: File system usage exceeded major L...
Nov 22, 2018, 7:47 PM	Healthy	Completed filesystem inventory
Nov 22, 2018, 9:04 PM	Major	/: File system usage exceeded major L...

DEVICE NAME	CATEGORY	CLASS	ORGANIZATION	ID	IP ADDRESS	STATE	COLLECTION STATE
jht8xzu2	System.EM7	Sciencelogic, Inc. EM7 Data ...	System	4	192.168.33.249	Healthy	active
tonyalo	System.EM7	Sciencelogic, Inc. EM7 All-In...	System	5	192.168.33.240	Major	active
kk-dc01-244	System.EM7	Sciencelogic, Inc. EM7 Data ...	System	6	192.168.33.244	Minor	active
kk-hadr02-237	System.EM7	Sciencelogic, Inc. EM7 Datab...	System	7	192.168.33.160	Major	active
cg-aio	System.EM7	Sciencelogic, Inc. EM7 All-In...	System	8	192.168.33.161	Major	active
jht730.jtsuruta.sciencelogic.com	System.EM7	Sciencelogic, Inc. EM7 All-In...	System	9	192.168.33.163	Critical	active
ym_hadr_db02	System.EM7	Sciencelogic, Inc. EM7 Datab...	System	10	192.168.33.171	Healthy	active
ymHADRdb03	System.EM7	Sciencelogic, Inc. EM7 Datab...	System	11	192.168.33.172	Healthy	active
ymHA1	System.EM7	Sciencelogic, Inc. EM7 Datab...	System	12	192.168.33.170	Minor	active
AA-AIO-33-177	System.EM7	Sciencelogic, Inc. EM7 All-In...	System	13	192.168.33.177	Critical	active
ymHADR	System.EM7	Sciencelogic, Inc. EM7 Data ...	System	14	192.168.33.174	Healthy	active
qs-61	System.EM7	Sciencelogic, Inc. EM7 All-In...	System	15	192.168.33.187	Major	active

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

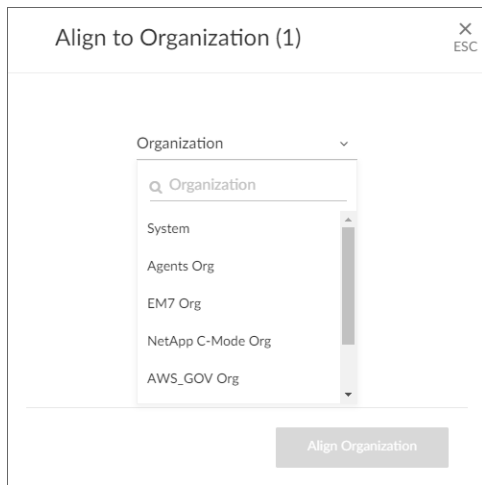
You can zoom in on a shorter time frame in the **Vitals** widget by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.

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

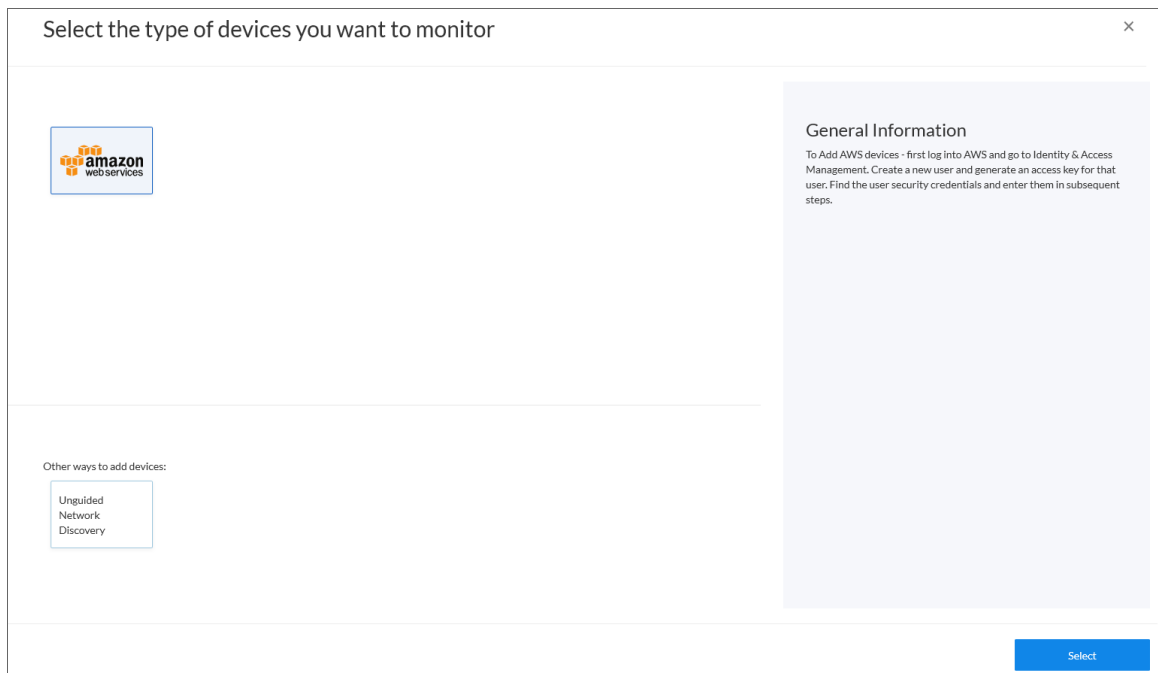
On the **Devices** page, you can add or "discover" new devices for monitoring in SL1. You add devices by creating a **discovery session**, which searches for devices on the network you specify.

You can use the Universal Discovery Framework process in SL1 that guides you through a variety of existing discovery types in addition to traditional SNMP discovery. This process lets you pick a discovery type based on the type of devices you want to monitor.

NOTE: The following procedure uses Amazon Web Services as an example of the discovery type. Some steps and fields might 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** page appears:

The screenshot shows a web interface titled "Create Guided Discovery Session" with a close button (ESC) in the top right corner. Below the title is a header "Choose credentials that connect your devices" and a "Create New" button. A table lists various credentials with columns for NAME, TYPE, and LAST EDIT. The "AWS_GOV" credential is selected with a blue checkmark. At the bottom, there are "Back" and "Next" buttons.

NAME	TYPE	LAST EDIT
<input type="checkbox"/> AppDynamics Example	SOAP/XML	Tue Feb 19 2019 19:08:49 GMT+0000 (UTC)
<input type="checkbox"/> AppDynamics Example export	SOAP/XML	Thu Mar 14 2019 16:43:44 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential - Proxy	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS Credential - Specific Region	SOAP/XML	Wed Jan 30 2019 18:15:13 GMT+0000 (UTC)
<input type="checkbox"/> AWS_COM_04	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input type="checkbox"/> AWS_COM_04-RO	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input checked="" type="checkbox"/> AWS_GOV	SOAP/XML	Tue Feb 12 2019 18:15:43 GMT+0000 (UTC)
<input type="checkbox"/> AWS_GOV Export	SOAP/XML	Thu Mar 14 2019 16:43:45 GMT+0000 (UTC)
<input type="checkbox"/> Azure Classic Credential SOAP	SOAP/XML	Wed Jan 30 2019 18:15:07 GMT+0000 (UTC)
<input type="checkbox"/> Azure Credential - Germany	SOAP/XML	Wed Jan 30 2019 18:15:34 GMT+0000 (UTC)

7. If the credential you need is not in the list, click **[Create New]** 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.

NOTE: You can also edit an existing credential on the **Credentials** page by clicking the **[Actions]** button (⋮) for the credential, selecting *Edit*, and editing that credential as needed.

8. Select a credential to allow SL1 to access a device and click **[Next]**. The **Root Device Details** page appears:

The screenshot shows a web interface titled "Create Guided Discovery Session" with a close button (X ESC) in the top right corner. The main heading is "Root Device Details". Below this, there are two input fields: "Root Device Name" with the value "AWSRootDevice" and "Collector Group Name" with a dropdown arrow. Under the "Collector Group Name" field, there is a search bar with the text "Q Search Collectors" and a list of results showing "CUG1 | fh-sl1-ranch-cu-37:10.2.18.37". At the bottom left, there is a "← Back" button, and at the bottom right, there is a "Create Discovery Session" button.

9. 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.

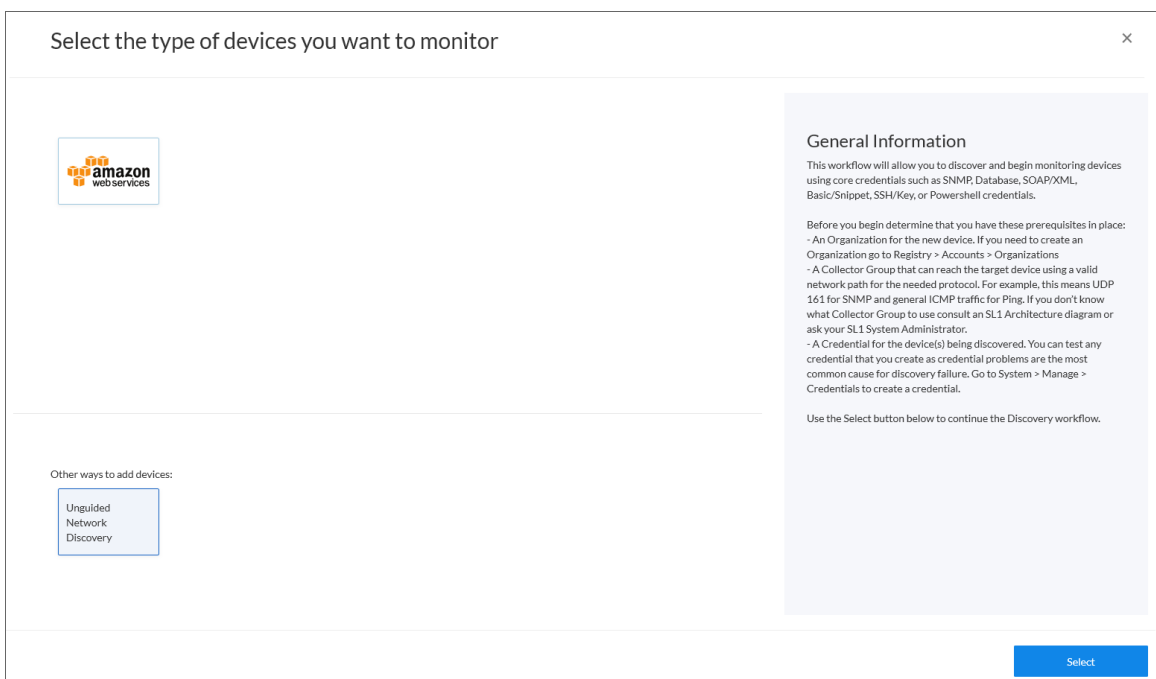
10. Click the **[Create Discovery Session]** button. A summary of the new discovery session appears on this page.
11. Click **[Close]**. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.

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.

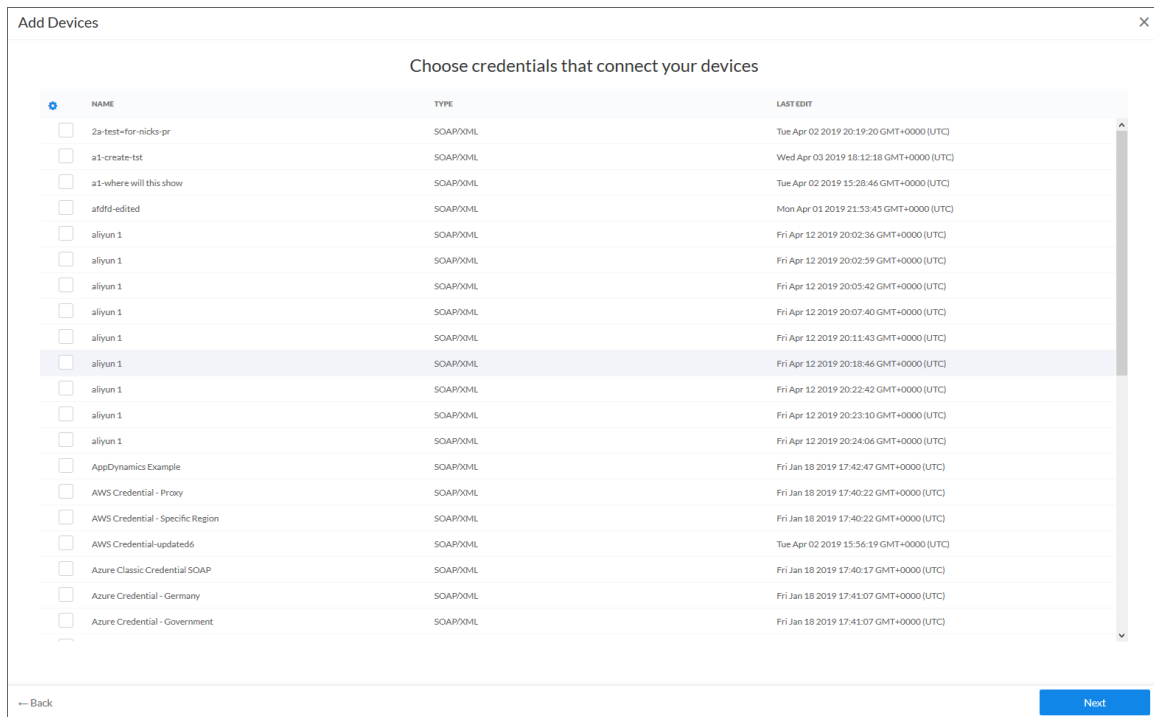
To run an unguided discovery:

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

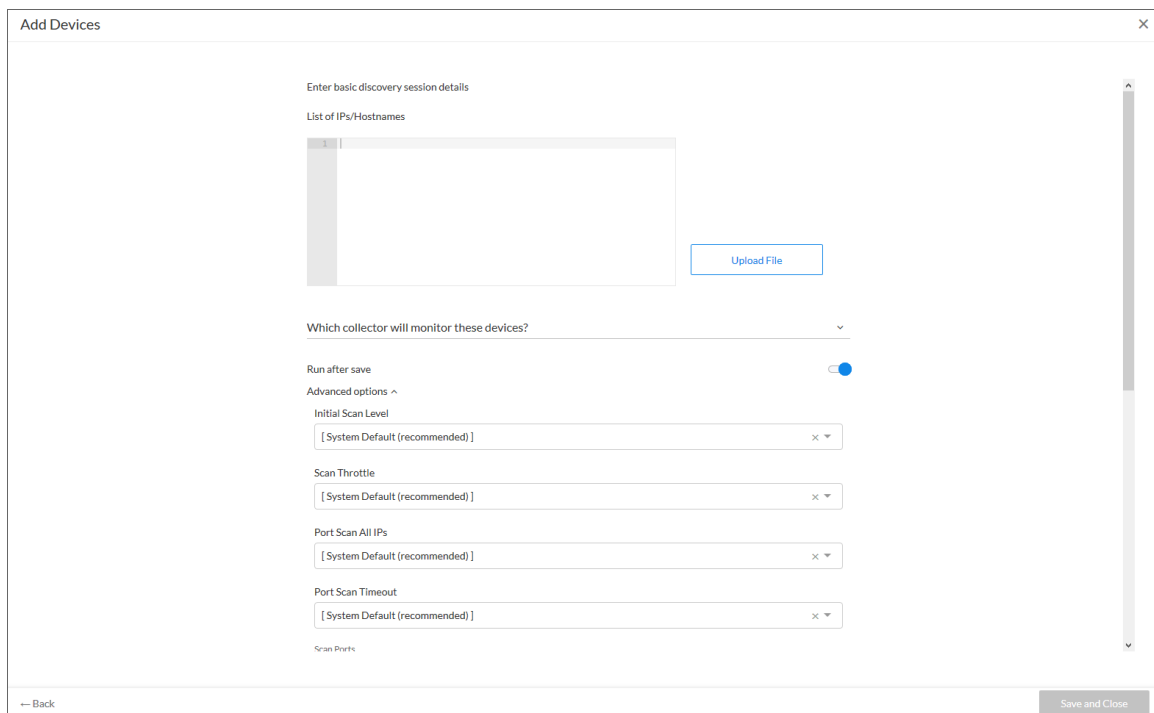


2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:
 - **Name**. Type a unique name for this 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. Select one or more SNMP credentials to allow SL1 to access a device's SNMP data and click **[Next]**. The Discovery Session Details page of the **Add Devices** wizard appears:



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

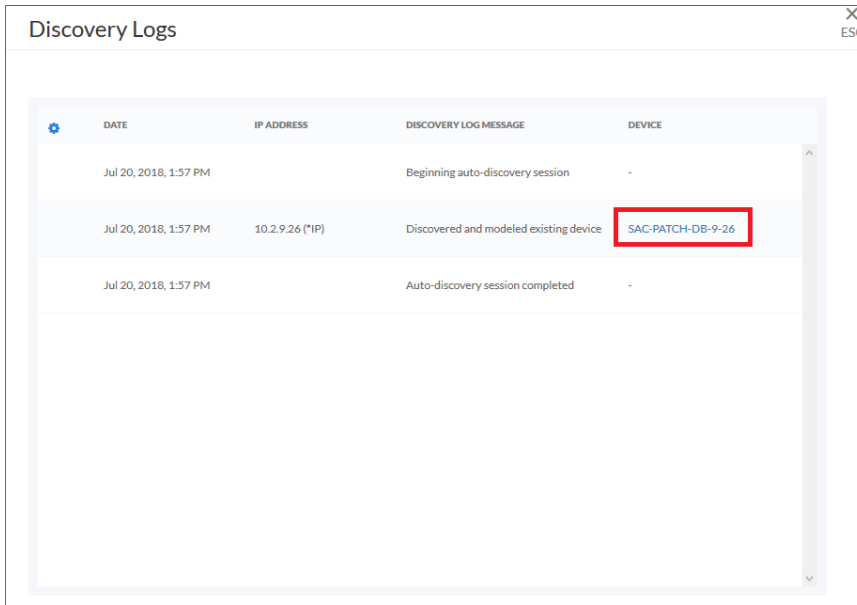
NOTE: For devices that don't support SNMP, option 6. *Deep Discovery* allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option 6. *Deep Discovery* is compute-intensive.

- **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**.

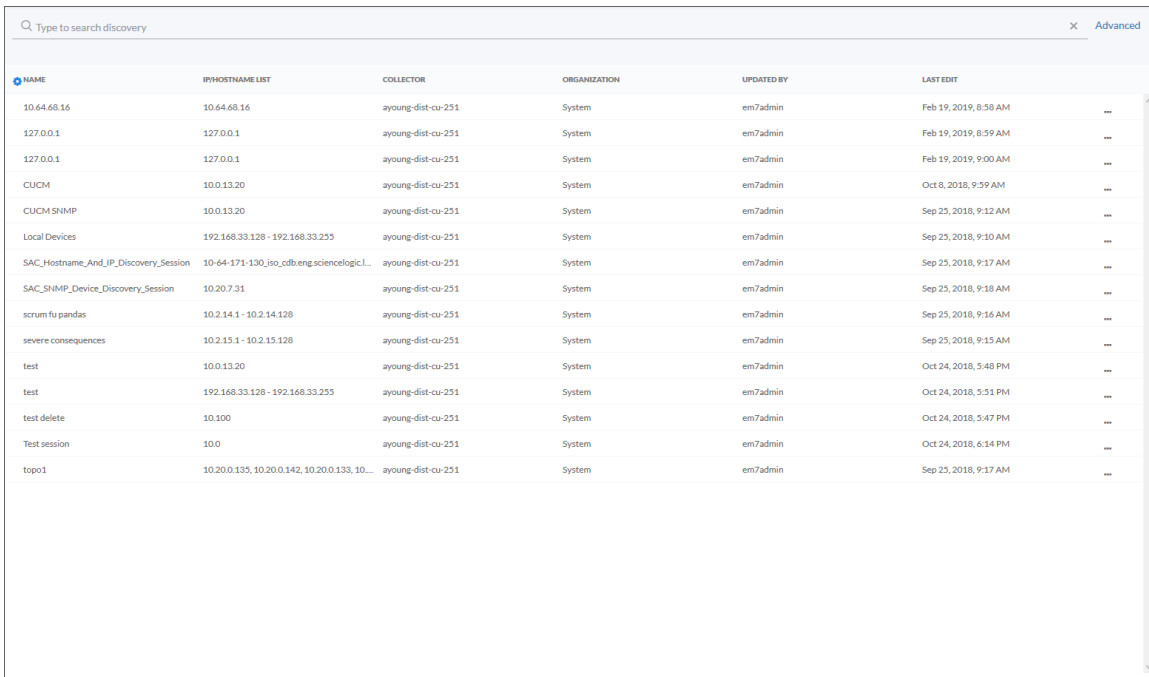
8. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
9. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant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



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

Working with Discovery Sessions

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



NAME	IP/HOSTNAME LIST	COLLECTOR	ORGANIZATION	UPDATED BY	LAST EDIT	
10.64.68.16	10.64.68.16	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 8:58 AM	...
127.0.0.1	127.0.0.1	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 8:59 AM	...
127.0.0.1	127.0.0.1	ayoung-dist-cu-251	System	em7admin	Feb 19, 2019, 9:00 AM	...
CUCM	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Oct 8, 2018, 9:59 AM	...
CUCM SNMP	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:12 AM	...
Local Devices	192.168.33.128 - 192.168.33.255	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:10 AM	...
SAC_Hostname_And_IP_Discovery_Session	10-64-171-130_iso_cdb.eng.sciencelogic...	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:17 AM	...
SAC_SNMP_Device_Discovery_Session	10.20.7.31	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:18 AM	...
scrum fu pandas	10.2.14.1 - 10.2.14.128	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:16 AM	...
severe consequences	10.2.15.1 - 10.2.15.128	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:15 AM	...
test	10.0.13.20	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:48 PM	...
test	192.168.33.128 - 192.168.33.255	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:51 PM	...
test delete	10.100	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 5:47 PM	...
Test session	10.0	ayoung-dist-cu-251	System	em7admin	Oct 24, 2018, 6:14 PM	...
topo1	10.20.0.135, 10.20.0.142, 10.20.0.133, 10...	ayoung-dist-cu-251	System	em7admin	Sep 25, 2018, 9:17 AM	...

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 screenshot displays the Device Investigator interface for the device `SILO.qa.sciencelogic.local`. The top navigation bar includes 'Info', 'Last 24 Hours', 'Compare Device', and 'Tools'. The main navigation tabs are 'Investigator', 'Interfaces', 'Configs', 'Events', and 'Collections'. The left sidebar shows the 'Device List' for `SILO.qa.sciencelogic.local` with a search bar and a 'Vitals' section containing 'Latency (s)' and 'CPU Utilization (%)'. The main content area is divided into three sections: 'Logs' (30 of 10238), 'Vitals: CPU Utilization (%)', and 'Vitals: Latency (s)'. The 'Logs' section contains a table of log entries:

DEVICE NAME	DATE/TIME	SOURCE	SEVERITY	MESSAGE
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'cluster_mgmt' has moved from i...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif06' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif04' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'cluster_mgmt' has moved from i...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif06' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif04' has moved from its ...

The 'Vitals: CPU Utilization (%)' chart shows a line graph with a y-axis from 0 to 100 and an x-axis from 18:00 to 15:00. The utilization is mostly low, with a spike to approximately 25% between 01:00 and 05:00. The 'Vitals: Latency (s)' chart is partially visible at the bottom.

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

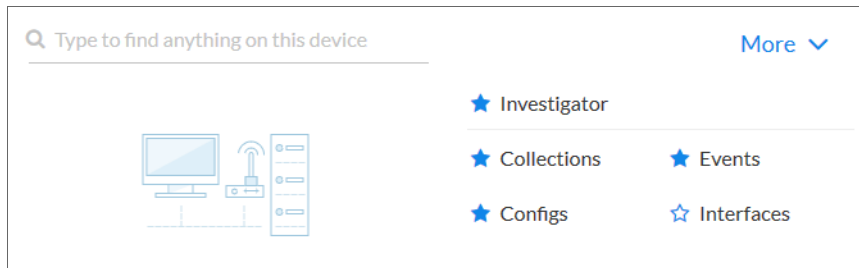
The **Device Investigator** page contains the following menus and buttons, which are available on all of the tabs:

- **Info**. This drop-down list 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 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 lets you select one or more devices on the **[Investigator]** tab to compare with the device you have currently selected.
- **Tools**. This button opens the **Tools** pane, which provides access to a set of network tools.
- **Combine Charts**. This option 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:

- **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.
- **Collections**. Displays a list of all Dynamic Applications aligned with a device.
- **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 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.
- **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.
- **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.
- **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**. This tab 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 list lets you search for and 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** dropdown list. You can also highlight search results using the Up and Down Arrow keys, and you can select a result by pressing **Enter**.

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 in the right-hand pane of the page.

The screenshot shows the 'Device Investigator' interface for the device 'SILO.qa.sciencelogic.local'. The 'Device List' pane on the left shows 'Logs' selected. The main area displays a 'Logs' table with the following data:

DEVICE NAME	DATE/TIME	SOURCE	SEVERITY	MESSAGE
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'cluster_mgmt' has moved from i...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif06' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:17 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif04' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'cluster_mgmt' has moved from i...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif06' has moved from its ...
SILO.qa.sciencelogic.local	Apr 1, 2019, 3:03 PM	dynamic	Minor	Netapp: Cluster Logical Interface 'TEST_lif04' has moved from its ...

Below the logs is a 'Vitals: CPU Utilization (%)' line chart showing a spike in utilization around 03:00. An 'Expand' button is visible below the chart.

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

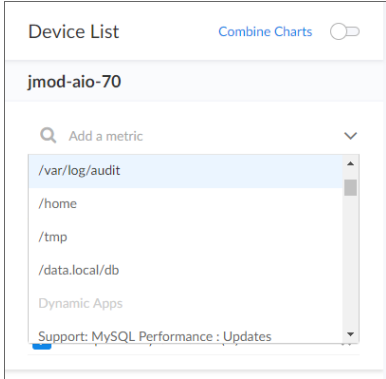
- **Logs**. Displays a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting. You can also click on the column headers for **Date/Time**, **Source**, **Event ID**, **Severity**, and **Message** to sort by that column.

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

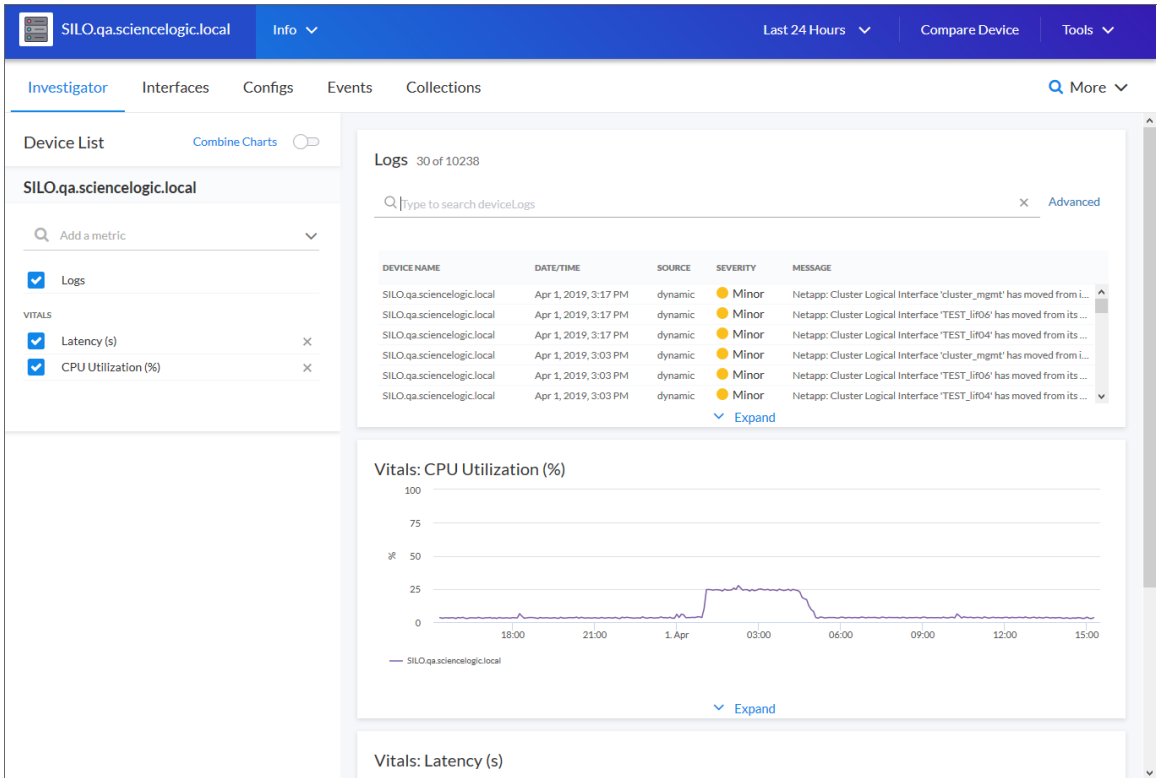
- **Latency**. Displays a widget for latency for the device over time, in milliseconds. Latency means the amount of time it takes SL1 to communicate with the device.
- **CPU Utilization**. Displays a widget for the total amount of CPU used over time, as a percentage of all available CPU.
- **Physical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



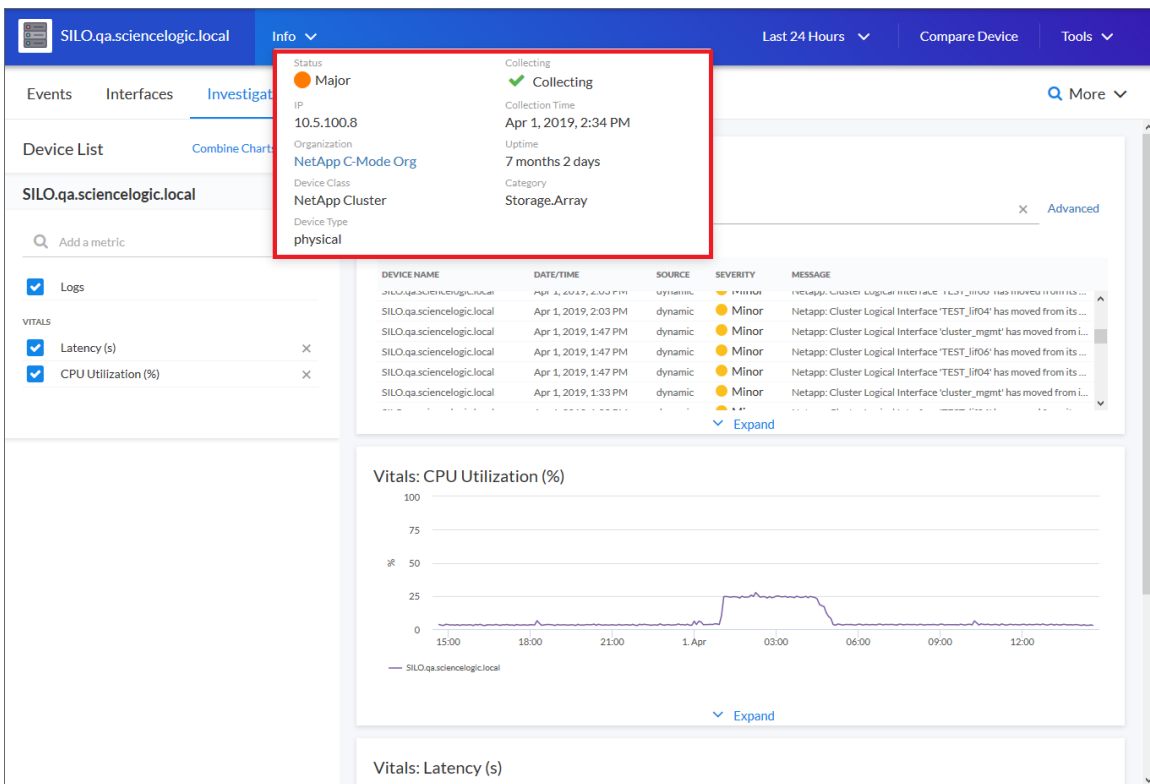
3. Some metrics might require you to make additional selections, such as the network interfaces associated with a device. Click the field and add one or more additional metrics, as needed.

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

- 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.
- To completely remove the metric and the widget from the **[Investigator]** tab, click the **[Clear]** button (✕) for that metric in the **Device List** pane.

The Info Drop-Down

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.

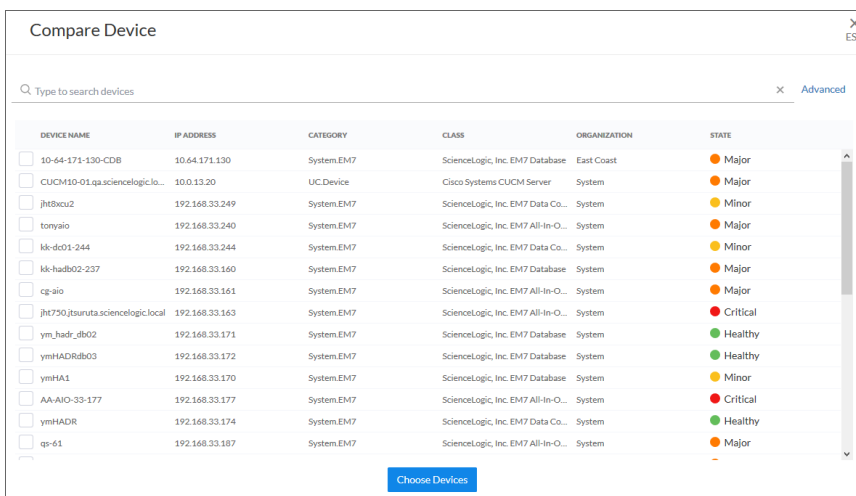
- **IP.** IP address of the device.
- **Collection Time.** Date and time of the most recent collection.
- **Organization.** The organization to which this device belongs. Click the organization name to view a detail page for the organization.
- **Uptime.** The number of days and hours that the device 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.

Comparing Devices on the Investigator Tab

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

To compare devices:

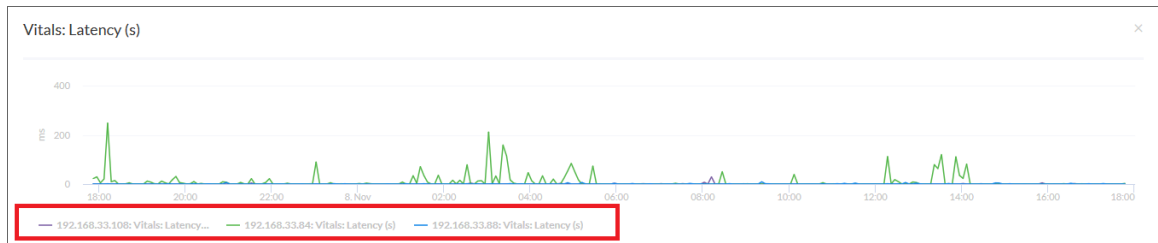
1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Compare Device]** button. The **Compare Device** modal page appears:




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.

- 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:

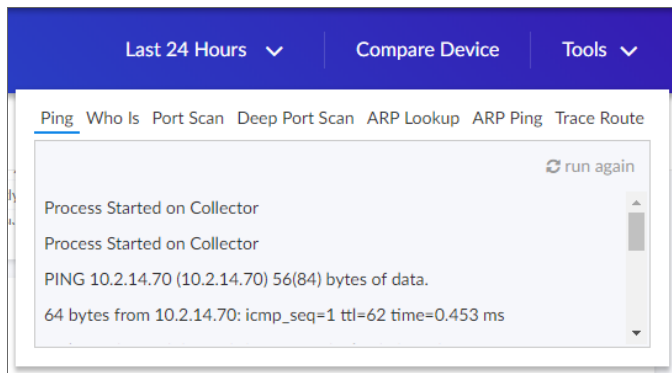


- To remove a device from a graph, click the device name in the legend on the x-axis of the graph. You can click the device name again to add the device back to the graph.
- To add more metrics, click the **Add a metric** field under each device and select the metrics.
- To remove a device from the Device 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 for a device, you can click the **Tools** menu to display the **Tools** panel. The **Tools** panel provides access to a set of network tools. The **Tools** panel lets you to run diagnostics on a device without leaving the the new user interface.



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

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

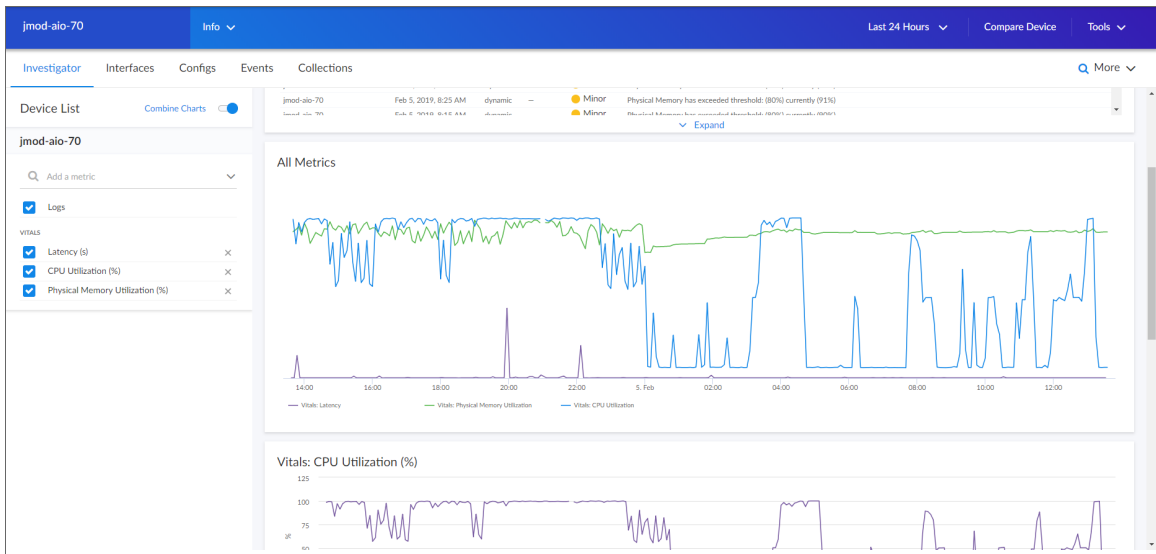
- **Ping**. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by SL1 to communicate with the device) and waits for a reply. SL1 then displays the number of seconds it took to receive a reply from the device and the number of bytes returned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

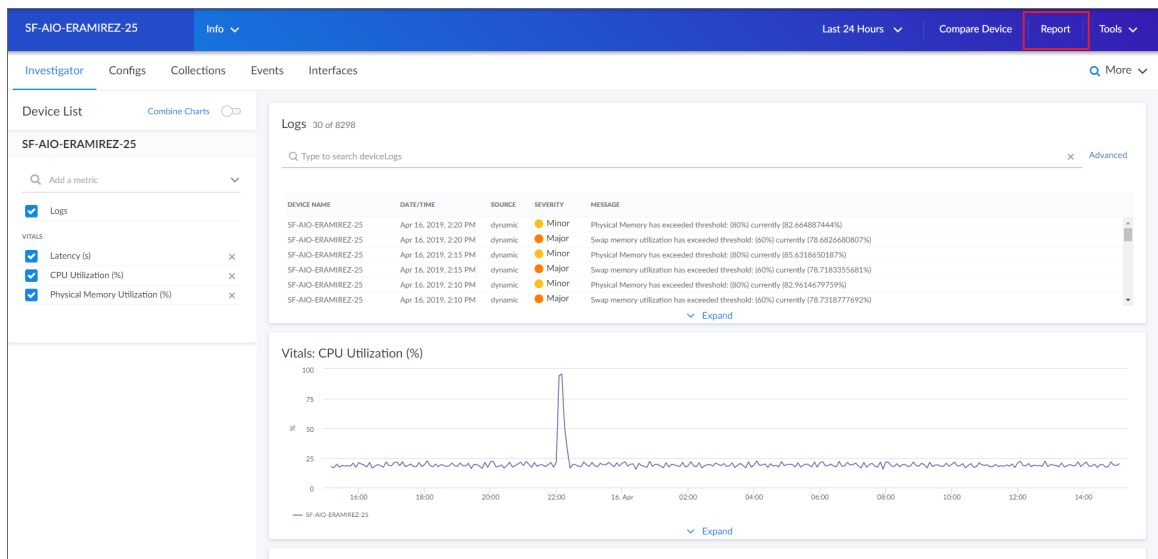


- To hide a metric from the **All Metrics** chart, click the metric label in the legend on the graph's x-axis. You can click the metric label again to add the metric back to the graph.
- You can also [compare devices](#) and view all of the compared devices in a combined chart:



Running a Device Report

From the **Device Investigator** page, you can generate a detailed report on that device. You can specify the information to include in the report (Full Report, Status, Processes, 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).



- On the **Device Investigator** page, click the **[Report]** button. The **Device Report** modal page appears.:

2. In the **Select Type** drop-down, select the type of report you want to generate. You can select *Full Report*, or 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 the **[Create Report]** button 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]**.

The screenshot displays the 'Settings' tab for a device named 'fh-s11-ranch-sn2-35'. The interface is organized into several sections:

- COLLECTION:** Includes 'Enable Collection' (checked), 'Collection Poller Agents' (dropdown), and 'Collection Type Standard' (dropdown).
- MONITORING:** Includes 'SNMP Read' (none), 'SNMP Write' (none), 'Availability Protocol TCP', 'Availability Port 161 - SNMP', 'Latency Protocol TCP', 'Latency Port ICMP', and 'Auto-Update' (checked).
- USER MAINTENANCE:** Includes 'Enable User Maintenance' (unchecked) and 'Enable Collection During Maintenance' (checked).
- ALERTS AND EVENTS:** Includes 'Event Mask Every 10 Minutes' (dropdown), 'Always Create Latency Alert' (unchecked), 'Allow Events to Auto-Clear' (checked), and 'Critical Ping Disabled' (dropdown).
- OTHER PREFERENCES:** Includes 'Accept All Logs' (checked), 'Daily Port Scans' (checked), 'Preserve Device Name' (checked), 'Disable Asset Update' (unchecked), 'Bypass Interface Inventory' (unchecked), and 'Dynamic Discovery' (checked).

Set the following collection preferences:

- **Enable Collection State.** Select this option to enable collection using the collector group specified in the following field.
- **Collection Provider.** 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.

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 Maintenance Collection.** 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.

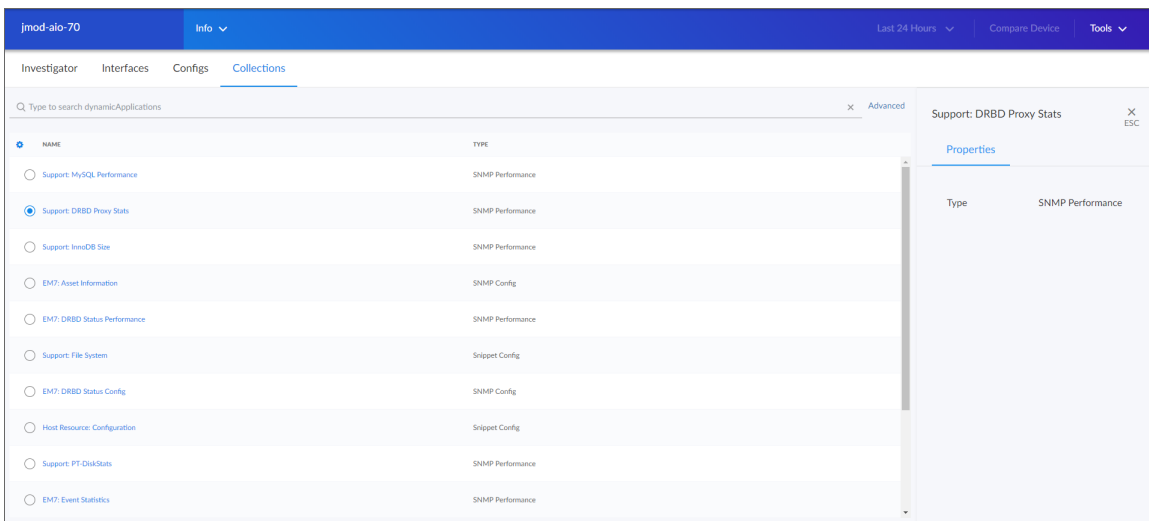
Set the following device preferences:

- **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 each device in the discovery session.
 - *Not Selected.* SL1 will attempt to discover network interfaces.
- **Dynamic Discovery.** If selected, SL1 will automatically assign the appropriate dynamic applications to the device during discovery.

The Collections Tab

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



The Configs Tab

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

The screenshot shows the Cisco Device Investigator interface for a device named 7609S-NPE3.cisco.com. The 'Configs' tab is active, displaying a list of Dynamic Applications on the left and configuration details on the right. The left pane shows 'Cisco: VLAN Configuration' selected. The right pane displays 'Cisco: VLAN Configuration - VLAN Information' and 'Cisco: VLAN Configuration - VTP Statistics'.

VLAN MTU	VLAN NAME	VLAN TYPE	VLAN STATE	VLAN ID
1500	default	ethernet	operational	1
1500	VLAN0110	ethernet	operational	110
1500	VLAN0120	ethernet	operational	120
1500	VLAN0130	ethernet	operational	130
1500	fddi-default	fddi	operational	1002
1500	token-ring-default	tokenRing	operational	1003

CONFIG DIGEST ERRORS	CONFIG REVISION NUMBER	ERR	IN ADVERTISE REQUESTS	IN SUBSET ADVERTISES	IN SUMMARY ADVERTISES	OUT ADVERTISE REQUESTS	OUT SUBSET ADVERTISES	OUT SUMMARY ADVERTISES
166526	169849		104538	68935	35231	168572	166330	136132

MODEL NAME	NAME	ADMIN STATUS	OPERATION STATUS	STATE CHANGE REASON	STATUS TRANSITION TIME	SERIAL NUMBER
7600-ES-4TG3CXL	module 3	Enabled	ok		31 days, 1:25:13	JAE1340K3IQ

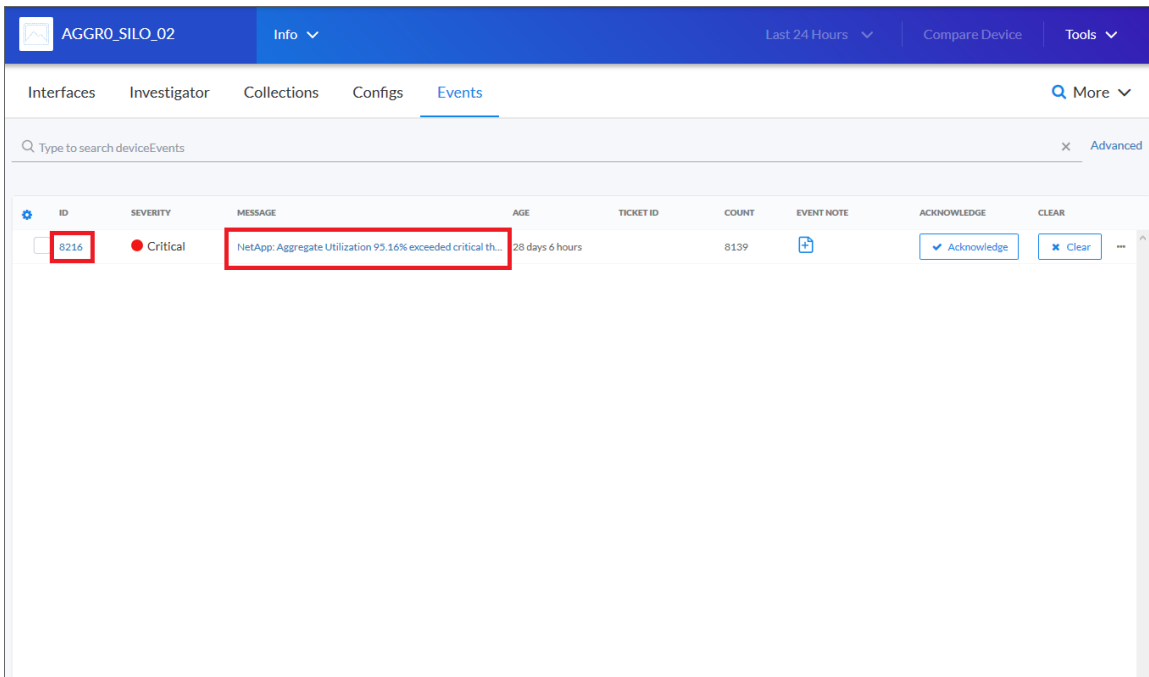
The pane on the left displays a list of Dynamic Applications associated with the device. To view the configuration data collected by a Dynamic Application, select it from the **Dynamic Apps** section on the left.

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. You can search by each field on the **[Events]** tab on the **Device Investigator** page.



ID	SEVERITY	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	ACKNOWLEDGE	CLEAR
8216	Critical	NetApp: Aggregate Utilization 95.16% exceeded critical th...	28 days 6 hours		8139		<input type="button" value="Acknowledge"/>	<input type="button" value="Clear"/>

TIP: To view the **Event Investigator** page for an event on this tab, click the linked text in the **ID** or the **Message** column, or click the **Actions** button (☰) for that event and select *View Event*.

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

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.

INTERFACE NAME	ALIAS	PORT	HARDWARE DESCRIPTION	MAC ADDRESS	CONNECTION SPEED	COLLECTION STATE	ADMIN STATUS	OPERATIONAL STATUS	COLLECTION RATE	COLLECT ERRORS	COLLECT DISCARD	ALERTS	ROLLOVER ALERT	INTERFACE INDEX
BR3/172		87	BRIDGE3/172	00:24:F9:4e:c0:e5	1447	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	87
BR3/286		88	BRIDGE3/286	00:24:F9:4e:c0:e6	895	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	88
BR3/400		89	BRIDGE3/400	00:24:F9:4e:c0:e7	1629	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	89
BR3/58		86	BRIDGE3/58	00:24:F9:4e:c0:e4	1139	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	86
BR4/170		64	BRIDGE4/170	00:24:F9:4c:80:e9	348	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	64
BR4/172		83	BRIDGE4/172	00:24:F9:4c:80:75	1000	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	83
BR4/286		84	BRIDGE4/286	00:24:F9:4c:80:76	958	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	84
BR4/400		85	BRIDGE4/400	00:24:F9:4c:80:77	254	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	85
BR4/58		82	BRIDGE4/58	00:24:F9:4c:80:74	994	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	82
CPP		69	Control Plane	00:00:00:00:00:00	9288	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	69
EO0/0		50	EOBC0/0	00:00:15:00:00:00	70	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	50
EO0/2		51	EOBC0/2	00:00:00:00:00:00	520	Enabled	Down	Down	5	Disabled	Disabled	Enabled	Disabled	51
Gi4/1		5	GigabitEthernet...	00:24:14:4b:48:...	226	Enabled	Down	Up	5	Disabled	Disabled	Enabled	Disabled	5
Gi4/1.S1.110	***VLAN 110-E...	62	GigabitEthernet...		499	Enabled	Down	Up	5	Disabled	Disabled	Enabled	Disabled	62
Gi4/1.S1.120	***VLAN 120-E...	63	GigabitEthernet...		26	Enabled	Down	Up	5	Disabled	Disabled	Enabled	Disabled	63
Gi4/1.S1.130	***VLAN 130-E...	65	GigabitEthernet...		2595	Enabled	Down	Up	5	Disabled	Disabled	Enabled	Disabled	65

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.

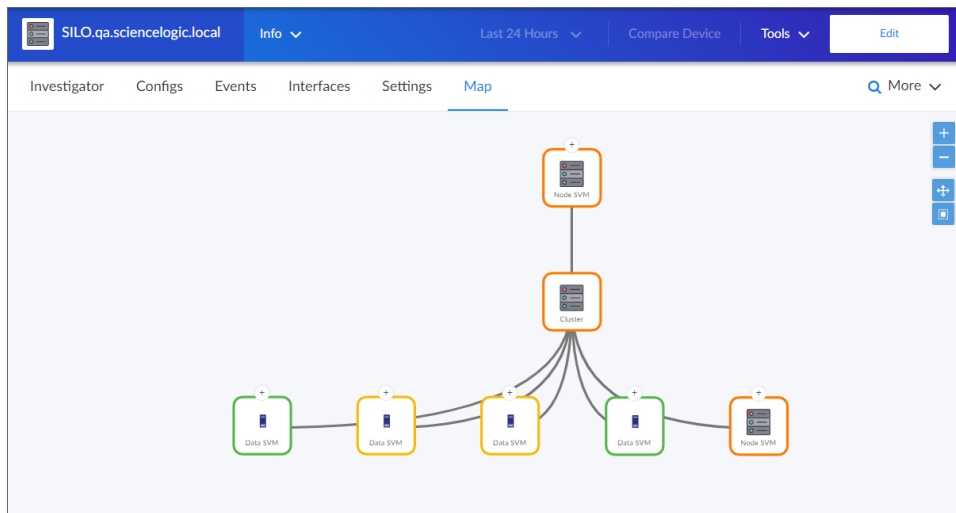
The Journals Tab

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 details on Maps, see the **Maps** manual.



The Monitors Tab

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

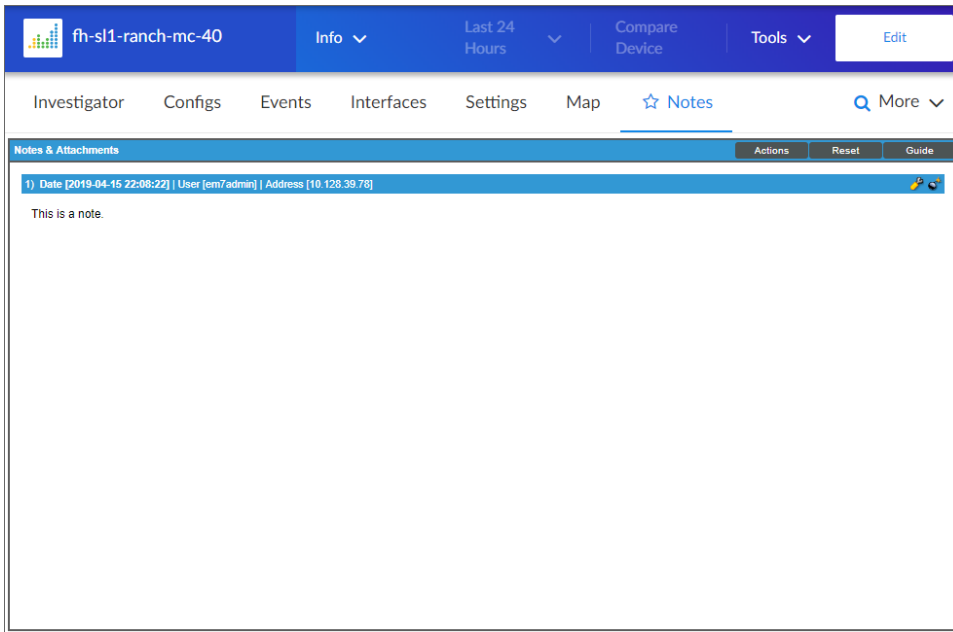
The **Monitoring Policies** page allows you to define policies that monitor:

- **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 system process.

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. For more details, see the section on [Adding a Note to a Device](#).



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.

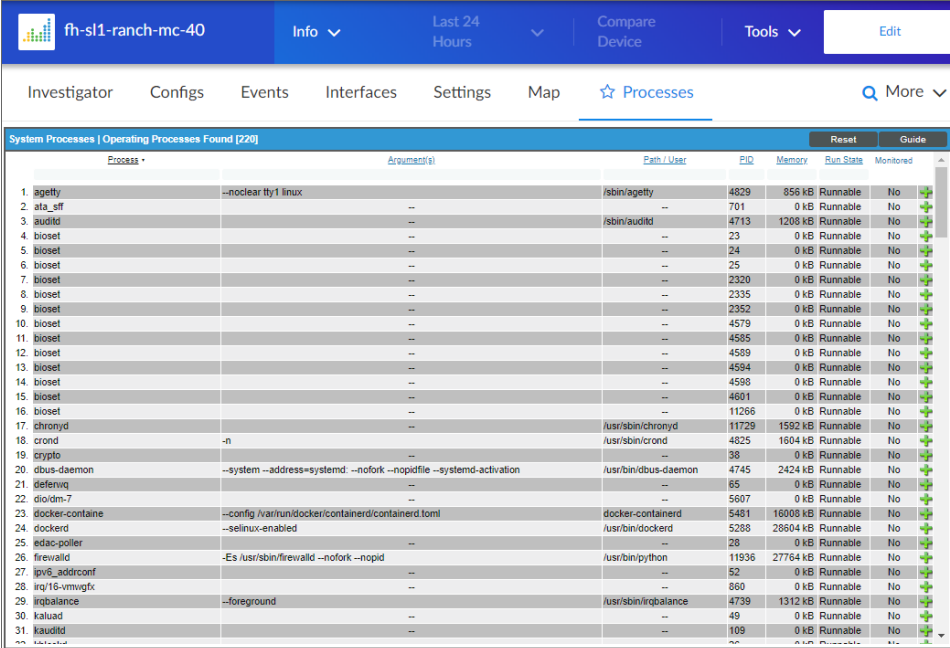
The screenshot shows the 'Ports' tab in the Device Investigator interface. The top navigation bar includes the device name 'SILO.qa.sciencelogic.local' and several dropdown menus: 'Info', 'Last 24 Hours', 'Compare Device', and 'Tools'. Below this, a secondary navigation bar contains 'Investigator', 'Configs', 'Events', 'Interfaces', 'Settings', 'Map', and 'Ports' (which is highlighted). The main content area is titled 'Port Security | Port Scan Results' and contains a table with the following data:

	Interface IP	Port Number	Service	Protocol	Certificate Issuer	Cert Expiration
1.	10.5.100.8	22	ssh	TCP	--	--
2.	10.5.100.8	80	http	TCP	--	--
3.	10.5.100.8	111	snmpc	TCP	--	--
4.	10.5.100.8	443	https	TCP	--	2016-04-27 10:10:44
5.	10.5.100.8	10000	snmp-sensor-mgmt	TCP	--	--
6.	10.5.100.8	30000		TCP	--	--

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 **System Processes** page helps you manage processes on your device. The System Processes page allows you to easily view details about each process running on the device.

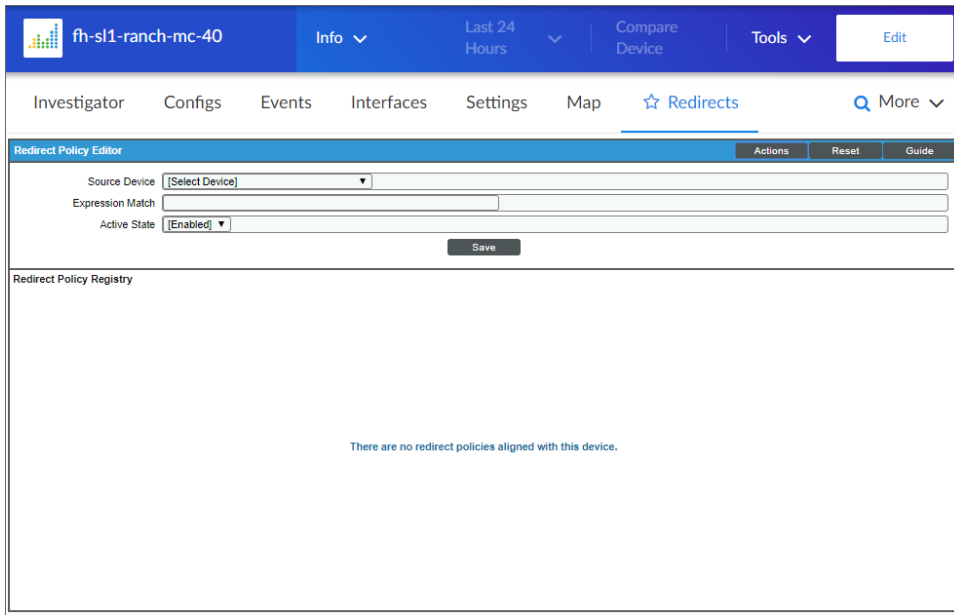


The screenshot shows the 'System Processes | Operating Processes Found [220]' interface. It features a table with columns for Process, Arguments, Path/User, PID, Memory, Exit State, and Monitored. The table lists various system processes such as agetty, ata_sff, auditd, bioset, chrontyd, crond, crypto, dbus-daemon, defernq, systemd-7, docker-containe, dockerd, fdac-poller, firewalld, ipv6_addrconf, irq/16-vmwgfx, irqbalance, kaload, and kauditd. Each row includes a process name, its command-line arguments, the path and user it runs as, its PID, memory usage, and its current state (e.g., Runnable).

Process	Arguments	Path/User	PID	Memory	Exit State	Monitored
1 agetty	--noclear tty1 linux	/sbin/agetty	4829	856 kB	Runnable	No
2 ata_sff	--	--	701	0 kB	Runnable	No
3 auditd	--	/sbin/auditd	4713	1208 kB	Runnable	No
4 bioset	--	--	23	0 kB	Runnable	No
5 bioset	--	--	24	0 kB	Runnable	No
6 bioset	--	--	25	0 kB	Runnable	No
7 bioset	--	--	2320	0 kB	Runnable	No
8 bioset	--	--	2335	0 kB	Runnable	No
9 bioset	--	--	2352	0 kB	Runnable	No
10 bioset	--	--	4579	0 kB	Runnable	No
11 bioset	--	--	4585	0 kB	Runnable	No
12 bioset	--	--	4589	0 kB	Runnable	No
13 bioset	--	--	4594	0 kB	Runnable	No
14 bioset	--	--	4598	0 kB	Runnable	No
15 bioset	--	--	4601	0 kB	Runnable	No
16 bioset	--	--	11266	0 kB	Runnable	No
17 chrontyd	--	/usr/sbin/chrontyd	11729	1592 kB	Runnable	No
18 crond	-n	/usr/sbin/crond	4825	1604 kB	Runnable	No
19 crypto	--	--	38	0 kB	Runnable	No
20 dbus-daemon	--system --address=systemd: --nofork --nopidfile --systemd-activation	/usr/bin/dbus-daemon	4745	2424 kB	Runnable	No
21 defernq	--	--	85	0 kB	Runnable	No
22 systemd-7	--	--	5607	0 kB	Runnable	No
23 docker-containe	--config /var/run/docker/containerd/containerd.toml	docker-containerd	5481	16008 kB	Runnable	No
24 dockerd	--selinux-enabled	/usr/bin/dockerd	5288	28604 kB	Runnable	No
25 fdac-poller	--	--	28	0 kB	Runnable	No
26 firewalld	-Es /usr/sbin/firewalld --nofork --nopid	/usr/bin/python	11936	27764 kB	Runnable	No
27 ipv6_addrconf	--	--	52	0 kB	Runnable	No
28 irq/16-vmwgfx	--	--	860	0 kB	Runnable	No
29 irqbalance	--foreground	/usr/sbin/irqbalance	4739	1312 kB	Runnable	No
30 kaload	--	--	49	0 kB	Runnable	No
31 kauditd	--	--	109	0 kB	Runnable	No

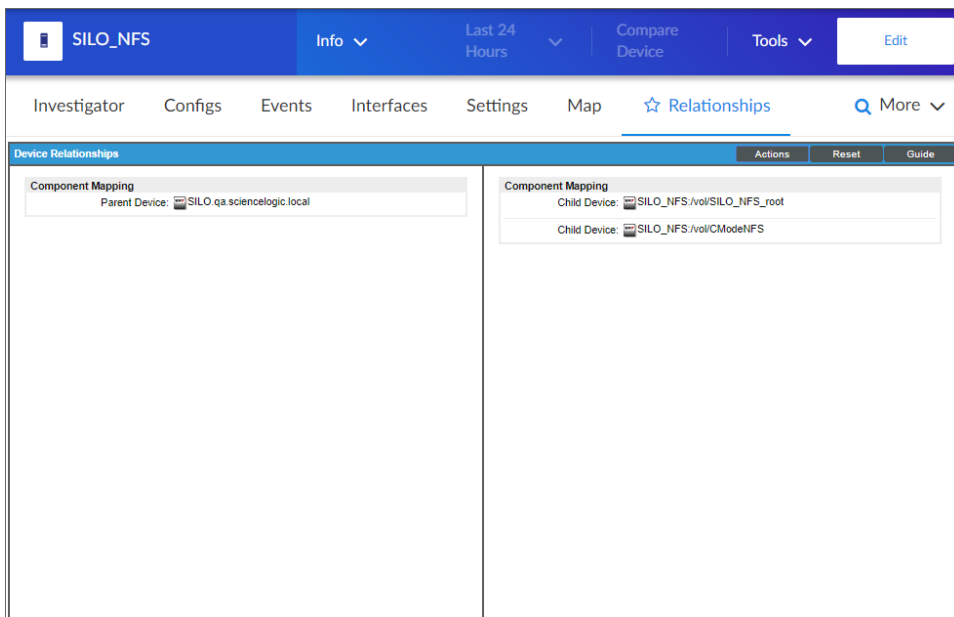
The Redirects Tab

On the **[Redirects]** tab of the **Device Investigator** page, you can redirect log entries from an IP-based device to a virtual device. For details on virtual devices, see the chapter on [Virtual Devices](#).



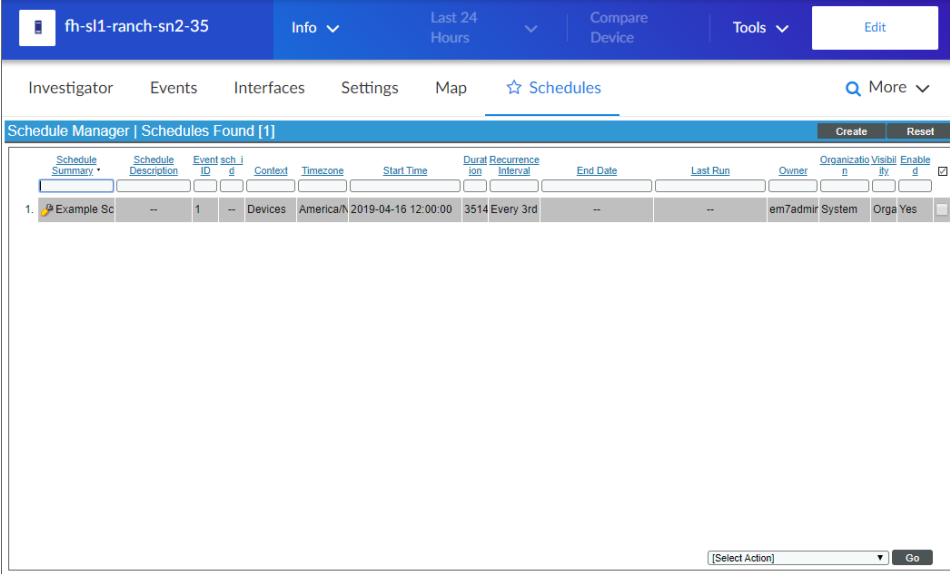
The Relationships Tab

The **[Relationships]** tab of the **Device Investigator** page displays information about parent-child relationships between devices. For details on device relationships, see the chapter on [Defining Device Relationships](#).



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. For details on scheduling maintenance for a device, see the chapter on [Maintenance](#).



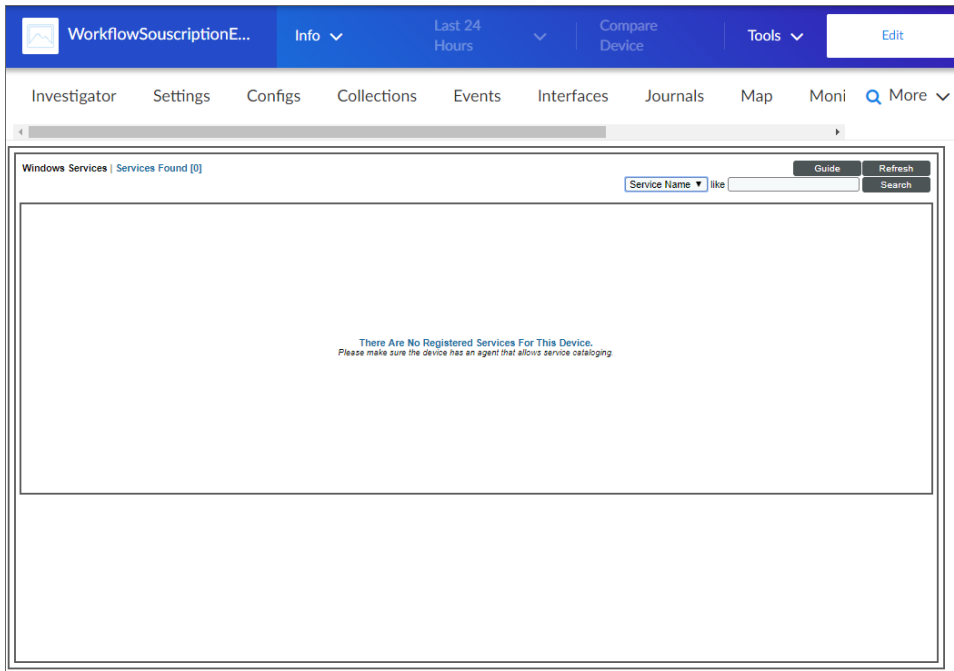
The screenshot shows the 'Schedules' tab in the Device Investigator interface. The top navigation bar includes 'Investigator', 'Events', 'Interfaces', 'Settings', 'Map', and 'Schedules'. Below the navigation, there is a 'Schedule Manager' section with 'Schedules Found [1]'. A table lists the scheduled tasks with the following columns: Schedule Summary, Schedule Description, Event ID, Schedule ID, Context, Timezone, Start Time, Duration, Recurrence Interval, End Date, Last Run, Owner, Organization, Visibility, and Enable. A single entry is visible in the table.

Schedule Summary	Schedule Description	Event ID	Schedule ID	Context	Timezone	Start Time	Duration	Recurrence Interval	End Date	Last Run	Owner	Organization	Visibility	Enable
1. Example Sc	--	1	--	Devices	America\N	2019-04-16 12:00:00	3514	Every 3rd	--	--	am7admin	System	Orga	Yes

The Services Tab

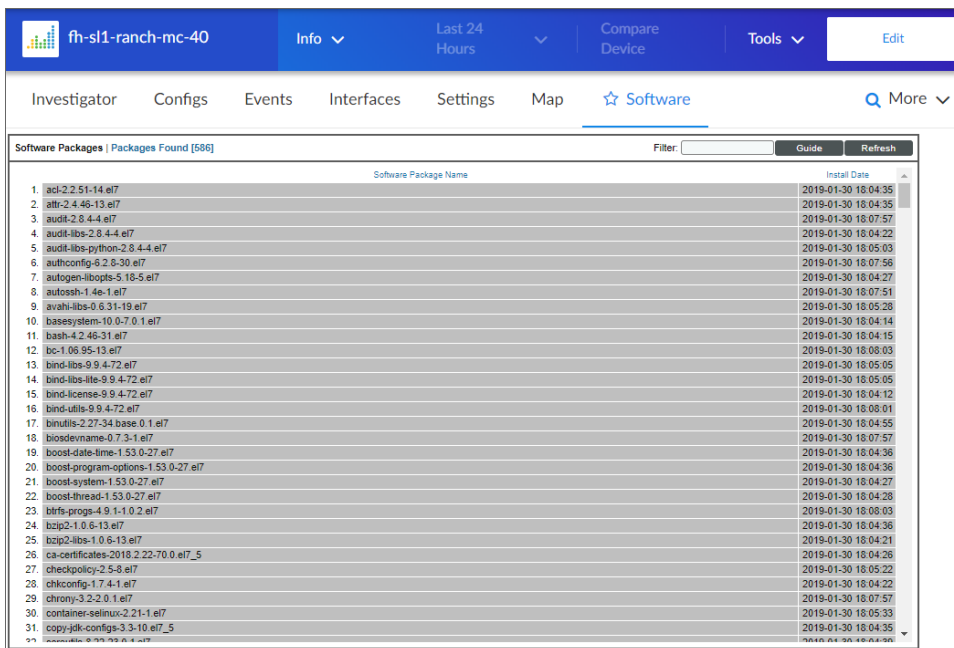
The **[Services]** tab in the **Device Investigator** page displays a list of all Windows services enabled on the device. Windows Services are long-running applications. These applications typically do not have a user interface or produce any visual output. Any messages associated with the service are 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 **Windows Services** page helps you manage services on your device. The **Windows Services** page allows you to easily view details on all the services running on the device.



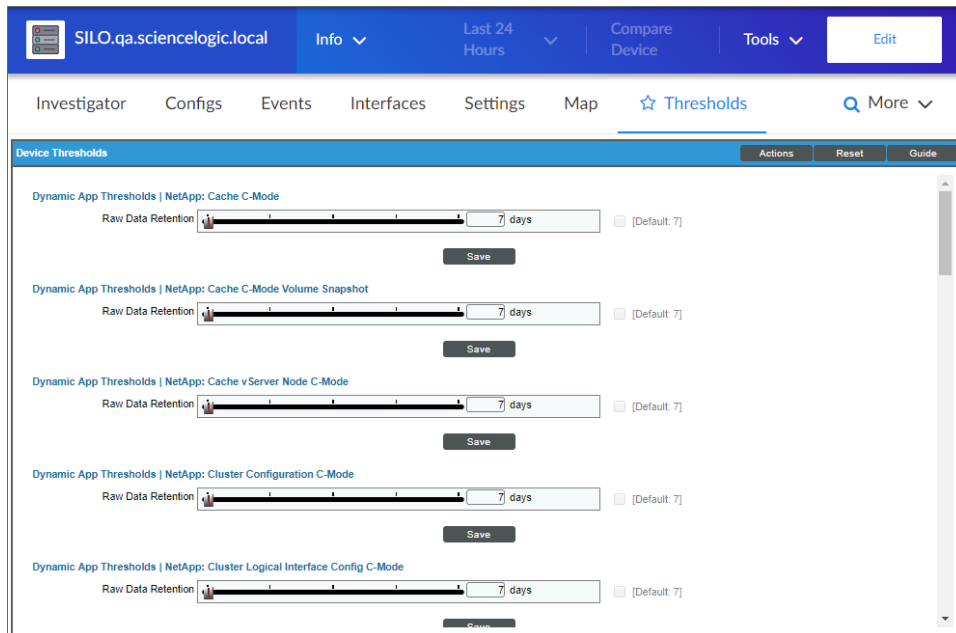
The Software Tab

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.




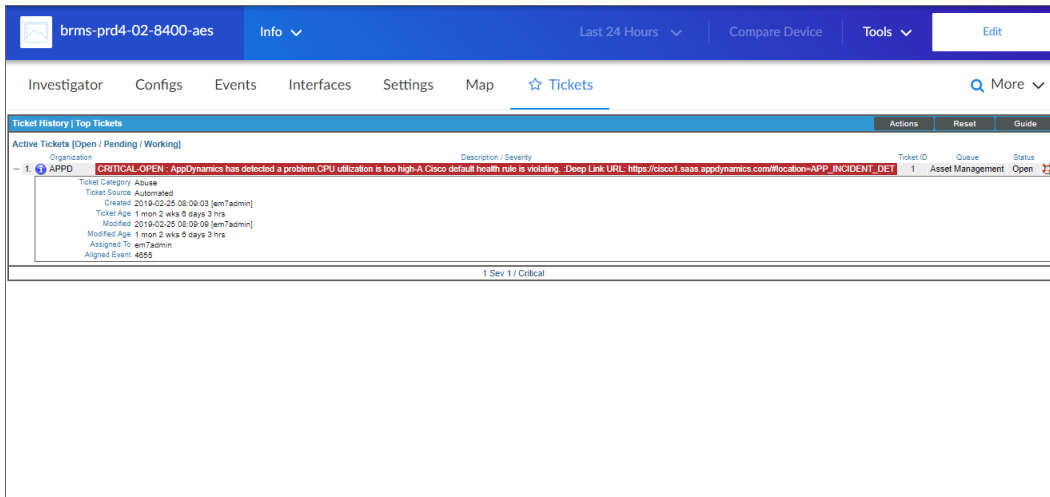
The Thresholds Tab

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. For details on device thresholds, see the chapter on [Thresholds and Data Retention](#).



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](#).



Assigning Icons to Devices and Device Classes

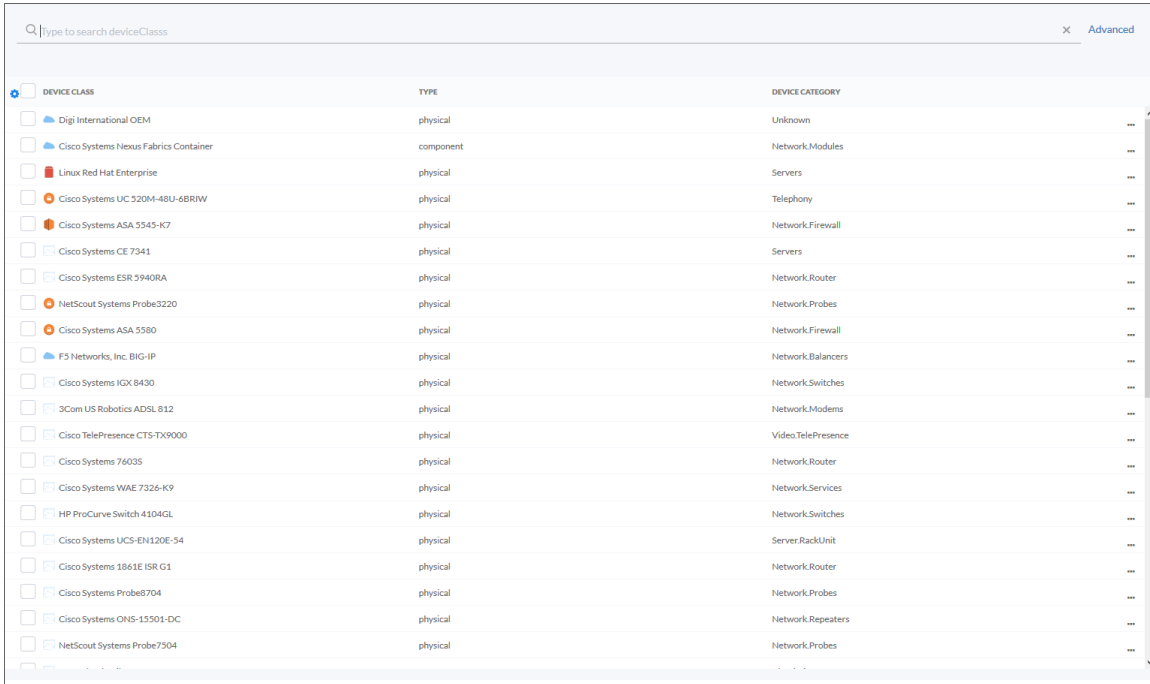
Each device in SL1 is associated with a **device class**. Typically, device classes map to a make/model pair, such as *Product Name / Model Number*. SL1 includes already-defined device classes for the most popular hardware. When possible, SL1 automatically assigns each discovered device to an existing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

You can also assign an icon to a specific device or device class. These icons will appear on the Devices and Device Investigator pages, as well as Device Class and Device Category pages.

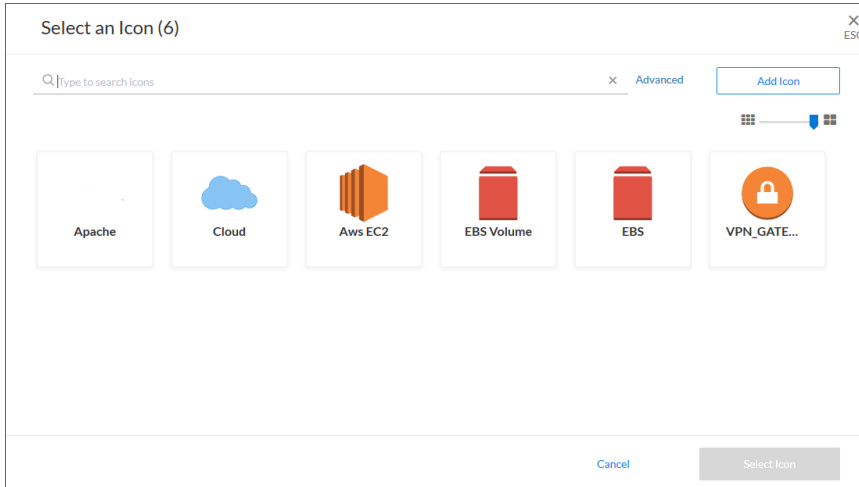


DEVICE CLASS	TYPE	DEVICE CATEGORY
<input type="checkbox"/> Digi International OEM	physical	Unknown
<input type="checkbox"/> Cisco Systems Nexus Fabrics Container	component	Network.Modules
<input type="checkbox"/> Linux Red Hat Enterprise	physical	Servers
<input type="checkbox"/> Cisco Systems UC 520M-48U-6BR1W	physical	Telephony
<input type="checkbox"/> Cisco Systems ASA 5545-K7	physical	Network.Firewall
<input type="checkbox"/> Cisco Systems CE 7341	physical	Servers
<input type="checkbox"/> Cisco Systems ESR 5940RA	physical	Network.Router
<input type="checkbox"/> NetScout Systems Probe3220	physical	Network.Probes
<input type="checkbox"/> Cisco Systems ASA 5580	physical	Network.Firewall
<input type="checkbox"/> F5 Networks, Inc. BIG-IP	physical	Network.Balancers
<input type="checkbox"/> Cisco Systems IGX 8430	physical	Network.Switches
<input type="checkbox"/> 3Com US Robotics ADSL 812	physical	Network.Modems
<input type="checkbox"/> Cisco TelePresence CTS-TX9000	physical	Video.TelePresence
<input type="checkbox"/> Cisco Systems 7603S	physical	Network.Router
<input type="checkbox"/> Cisco Systems WAE 7326-K9	physical	Network.Services
<input type="checkbox"/> HP ProCurve Switch 4104GL	physical	Network.Switches
<input type="checkbox"/> Cisco Systems UCS-EN120E-54	physical	Server.RackUnit
<input type="checkbox"/> Cisco Systems 1861E ISR G1	physical	Network.Router
<input type="checkbox"/> Cisco Systems Probe8704	physical	Network.Probes
<input type="checkbox"/> Cisco Systems ONS-15501-DC	physical	Network.Repeaters
<input type="checkbox"/> NetScout Systems Probe7504	physical	Network.Probes

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

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

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



TIP: To assign more than one device 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

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

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

- An "Icon name" text input field.
- An "ADD TAGS" section with a "#" icon and a "New tag" text input field.
- A large dashed box labeled "Browse or Drop" for file selection.
- A "REUSE TAGS" section.
- A list of requirements for icons: "Icons must: Be SVG format, Be no more than 40kb, Not be animated, Not contain bitmaps".
- "Cancel" and "Add Icon" buttons at the bottom.

- In the **Icon name** field, type a name for the icon you want to upload.
- In the **Add Tags** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
- 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.
- Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
- Click the **[Select Icon]** button to add the icon to the selected device class on the **Devices** or **Device Classes** pages.

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), you can view a list of existing device categories and create new device categories. You can also assign an icon to a specific device category, and those icons will appear on Device Class and Device Category pages. The icons also appear on Maps as well as Device Investigator, Service Investigator, and Application Investigator pages.

CATEGORY NAME	LAST EDITED BY	LAST EDITED
Cloud	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Account	em7admin	Sep 24, 2018, 3:24 PM
Cloud.AppService	em7admin	Sep 24, 2018, 3:24 PM
Cloud.AvailabilityZone	em7admin	Sep 24, 2018, 3:24 PM
Cloud.BigData	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Compute	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Database	em7admin	Sep 24, 2018, 3:24 PM
Cloud.IaaS	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Location	em7admin	Sep 24, 2018, 3:23 PM
Cloud.Network	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Region	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Service	em7admin	Sep 24, 2018, 3:24 PM
Cloud.Storage	em7admin	Sep 24, 2018, 3:24 PM
Environmental.CATV	em7admin	Sep 24, 2018, 3:24 PM
Environmental.HVAC	em7admin	Sep 24, 2018, 3:24 PM
Environmental.PDU	em7admin	Sep 24, 2018, 3:24 PM
Environmental.Security	em7admin	Sep 24, 2018, 3:24 PM
Environmental.UPS	em7admin	Sep 24, 2018, 3:24 PM
Environmental.Utility	em7admin	Sep 24, 2018, 3:24 PM
Environmental.Video	em7admin	Sep 24, 2018, 3:24 PM
Network.Access	em7admin	Sep 24, 2018, 3:24 PM

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:

Add new Category X
ESC

Category Name EDIT USER

ICON EDIT DATE

Browse

Save Category

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

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

4. On the **Add New Category** window, click the **[Save Category]** button. The category is added to the **Device Categories** 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 assign an icon to an existing device category:

1. On the **Device Categories** page, locate the device category for which you want to add an icon.
2. Click the **Actions** button (☰) for that device category and select *Assign Icon*. If you want to assign an icon to more than one device class at once, select the checkboxes next to those device classes and click **Assign Icon** in the blue bar at the bottom of the screen. The **Select an Icon** window appears.
3. To use an existing icon, select that icon from the list of icons and click the **[Select Icon]** button.
4. To upload an icon from your local drive, make sure that the image file meets the following criteria:
 - The image file should be in .SVG format.
 - The file should not be larger than 40 KB.
 - The file should not be animated.
 - The file should not contain bitmaps
5. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears.
6. In the **Icon name** field, type a name for the icon you want to upload.
7. In the **Add Tags** field, type a short descriptor for the icon, without spaces. You can use this tag to search for this icon later.
8. You can click the **Browse or Drop** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
9. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
10. Click the **[Select Icon]** button to add the icon to the selected device class on the **Device Categories** page.



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:

<i>Viewing the List of All Devices</i>	75
<i>Generating a Report for Multiple Devices</i>	85
<i>Generating a Report for a Single Device</i>	87
<i>Viewing the List of Component Devices</i>	89
<i>Bulk Actions in the Device Management Page</i>	95
<i>Bulk Actions for Component Devices</i>	97
<i>Bulk Merging and Unmerging of Devices</i>	98

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:

Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	SL Agent	Actions
10-64-171-130-CDB	10.64.171.130	System:EM7	ScienceLogic, Inc. EM7 Database	1	System	Minor	CUJG	Active	EM7 Default V2	V2	No	[Icons]
7809S-NPE3-cisco.com	10.20.7.31	Network:Router	Cisco Systems 7809S	2	System	Minor	CUJG	Active	Cisco SNMPv2 - EV2	V2	No	[Icons]
AA-AIO-33-177	192.168.33.177	System:EM7	ScienceLogic, Inc. EM7 All-in-One	13	System	Critical	CUJG	Active	EM7 Default V3	V3	No	[Icons]
asupekar-ao-92	10.2.15.92	System:EM7	ScienceLogic, Inc. EM7 All-in-One	20	System	Minor	CUJG	Active	EM7 Default V2	V2	No	[Icons]
Automation-system-1-110	10.2.15.110	System:EM7	ScienceLogic, Inc. EM7 All-in-One	72	System	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
Automation_GM_Bc_10215111	10.2.15.111	System:EM7	ScienceLogic, Inc. EM7 All-in-One	73	System	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
gyoung-dst-251	127.0.0.1	System:EM7	ScienceLogic, Inc. EM7 Data Collector	88	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
CB-6.4AIO.33.205	192.168.33.205	System:EM7	ScienceLogic, Inc. EM7 All-in-One	25	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
CB-8.5AIO.33.204	192.168.33.204	System:EM7	ScienceLogic, Inc. EM7 All-in-One	24	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
og-ao	192.168.33.161	System:EM7	ScienceLogic, Inc. EM7 All-in-One	8	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
CUCM10-01.qa.sciencelogic.local	10.0.13.20	UC:Device	Cisco Systems CUCM Server	3	System	Minor	CUJG	Active	SNMP Public V2	V2	No	[Icons]
DB1	192.168.33.211	System:EM7	ScienceLogic, Inc. EM7 Database	23	System	Minor	CUJG	Unavailable	EM7 Default V3	V3	No	[Icons]
DB2	192.168.33.222	System:EM7	ScienceLogic, Inc. EM7 Database	41	System	Minor	CUJG	Unavailable	EM7 Default V3	V3	No	[Icons]
EM7-HADR-CUJG	192.168.33.147	System:EM7	ScienceLogic, Inc. EM7 Data Collector	85	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
em7-hadr-db1	192.168.33.141	System:EM7	ScienceLogic, Inc. EM7 Database	84	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
em7-hadr-db2	192.168.33.146	System:EM7	ScienceLogic, Inc. EM7 Database	85	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
em7ao	192.168.33.180	System:EM7	ScienceLogic, Inc. EM7 All-in-One	19	System	Critical	CUJG	Active	EM7 Default V3	V3	No	[Icons]
em7ao	10.64.98.16	System:EM7	ScienceLogic, Inc. EM7 All-in-One	87	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
garyob890	192.168.33.129	System:EM7	ScienceLogic, Inc. EM7 Database	81	System	Minor	CUJG	Active	EM7 Default V3	V3	No	[Icons]
gmstack01	10.2.15.100	System:EM7	ScienceLogic, Inc. EM7 All-in-One	60	West Coast	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
gmstack02	10.2.15.101	System:EM7	ScienceLogic, Inc. EM7 All-in-One	59	East Coast	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
gmstack03	10.2.15.102	System:EM7	ScienceLogic, Inc. EM7 All-in-One	62	System	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
gmstack04	10.2.15.103	System:EM7	ScienceLogic, Inc. EM7 All-in-One	61	System	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]
tomstack05	10.2.15.104	System:EM7	ScienceLogic, Inc. EM7 All-in-One	63	System	Minor	CUJG	Unavailable	EM7 Default V2	V2	No	[Icons]

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 agent is 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:

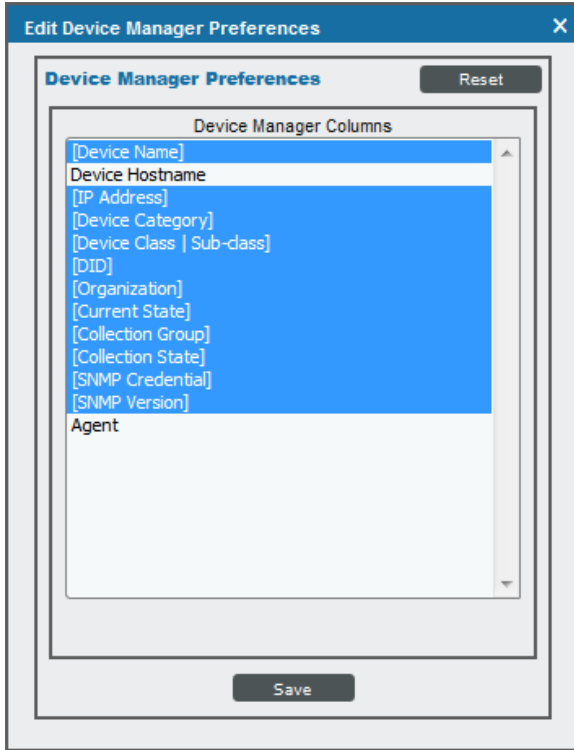
- *Device Administration* (). Leads to the **Device Properties** page, where you can define basic device parameters and parameters for discovery. From the **Device Properties** page, you can also access the other pages in the *Device Administration* tools.
- *Device Management* (). Leads to the **Device 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* tools.
- *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** 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 contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^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!*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!^s*i!*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 "sXiXo" 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. Jvolflexboot@lan.kun.lun		Storage.LUN	NetApp	LUN C-Mode	12977	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
1. JvolflexbootC1_B2_esxi		Storage.LUN	NetApp	LUN C-Mode	12975	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
2. JvolflexbootC1_B3_esxi		Storage.LUN	NetApp	LUN C-Mode	12987	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
3. JvolflexbootC2_B5_esxi		Storage.LUN	NetApp	LUN C-Mode	12970	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
4. JvolflexbootC2_B6_esxi		Storage.LUN	NetApp	LUN C-Mode	12972	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
5. JvolflexbootC2_B7_esxi		Storage.LUN	NetApp	LUN C-Mode	12976	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
6. JvolflexbootC5_S1_esxi		Storage.LUN	NetApp	LUN C-Mode	12973	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
7. Jvolflexi_shared_ds@Shared_DS		Storage.LUN	NetApp	LUN C-Mode	12962	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
8. Jvolflexi_shared_ds@Shared_DS_clone	10.0.13.20.163750	Storage.LUN	NetApp	LUN C-Mode	12960	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
9. Jvolflexi_shared_ds@VDP_Lun		Storage.LUN	NetApp	LUN C-Mode	12958	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
10. Jvolflexi_shared_ds@volflexi_shared_jpeg		Storage.LUN	NetApp	LUN C-Mode	12961	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
11. JvolHHA_SAIha_sas.lun		Storage.LUN	NetApp	LUN C-Mode	12978	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
12. JvolHnf_shared_2_ds_volHnf_shared_2_ds		Storage.LUN	NetApp	LUN C-Mode	12965	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
13. JvolHnf@fscsi1.lun		Storage.LUN	NetApp	LUN C-Mode	12967	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
14. JvolHnetapp_em@netapp_em7.lun		Storage.LUN	NetApp	LUN C-Mode	12964	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
15. JvolHNew_Shared_DS_volHNew_Shared_DS		Storage.LUN	NetApp	LUN C-Mode	12974	SILO	Healthy	CUG	Unavailable	SNMP Public V2	V2
16. JvolHvol0.lun0		Storage.LUN	NetApp	LUN	14073	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
17. JvolHvol1.lun0		Storage.LUN	NetApp	LUN	14072	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
18. JvolHvol1.lun0		Storage.LUN	NetApp	LUN	14070	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
19. JvolHvol1.lun1		Storage.LUN	NetApp	LUN	14068	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
20. JvolHvol1.lun2		Storage.LUN	NetApp	LUN	14071	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
21. JvolHvol1.lun4		Storage.LUN	NetApp	LUN	14069	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
22. JvolHvol2.lun0		Storage.LUN	NetApp	LUN	14075	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
23. JvolHvol2.lun1		Storage.LUN	NetApp	LUN	14074	Cloud-Hosting	Healthy	CUG	Active	SNMP Public V2	V2
24. 10.0.13.20-CTIManager		UC Service	Cisco Systems	CTI Manager Service	14569	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. 10.0.13.20-1flp		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. 10.0.13.21-1flp		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. 10.0.13.22-1flp		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. 10.168.37.38		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. 192.168.53.245-1flp		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	13023	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		DEM	Cisco Systems	Nexus vPC	14565	SILO	Healthy	CUG	Unavailable	Cisco SNMP V2	V2
54. 20_Po13_Flexpod - Nexus_b		DEM	Cisco Systems	Nexus vPC	14568	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).

Device Manager | Devices Found [88] TRIAL LICENSE 30 DAYS REMAINING

Device Name	IP Address	Device Category	Device Class / Sub-class	EM7	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Group	SL Agent	Actions
10-64-171-130-CDB	10.64.171.130	System EM7	ScenoeLogic, Inc EM7 Database	1	System	Map	CUG	Active	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
7809S-NPE3.cisco.com	10.20.7.31	Network.Router	Cisco Systems 7809S	2	System	Map	CUG	Active	Cisco SNMPv2 - EV2	V3	No	[Report] [Refresh] [Refresh] [Refresh]
AA-AIO-35-177	192.168.33.177	System EM7	ScenoeLogic, Inc EM7 All-in-One	13	System	Critical	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
tsupekar-ai-o-62	10.2.15.62	System EM7	ScenoeLogic, Inc EM7 All-in-One	20	System	Map	CUG	Active	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
Automation-system1-110	10.2.15.110	System EM7	ScenoeLogic, Inc EM7 All-in-One	72	System	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
Automation_GM_R_10215111	10.2.15.111	System EM7	ScenoeLogic, Inc EM7 All-in-One	73	System	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
syung-dsl-cu-251	127.0.0.1	System EM7	ScenoeLogic, Inc EM7 Data Collector	88	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
CB-8.4AIO.33.205	192.168.33.205	System EM7	ScenoeLogic, Inc EM7 All-in-One	25	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
CB-8.5AIO.33.204	192.168.33.204	System EM7	ScenoeLogic, Inc EM7 All-in-One	24	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
cg-ai-o	192.168.33.161	System EM7	ScenoeLogic, Inc EM7 All-in-One	8	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
CUCM10-01.qa.scenoeologic.local	10.0.13.20	UC Device	Cisco Systems CUCM Server	3	System	Map	CUG	Active	SNMP Public V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
DB1	192.168.33.211	System EM7	ScenoeLogic, Inc EM7 Database	23	System	Map	CUG	Unavailable	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
DB2	192.168.33.222	System EM7	ScenoeLogic, Inc EM7 Database	41	System	Map	CUG	Unavailable	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
EM7-HADR-CUO	192.168.33.147	System EM7	ScenoeLogic, Inc EM7 Data Collector	86	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
em7-hadr-db1	192.168.33.141	System EM7	ScenoeLogic, Inc EM7 Database	84	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
em7-hadr-db2	192.168.33.146	System EM7	ScenoeLogic, Inc EM7 Database	85	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
em7-ao	192.168.33.180	System EM7	ScenoeLogic, Inc EM7 All-in-One	19	System	Critical	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
em7-ao	10.64.98.16	System EM7	ScenoeLogic, Inc EM7 All-in-One	87	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
gsarydb990	192.168.33.129	System EM7	ScenoeLogic, Inc EM7 Database	61	System	Map	CUG	Active	EM7 Default V3	V3	No	[Report] [Refresh] [Refresh] [Refresh]
gmrstack01	10.2.15.100	System EM7	ScenoeLogic, Inc EM7 All-in-One	80	West Coast	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
gmrstack02	10.2.15.101	System EM7	ScenoeLogic, Inc EM7 All-in-One	59	East Coast	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
gmrstack03	10.2.15.102	System EM7	ScenoeLogic, Inc EM7 All-in-One	02	System	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]
gmrstack04	10.2.15.103	System EM7	ScenoeLogic, Inc EM7 All-in-One	01	System	Map	CUG	Unavailable	EM7 Default V2	V2	No	[Report] [Refresh] [Refresh] [Refresh]

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						

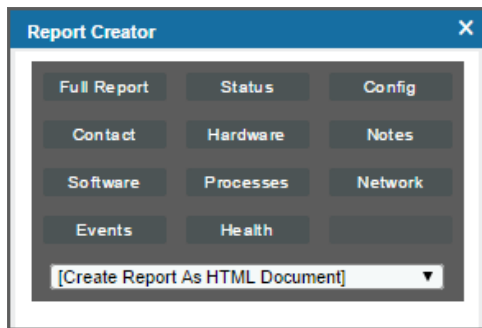
To generate a detailed report on a single device:

1. Log in to SL1.

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

Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection State	Collection Size	SNMP Credential	SNMP Version	SL Agent
10-64-171-130-CDB	10.64.171.130	System:EM7	ScienceLogic, Inc EM7 Database	1	System	Minor	CUG	Active	EM7 Default V2	V2	No
70095-NPE3.cisco.com	10.20.7.31	Network:Router	Cisco Systems 70095	2	System	Minor	CUG	Active	Cisco SNMPV2 - EV2	No	No
AA-AIO-33-177	192.168.33.177	System:EM7	ScienceLogic, Inc EM7 All-in-One	13	System	Critical	CUG	Active	EM7 Default V3	V3	No
tsupekar-ai-o-92	10.2.15.92	System:EM7	ScienceLogic, Inc EM7 All-in-One	29	System	Minor	CUG	Active	EM7 Default V2	V2	No
Automation-system1-110	10.2.15.110	System:EM7	ScienceLogic, Inc EM7 All-in-One	72	System	Minor	CUG	Unavailable	EM7 Default V2	V2	No
Automation_GM_Bv_10215111	10.2.15.111	System:EM7	ScienceLogic, Inc EM7 All-in-One	73	System	Minor	CUG	Unavailable	EM7 Default V2	V2	No
zyoung-dist-ou-251	127.0.0.1	System:EM7	ScienceLogic, Inc EM7 Data Collector	88	System	Minor	CUG	Active	EM7 Default V3	V3	No
CB-6-AAIO.33.205	192.168.33.205	System:EM7	ScienceLogic, Inc EM7 All-in-One	25	System	Minor	CUG	Active	EM7 Default V3	V3	No
CB-6-5AIO.33.204	192.168.33.204	System:EM7	ScienceLogic, Inc EM7 All-in-One	24	System	Minor	CUG	Active	EM7 Default V3	V3	No
cg-ai-o	192.168.33.181	System:EM7	ScienceLogic, Inc EM7 All-in-One	8	System	Minor	CUG	Active	EM7 Default V3	V3	No
CUCM10-01.qa.scienelocio.local	10.0.13.20	UC:Device	Cisco Systems CUCM Server	3	System	Minor	CUG	Active	SNMP Public V2	V2	No
DB1	192.168.33.211	System:EM7	ScienceLogic, Inc EM7 Database	23	System	Minor	CUG	Unavailable	EM7 Default V3	V3	No
DB2	192.168.33.222	System:EM7	ScienceLogic, Inc EM7 Database	41	System	Minor	CUG	Unavailable	EM7 Default V3	V3	No
EM7-HADR-CUJ	192.168.33.147	System:EM7	ScienceLogic, Inc EM7 Data Collector	86	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7-hadr-dt1	192.168.33.141	System:EM7	ScienceLogic, Inc EM7 Database	84	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7-hadr-dt2	192.168.33.146	System:EM7	ScienceLogic, Inc EM7 Database	85	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7-ao	192.168.33.180	System:EM7	ScienceLogic, Inc EM7 All-in-One	19	System	Critical	CUG	Active	EM7 Default V3	V3	No
em7ao	10.64.98.16	System:EM7	ScienceLogic, Inc EM7 All-in-One	87	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7db880	192.168.33.129	System:EM7	ScienceLogic, Inc EM7 Database	81	System	Minor	CUG	Active	EM7 Default V3	V3	No
em7stack01	10.2.15.100	System:EM7	ScienceLogic, Inc EM7 All-in-One	80	West Coast	Minor	CUG	Unavailable	EM7 Default V2	V2	No
em7stack02	10.2.15.101	System:EM7	ScienceLogic, Inc EM7 All-in-One	59	East Coast	Minor	CUG	Unavailable	EM7 Default V2	V2	No
em7stack03	10.2.15.102	System:EM7	ScienceLogic, Inc EM7 All-in-One	62	System	Minor	CUG	Unavailable	EM7 Default V2	V2	No
em7stack04	10.2.15.103	System:EM7	ScienceLogic, Inc EM7 All-in-One	61	System	Minor	CUG	Unavailable	EM7 Default V2	V2	No

- In the **Device Manager** page, find the device for which you want to generate a detailed report. Select the printer icon () for that device.
- 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.



- 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:

Device Components Devices Found [35]											Actions	Reset	Guide
Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Current State	Collection Group	Collection State					
172.16.243.29	172.16.243.29	ContactCenter	Cisco Systems Voice Portal (CVP)	131	RNG	Notice	CUG	Active					
172.16.243.38	172.16.243.38	ContactCenter	Cisco Systems Voice Portal (CVP)	133	RNG	Major	CUG	Active					
172.16.243.39	172.16.243.39	ContactCenter	Cisco Systems Voice Portal (CVP)	134	RNG	Minor	CUG	Active					
198.18.133.201:common	--	Infrastructure	Cisco Systems ACI Tenant	1328	Cisco_ACI_Regression_Test	Healthy	CUG	Active					
198.18.133.201:infra	--	Infrastructure	Cisco Systems ACI Tenant	1322	Cisco_ACI_Regression_Test	Healthy	CUG	Active					
198.18.133.202:common	--	Infrastructure	Cisco Systems ACI Tenant	1333	Cisco_ACI_Regression_Test	Healthy	CUG	Active					
198.18.133.202:infra	--	Infrastructure	Cisco Systems ACI Tenant	1339	Cisco_ACI_Regression_Test	Healthy	CUG	Active					
Amazon	--	Service	Service AWS Service	1628	AWS Elana	Healthy	CUG	Active					
apic1	198.18.133.200	Utility	Cisco Systems ACI	1557	Cisco_ACI_Regression_Test	Minor	CUG	Active					
apic1:common	--	Infrastructure	Cisco Systems ACI Tenant	339	Cisco_ACI_Regression_Test	Minor	CUG	Active					
apic1:infra	--	Infrastructure	Cisco Systems ACI Tenant	337	Cisco_ACI_Regression_Test	Minor	CUG	Active					
AZURE CLASSIC SSH	--	Service	Microsoft Azure Services Classic	4594	Azure CLASSIC SSH	Healthy	CUG	Active					
CUCM10-01 qa.sciencelogic.local	10.0.13.20	Cluster	Cisco Systems CUCM Cluster	169	RNG	Major	CUG	Active					
cucm8	10.168.44.22	Cluster	Cisco Systems CUCM Cluster	1276	System	Healthy	CUG	User-Disabled					
CUCM9-01 qa.sciencelogic.local	10.64.160.10	Cluster	Cisco Systems CUCM Cluster	168	RNG	Minor	CUG	Active					
CUC11 dfoaid.cisco.com	10.2.10.76	ContactCenter	Cisco Systems Contact Center (CCE)	1274	System	Minor	CUG	Unavailable					
dc2aCUCM01.corp.sciencelogic.net	10.128.11.32	Cluster	Cisco Systems CUCM Cluster	1275	System	Major	CUG	Active					
fxepodc1b1	10.5.100.20	Pingable	Linux ICMP	410	UCS	Notice	CUG	Active					
ms-082-dcqa1	10.1.0.140	Servers	Microsoft Windows Server 2008 R2	5614	RS_PowershellDevices	Minor	CUG	Active					
ms-082-lync	10.1.0.139	Servers	Microsoft Windows Server 2008 R2	5615	RS_PowershellDevices	Major	CUG	Active					
ms12c-dc-qa14	10.1.0.137	Servers	Microsoft Windows Server 2012 R2	5611	RS_PowershellDevices	Minor	CUG	Active					
ms12c-lync13	10.1.0.142	Servers	Microsoft Windows Server 2012 R2	5613	RS_PowershellDevices	Minor	CUG	Active					
Office365_MSDN	--	Account	Microsoft Office 365 Account	1086	RS_Office365	Healthy	CUG	Active					
POD7-AW1.caasdemo.com	172.16.243.37	ContactCenter	Cisco Systems Contact Center (CCE)	135	RNG	Healthy	CUG	Active					
POD7-PG1A.caasdemo.com	172.16.243.23	ContactCenter	Cisco Systems Contact Center (CCE)	128	RNG	Healthy	CUG	Active					

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 SL 1 .
- **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.

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.

Device Components Devices Found [35]										Actions	Reset	Guide																																																																														
Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																		
172.16.243.29	172.16.243.29	ContactCenter	Cisco Systems Voice Portal (CVP)	131	RNG	Notice	CUG	Active																																																																																		
<table border="1"> <thead> <tr> <th>Device Name</th> <th>IP Address</th> <th>Device Category</th> <th>Device Class / Sub-class</th> <th>DID</th> <th>Organization</th> <th>Current State</th> <th>Collection Group</th> <th>Collection State</th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>H323 2</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP H323 Instance</td> <td>141</td> <td>RNG</td> <td>Major</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ICM 4</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP ICM Instance</td> <td>143</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>IVR 3</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP IVR Instance</td> <td>142</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>SIP 1</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP SIP Instance</td> <td>140</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>VXML 5</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP VXML Instance</td> <td>144</td> <td>RNG</td> <td>Major</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>													Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State					H323 2	--	ContactCenter	Cisco Systems CVP H323 Instance	141	RNG	Major	CUG	Active					ICM 4	--	ContactCenter	Cisco Systems CVP ICM Instance	143	RNG	Healthy	CUG	Active					IVR 3	--	ContactCenter	Cisco Systems CVP IVR Instance	142	RNG	Healthy	CUG	Active					SIP 1	--	ContactCenter	Cisco Systems CVP SIP Instance	140	RNG	Healthy	CUG	Active					VXML 5	--	ContactCenter	Cisco Systems CVP VXML Instance	144	RNG	Major	CUG	Active				
Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																		
H323 2	--	ContactCenter	Cisco Systems CVP H323 Instance	141	RNG	Major	CUG	Active																																																																																		
ICM 4	--	ContactCenter	Cisco Systems CVP ICM Instance	143	RNG	Healthy	CUG	Active																																																																																		
IVR 3	--	ContactCenter	Cisco Systems CVP IVR Instance	142	RNG	Healthy	CUG	Active																																																																																		
SIP 1	--	ContactCenter	Cisco Systems CVP SIP Instance	140	RNG	Healthy	CUG	Active																																																																																		
VXML 5	--	ContactCenter	Cisco Systems CVP VXML Instance	144	RNG	Major	CUG	Active																																																																																		
172.16.243.38	172.16.243.38	ContactCenter	Cisco Systems Voice Portal (CVP)	133	RNG	Major	CUG	Active																																																																																		
<table border="1"> <thead> <tr> <th>Device Name</th> <th>IP Address</th> <th>Device Category</th> <th>Device Class / Sub-class</th> <th>DID</th> <th>Organization</th> <th>Current State</th> <th>Collection Group</th> <th>Collection State</th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>Reporting 1</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP Reporting Instance</td> <td>145</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>													Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State					Reporting 1	--	ContactCenter	Cisco Systems CVP Reporting Instance	145	RNG	Healthy	CUG	Active																																																								
Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																		
Reporting 1	--	ContactCenter	Cisco Systems CVP Reporting Instance	145	RNG	Healthy	CUG	Active																																																																																		
172.16.243.39	172.16.243.39	ContactCenter	Cisco Systems Voice Portal (CVP)	134	RNG	Minor	CUG	Active																																																																																		
<table border="1"> <thead> <tr> <th>Device Name</th> <th>IP Address</th> <th>Device Category</th> <th>Device Class / Sub-class</th> <th>DID</th> <th>Organization</th> <th>Current State</th> <th>Collection Group</th> <th>Collection State</th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>H323 2</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP H323 Instance</td> <td>147</td> <td>RNG</td> <td>Major</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>ICM 4</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP ICM Instance</td> <td>148</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>IVR 3</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP IVR Instance</td> <td>149</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>SIP 1</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP SIP Instance</td> <td>146</td> <td>RNG</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>VXML 5</td> <td>--</td> <td>ContactCenter</td> <td>Cisco Systems CVP VXML Instance</td> <td>150</td> <td>RNG</td> <td>Major</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>													Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State					H323 2	--	ContactCenter	Cisco Systems CVP H323 Instance	147	RNG	Major	CUG	Active					ICM 4	--	ContactCenter	Cisco Systems CVP ICM Instance	148	RNG	Healthy	CUG	Active					IVR 3	--	ContactCenter	Cisco Systems CVP IVR Instance	149	RNG	Healthy	CUG	Active					SIP 1	--	ContactCenter	Cisco Systems CVP SIP Instance	146	RNG	Healthy	CUG	Active					VXML 5	--	ContactCenter	Cisco Systems CVP VXML Instance	150	RNG	Major	CUG	Active				
Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																		
H323 2	--	ContactCenter	Cisco Systems CVP H323 Instance	147	RNG	Major	CUG	Active																																																																																		
ICM 4	--	ContactCenter	Cisco Systems CVP ICM Instance	148	RNG	Healthy	CUG	Active																																																																																		
IVR 3	--	ContactCenter	Cisco Systems CVP IVR Instance	149	RNG	Healthy	CUG	Active																																																																																		
SIP 1	--	ContactCenter	Cisco Systems CVP SIP Instance	146	RNG	Healthy	CUG	Active																																																																																		
VXML 5	--	ContactCenter	Cisco Systems CVP VXML Instance	150	RNG	Major	CUG	Active																																																																																		
198.18.133.201-common	--	Infrastructure	Cisco Systems ACI Tenant	1328	Cisco_ACI_Regression_Test	Healthy	CUG	Active																																																																																		
<table border="1"> <thead> <tr> <th>Device Name</th> <th>IP Address</th> <th>Device Category</th> <th>Device Class / Sub-class</th> <th>DID</th> <th>Organization</th> <th>Current State</th> <th>Collection Group</th> <th>Collection State</th> <th></th> <th></th> <th></th> <th></th> </tr> </thead> <tbody> <tr> <td>default</td> <td>--</td> <td>Infrastructure</td> <td>Cisco Systems ACI Application Network Profile</td> <td>1338</td> <td>Cisco_ACI_Regression_Test</td> <td>Healthy</td> <td>CUG</td> <td>Active</td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>													Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State					default	--	Infrastructure	Cisco Systems ACI Application Network Profile	1338	Cisco_ACI_Regression_Test	Healthy	CUG	Active																																																								
Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State																																																																																		
default	--	Infrastructure	Cisco Systems ACI Application Network Profile	1338	Cisco_ACI_Regression_Test	Healthy	CUG	Active																																																																																		
198.18.133.201-infra	--	Infrastructure	Cisco Systems ACI Tenant	1322	Cisco_ACI_Regression_Test	Healthy	CUG	Active																																																																																		

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, click the **[Apply]** button to filter the list of devices.
 5. To reset each field and apply no filters, click the **[Reset]** button.

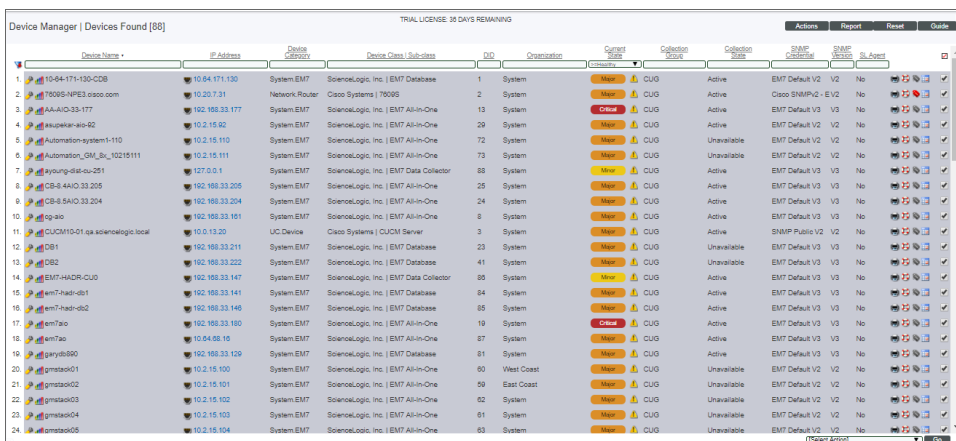
TIP: You can perform an advanced filter and then perform a second advanced filter on the results of the first advanced filter. You can continue to modify and apply an advanced filter multiple times.

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.



Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State	SNMP Community	SNMP Version	SNMP Agent	...
10.44.171.130-C2B8	10.44.171.130	System:EM7	ScienetLogic, Inc. EM7 Database	1	System	OK	CUG	Active	EM7 Default V2	V2	No	<input type="checkbox"/>
7005-19E3-0300.com	10.20.7.31	Network Router	Cisco Systems 7005	2	System	OK	CUG	Active	Cisco SNMP v2 - E	V2	No	<input type="checkbox"/>
...	<input type="checkbox"/>

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 chapter on **Device Logs**.
- **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 chapter 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 chapter **Graphing Data from Multiple Dynamic Applications in a Single Dashboard Widget**.
- **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 chapter 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 be 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 chapter](#).

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

NOTE: You cannot delete a parent device or root device that has associated component devices. To delete a root device, you must first delete all device components for that root device. To delete the component devices, you must first disable collection and then delete the devices. You can then delete the root device.

- **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 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.
 - 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.

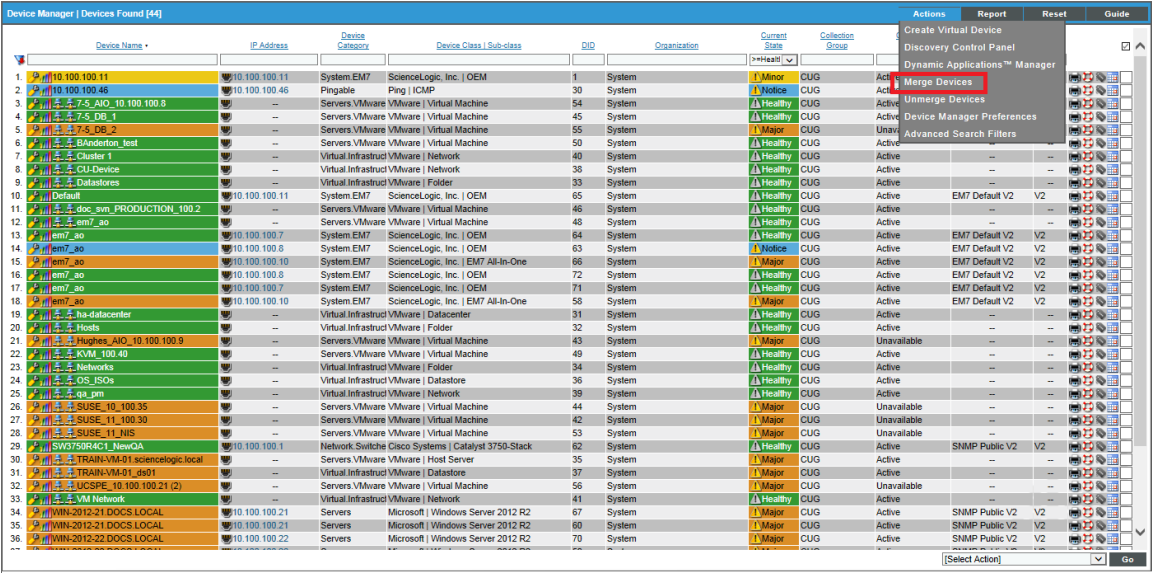
Performing a Bulk Device Merge

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.

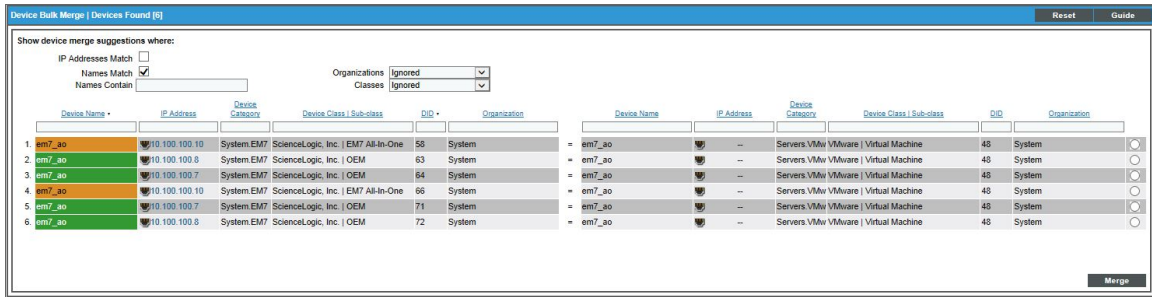
To perform a bulk device merge:

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 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 you 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**.

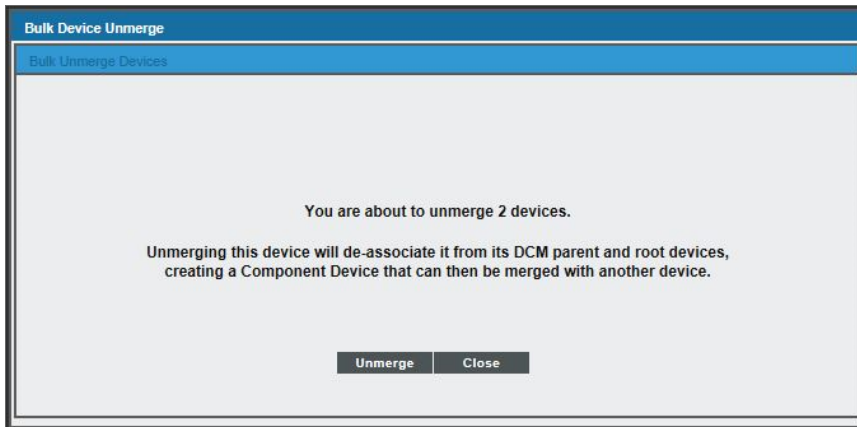
The screenshot shows the 'Device Manager | Devices Found [44]' interface. A table lists various devices with columns for Device Name, IP Address, Device Category, Device Class | Sub-class, DID, Organization, Current State, Collection Scope, and Actions. The 'Actions' menu is open, and 'Unmerge Devices' is highlighted. Other options include 'Create Virtual Device', 'Discovery Control Panel', 'Dynamic Applications™ Manager', 'Merge Devices', 'Device Manager Preferences', and 'Advanced Search Filters'.

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.

The screenshot shows the 'Device Bulk Unmerge | Devices Found [2]' interface. It displays a table with columns for Device Name, IP Address, Device Category, Device Class | Sub-class, DID, Organization, Device Name, IP Address, Device Class | Sub-class, DID, Organization, Merged By, and Merged Date. Two rows are visible, each with a checkbox in the final column. An 'Unmerge' button is located at the bottom right of the table.

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Device Name	IP Address	Device Class Sub-class	DID	Organization	Merged By	Merged Date	
Default	10.100.1	System	ScienceLogic, Inc. OEM	65	System	CU-Device	--	VMware Network	38	System	em7admin	2015-01-22 16:42	<input type="checkbox"/>
em7_ao	10.100.1	System	ScienceLogic, Inc. EM7 F58	System	System	em7_ao	--	VMware Virtual Machine	48	System	em7admin	2015-01-21 21:02	<input type="checkbox"/>

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.

Viewing Details in the Device Reports Panel

Overview

This chapter describes the **Device Reports** panel on the **Device Manager** page (Devices > Device Manager). The **Device Reports** panel lets you view detailed information about the data that SL1 has gathered from 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:

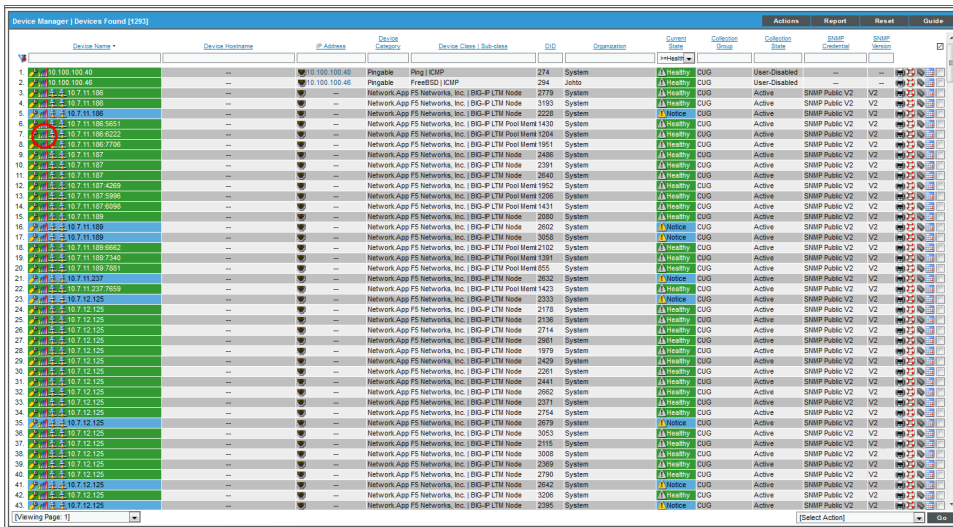
<i>What is the Device Reports panel?</i>	105
<i>Device Dashboards in the Device Summary Page</i>	108
<i>The Default Device Summary Page</i>	110
<i>Shortcut Keys for Device Reports panel</i>	117

What is the Device Reports panel?

The **Device Reports** panel allows you to view detailed information that SL1 has gathered from each device and view reports generated from that information. The **Device Reports** panel is for viewing information, rather than for administering the device.

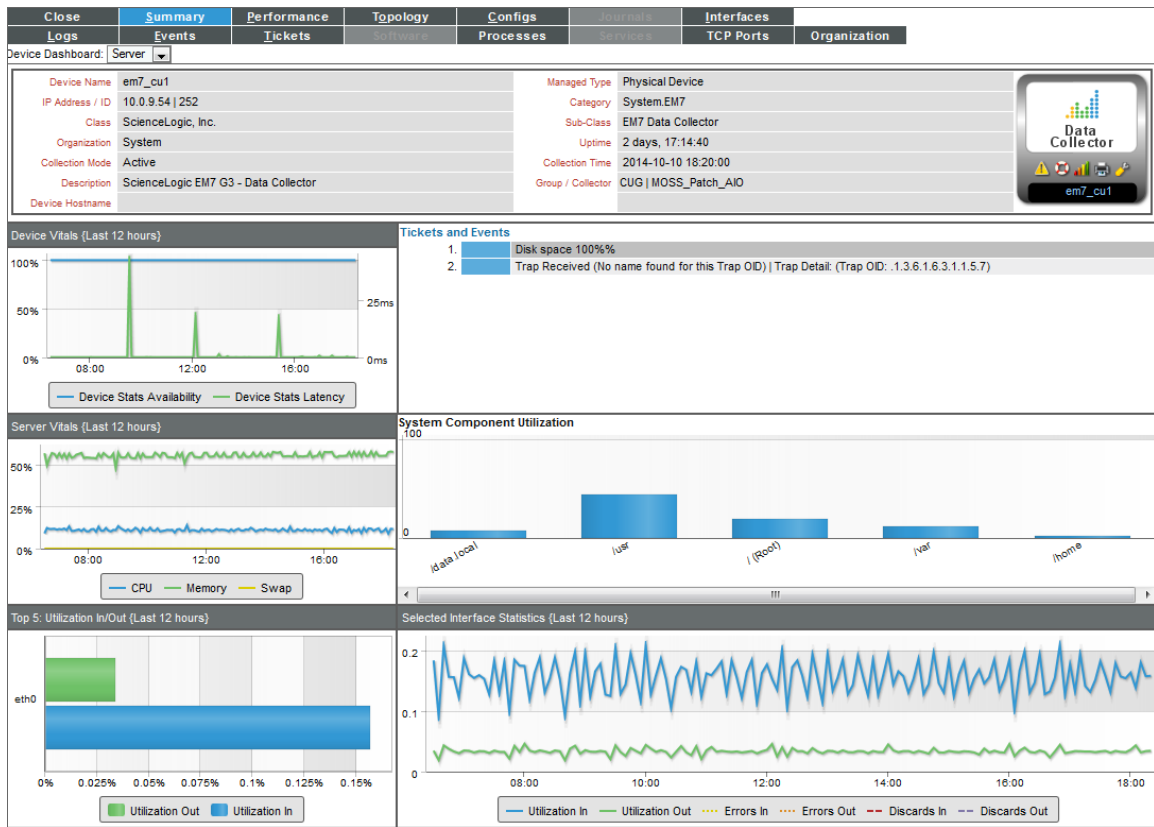
To access the **Device Reports** panel for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to view the **Device Reports** panel. Select its bar graph () icon.



Device Name	Device Hostname	IP Address	Device Class / Sub-class	OID	Organization	Current State	Collection Rate	Collection Rate	SNMP Credential	SNMP Version
10.100.100.40	--	10.100.100.40	Pinable	FreeBSD / ICMP	294	System	Healthy	CFG	User-Disabled	--
10.100.100.46	--	10.100.100.46	Pinable	FreeBSD / ICMP	294	John	Healthy	CFG	User-Disabled	--
10.107.11.106	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2779	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.106	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2193	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.186	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2222	System	Notice	CFG	Active	SNMP Public V2
10.107.11.186.5651	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1430	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.186.5922	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1204	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.186.7700	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1951	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2496	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2391	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2840	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187.2269	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1952	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187.2668	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1206	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.187.2668	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1431	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.189	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2880	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.189	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2802	System	Notice	CFG	Active	SNMP Public V2
10.107.11.189	--	--	Network App FS Networks, Inc.	BIG-PLM Node	3058	System	Notice	CFG	Active	SNMP Public V2
10.107.11.189.2662	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	2102	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.189.7340	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	1931	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.189.7681	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	855	System	Healthy	CFG	Active	SNMP Public V2
10.107.11.189.7689	--	--	Network App FS Networks, Inc.	BIG-PLM Pool Mem	2626	System	Notice	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	1423	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2333	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2179	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2138	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2714	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2681	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	1979	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2429	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2201	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2441	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2662	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2371	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2754	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2676	System	Notice	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	3053	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2115	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	3008	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2369	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2790	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2642	System	Notice	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	3206	System	Healthy	CFG	Active	SNMP Public V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-PLM Node	2395	System	Notice	CFG	Active	SNMP Public V2

3. The **Device Reports** panel includes the following tabs and pages:



Tab	Description
Summary	The Device Summary page provides a one-stop overview of a device. This page displays one or more Device Dashboards that are aligned with the device. To switch between the dashboards that are available for a device, select a dashboard in the Device Dashboard drop-down list in the upper-left of the page.
Performance	The Device Performance page allows you to view many detailed reports for the selected device, including reports on availability, latency, CPU usage, memory usage, file system usage, network interfaces and bandwidth usage, domain name availability, Email round-trip speed, SOAP/XML transactions, system-process availability, TCP/IP Port availability, web content availability, and custom reports based on data collected from the device by Dynamic Applications.

Tab	Description
Topology	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; hypervisors and their virtual machines; network devices that use CDP (Cisco Discovery Protocol) or LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in CDP tables or LLDP tables; links between network devices that use CDP or LLDP and devices that are specified as neighbors in CDP tables or LLDP tables; device relationships created with Dynamic Applications; manually created parent-child relationships that affect event correlation.
Configs	<p>The Configuration Report page displays configuration information collected by Dynamic Applications. All objects of type "config" are included in the Configuration Report page.</p> <p>In the Dynamic Applications Collections Objects page (System > Manage > Applications > Collections), users can define which objects will be grouped together, which table each object will appear in, and whether SL1 will track changes in each object's value.</p> <p>For details on Dynamic Applications and configuration objects, see one of the manuals on Dynamic Applications.</p>
Journals	<p>The Journal View page displays journal entry information collected from the device by journal Dynamic Applications.</p> <p>For details on the Journal View page, see the Snippet Dynamic Application manual.</p>
Interfaces	The Interfaces Found page displays detailed information about the network interfaces on the device.
Logs	The Device Logs & Messages page displays all the messages SL1 has generated about the device.
Events	<p>The Viewing Active Events page displays a list of all events associated with the device.</p> <p>For details on events, see the manual Events.</p>
Tickets	<p>The Ticket History page displays a list of all tickets, both open and resolved, associated with the device.</p> <p>For details on tickets and ticket administration, see the manual Ticketing.</p>
Software	The Software Packages page displays a list of all the software installed on the device. If possible, the installation date is also displayed.
Processes	The System Processes page displays information about the processes running on the device.
Services	The Windows Services page displays a list of all Windows services enabled on the device.
TCP Ports	The Port Security 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.

Tab	Description
Organization	<p>Leads to the Organizational Summary page and the Organization Administration panel, where you can view and edit details about the organization associated with the device.</p> <p>For details on organizations and organization administration, see the manual Organizations and Users.</p>
Asset	<p>Leads to the Asset Properties page and the Asset Administration panel, where you can view and edit the asset record for the device.</p> <p>For details on asset records and asset administration, see the manual Asset Management.</p>

Device Dashboards in the Device Summary Page

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.

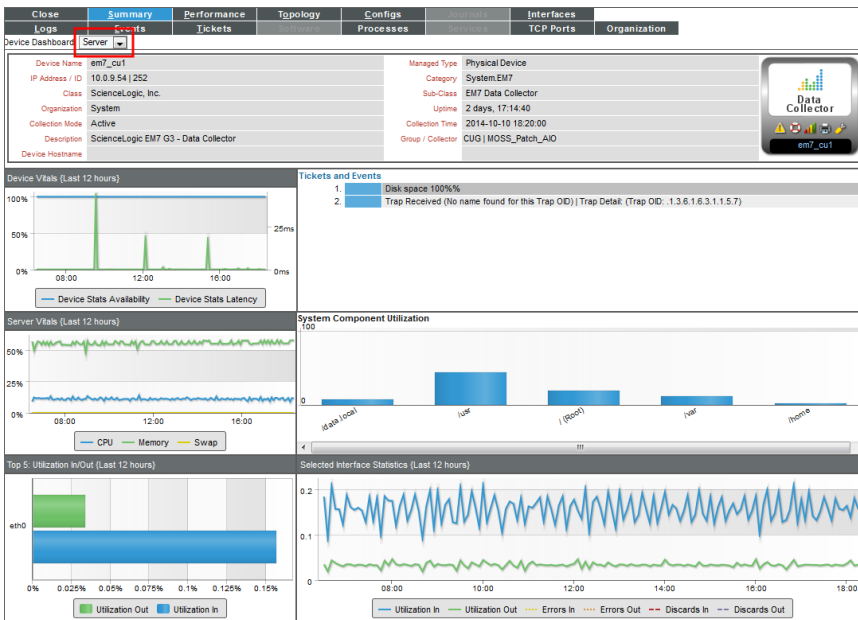
NOTE: If the *Prefer Global Device Summary Dashboard Over Category/Class* checkbox is checked in the **Behavior Settings** page (System > Settings > Behavior) and a device is not manually aligned with a device dashboard, the dashboard that is defined as the "Global Default" is displayed.

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.

In addition to the default dashboard for a device, you can also view other device dashboards in the **Device Summary** page. The other dashboards that are available for a device are based on the device class and device category assigned to the device and the Dynamic Applications to which the device is subscribed.

To view a device dashboard other than the global default device dashboard:

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 the **Device Summary** page. Select its bar graph (📊) icon.
3. The **Device Summary** page appears, displaying either the global default device dashboard or the device dashboard that has been manually assigned to this device.
4. To select a different device dashboard, select the drop-down menu in the upper-left corner of the **Device Summary** page:



Device Dashboards are defined in the **Device Dashboards** page (System > Customize > Device Dashboards) and aligned with the device in the **Device Properties** page (Devices > Device Manager > wrench icon) in the **Dashboard** field:

The screenshot shows the 'Device Properties' page for a device named 'em7_cu1'. The page is divided into several sections:

- Identification:** Fields for Device Name (em7_cu1), IP Address ([10.0.9.54 - verified]), and Organization ([System]).
- Monitoring & Management:** A section with various dropdown menus for configuration:
 - Device Class: ScienceLogic, Inc. EM7 Data Collector
 - SNMP Read/Write: [EM7 Default V2] | [None]
 - Availability Port: [UDP] | [161 - SNMP]
 - Latency Port: [ICMP] | [ICMP]
 - Avail-Latency Alert: [Disable]
 - User Maintenance: [Disabled] | [Maintenance Collection Enabled]
 - Collection: [Enabled] | [CUG]
 - Coll. Type: [Standard]
 - Critical Ping: [Disabled]
 - Dashboard: [None]** (highlighted with a red box)
 - Event Mask: [Group in blocks every 10 minutes]
- Preferences:** A list of checkboxes for various settings:
 - Auto-Clear Events:
 - Accept All Logs:
 - Daily Port Scans:
 - Auto-Update:
 - Scan All IPs:
 - Dynamic Discovery:
 - Preserve Hostname:
 - Disable Asset Update:

For information on how to create a device dashboard and how to align it to a device, device class, device category, or a Dynamic Application, see the chapter on [Device Dashboards](#).

The Default Device Summary Page

This section describes device dashboard that is configured as the global default when SL1 is installed. This default device dashboard provides a one-stop overview of a device.

NOTE: The global default dashboard can be changed. The dashboard describes in this section might not be the global default dashboard in your SL1 system.

To access the **Device Summary** page for a device:

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

- In the **Device Manager** page, find the device for which you want to view the **Device Summary** page. Select its bar graph icon.

Device Name	Device Hostname	IP Address	Device Subclass	Device Class / Sub-class	DCG	Organization	Current State	Collection Status	Collection Rate	SNMP Credentials	SNMP Message
10.100.100.40	--	10.100.100.40	Pingable	Ping / ICMP	274	System	Healthy	CUG	User-Disabled	--	--
10.100.100.46	--	10.100.100.46	Pingable	FreeBSD / ICMP	294	John	Healthy	CUG	User-Disabled	--	--
10.7.11.186	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.188	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.188	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.11.188	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1430	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.188-8222	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1204	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.188-7706	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1951	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187-4289	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	1952	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187-5996	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1206	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.187-6048	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1431	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2690	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.11.189-6662	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	2102	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.189-7240	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1391	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.189-7881	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	855	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.11.237	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.11.237-7659	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1423	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2281	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2662	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2389	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2
10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2

- The **Device Summary** page appears (along with the tabs for the **Device Reports** panel):

The screenshot shows the Device Summary page for device 10.0.2.58. The page includes the following sections:

- Device Information:**
 - Device Name: 10.0.2.58
 - IP Address / ID: 10.0.2.58 | 3
 - Class: ScienceLogic, Inc.
 - Organization: System
 - Collection Mode: Active
 - Description: ScienceLogic EM7 G3 - Data Collector
 - Managed Type: Physical Device
 - Category: System EM7
 - Sub-Class: EM7 Data Collector
 - Uptime: 13 days, 00:45:16
 - Collection Time: 2015-06-02 17:55:00
 - Group / Collector: CUG / MOSS_Patch_AIO
- Vitals [Current]:**
 - Overall Health: Notice
 - Availability: Ok
 - Latency: 0.1585 ms
 - CPU: 5.39%
 - Memory: 75.04%
 - Swap: 50%
- Vitals [Average]:**
 - Avail (24 Hr): 100%
 - Latency (24 Hr): 0.14 ms
- Monitors:**
 - /data.local: 27.000%
 - user: 82.000%
 - / (Root): 50.000%
 - ivar: 9.000%
 - /home: 2.000%
 - Avail_collect_c: Healthy
- System Component Utilization:**
 - Bar chart showing utilization for /data.local, user, / (Root), ivar, /home.
- Tickets and Events:**
 - 1 ticket: [Trap Received: cbgpPeerPrevState] | Trap Detail: cbgpPeerPrefixAccepted92.168.33.20.3; (Trap OID: 1.3.6.1.4.1.9.1.87.1.2.1.1.8)
 - Active Events: 1
 - Cleared Events: 305
 - Active Tickets (OWP): --
 - Resolved Tickets: --
 - Log Messages: 10,000
 - Software Titles: --
 - Processes: 45
 - Services: --
- Hourly Interface Usage:**
 - Line graph showing % In and % Out usage for eth0 from 27 May to 02 Jun.

- The **Device Summary** page displays the following read-only information about the device:

- Vitals.** Information about the overall health of the device.
- Tickets and Events.** List of active tickets and events associated with the device.

- **Elements.** List of elements associated with the device and links to a page with details on each element.
- **Monitors.** List of monitoring policies associated with the device.
- **System Component Utilization.** Overview of CPU, memory, swap, and file system usage.
- **Hourly Interface Usage.** Overview of the hourly bandwidth usage of the primary interface.

5. Each pane is described in detail in the sections below.

NOTE: Data can be up to 1 hour old in the **Device Summary** page.

Read-Only Information

Each page in the **Device Administration** panel and the **Device Reports** panel displays 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 a 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.

Vitals

The Default device dashboard includes the **Vitals** pane. This pane displays information about the overall health of the device. You can view information on the following:

- **Device Rating.** The amount of the available monitoring capacity of the SL1 system that is used by this device. The device rating is calculated hourly, based on the license that was used to install the SL1 system and the amount of collection it is performing for this device, among other statistics.

NOTE: The **Device Rating** field appears only for users of type "Administrator".

- **Overall Health.** The condition of the device. This correlates with the condition of the most severe outstanding events. Clicking on this field leads to the System Vitals Summary Report, in the **Device Performance** page. Possible values for this field are:
 - **Critical.** Critical events are those that require immediate attention.
 - **Major.** Major events are those that require immediate investigation.
 - **Minor.** Minor events are those that need to be investigated before problems become severe.
 - **Notice.** Notice events are those that require attention but are not problem-related.
 - **Healthy.** Healthy events are those that are not urgent.
- **Availability.** Availability means the device's ability to accept connections and data from the network. The possible values are "okay" and "critical" or "undefined". Clicking on the value leads to System Availability Report, in the **Device Performance** page for the device.
 - A device will have an availability of "undefined" if SL1 is not monitoring availability for the device. This applies mostly to Virtual Devices and Component Devices with no aligned component identifiers of type "Availability".
- **Latency.** Latency for the device. Latency means the amount of time it takes SL1 to communicate with the device. The value in this field specifies the number of milliseconds it takes to communicate with the device. Clicking on the value leads to System Latency Report, in the **Device Performance** page for the device.

- **Avail (24 Hr.)**. The device's average availability for the last 24 hours. Availability will be displayed in percent value. Clicking on this field leads to the System Vitals Summary Report, in the **Device Performance** page.
- **Latency (24 Hr.)**. The device's average latency for the last 24 hours. The value in this field specifies the average number of milliseconds it took to communicate with the device. Clicking on the value leads to System Latency Report, in the **Device Performance** page for the device.
- **CPU Usage**. Displays total CPU usage, in percent. Clicking on the value leads to the Overall CPU Utilization Report, in the **Device Performance** page for the device.
- **Memory Usage**. Displays total memory usage, in percent. Clicking on the value leads to the Overall Memory Utilization report, in the **Device Performance** page for the device.
- **Swap Usage**. Displays total memory usage, in percent. Clicking on the value leads to the Overall Virtual Memory Utilization report, in the **Device Performance** page for the device.

Tickets and Events

The Normal device dashboard (the default dashboard) includes the **Tickets and Events** pane. This pane displays a list of active events associated with the device. For each event, the pane displays:

- **Date and time**. Date and time the event last occurred on the device.
- **Message**. The event message. The message is color-coded for severity.
 - **Critical**. Critical events are those that require immediate attention.
 - **Major**. Major events are those that require immediate investigation.
 - **Minor**. Minor events are those that need to be investigated before problems become severe.
 - **Notice**. Notice events are those that require attention but are not problem-related.
 - **Healthy**. Healthy events are those that are not urgent.

Clicking on an event displays the **Event Summary** modal page, where you can view details about the event.

For details on events, see the manual **Events**.

The **Tickets and Events** pane displays a list of active tickets associated with the device. For each ticket, the pane displays:










- **Ticket ID**. Unique numeric ID, automatically assigned to the ticket by SL1.
- **Message**. The ticket message. The message is color-coded for severity.
 - **Critical**. Critical tickets are those that require immediate attention.
 - **Major**. Major tickets are those that require immediate investigation.
 - **Minor**. Minor ticket are those that need to be investigated before problems become severe.
 - **Notice**. Notice ticket are those that require attention but are not problem-related.
 - **Healthy**. Healthy tickets are those that are not urgent.


Clicking on a ticket displays the **Ticket Summary** modal page, where you can view details about the ticket.

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

Elements

The Normal device dashboard (the default dashboard) includes the **Elements** pane. This pane displays information about the elements associated with the device. This pane can contain entries for one or more of the following:

- **Active Events**. Specifies the number of active events associated with the device. Clicking on the events icon () or the number of events leads to the **Viewing Active Events** page, where you can view details about the list of active events associated with the device.
- **Cleared Events**. Specifies the number of events that have been cleared or automatically resolved. Clicking on the events icon () or the number of events leads to the **Viewing Cleared Events** page, where you can view details about the list of active events associated with the device.
- **Active Tickets (OWP)**. Specifies the number of active tickets associated with the device. Clicking on the life-ring icon () or the number of tickets leads to the **Ticket History** page, where you can view details about the active tickets for the device.
- **Resolved Tickets**. Specifies the number of resolved tickets associated with the device. Clicking on the life-ring icon () or the number of tickets leads to the **Ticket History** page, where you can view details about the resolved tickets for the device.
- **Log Messages**. Specifies the number of log entries associated with the device. Clicking on the page icon () or the number of log entries leads to the **Device Logs & Messages** page, where you can view details about each log entry associated with the device.
- **Asset Record**. Specifies whether or not an asset record has been created for the device. The possible values are "Yes" and "No". Clicking on the asset icon () or "Yes" or "No" leads to the **Asset Properties** page, where you can create an asset record or view details of an existing the asset report.
- **Product Services**. Specifies the number of product or service SKUs associated with the device. Clicking on the barcode icon or the number of products displays the **Product Services** modal page. In this page, you can view details about the products associated with the device.
- **Software Titles**. Specifies the number of software titles found on the device. Clicking on the software icon () or the number of software titles leads to the **Software Packages** page, where you can view details about the software titles on the device.
- **Processes**. Specifies the number of processes running on the device. Clicking on the gear icon () or the number of processes leads to the **System Processes** page, where you can view details about the processes running on the device.
- **Services**. Specifies the number of Windows services running on the device. Clicking on the gear icon () or the number of services leads to the **Windows Services** page, where you can view details about the Windows services running on the device.

- **TCP Ports.** Specifies the number of open TCP ports on the device. Clicking on the port icon () or the number open ports leads to the **Port Security** page, where you can view details about the open ports on the device.

Monitors

The Normal device dashboard (the default dashboard) includes the **Monitors** pane. This pane displays information about the monitoring policies associated with the device. This pane can display the following:

- **Domain Name.** Displays the status of a domain-name, based on the domain-monitoring policy associated with the device. Clicking on the policy name or the status leads to the DNS Report, in the **Device Performance** page for the device.
- **System Processes.** Displays the status of a system process, based on the system-process monitoring policy associated with the device. Clicking on the policy name or the status leads to the Process Report, in the **Device Performance** page for the device.
- **SOAP/XML Transactions.** Displays the availability of a SOAP/XML server and content, based on the SOAP/XML transaction policy associated with the device. Clicking on the policy name or the status leads to the Data Transaction Report | Availability, in the **Device Performance** page for the device.
- **Web content.** Displays the status of specific web content, based on the web content policy associated with the device. Clicking on the policy name or the status leads to the Content Verification Report | Availability, in the **Device Performance** page for the device.
- **File systems.** For each monitored file system, specifies the percentage current used. Clicking on the name of the file system or its percentage value displays the File System Report, in the **Device Performance** page for the device.

For details on monitoring policies, see [Monitoring Domain Servers and DNS Records](#), [Monitoring Email Round-Trips](#), [Monitoring SOAP and XML Transactions](#), and [Monitoring Web Content](#).

System Component Utilization

The Normal device dashboard (the default dashboard) includes the **System Component Utilization** pane. This pane displays information about hardware usage by the device. The graph displays information about the following hardware components:

- **CPU.** Displays the total amount of CPU currently being used, in percent. Clicking on this bar in the graph leads to the Overall CPU Utilization Report, in the **Device Performance** page for the device.
- **Memory.** Displays total amount of memory currently being used, in percent. Clicking on this bar in the graph leads to the Overall Virtual Memory Utilization Report, in the **Device Performance** page for the device.
- **Swap.** Displays the total amount of swap space currently being used, in percent. Clicking on this bar in the graph leads to the Overall Virtual Memory Utilization Report, in the **Device Performance** page for the device.
- **File Systems.** For each file-system on the device, displays percent of disk-space used. Clicking on this bar in the graph leads to the File System Report in the **Device Performance** page for the device.

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), that file system does not appear in the System Component Utilization pane.

Hourly Interface Usage

The Normal device dashboard (the default dashboard) includes the **Hourly Interface Usage** pane. This pane displays the bandwidth usage for the a selected interface on the device. The graph uses two distinct colors to display the average incoming and outgoing bandwidth used by the network interface, in hourly increments.

You can select the following parameters for the graph:

- **Measurement.** Based on your account preferences, this field is set to either Utilization (%) or the unit of measure specified in the **Measurement** field in the **Interface Properties** page by default. For the current login session, you can select a different unit of measure. Choices are: Octets, Utilization (%), Kilobytes, Megabytes, Gigabytes, Terabytes, or Petabytes. Until you log out of your current user interface session, the **Hourly Interface** usage graph will use the unit of measure you select in this field.
- **Interface.** By default, SL1 displays the interface for which you have selected **Display on Summary** in the **Interface Properties** page. For the current login session, you can select a different interface to display. Until you log out of your current user interface session, the Hourly Interface usage graph will display data about the interface you select in this field.

Mousing over any area of the graph displays the bandwidth values and the date and time associated with the data point.

Highlighting an area on the graph by clicking and dragging zooms in on the selected area. Clicking on the Show-All icon returns the graph to its default display.

Shortcut Keys for Device Reports panel

When you view information for a device by selecting its bar graph icon () , you enter the **Device Reports** panel.

When you enter the **Device Reports** panel, you can use the following shortcut keys to navigate the tabbed pages and the entries in the menus on a page.

Page or Tab	Shortcut Keys
Administer Bookmarks page	Ctrl + Alt + B
Configuration Report page	Ctrl + Alt + C
Viewing Active Events page	Ctrl + Alt + E
Guides page	Ctrl + Alt + G

Page or Tab	Shortcut Keys
Interfaces Found page	Ctrl + Alt + I ("eye")
Device Logs & Messages page	Ctrl + Alt + L
Performance Tab (System Vitals page, by default)	Ctrl + Alt + P
Device Summary page	Ctrl + Alt + S
Ticket History page	Ctrl + Alt + T
Exit the Device Report panel	Ctrl + Alt + X
Device Summary page	Ctrl + Alt + . ("period")
Ticket Editor page	Ctrl + Alt + <Enter>

Chapter



6

Viewing Performance Graphs

Overview

This chapter describes the **[Performance]** tab of the **Device Reports** panel on the **Device Manager** page (Devices > Device Manager). The **[Performance]** tab displays performance graphs for hardware, monitoring policies, and Dynamic Applications.

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:

<i>Features of the Performance Tab</i>	120
<i>Viewing System Vitals for a Device</i>	122
<i>Viewing Availability Reports for a Device</i>	124
<i>Viewing Latency Reports for a Device</i>	127
<i>Viewing a Report on CPU Usage for a Device</i>	130
<i>Viewing a Report on Physical Memory Usage for a Device</i>	132
<i>Viewing a Report on Virtual Memory Usage for a Device</i>	134
<i>Viewing a Report on File System Usage for a Device</i>	136
<i>Viewing Reports on Network Interfaces</i>	140
<i>Default Reports for Network Interfaces</i>	141
<i>CBQoS Reports for Network Interfaces</i>	149
<i>Viewing Reports about DNS Servers and DNS Records for a Device</i>	161

Viewing Reports on an Email Round-Trip Monitoring Policy	163
Viewing Reports on an SOAP or XML Transaction Policy	165
Viewing Availability Reports for a Single System Process on a Device	171
Viewing Port Availability Reports for a Single Device	174
Viewing Reports for a Web Content Policy	175
Viewing Availability Reports for a Single Windows Service on a Device	182

Features of the Performance Tab

The **[Performance]** tab of the **Device Reports** panel displays performance graphs for hardware, monitoring policies, and Dynamic Applications. From the **Performance** page, you can view the one or more of the following types of reports (among others). These reports are described in this chapter.

- **System Vitals**. Displays the device's availability, latency, overall CPU usage, overall memory usage, and overall virtual memory usage, all displayed on separate lines and graphed over time.
- **System Availability**. Displays the device's availability, graphed over time. Availability means the device's ability to accept connections and data from the network
- **System Latency**. Availability. Displays the device's latency, graphed over time. Latency means the amount of time it takes SL1 to communicate with the device.
- **CPU Utilization**. Displays the device's total CPU usage, in percentage. If a device contains multiple CPUs, the report displays the total combined CPU usage, in percent.
- **Memory Utilization**. This report displays total memory usage over time, in percent.
- **Virtual Memory Utilization**. This report displays total virtual memory usage over time, in percent.
- **File Systems**. The File System reports display the amount of disk-space used, in percent, for a device. For each discovered file system on the device, SL1 generates a file system report. This report displays the file system usage, over time, in percent. For devices with multiple file systems, SL1 also generates a Composite report, which displays file system usage, over time, in percent, for each file system, but on a single graph.

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), that file system does not appear in the File System reports in the **Device Performance** page.

- **Network Interfaces**. For each discovered network interface on the device, SL1 generates five reports:
 - Utilization, Bandwidth Usage, and Bandwidth Usage (Stacked), which display bandwidth usage over time
 - Errors and Discards and Errors and Discards %, which display errors and discards over time

If an interface is configured for CBQoS and you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior), SL1 will display the collected CBQoS data in reports. For each CBQoS Policy and each class map under that policy, SL1 can generate reports on the following based on the CBQoS configuration:

- Class Maps
 - Policing
 - Sets
 - Match Statements
 - Queuing
 - Sets
 - Traffic Shaping
 - WRED
- **Domain Name Monitors.** Displays the availability of the domain-name server and the specified record on that domain server over time, in percent. The report also displays the lookup time for each request (each time SL1 contacts the server).
 - **Email Round-Trip Monitors.** Displays the number of milliseconds it takes to send a message to an external mail server and then receive a response message back from that external mail server.
 - **SOAP/XML Transaction Monitors.** For each SOAP/XML transaction monitoring policy, displays multiple reports, including a report on the availability of the SOAP or XML server and specific content on the server. Also displays reports on page size, download speed, lookup time, connection time, and transaction time.
 - **System Process Monitors.** The System Process reports displays availability of system processes. For each monitored system process, SL1 generates a process report. This report displays availability of that process, in percent. For devices with multiple monitored processes, SL1 also generates a Composite report, which displays availability of multiple processes over time, but on a single graph.
 - **TCP/IP Port Monitors.** For each monitored port, displays availability of that port, in percent. Availability means the port's ability to accept connections and data from the network.
 - **Web Content Monitors.** For each web content monitoring policy, displays multiple reports, including a report on the availability of the web server and specific content on the server. Also displays reports on page size, download speed, lookup time, connection time, and transaction time.
 - **Windows Service Monitors.** For each monitored Windows Service, displays availability of that Windows service, in percent. Availability means whether the service is enabled and running.
 - **Collection Groups and Collection Labels.** For each Collection Label assigned to a Dynamic Application to which the device subscribes, displays collected values for the aligned presentation object, over time. For more information on Collection Labels, see the chapter [Graphing Data from Multiple Dynamic Applications in a Single Dashboard Widget](#).

The list of links in the Navigation Bar can also include links to reports (presentation objects) defined in the Dynamic Applicationsto which the device subscribes .

NOTE: Component devices that were discovered using component mapping in Dynamic Applications might display **only** reports defined in a Dynamic Application.


Viewing System Vitals for a Device

The System Vitals Summary Report displays multiple device-parameters in a single graph. The System Vitals Summary Report trends the following parameters:

- System Availability (Availability means the device's ability to accept connections and data from the network.)
- System Latency (Latency means the amount of time it takes SL1 to communicate with the device.)
- Overall CPU Usage
- Overall Physical Memory Usage
- Overall Swap Usage

The graph displays system availability, system latency, memory usage, virtual-memory usage, and CPU usage for the selected duration.

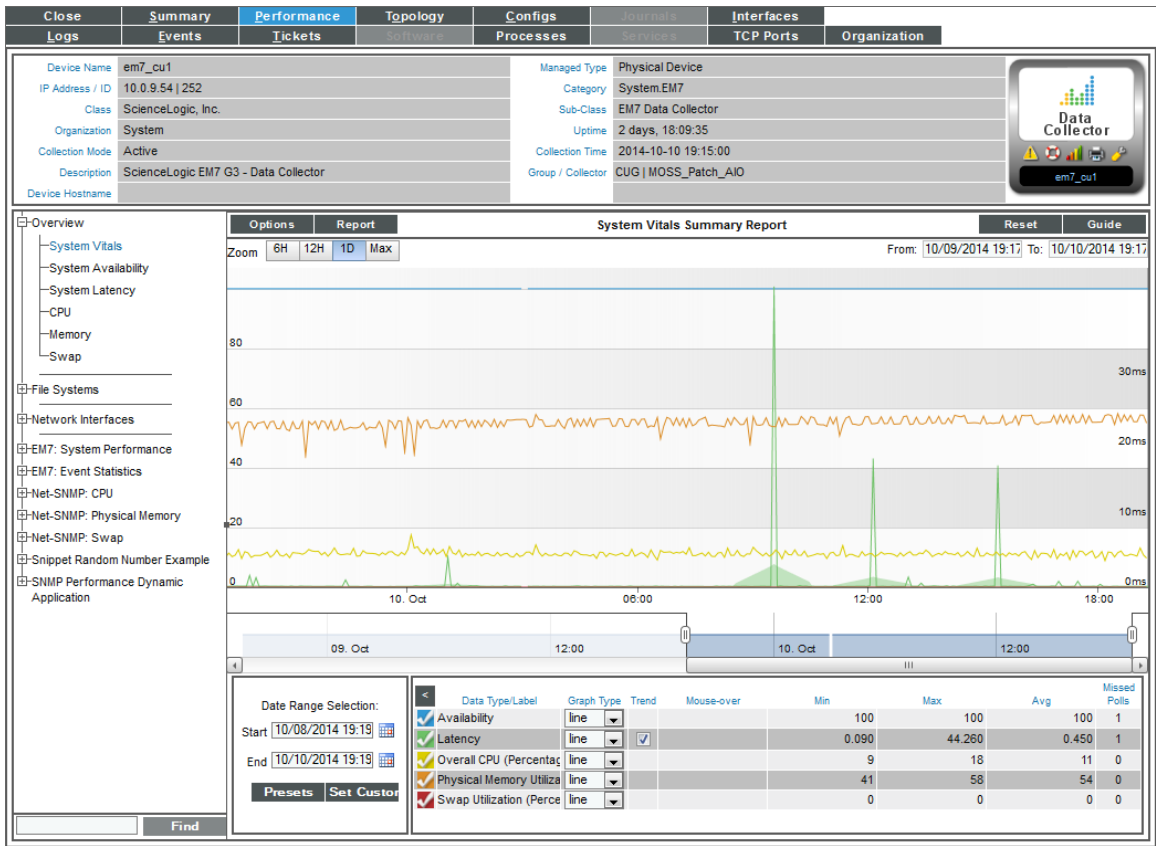
To view the System Vitals report for a device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to view the vitals report. Select its bar graph icon .

Device Manager (Devices Found [1293])													Actions	Report	Reset	Guide
Device Name	Device Hostname	IP Address	Device Gateway	Device Class / Sub-class	DID	Organization	Current State	Collection Status	Collection State	SNMP Capable	SNMP Version					
1	10.100.100.40	--	10.100.100.40	Pingable	Ping / ICMP	274	System	Healthy	CUG	User-Disabled	--	--				
2	10.100.100.46	--	10.100.100.46	Pingable	FreeBSD / ICMP	294	Johto	Healthy	CUG	User-Disabled	--	--				
3	10.7.11.186	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2				
4	10.7.11.186	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2				
5	10.7.11.186	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2226	System	Notice	CUG	Active	SNMP Public V2	V2				
6	10.7.11.186.5951	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2				
7	10.7.11.186.8222	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1204	System	Healthy	CUG	Active	SNMP Public V2	V2				
8	10.7.11.186.7706	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1951	System	Healthy	CUG	Active	SNMP Public V2	V2				
9	10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2498	System	Healthy	CUG	Active	SNMP Public V2	V2				
10	10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2				
11	10.7.11.187	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2				
12	10.7.11.187.4289	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1952	System	Healthy	CUG	Active	SNMP Public V2	V2				
13	10.7.11.187.5996	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1206	System	Healthy	CUG	Active	SNMP Public V2	V2				
14	10.7.11.187.5090	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1431	System	Healthy	CUG	Active	SNMP Public V2	V2				
15	10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2080	System	Healthy	CUG	Active	SNMP Public V2	V2				
16	10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2				
17	10.7.11.189	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2				
18	10.7.11.189.6662	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	2102	System	Healthy	CUG	Active	SNMP Public V2	V2				
19	10.7.11.189.7240	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1391	System	Healthy	CUG	Active	SNMP Public V2	V2				
20	10.7.11.189.7881	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	855	System	Healthy	CUG	Active	SNMP Public V2	V2				
21	10.7.11.237	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2				
22	10.7.11.237.7659	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem	1423	System	Healthy	CUG	Active	SNMP Public V2	V2				
23	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2933	System	Notice	CUG	Active	SNMP Public V2	V2				
24	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2				
25	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2				
26	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2				
27	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2651	System	Healthy	CUG	Active	SNMP Public V2	V2				
28	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2				
29	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2				
30	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2				
31	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2				
32	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2952	System	Healthy	CUG	Active	SNMP Public V2	V2				
33	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2				
34	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2				
35	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2				
36	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2				
37	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2				
38	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2				
39	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2				
40	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2				
41	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2				
42	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2				
43	10.7.12.125	--	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2				

3. In the **Device Reports** panel, select the **[Performance]** tab.

- In the **[Performance]** tab, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **System Vitals**.



- The System Vitals report displays multiple device-parameters for the selected date and time range.
 - The y-axis displays usage, in percent, to the left and actual value to the right.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - Each parameter is represented by a color-coded line.
 - Mousing over any point in any line displays the high, low, and average value at that time-point in the **Data Table** pane.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.
- The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
- The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report. Displays a list of formats for saving the report.

8. The **Data Table** at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
- **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the check mark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.

Viewing Availability Reports for a Device

The System Availability report displays information about the device's availability. Availability means the device's ability to accept connections and data from the network.

During polling, a device has two possibly availability values:

- 100%. Device is up and running.
- 0%. Device is not accepting connections and data from the network.

By default, the method of discovery determines how the SL1 monitors availability for a device:


- If the agent is installed and creates a device record before the device is discovered as an SNMP or pingable device, availability is measured based on uptime data collected by the agent.
- If the device is discovered as an SNMP or pingable device before the agent is installed, availability is monitored with the method specified in the discovery session (SNMP, ICMP, or TCP).

For devices that SL1 discovers with the discovery tool (Devices > Add Devices button), SL1 determines availability by checking the status of the port specified in the **Availability Port** field in the **Device Properties** page. SL1 collects device-availability data every five minutes, as specified in the process "Data Collection: Availability" (in the **Process Manager** page).

For component devices that SL1 discovers with component mapping Dynamic Applications, SL1 determines availability by checking the status of a collection object.

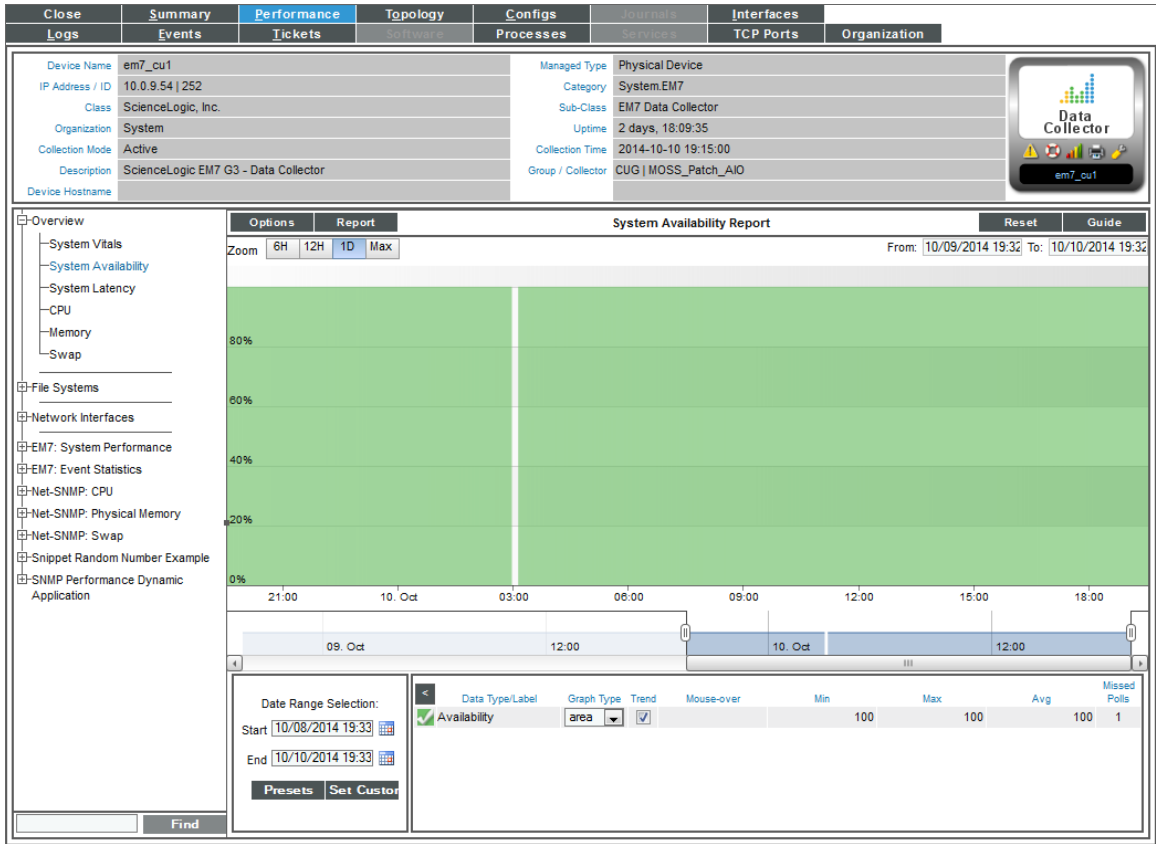
For devices that SL1 discovers with the agent, SL1 collects uptime data from the agent every 5 minutes, and uses this value to determine device availability.

To view the System Availability report 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 view the availability report. Select its bar graph icon ()

Device Manager Devices Found (1293)													Actions	Report	Reset	Guide
Device Name	Device Hostname	IP Address	Device Category	Device Class / Sub-class	OID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version					
1	10.100.100.40	10.100.100.40	Pingable	Ping [CMP]	274	System	Healthy	CUG	User-Disabled	--	--					
2	10.100.100.45	10.100.100.45	Pingable	FreeBSD [CMP]	294	John	Healthy	CUG	User-Disabled	--	--					
3	10.7.11.186	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2					
4	10.7.11.188	--	Network App F5 Networks, Inc.	[BG-PLTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2					
5	10.7.11.188	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2					
6	10.7.11.188.8581	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1430	System	Healthy	CUG	Active	SNMP Public V2	V2					
7	10.7.11.188.8222	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1204	System	Healthy	CUG	Active	SNMP Public V2	V2					
8	10.7.11.188.7798	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1951	System	Healthy	CUG	Active	SNMP Public V2	V2					
9	10.7.11.187	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2					
10	10.7.11.187	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2					
11	10.7.11.187	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2					
12	10.7.11.187.4269	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1952	System	Healthy	CUG	Active	SNMP Public V2	V2					
13	10.7.11.187.5996	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1206	System	Healthy	CUG	Active	SNMP Public V2	V2					
14	10.7.11.187.6088	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1431	System	Healthy	CUG	Active	SNMP Public V2	V2					
15	10.7.11.188	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2686	System	Healthy	CUG	Active	SNMP Public V2	V2					
16	10.7.11.188	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2					
17	10.7.11.188	--	Network App F5 Networks, Inc.	[BG-PLTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2					
18	10.7.11.188.6662	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	2102	System	Healthy	CUG	Active	SNMP Public V2	V2					
19	10.7.11.188.7340	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1391	System	Healthy	CUG	Active	SNMP Public V2	V2					
20	10.7.11.188.7651	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	655	System	Healthy	CUG	Active	SNMP Public V2	V2					
21	10.7.11.237	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2					
22	10.7.11.237.7659	--	Network App F5 Networks, Inc.	[BG-PLTM Pool Mem1	1423	System	Healthy	CUG	Active	SNMP Public V2	V2					
23	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2					
24	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2					
25	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2					
26	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2					
27	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2					
28	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2					
29	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2426	System	Healthy	CUG	Active	SNMP Public V2	V2					
30	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2					
31	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2					
32	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2662	System	Healthy	CUG	Active	SNMP Public V2	V2					
33	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2					
34	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2754	System	Notice	CUG	Active	SNMP Public V2	V2					
35	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2					
36	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2					
37	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2					
38	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2					
39	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2					
40	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2					
41	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2					
42	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2					
43	10.7.12.125	--	Network App F5 Networks, Inc.	[BG-PLTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2					

- In the **Device Reports** panel, select the Performance tab.



- In the Performance tab, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **System Availability**.
- The System Availability report displays system availability for the selected date and time range.
 - The y-axis displays usage, in percent to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - Mousing over any point in any line displays (in the **Data Table** pane) the high, low, and average value at the selected time-point.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.
- The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
- The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report. Displays a list of formats for saving the report.


8. The **Data Table** at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
- **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the check mark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.












































Viewing Latency Reports for a Device

The System Latency report displays a graph with information about a single device's latency over time.

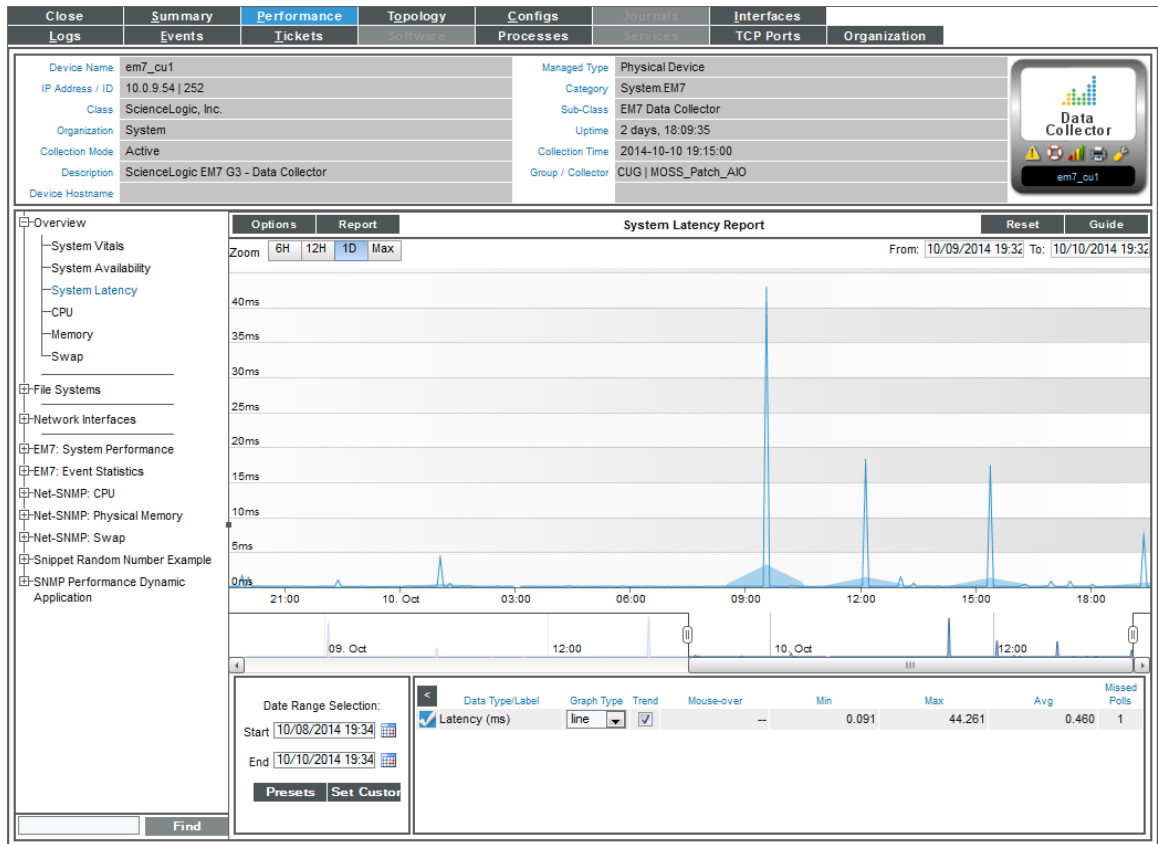
To view the System Latency report for a device:

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

- In the **Device Manager** page, find the device for which you want to view the latency report. Select its bar graph icon ().

Device Manager Devices Found (1293)												
Device Name	Device Hostname	IP Address	Device Subcategory	Device Class / Sub-class	DCG	Organization	Current State	Collection Status	Collection State	SNMP Credentials	SNMP Message	Actions
1	10.100.100.40	10.100.100.40	Pingable	Ping / ICMP	274	System	Healthy	CUG	User-Disabled	--	--	
2	10.100.100.46	10.100.100.46	Pingable	FreeBSD / ICMP	294	John	Healthy	CUG	User-Disabled	--	--	
3	10.7.11.186	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2	
4	10.7.11.186	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2	
5	10.7.11.186	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2	
6	10.7.11.188.8222	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1430	System	Healthy	CUG	Active	SNMP Public V2	V2	
7	10.7.11.188.8222	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1204	System	Healthy	CUG	Active	SNMP Public V2	V2	
8	10.7.11.188.7706	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1951	System	Healthy	CUG	Active	SNMP Public V2	V2	
9	10.7.11.187	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2	
10	10.7.11.187.183	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2	
11	10.7.11.187	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2	
12	10.7.11.187.4289	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1952	System	Healthy	CUG	Active	SNMP Public V2	V2	
13	10.7.11.187.5996	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1206	System	Healthy	CUG	Active	SNMP Public V2	V2	
14	10.7.11.187.6686	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1431	System	Healthy	CUG	Active	SNMP Public V2	V2	
15	10.7.11.189	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2690	System	Healthy	CUG	Active	SNMP Public V2	V2	
16	10.7.11.189	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2	
17	10.7.11.189	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2	
18	10.7.11.189.6662	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	2102	System	Healthy	CUG	Active	SNMP Public V2	V2	
19	10.7.11.189.7240	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1361	System	Healthy	CUG	Active	SNMP Public V2	V2	
20	10.7.11.189.7831	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	855	System	Healthy	CUG	Active	SNMP Public V2	V2	
21	10.7.11.237	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2	
22	10.7.11.237.7659	--	Network App F5 Networks, Inc.	BIG-IP LTM Pool Mem1	1423	System	Healthy	CUG	Active	SNMP Public V2	V2	
23	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2	
24	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2	
25	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2	
26	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2	
27	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2	
28	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2	
29	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2	
30	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2	
31	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2	
32	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2602	System	Healthy	CUG	Active	SNMP Public V2	V2	
33	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2	
34	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2	
35	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2	
36	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2	
37	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2	
38	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2	
39	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2	
40	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2	
41	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2	
42	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2	
43	10.7.12.125	--	Network App F5 Networks, Inc.	BIG-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2	

- In the **Device Reports** panel, select the Performance tab.



- In the Performance tab, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **System Latency**.
- The System Latency report displays system latency for the selected date and time range.
 - The y-axis displays latency, in milliseconds, to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - Mousing over any point in any line displays the high, low, and average value at that time-point in the Data Table pane.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.
- The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
- The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report. Displays a list of formats for saving the report.



8. The Data Table at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
- **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the check mark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.

Viewing a Report on CPU Usage for a Device

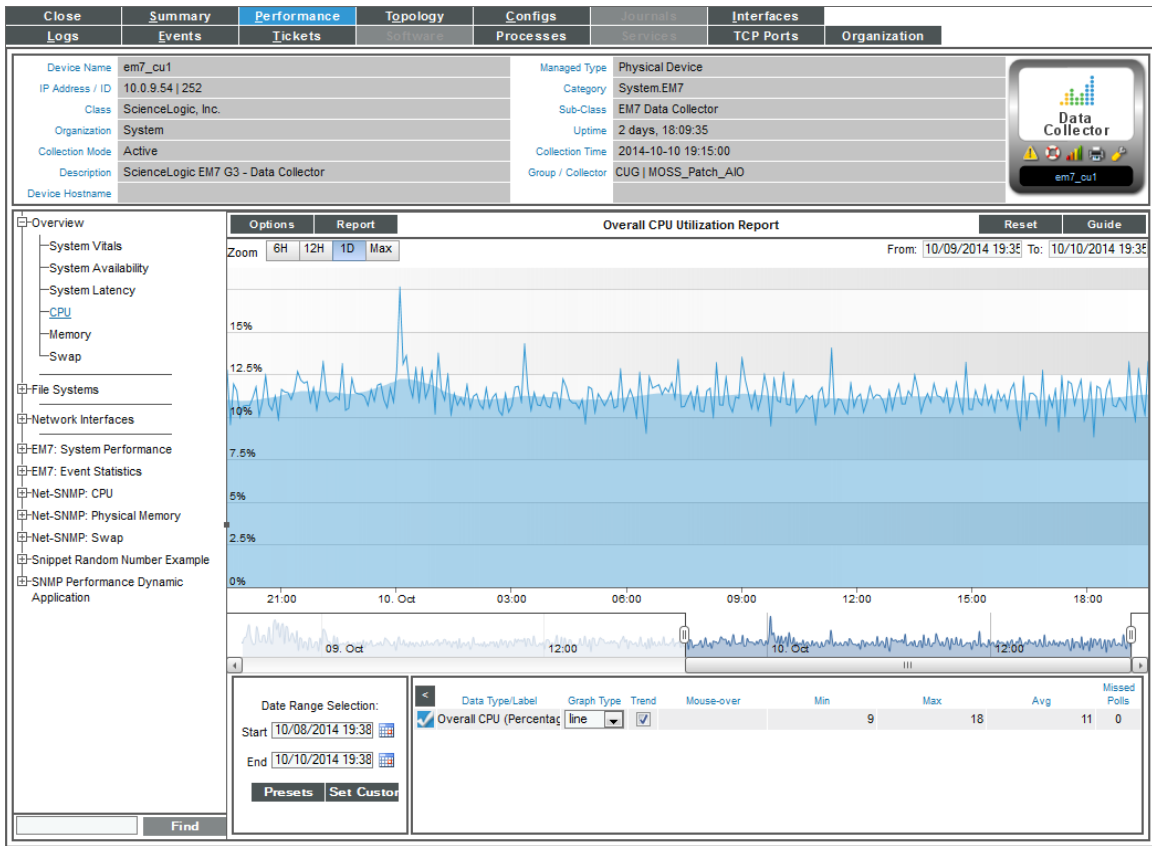
For each device for which SL1 discovered a CPU, you can view a CPU Utilization report.

The CPU Utilization report displays the device's total CPU usage, in percentage. If a device contains multiple CPUs, the report displays the total combined CPU usage, in percent.

To view the CPU Utilization report for a device:

1. You can access the CPU Utilization report from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device where the CPU resides, and select its bar graph icon .
 - Go to the **Device Hardware** page (Devices > Hardware), filter by CPU, find the device where the CPU resides, and select its bar graph icon .
2. When the **Device Reports** panel appears, select the Performance tab.

- In the **Device Performance** page, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **CPU Utilization**.





- The Overall CPU Utilization report displays total CPU usage and average CPU usage over time. If a device contains multiple CPUs, the report displays the total combined CPU usage, in percent, and the combined average CPU usage, in percent. The graph displays CPU usage for the selected date and time range.
 - The y-axis displays usage, in percent to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - Mousing over any point in any line displays (in the Data Table pane) the high, low, and average value at the select time-point.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.
- The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
- The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report, and displays a list of formats for saving the report.

7. The Data Table at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
 - **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the checkmark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** This column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.

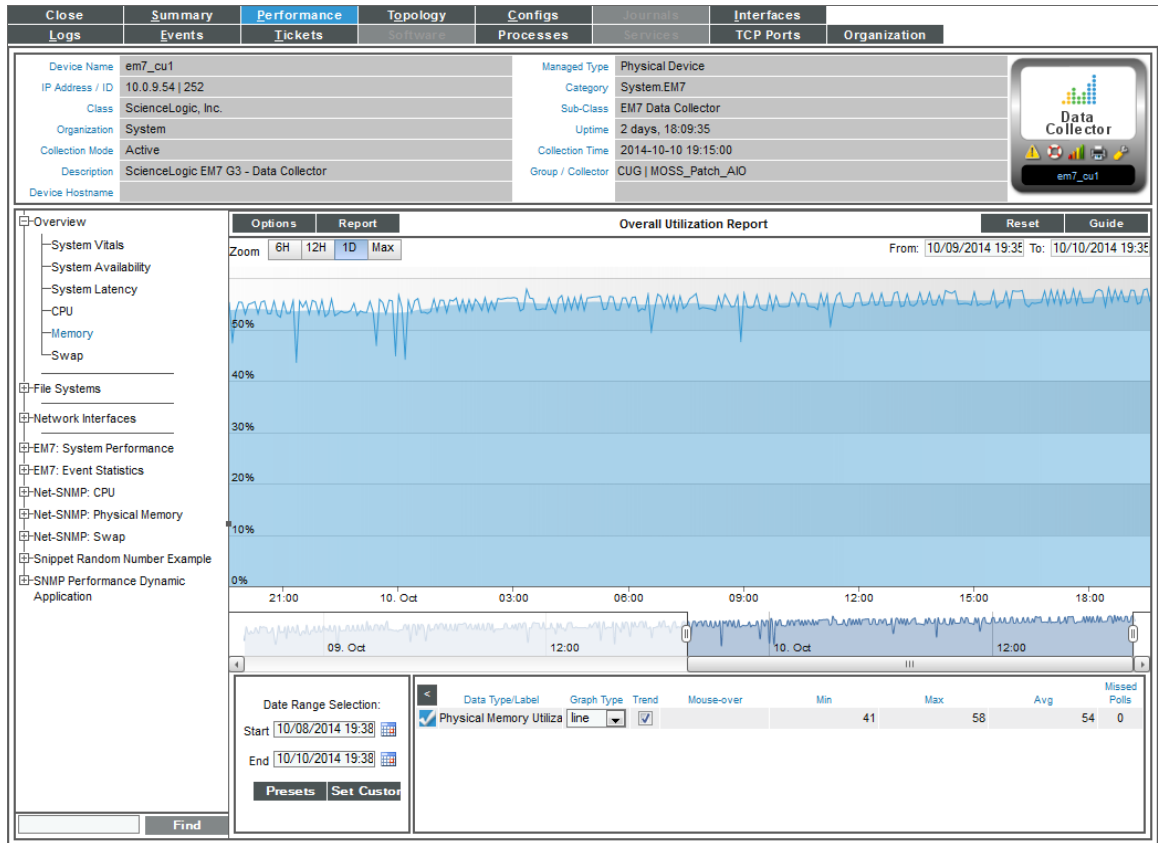
Viewing a Report on Physical Memory Usage for a Device

You can view an Overall Memory Utilization report for each device for which SL1 has discovered physical memory. The Overall Memory Utilization Report displays total memory usage and average memory usage over time.

To view the Overall Memory Utilization report for a device:

1. You can access the Memory Utilization report from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device where the memory resides, and select its bar graph icon .
 - Go to the **Device Hardware** page (Devices > Hardware), filter by CPU, find the device where the memory resides, and select its bar graph icon .

2. When the **Device Reports** panel appears, select the Performance tab.
3. In the **Device Performance** page, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **Memory Utilization**





4. The Overall Memory Utilization report displays total memory usage and average memory usage over time. The graph displays memory usage for the selected date and time range.
 - The y-axis displays memory usage, in percent, to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - If the report includes both physical memory and virtual memory, each is represented by a color-coded stack and color-coded line on the graph.
 - The line graph represents actual usage and the stack represents average usage.
 - Mousing over any point in any line (in the Data Table pane) displays the high, low, and average value at the selected time-point.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

5. The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
6. The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report, and displays a list of formats for saving the report.
7. The Data Table at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
 - **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the checkmark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL 1 was unable to collect the data within the time span of the report.

Viewing a Report on Virtual Memory Usage for a Device

The Overall Virtual Memory Utilization Report displays total virtual memory usage and average virtual memory usage over time.

To view the Overall Virtual Memory Utilization report for a device:

1. You can access the Overall Virtual Memory Utilization report from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device where the virtual memory resides, and select its bar graph icon (.
 - Go to the **Device Hardware** page (Devices > Hardware), filter by CPU, find the device where the virtual memory resides, and select its bar graph icon (.
2. When the **Device Reports** panel appears, select the **[Performance]** tab.
3. In the **Device Performance** page, go to the NavBar (list of links in the left pane), expand the **Overview** link, and select **Virtual Memory Utilization**.



4. The Overall Virtual Memory Utilization report displays total memory usage and average memory usage over time. The graph displays memory usage for the selected date and time range.
 - The y-axis displays virtual memory usage, in percent, to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
 - Mousing over any point in any line displays the high, low, and average value at that time-point in the **Data Table** pane.
 - You can use your mouse to scroll the report to the left and right.
 - In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.
5. The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
6. The **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report, and displays a list of formats for saving the report.
7. The Data Table at the bottom of each report allows you to view details about each data point and view information about the entire report. The data table includes the following:
 - **Data Type/Label**. For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the checkmark toggles on and off the data in the report.
 - **Graph Type**. For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend**. Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover**. When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min**. The column displays the minimum value for the data type in the report.
 - **Max**. This column displays the maximum value for the data type in the report.
 - **Avg**. This column displays the average value for the data type in the report.
 - **Missed Polls**. This column displays the number of times SL1 was unable to collect the data within the time span of the report.

Viewing a Report on File System Usage for a Device

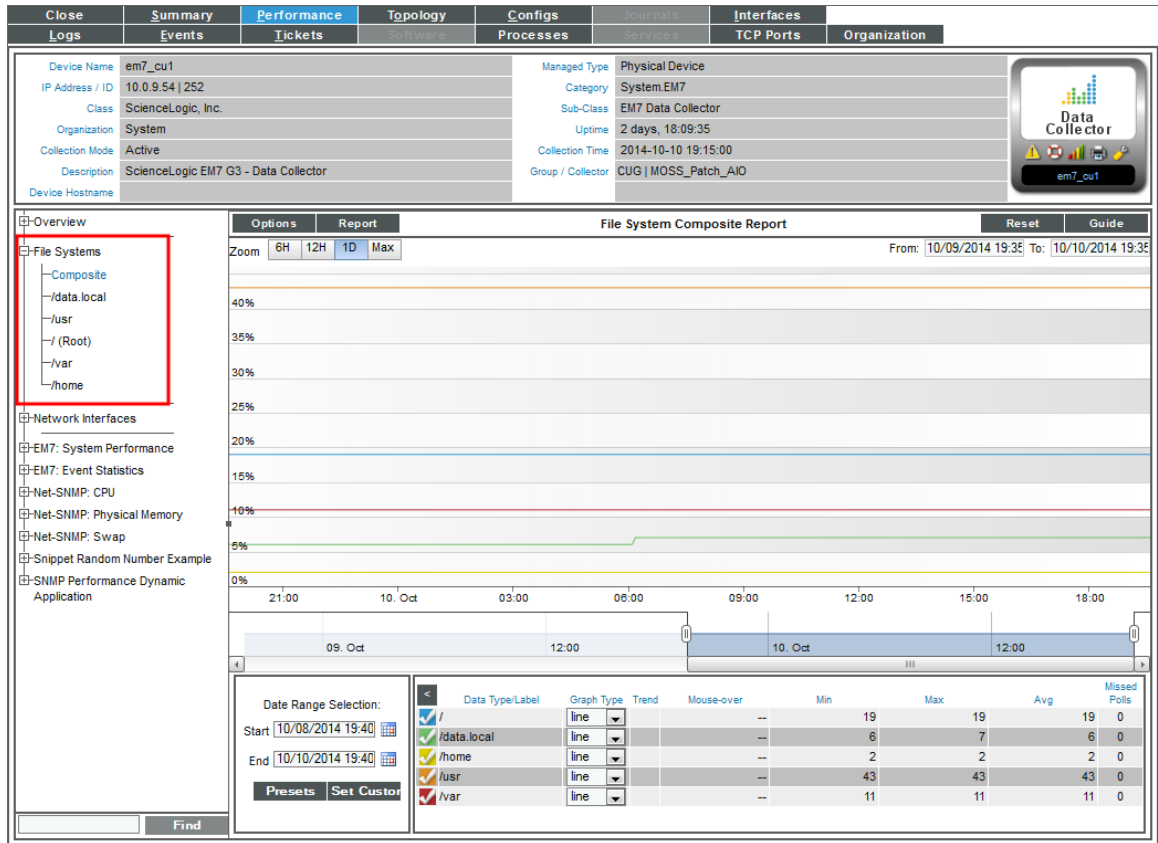
The File System reports display the amount of disk-space used, in percent, for a device. For each discovered file system on the device, SL1 generates a file system report. This report displays the file system usage, over time, in percent. For devices with multiple file systems, SL1 also generates a Composite report, which displays file system usage, over time, in percent, for each file system, but on a single graph.

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), SL1 does not generate a File System Report for that file system.

To view the file-system reports for a device:

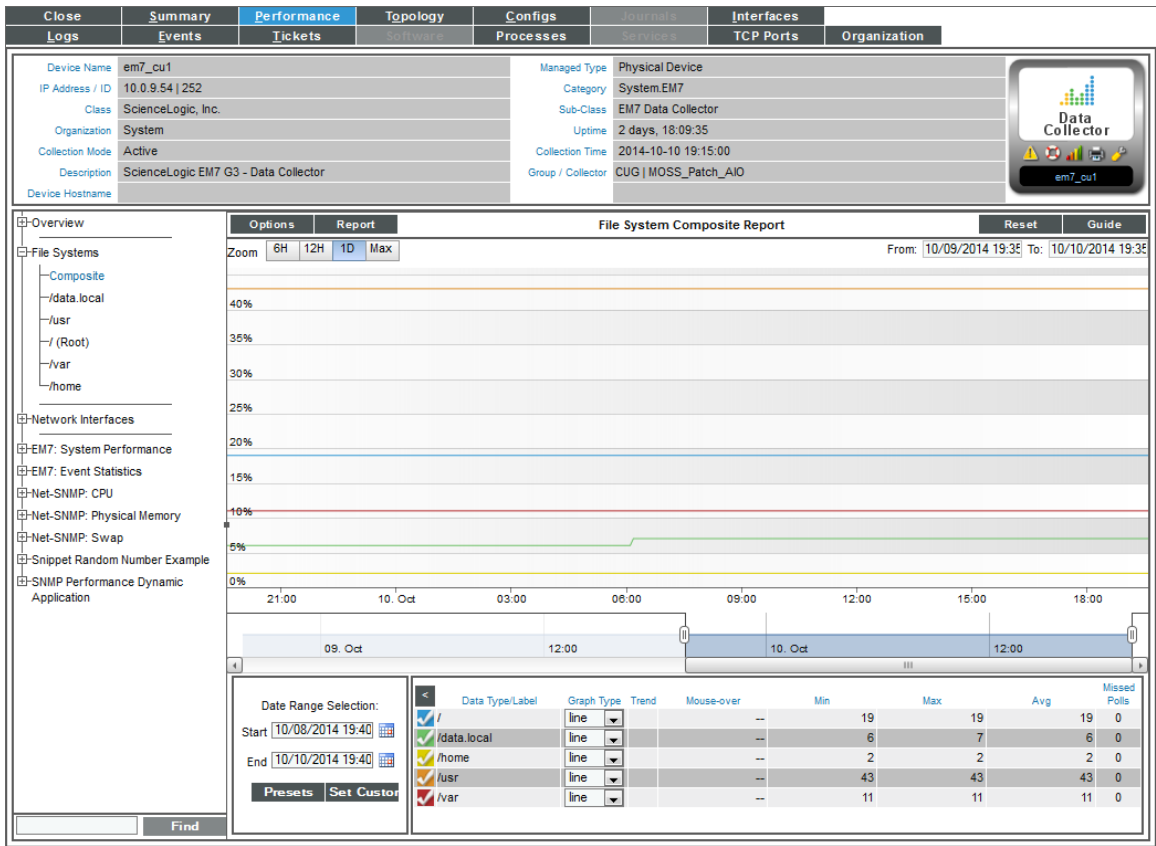
1. You can access the File System reports from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device where the file system resides, and select its bar graph icon ().
 - Go to the **Device Hardware** page (Devices > Hardware), filter by CPU, find the device where the file system resides, and select its bar graph icon ().

2. When the **Device Reports** panel appears, select the Performance tab.
3. In the **Device Performance** page, go to the NavBar (list of links in the left pane), and expand the **File System Overview** link.



4. If a device has multiple file systems, you can select from two types of reports:
 - **Composite**. Leads to the File System Composite Report, where you can view percent of disk-space used for all file systems on the device. Each file system is represented by a color-coded line.
 - **File System Name**. For a selected file system, the File system Report displays file system usage, over time, in percent.

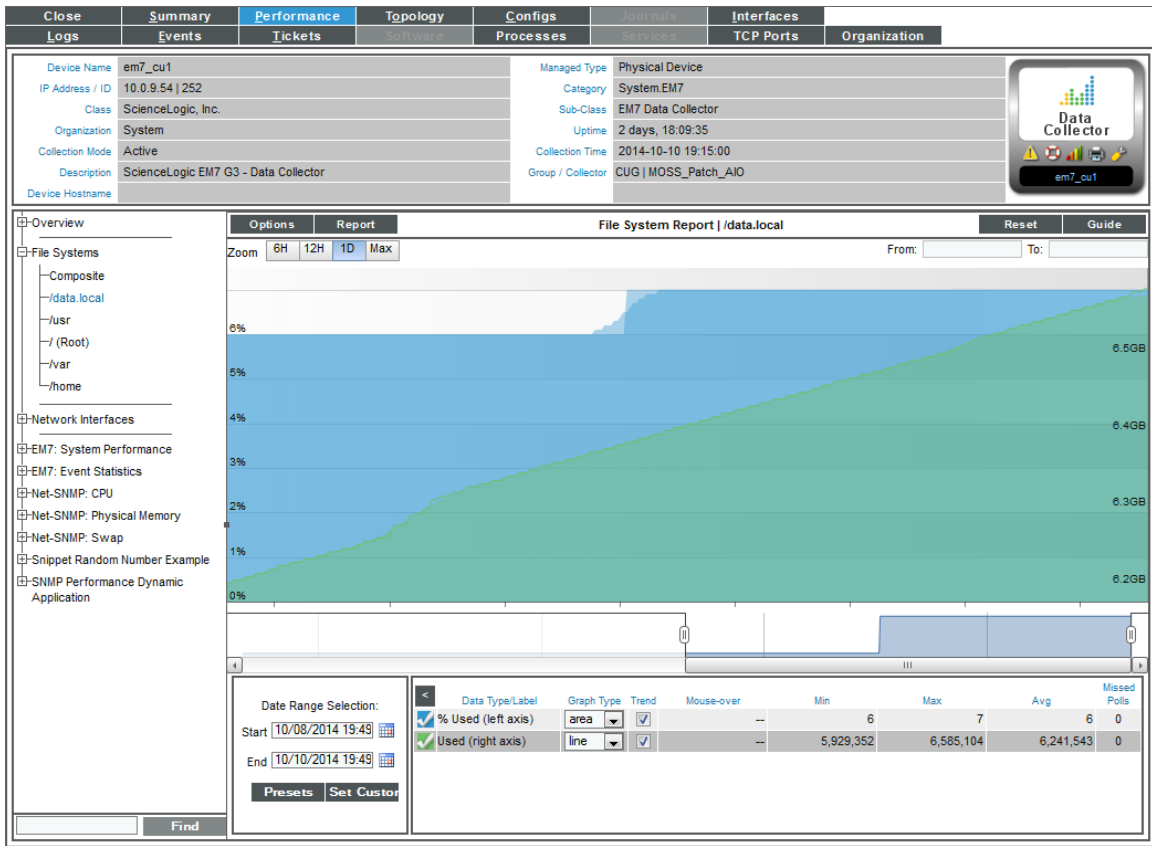
5. The File System Composite Report displays percent of disk-space used for all file systems on the device.



6. The File System Composite Report displays the following:

- The File System Composite Report displays percent of disk-space used on the y-axis and time of day on the x-axis. The report displays data from the last 24 hours.
- The y-axis displays usage, in percent.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Each file system is represented by a color-coded line.
- Mousing over any point in any line displays (in the Data Table pane) the high, low, and average value on each file system at the selected time-point.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

7. The File System Report displays file system usage, for a single file system, over time, in percent.



8. The File System Report displays the following:

- The graph displays a color-coded line for percent usage and a color-coded line for amount used (in MBs).
- The y-axis displays usage, in percent to the left and actual amount used, in MB, to the right.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Each parameter is represented by a color-coded line.
- Mousing over any point in any line displays (in the Data Table pane) the high, low, and average value at the selected time-point.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

9. In both types of file-system reports, the **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.

10. In both types of file-system reports, the **[Reports]** menu in the upper left of the report allows you to export and save the current data and graph as a report, and displays a list of formats for saving the report.

11. In both types of file-system reports, the Data Table at the bottom of each report allows you to view details about each data point and view overview information about the entire report. The data table includes the following:

- **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the checkmark toggles on and off the data in the report.
- **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
- **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
- **Mouseover.** When you mouseover the graph, this column displays the exact value for each data type at that time point on the graph.
- **Min.** The column displays the minimum value for the data type in the report.
- **Max.** This column displays the maximum value for the data type in the report.
- **Avg.** This column displays the average value for the data type in the report.
- **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.

Viewing Reports on Network Interfaces

For each discovered network interface on a device, SL1 generates five network interface reports. These five reports display:

- Utilization
- Bandwidth Usage
- Bandwidth Usage (Stacked)
- Errors and Discards
- Errors and Discards %

If an interface is configured for CBQoS and you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior), SL1 will display the collected CBQoS data in reports. For each CBQoS Policy and each class map under that policy, SL1 can generate reports on the following based on the CBQoS configuration:

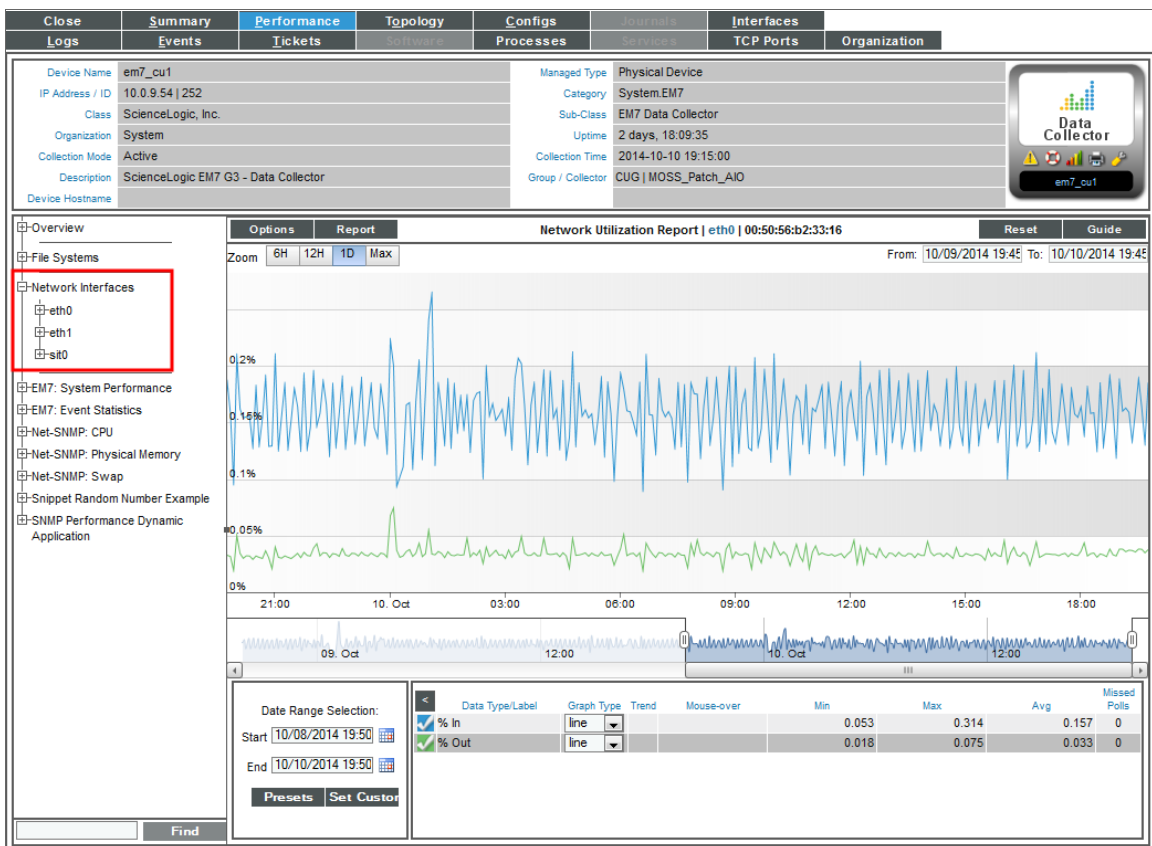
- Class Maps
- Policing
- Sets
- Match Statements

- Queuing
- Sets
- Traffic Shaping
- WRED

Default Reports for Network Interfaces

To view the five default network interface reports for a device:

1. You can access the network interface reports from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device with the desired network interface, and click its bar graph icon (📊).
 - Go to the **Device Hardware** page (Devices > Hardware), find the device with the desired network interface, and click its bar graph icon (📊).
2. When the **Device Reports** panel appears, click the **Performance** tab.
3. In the **Device Performance** page, go to the NavBar (the list of links in the left pane), and expand the **Network Interfaces** link.

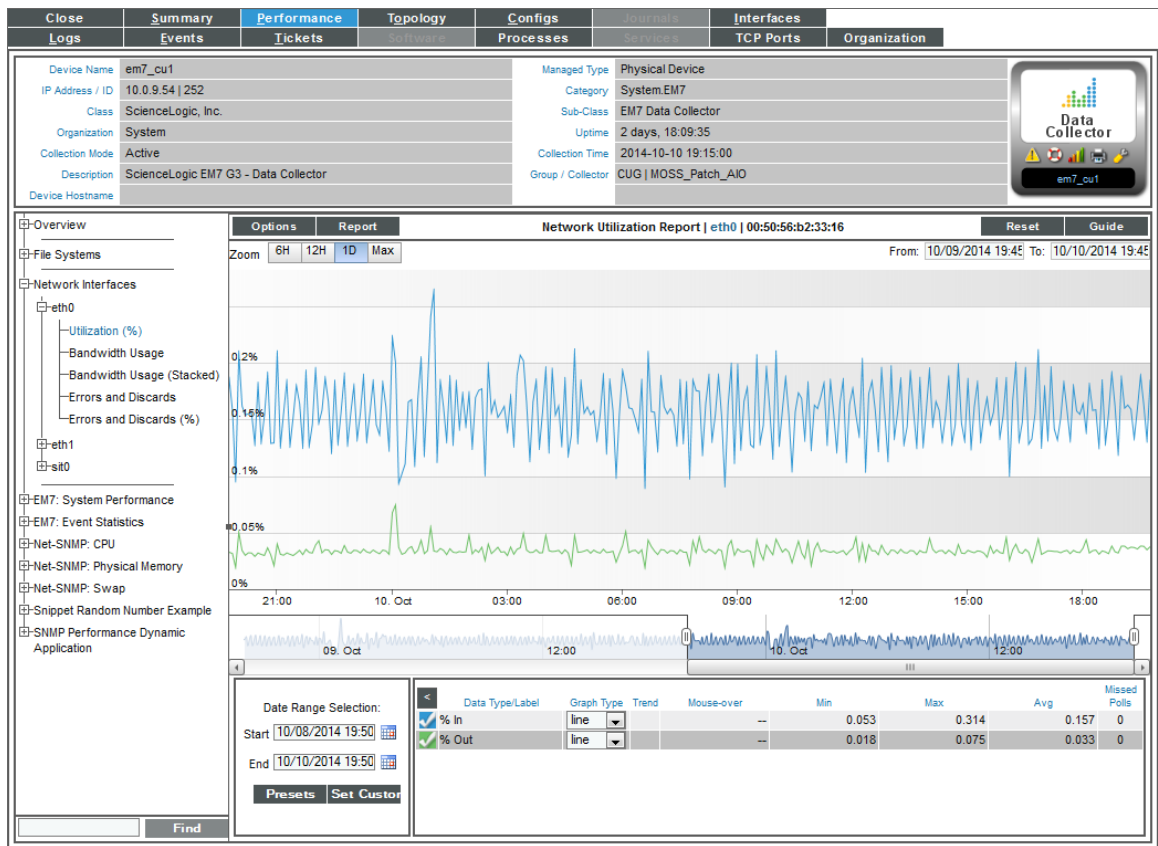


4. When you expand a network interface, links to each network interface report appear under that interface. Each reports is described below.
5. In all of the network interface reports, the **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
6. In all of the network interface reports, the **[Reports]** menu in the upper left of the report enables you to export and save the current data and graph as a report, and displays a list of formats for saving the report.
7. In all of the network interface reports, the **Data Table** at the bottom of each report enables you to view details about each data point and view overview information about the entire report. The data table includes the following:
 - **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color-coded in the report. Clicking on the check mark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouse over the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL1 was unable to collect the data within the time span of the report.

Network Utilization Report

The **Network Utilization Report** displays trends for the following parameters:

- Percentage of bandwidth used by inbound traffic to the device through the selected network interface
- Percentage of bandwidth used by outbound traffic from the device through the selected network interface



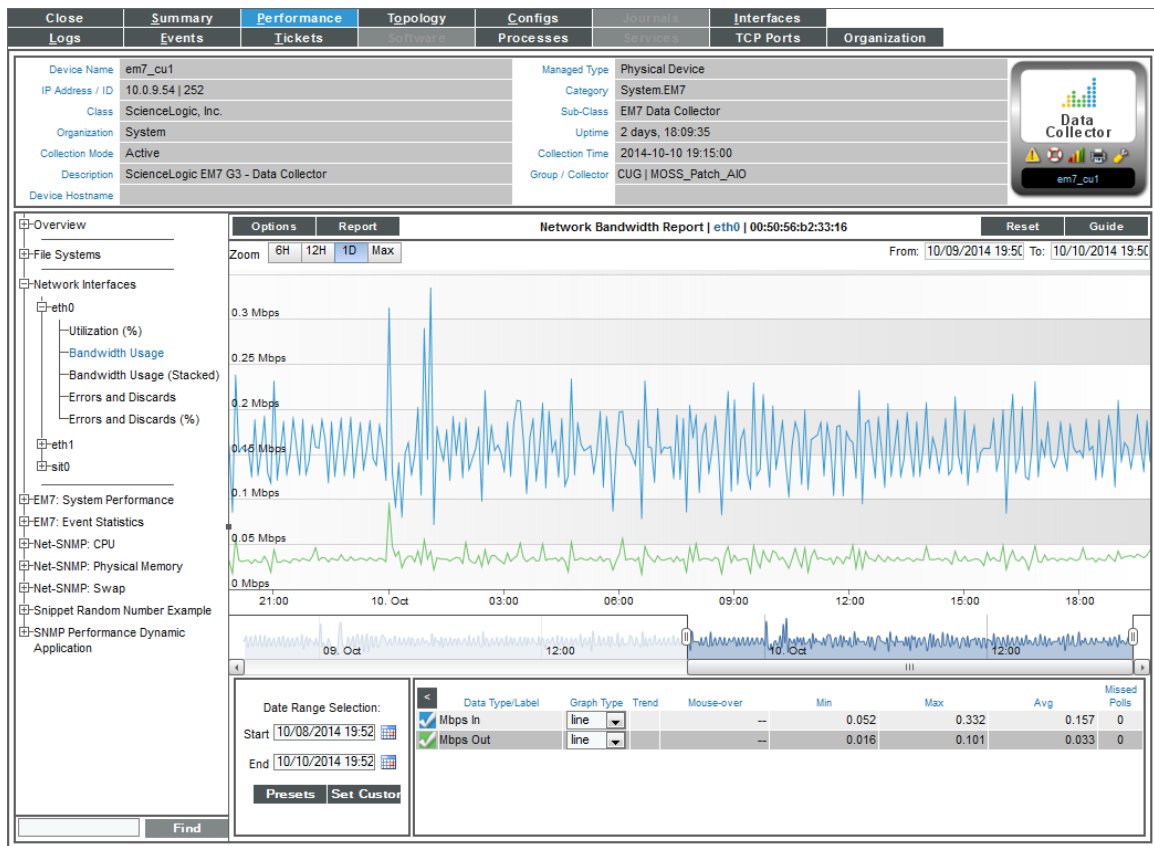
The **Network Utilization Report** displays a color-coded line for percentage in and a color-coded line for percentage out.

- The y-axis displays usage, in percent, to the left.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the high, low, and average value at that time point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

Network Bandwidth Usage Report

The **Network Bandwidth Usage Report** displays trends for the following parameters:

- Number of octets of data traveling into the device through the selected network interface
- Number of octets of data traveling out from the device through the selected network interface



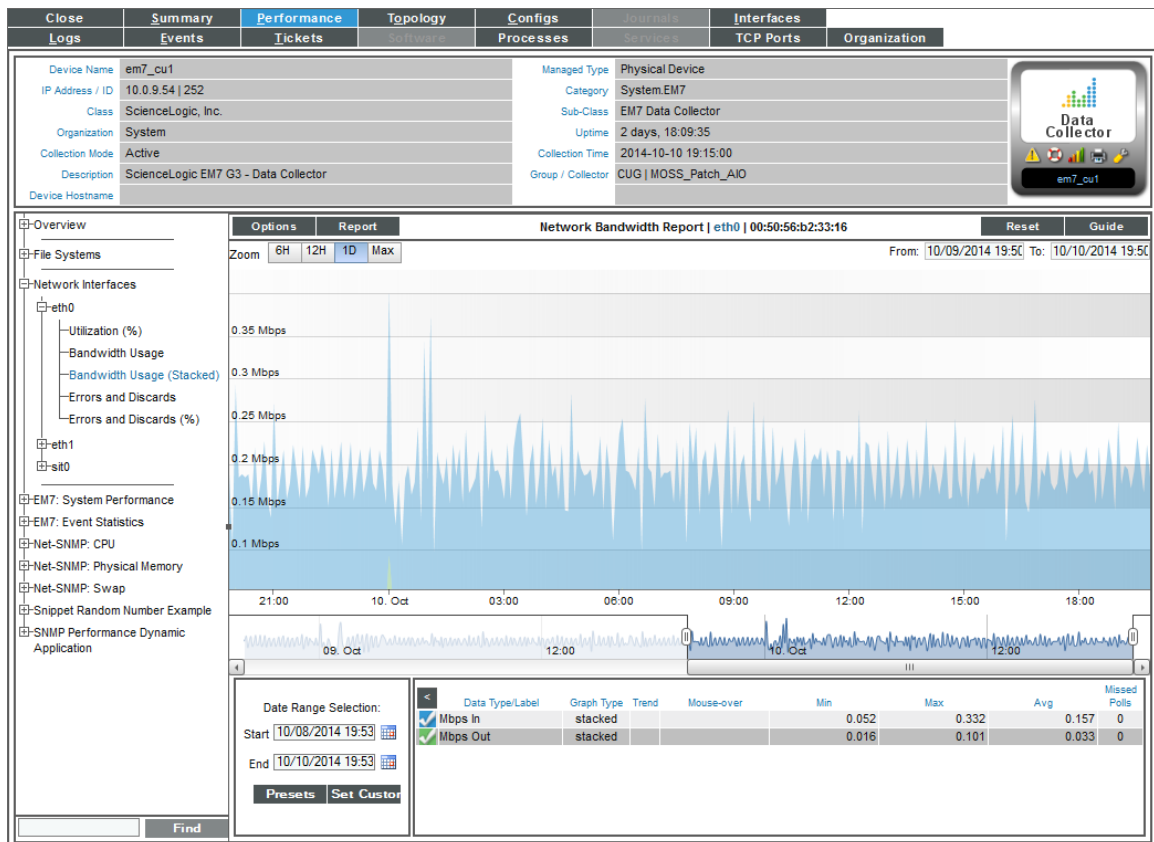
The **Network Bandwidth Usage Report** graph displays a color-coded line for octets in and a color-coded line for octets out.

- The y-axis displays bandwidth usage, in octets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Each parameter is represented by a color-coded line.
- Mousing over any point in any line displays the high, low, and average value at that time point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

Network Bandwidth Usage Report (Stacked)

The **Network Bandwidth Report (Stacked)** displays trends for the following parameters:

- Number of octets of data traveling into the device through the selected network interface
- Number of octets of data traveling out from the device through the selected network interface



The **Network Bandwidth Report (Stacked)** graph displays a color-coded stack for octets in and a color-coded stack for octets out.

- The y-axis displays bandwidth usage, over time.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Each parameter is represented by a color-coded stack (similar to an area graph).
- Mousing over any point in a stack displays the high, low, and average value at that time point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.

- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

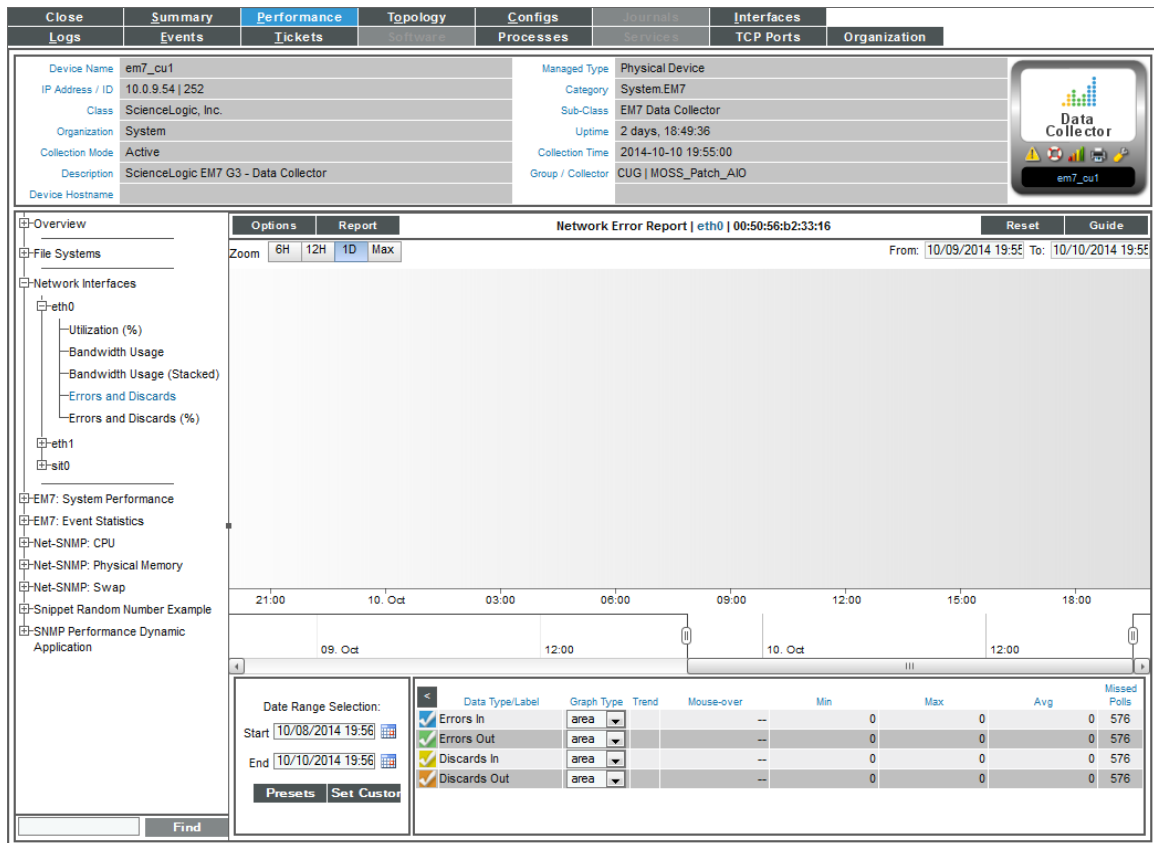
Network Error Report

The **Network Error Report** displays trends for the following parameters:

- Number of errors that occurred in data traveling into the device through the selected network interface
- Number of errors that occurred in data traveling out from the device through the selected network interface
- Number of discards that occurred in data traveling into the device through the selected network interface
- Number of discards that occurred in data traveling out from the device through the selected network interface

Packet errors occur when packets are lost due to hardware problems such as breaks in the network or faulty adapter hardware.

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.



The **Network Error Report** graph displays a color-coded line for errors in, errors out, discards in, and discards out.

- The y-axis displays number of errors and discards.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).
- Each parameter is represented by a color-coded line.
- Mousing over any point in any line displays the high, low, and average value at that time point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

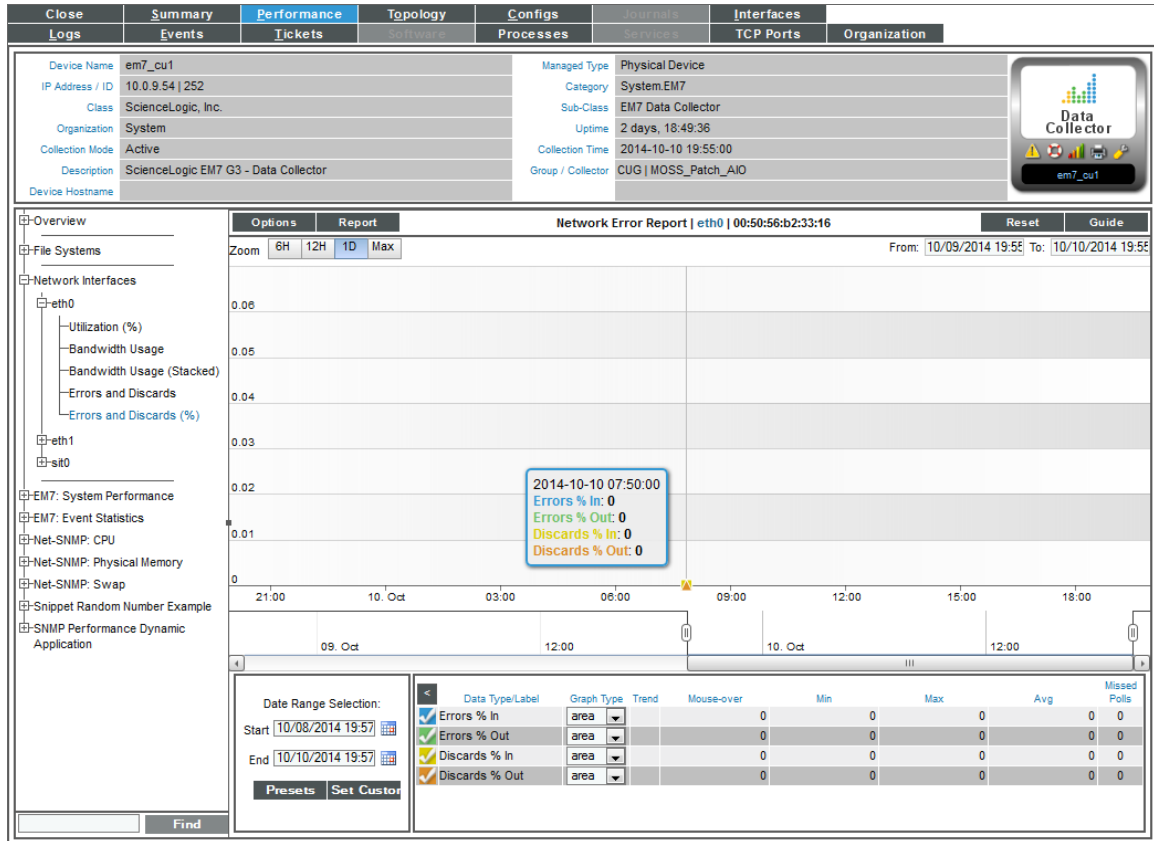
Network Error Report (Percent)

The **Network Error Report (%)** displays trends for the following parameters:

- Percentage of errors that occurred in data traveling into the device through the selected network interface
- Percentage of errors that occurred in data traveling out from the device through the selected network interface
- Percentage of discards that occurred in data traveling into the device through the selected network interface
- Percentage of discards that occurred in data traveling out from the device through the selected network interface

Packet Errors occur when packets are lost due to hardware problems such as breaks in the network or faulty adapter hardware.

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.





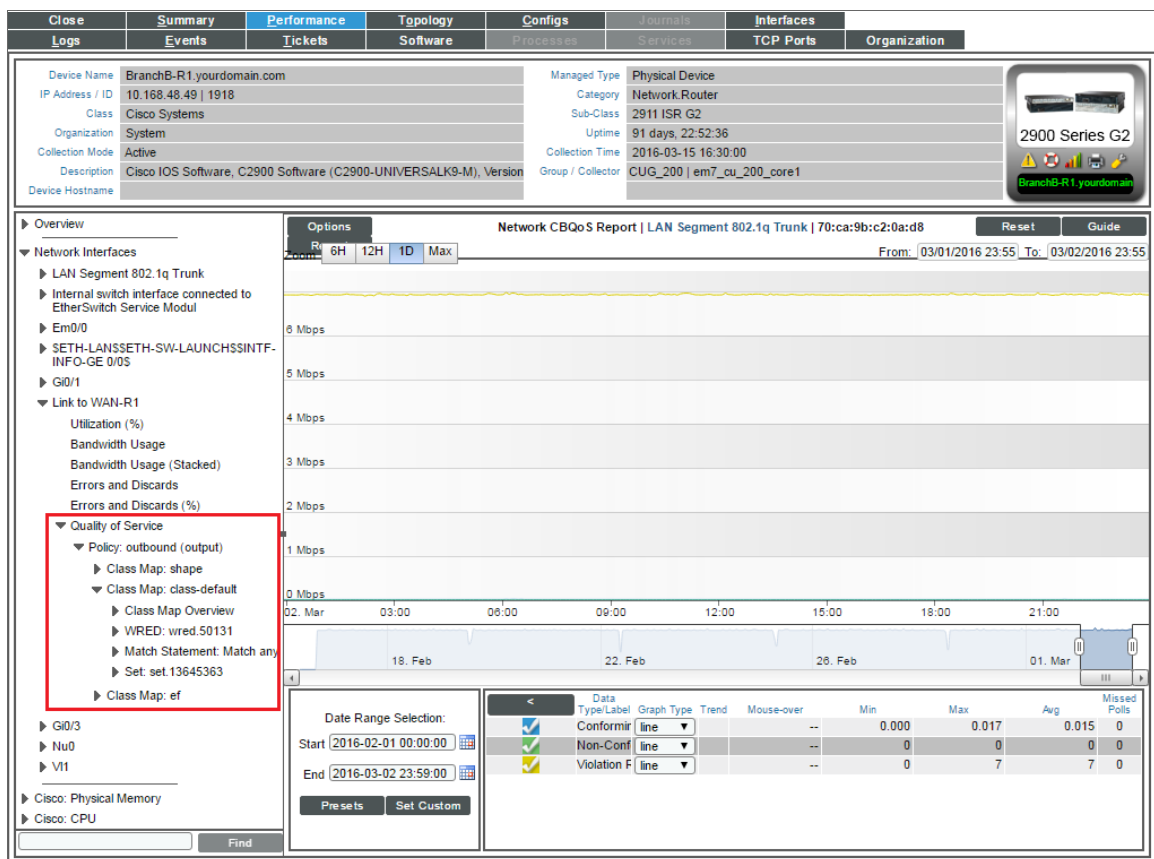
The **Network Error Report (%)** graph displays a color-coded line for errors % in, errors % out, discards % in, and discards % out.

- The y-axis displays percentage of errors and discards.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Each parameter is represented by a color-coded line.
- Mousing over any point in any line displays the high, low, and average value at that time point in the **Data Table** pane.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

CBQoS Reports for Network Interfaces

To view the CBQoS reports for a network interface:

1. You can access the network interface reports from two places:
 - Go to the **Device Manager** page (Devices > Device Manager), find the device with the desired network interface, and click its bar graph icon (.
 - Go to the **Device Hardware** page (Devices > Hardware), find the device with the desired network interface, and click its bar graph icon (.
2. When the **Device Reports** panel appears, click the **Performance** tab.
3. In the **Device Performance** page, go to the NavBar (the list of links in the left pane), and expand the **Network Interfaces** link.



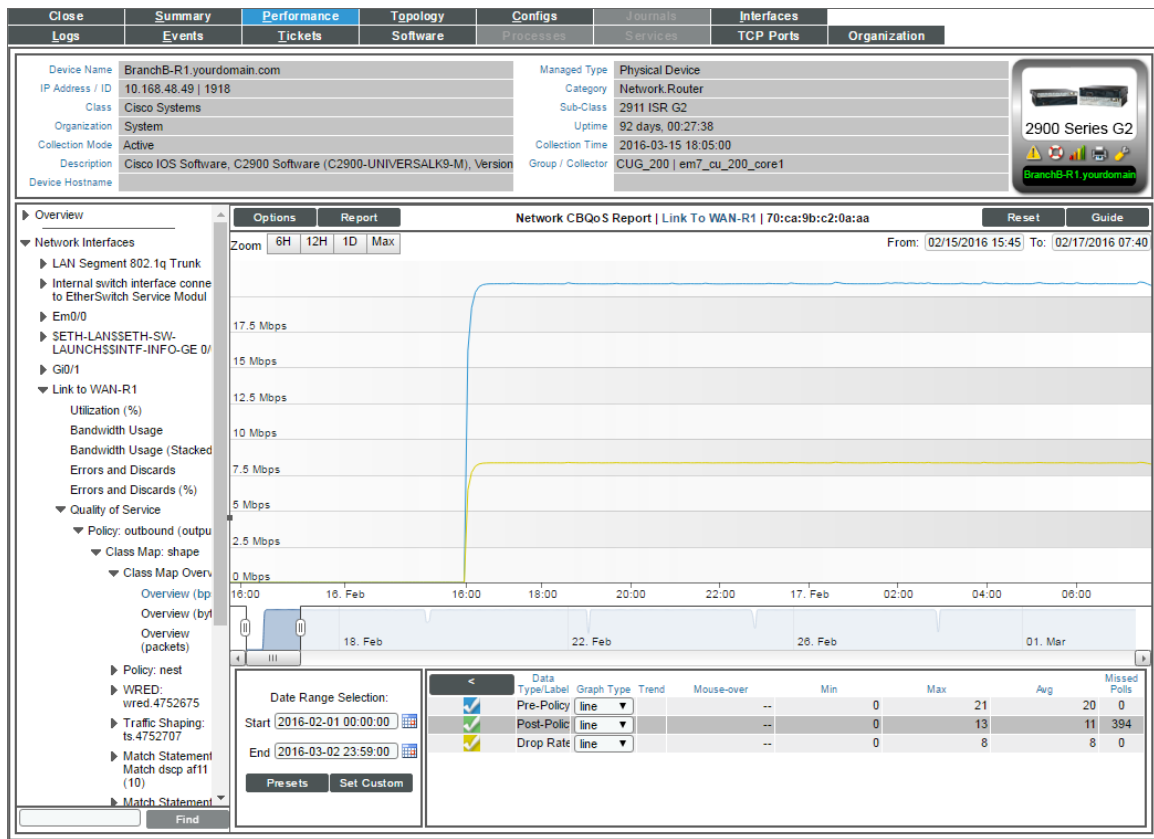
4. When you expand a network interface for which CBQoS has been enabled, you will see an entry for Quality of Services. When you expand the **Quality of Service** link, you will see entries for the CBQoS report with a link to each CBQoS report. Each report is described below.

5. In all of the network interface reports, the **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
6. In all of the network interface reports, the **[Reports]** menu in the upper left of the report enables you to export and save the current data and graph as a report, and displays a list of formats for saving the report.
7. In all of the network interface reports, the **Data Table** at the bottom of each report enables you to view details about each data point and view overview information about the entire report. The data table includes the following:
 - **Data Type/Label.** For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the check mark toggles on and off the data in the report.
 - **Graph Type.** For selected reports, allows you to specify how you want the data type to be represented in the report. Choices include candlestick, line, stepline, column, area, or stacked. For some reports, the graph type is static and you cannot select a graph type.
 - **Trend.** Toggles on and off a trendline. The trendline shows a bi-directional weighted average, which "smooths" the data for easier consumption. This trending appears as a shaded area superimposed over the graph.
 - **Mouseover.** When you mouse over the graph, this column displays the exact value for each data type at that time point on the graph.
 - **Min.** The column displays the minimum value for the data type in the report.
 - **Max.** This column displays the maximum value for the data type in the report.
 - **Avg.** This column displays the average value for the data type in the report.
 - **Missed Polls.** This column displays the number of times SL 1 was unable to collect the data within the time span of the report.

Class Map Overview

For the selected interface, the **Class Map Overview Report** displays trends for the following parameters:

- total interface utilization, in either % used (versus total available), bytes, bps, or packets, over time before applying the CBQoS policy
- total interface utilization, in either % used (versus total available), bytes, bps, or packets, over time after applying the CBQoS policy
- total dropped traffic, in either % used (versus total available), bytes, bps, or packets, over time for the class map



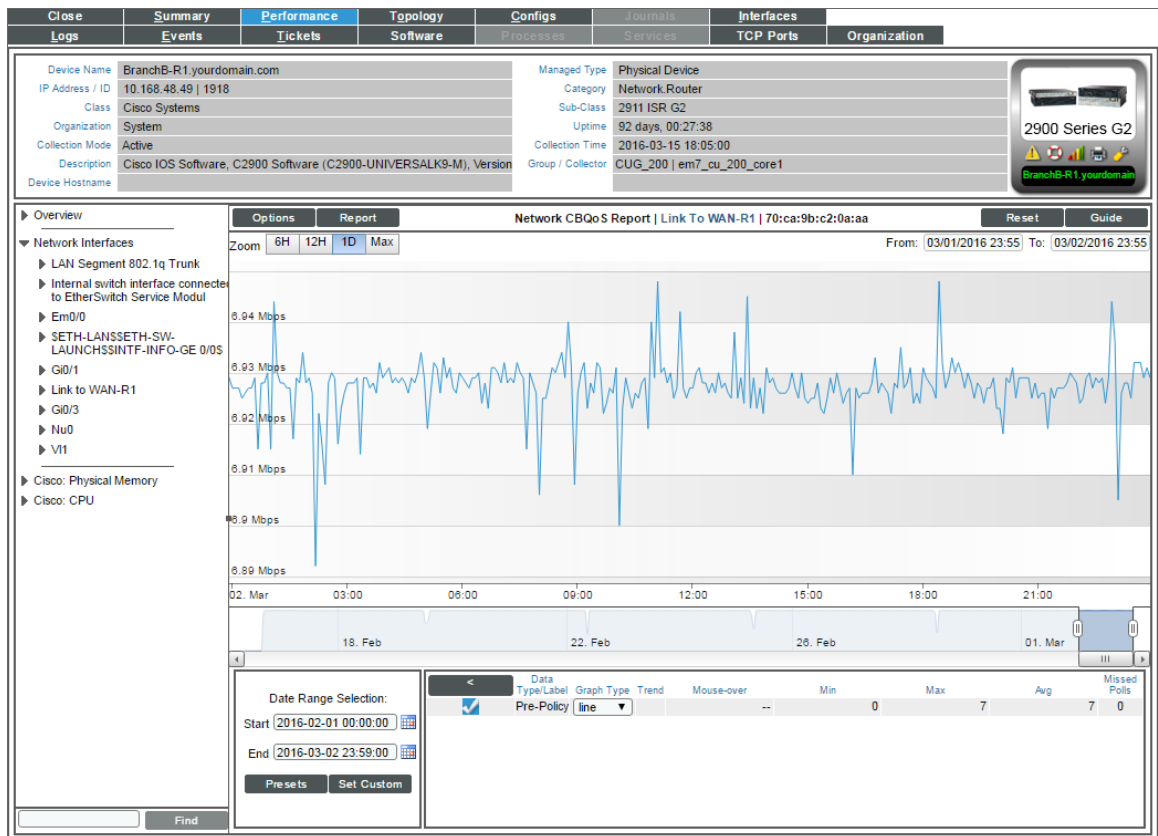
The graph displays a color-coded line for Pre-Policy, Post-Policy, and Dropped.

- The y-axis displays volume in either Mbytes, bps, or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the Pre-Policy, Post-Policy, and Dropped value at that time point.
- You can use your mouse to scroll the report to the left and right.

Match Statements Overview

For the selected interface, the **Match Statements Overview Report** displays trends for the following parameters:

- total packets (in either bps, bytes, or packets) over time that match the U32 filter before the Match Statement is applied
- total packets (in either bps, bytes, or packets) over time that match the L32 filter before the Match Statement is applied
- total packets (in either bps, bytes, or packets) over time before the Match Statement is applied



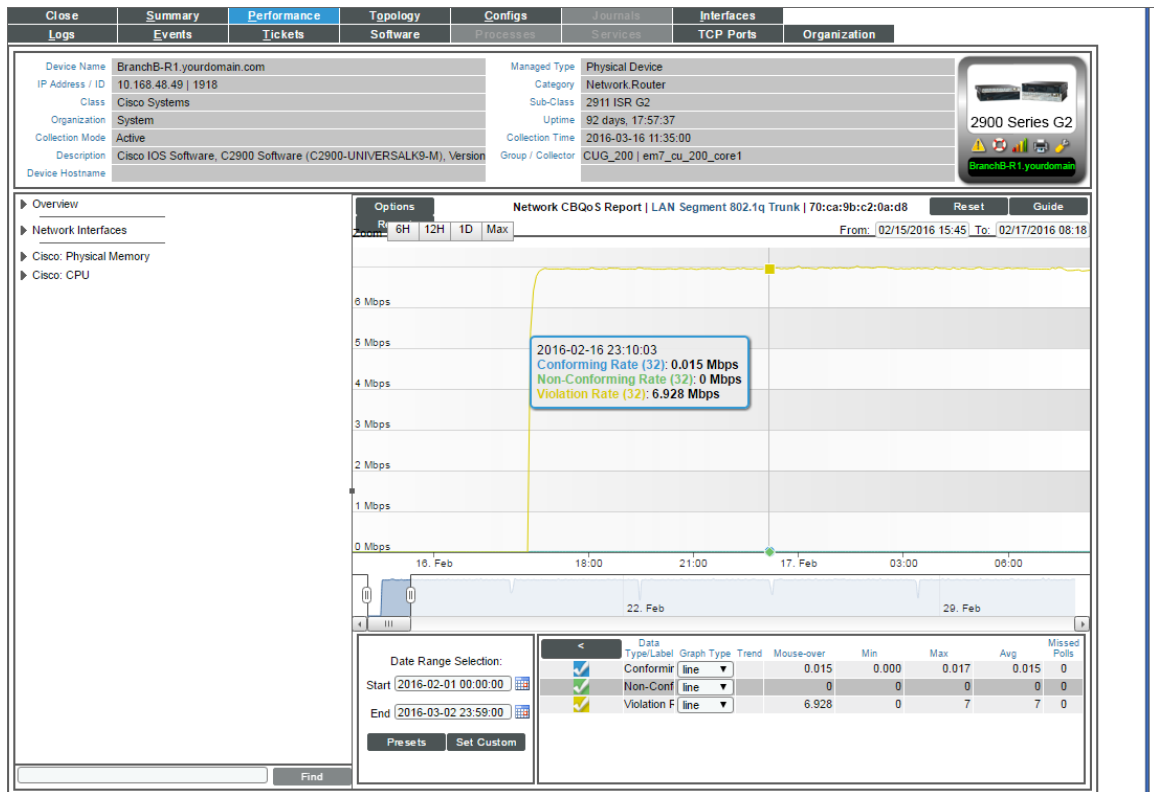
The graph displays a color-coded line for Pre-Policy Inbound (U32), Pre-Policy Inbound (L32), and Pre-Policy Inbound.

- The y-axis displays volume in either Mbytes, bps, or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the Conforming, Non-Conforming, and Violations values at that time-point.
- You can use your mouse to scroll the report to the left and right.

Policing Overview

For the selected interface, the **Policing Overview Report** displays trends for the following parameters:

- total traffic (in either bytes, bps, or packets) over time that conform to the policing policy
- total traffic (in either bytes, bps, or packets) over time that do not conform to the policing policy
- total traffic (in either bytes, bps, or packets) over time that violate the policing policy



The graph displays a color-coded line for Conforming, Non-Conforming, and Violations.

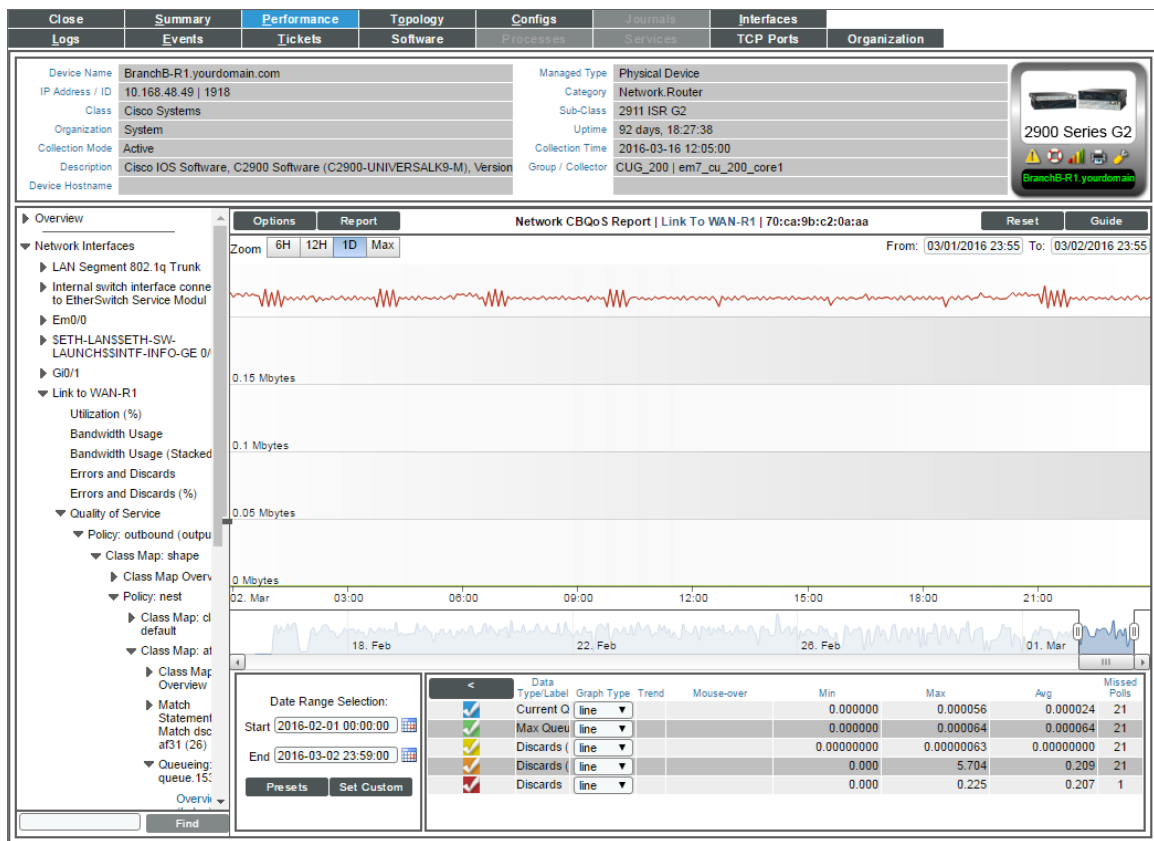
- The y-axis displays volume in either Mbytes, bps, or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the Conforming, Non-Conforming, and Violations values at that time-point.
- You can use your mouse to scroll the report to the left and right.

Queueing Overview

For the selected interface, the Queueing Overview Report displays trends for the following parameters:

- total discarded traffic (in either bytes or bps) over time for the queuing policy
- queue depth (in either bytes or bps) over time for the queuing policy

NOTE: If a queue is marked as "priority" in CBQoS, the text **Priority** appears in parentheses next to the entry in the navbar.



The graph displays a line for total discarded traffic:

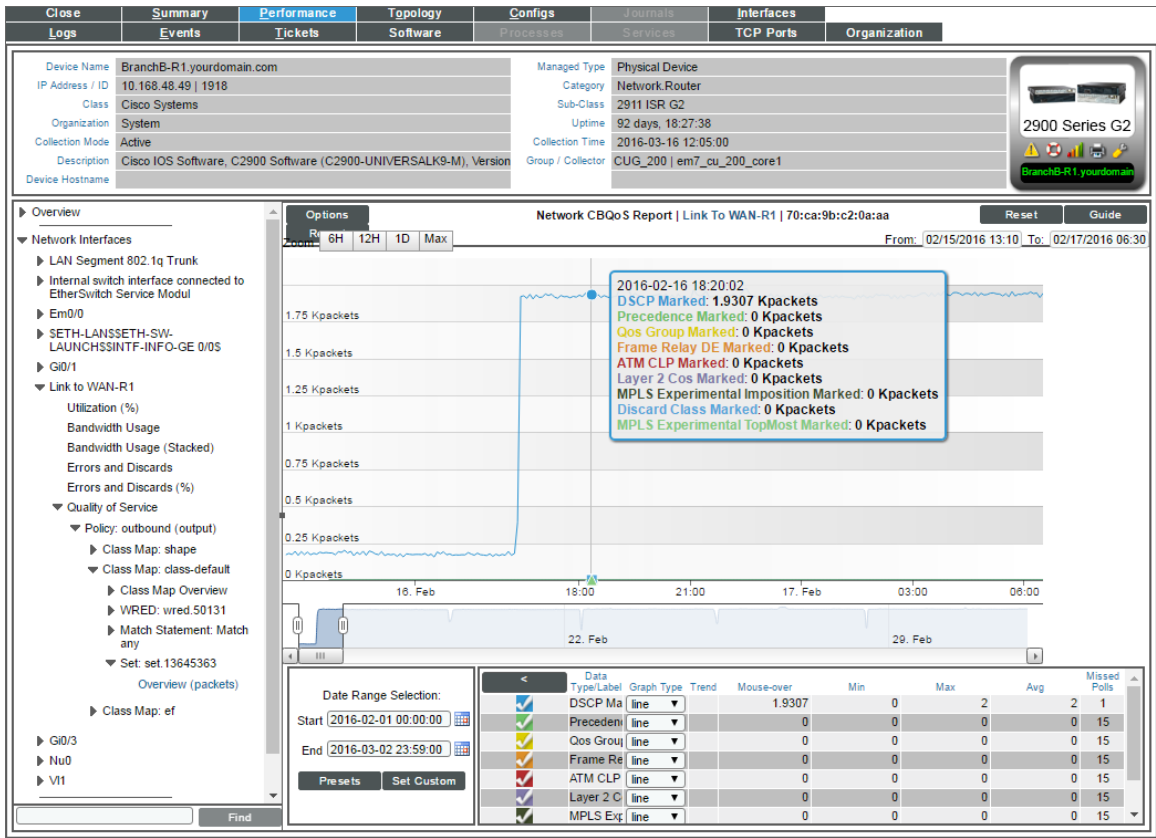
- The y-axis displays volume in either bytes or bps.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the number or discards at that time-point.
- You can use your mouse to scroll the report to the left and right.

Set Overview

For the selected interface, the **Set Overview Report** displays trends for the following parameters:

- total traffic (in either bps, bytes, or packets) over time where the **Discard Class** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **DSCP** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **DSCP Tunnel** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the Frame Relay DE bit is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the Frame Relay FECN BECN bit is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **MPLS Experimental Implosion** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **MPLS Experimental TopMost** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **Precedence** field is marked by the Set policy
- total traffic (in either bps, bytes, or packets) over time where the **QoS Group** field is marked by the Set policy

- total traffic (in either bps, bytes, or packets) over time where the **SRP Priority** field is marked by the Set policy



The graph displays a color-coded line for each of the metrics described above.

- The y-axis displays volume in either Mbytes, bps, or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the values for each metric at that time-point.
- You can use your mouse to scroll the report to the left and right.

Traffic Shaping Overview

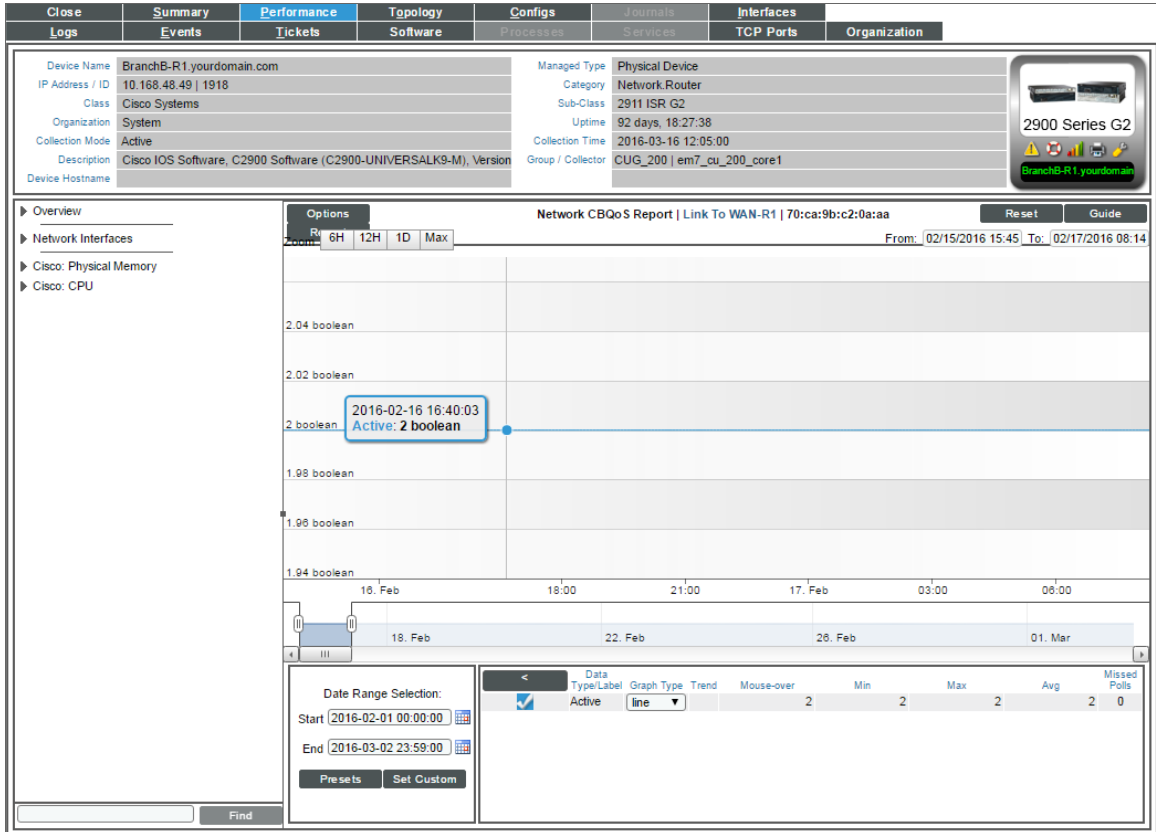
For the selected interface, the **Traffic Shaping Overview Report** for each traffic shaping policy includes two reports:

- Overview (boolean)
- Overview (in either bytes or packets)

Overview (boolean)

For the selected interface, the **Overview (boolean)** report displays trends for the following parameters:

- **Active**. Specifies whether the traffic shaper is active over time for the traffic shaping policy. Possible values are "0" for "Not active" and "1" for "active". However, you might see values other than 1 or 0 in this report. If a report contains any other value, it is an average of multiple readings. For example, if during a five-minute interval, SL1 gathered five readings and during one of those readings, there was no traffic, so the traffic shaper was not active, the average would be 0.8 (1 + 1 + 1 + 1 + 0 = 4; 4/5 = 0.8).



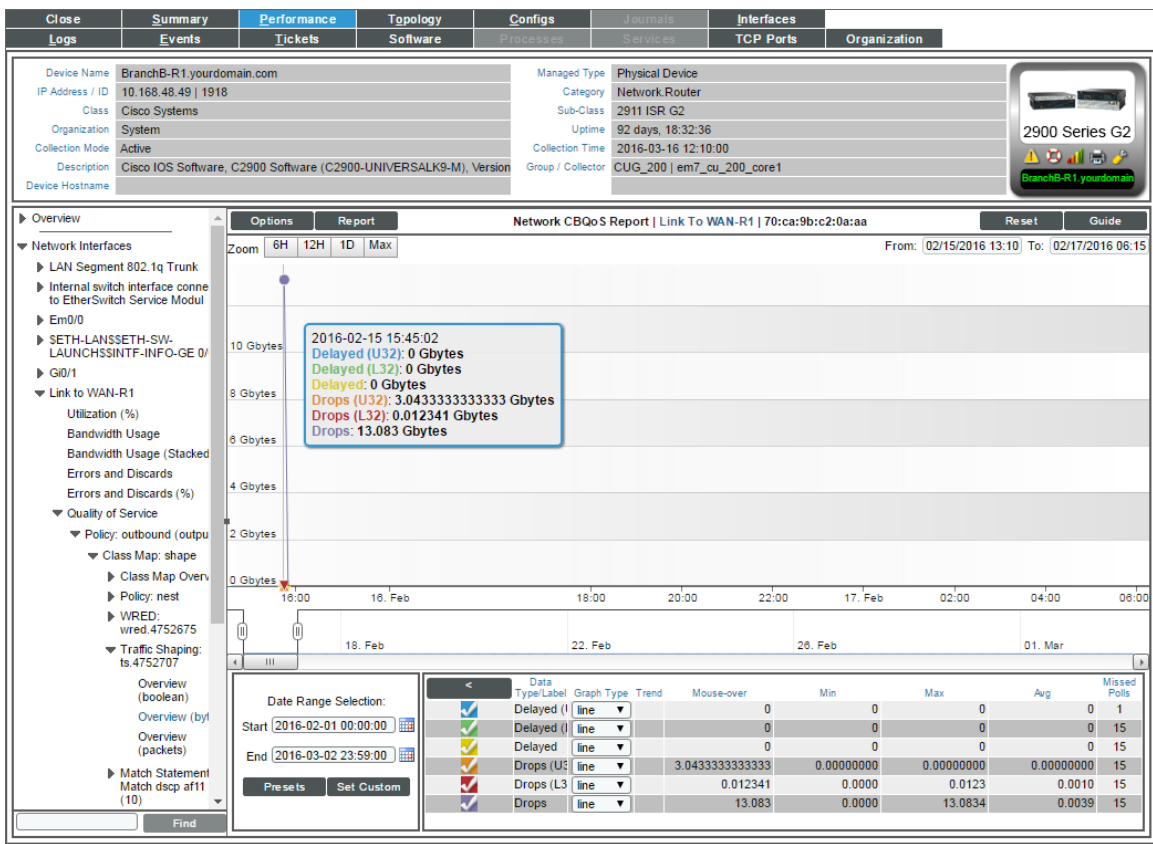
The graph displays a color-coded line for each of the metrics (described previously):

- The y-axis displays volume in either Mbytes or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays a value for the metric described above at that time-point.
- You can use your mouse to scroll the report to the left and right.

Overview (in either bytes or packets)

For the selected interface, the **Overview (bytes)** and **Overview (packets)** reports display trends for the following parameters:

- Delayed packets (in either bytes or packets) over time that match the U32 filter for the traffic shaping policy
- Delayed packets (in either bytes or packets) over time that match the L32 filter for the traffic shaping policy
- Delayed packets (in either bytes or packets) over time for the traffic shaping policy
- Dropped packets (in either bytes or packets) over time that match the U32 filter for the traffic shaping policy
- Dropped packets (in either bytes or packets) over time that match the L32 filter for the traffic shaping policy
- Dropped packets (in either bytes or packets) over time for the traffic shaping policy



The graph displays a color-coded line for each of the metrics (described previously):

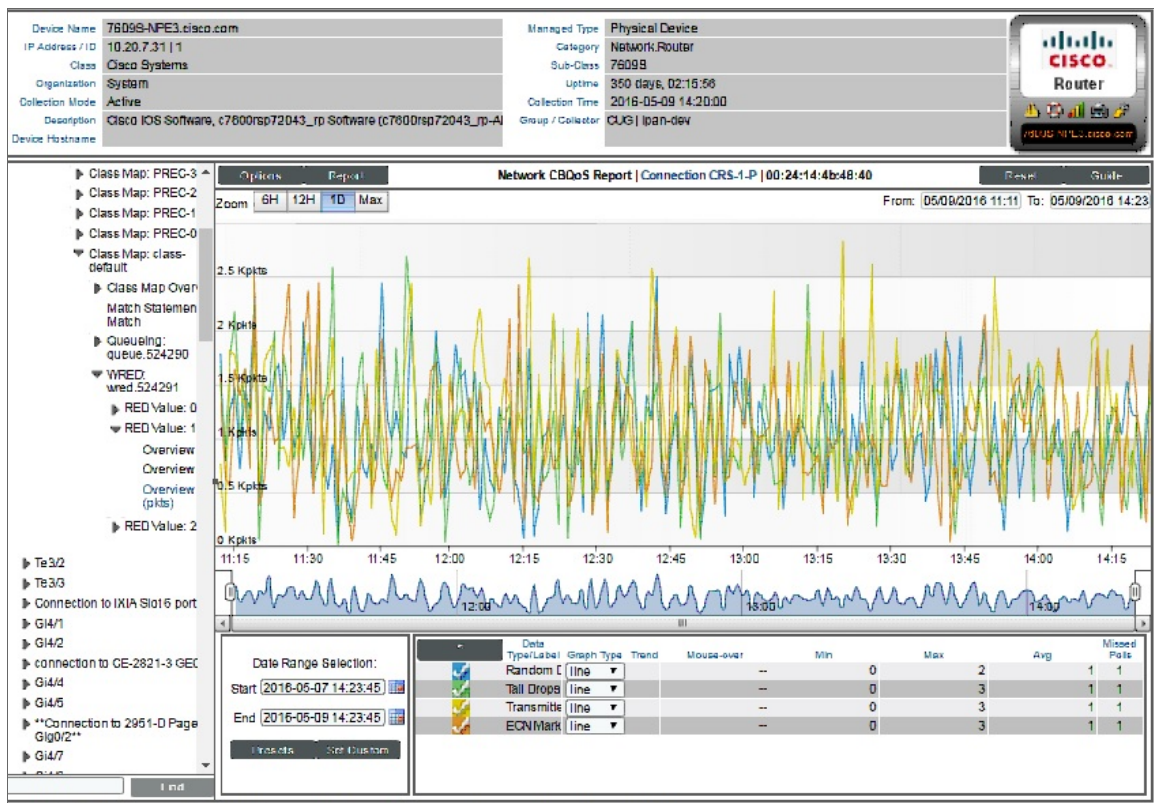
- The y-axis displays volume in either Mbytes or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays a value for each of the metrics described above at that time-point.
- You can use your mouse to scroll the report to the left and right.

WRED Overview

For the selected interface, the **RED Overview** report for each WRED policy includes two reports:

- Overview (in either bytes or packets)
- Overview (items)

Overview (in either bytes or packets)



For the selected interface, the **Overview (bytes)** and **Overview (packets)** reports display trends for the following parameters:

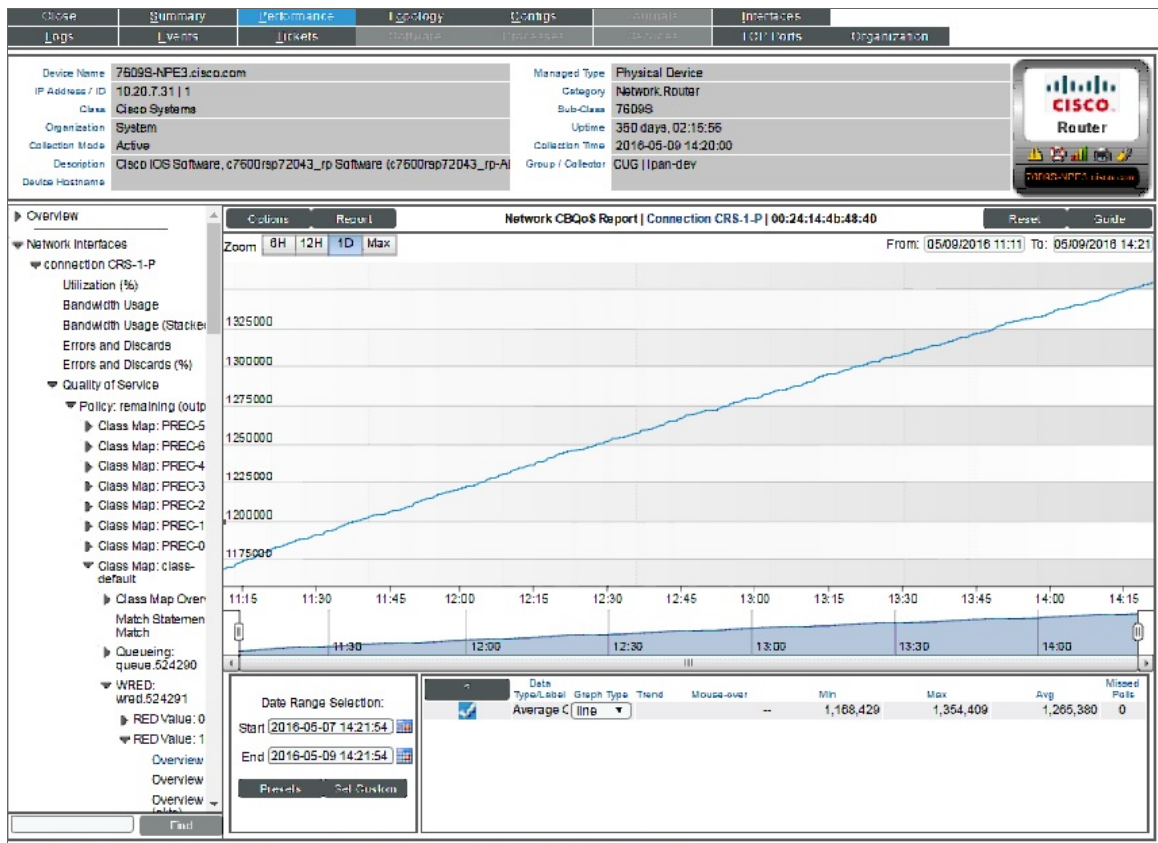
- Random drops (in either bytes or packets) over time for the RED policy
- Random drops (in either bytes or packets) over time that match the U32 filter for the RED policy
- Random drops (in either bytes or packets) over time that match the L32 filter for the RED policy
- Tail drops (in either bytes or packets) over time for the RED policy
- Tail drops (in either bytes or packets) over time that match the U32 filter for the RED policy
- Tail drops (in either bytes or packets) over time that match the L32 filter for the RED policy
- Transmitted traffic (in either bytes or packets) over time that match the L32 filter for the RED policy

- Total packets (in either bytes or packets) over time where the ECN bit is marked by the RED policy
- Total packets (in either bytes or packets) over time that match the U32 filter and where the ECN bit is marked by the RED policy

The graph displays a color-coded line for each of the metrics described above:

- The y-axis displays volume in either Mbytes or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays a value for each of the metrics described above at that time-point.
- You can use your mouse to scroll the report to the left and right.

Overview (items)



For the selected interface, the **Overview (items)** report displays trends for the following parameters:

- Average Queue Size (in items) over time for each queue aligned with the RED policy.

The graph displays a color-coded line for each queue:


- The y-axis displays volume in items.

- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays a value for average queue size at that time-point.
- You can use your mouse to scroll the report to the left and right.


Viewing Reports about DNS Servers and DNS Records for a Device

When you define a domain-name monitoring policy, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

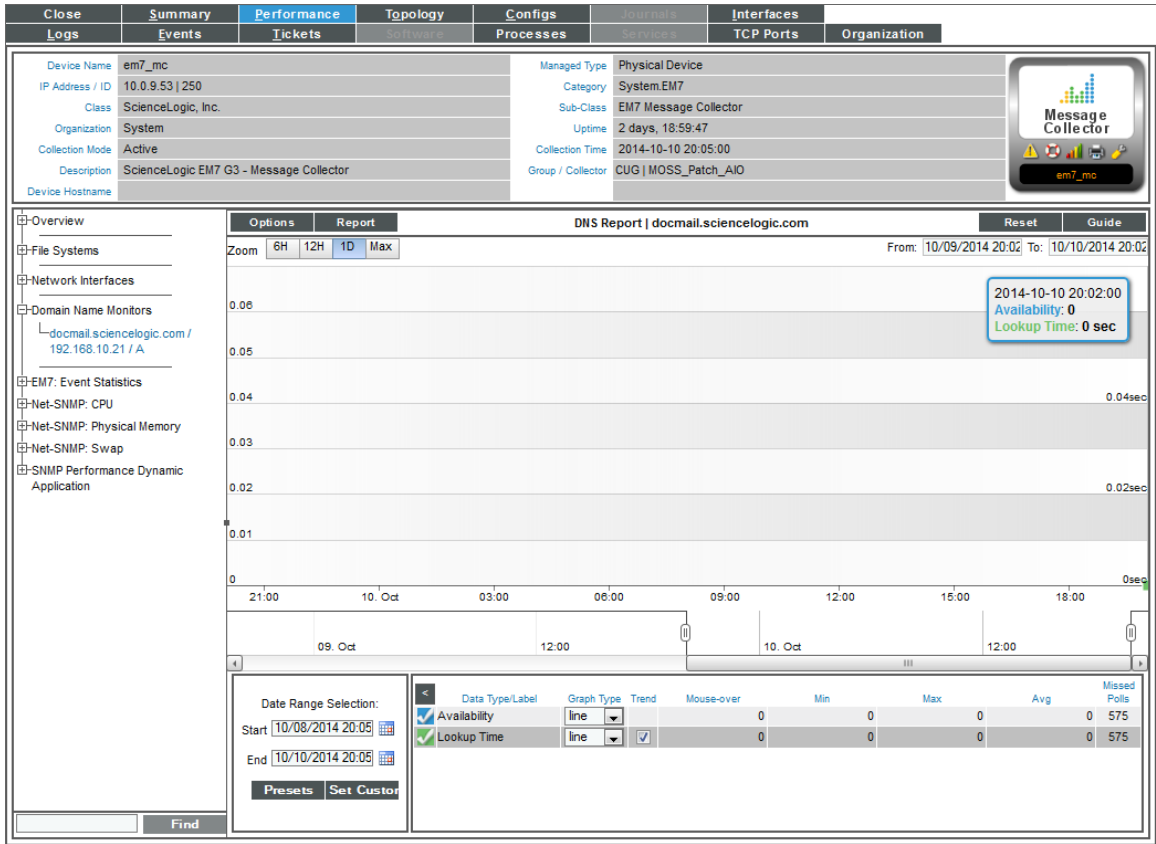
There are two ways to navigate to the report for domain-name monitoring:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar-graph icon () for the device.
 - In the Device Reports panel, select the **Performance** tab.
 - In the left NavBar, expand Domain Name Monitors and select the policy for which you want to view the report.

Or:

2. From the **Domain Name Monitoring** page (Registry > Monitors > Domain Name):
 - In the **Domain Name Monitoring** page, find the domain-name policy for which you want to see a report.
 - Select the bar graph icon in the *Domain/Zone* field()

3. The **Device Performance** page appears, with the DNS Report displayed.



4. The DNS Report displays multiple parameters in a single graph. The DNS Report trends the following parameters:

- **Availability.** Availability of the specified name server and of a specific record and specific content in that record. Availability is 100% for a poll if the name server responded, the lookup returned a record, and the result match specified in the policy did not generate an event. If availability is not 100% for a poll, availability is 0% for that poll.
- **Lookup Time.** The amount of time it took the DNS server to access the specified DNS record, search it, and return a result to SL1.

The graph displays a color-coded line for availability and for latency, for the selected duration.


- The y-axis displays availability, in percent to the left, and latency time, in milliseconds to the right.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the high, low, and average value at that time-point in the Data Table pane.
- You can use your mouse to scroll the report to the left and right.

- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.


Viewing Reports on an Email Round-Trip Monitoring Policy

When you define a policy to monitor Email round-trips, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

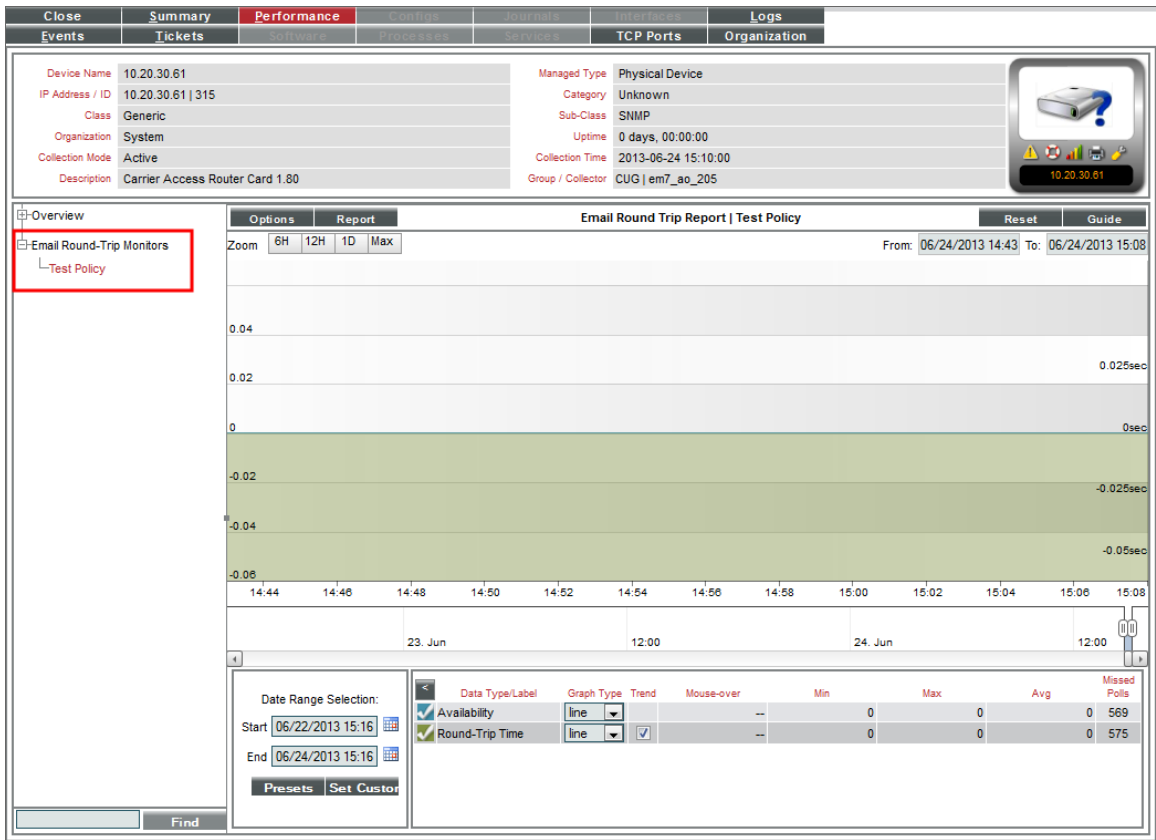
There are two ways to navigate to the report for Email round-trip monitoring:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
 - In the **Device Reports** panel, select the **Performance** tab.
 - In the NavBar, expand Email Round-Trip Monitors and select the policy for which you want to view the report.

Or:

2. From the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip):
 - In the **Email Round-Trip Monitoring** page, find the Email round-trip policy for which you want to see a report.
 - Select its bar graph icon in the *Policy Name* field ()

3. The **Device Performance** page appears, with the Email Round-Trip Report displayed.



4. The Email Round-Trip Report displays results from an Email round-trip policy. The report trends the following parameters:

- **Availability.** The availability of an Email server. Availability means whether SL1 received a reply Email from the Email server.
- **Round-Trip Time.** The amount of time it takes to send an Email message from SL1 to an external mail server and then back to SL1.

The graph displays the total time for the entire Email transaction from SL1 to the external server and back to SL1.


- The y-axis displays the speed of the entire Email transaction from SL1 to the external server and back to SL1, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the high, low, and average value at that time-point in the Data Table pane.
- You can use your mouse to scroll the report to the left and right.

- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.


Viewing Reports on an SOAP or XML Transaction Policy

The **Data Transaction Reports** page display results from a SOAP/XML transaction policy. Each of these policies monitors a server-to-server transaction that uses HTTP and can post files or forms (for example, SOAP/XML, Email, or RSS feeds). SL1 sends a request and some data and then examines the result of the transaction and compares it to a specified expression match.

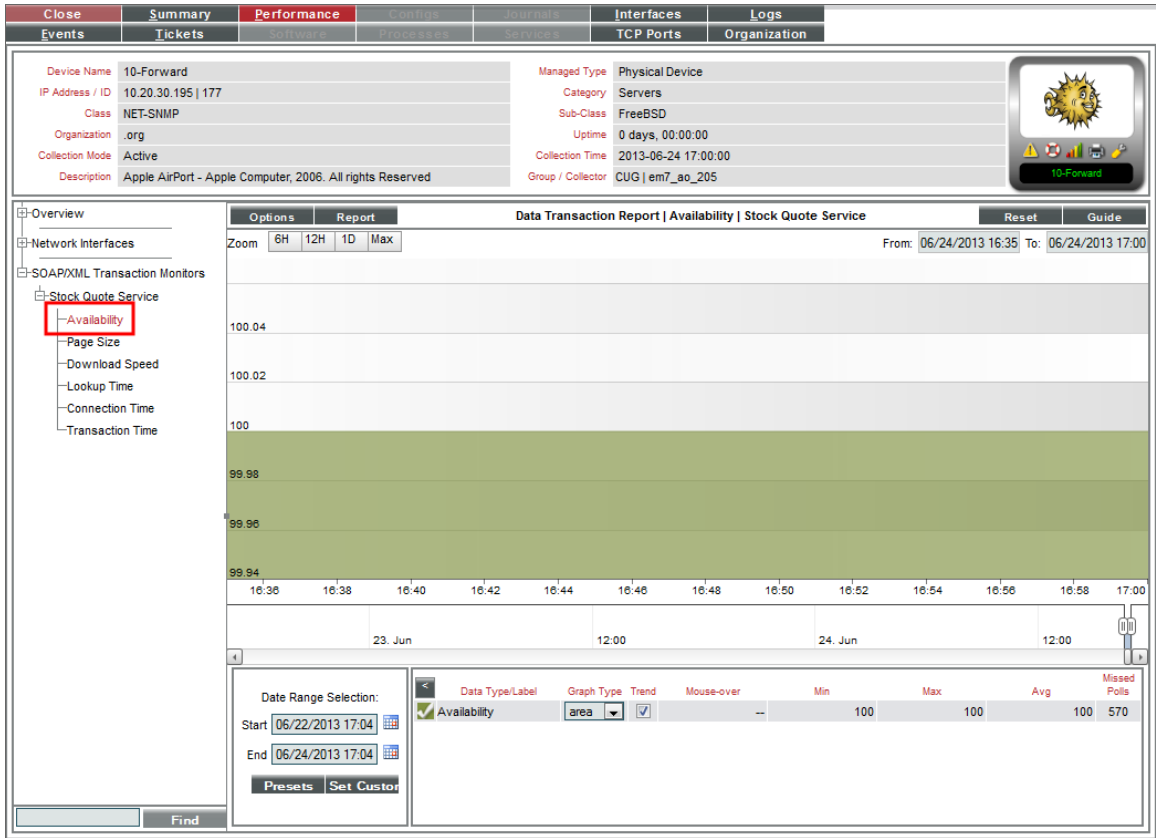
There are two ways to navigate to the reports for SOAP/XML Transactions policies:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
 - In the **Device Reports** panel, select the **Performance** tab.
 - In the NavBar, expand SOAP/XML Transaction Monitors and select the policy for which you want to view the report.

Or:

2. From the **SOAP/XML Transaction Monitoring** page (Registry > Monitors > SOAP/XML Transactions):
 - In the **SOAP/XML Transaction Monitoring** page, find the SOAP/XML transaction policy for which you want to see a report.
 - Select its bar graph icon in the *Policy Name* field()

3. The **Device Performance** page appears, with the Data Transaction Report | Availability report displayed.

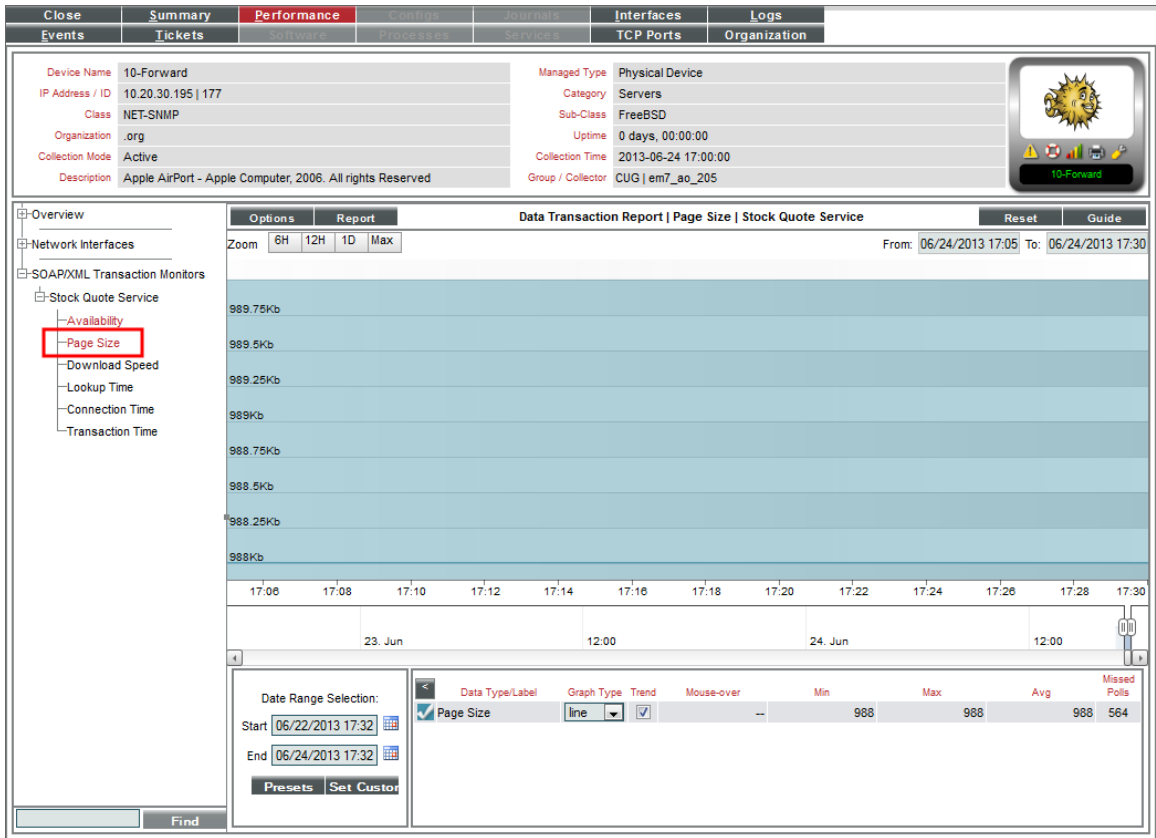


4. The Data Transaction Report | Availability report displays results from a SOAP/XML Transaction policy. The report trends the parameters described below. The Data Transaction Report | Availability report displays the availability of the external server and the availability of the specified data.

- The y-axis displays availability, in percent to the left.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the high, low, and average value at that time-point in the Data Table pane.
- You can use your mouse to scroll the report to the left and right.
- In a graph of normalized data, clicking on a data point zooms in on that time period and shows the non-normalized data.

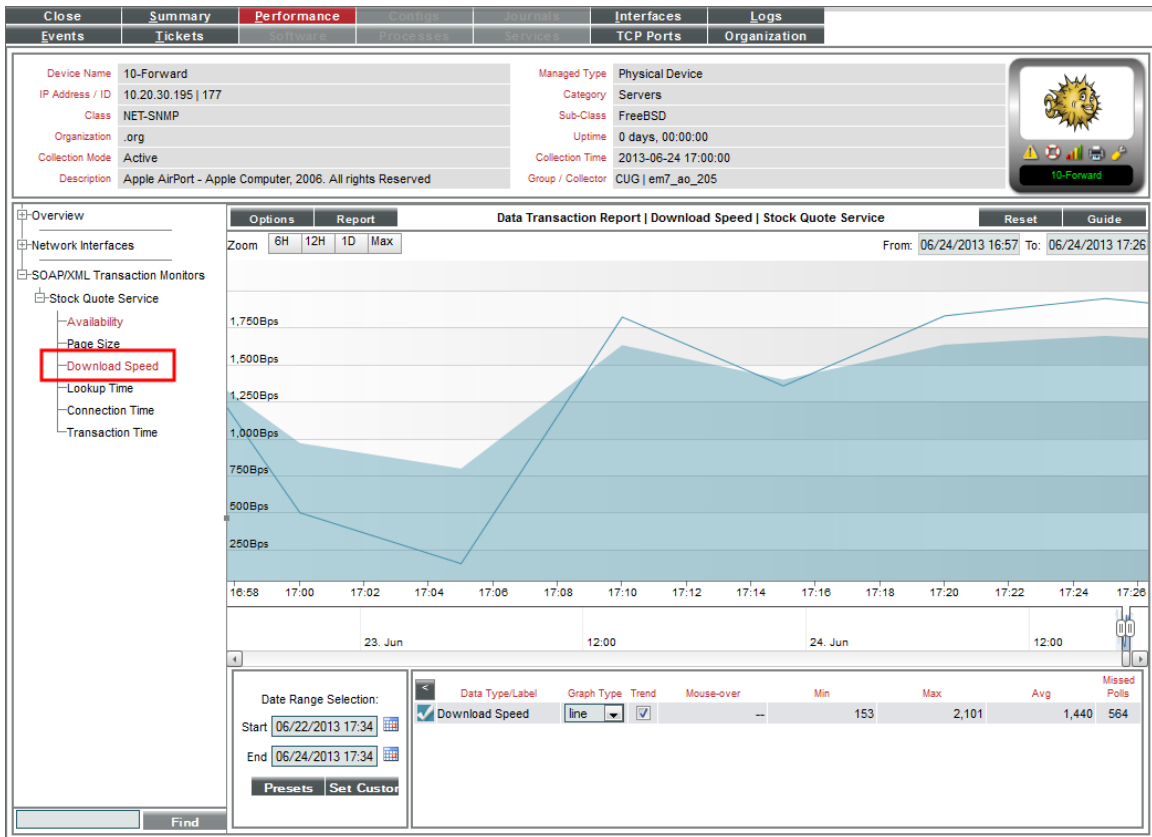
5. For each SOAP/XML Transaction policy, you can also view the following additional reports. To view them, select the appropriate entries in the NavBar:

- **Page Size.** The Data Transaction Report | Page Size report displays information about the size of the page specified in the URL of the policy. The graph displays the page size of the specified URL for the selected duration.



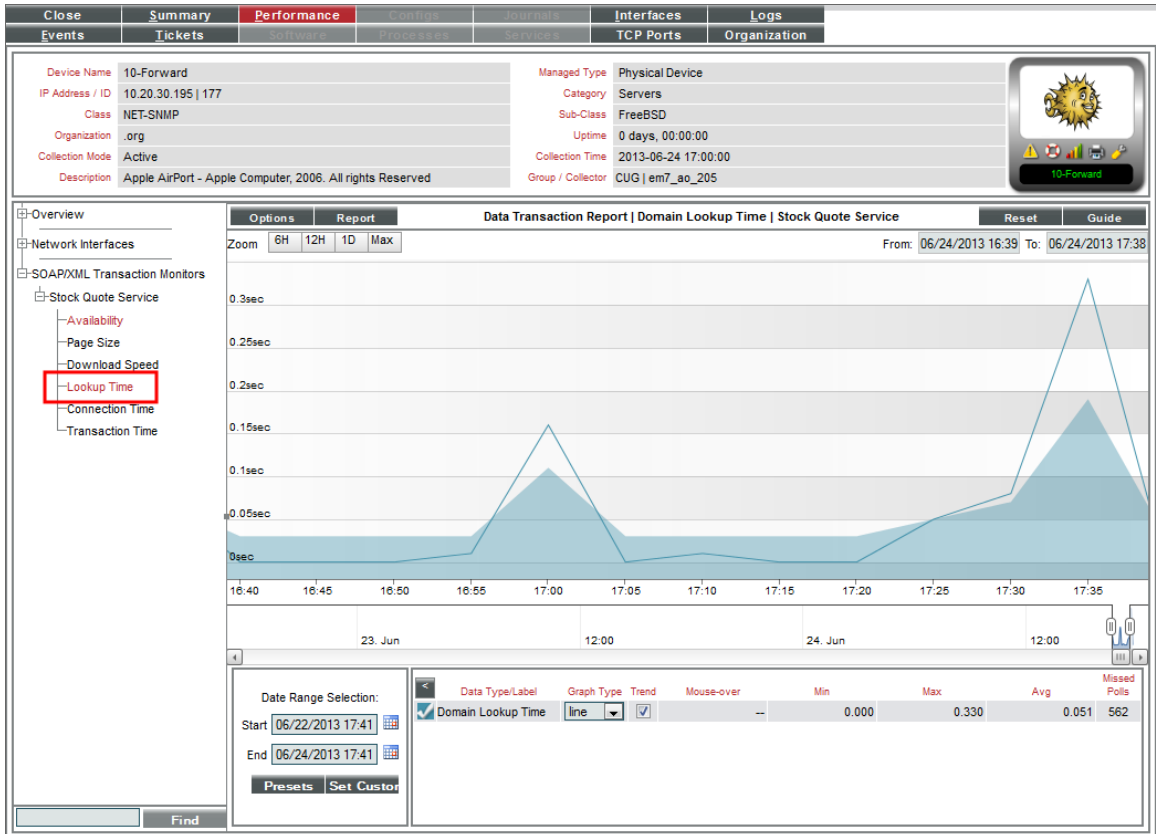
- The y-axis displays size in kilobytes per second (Kb).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

- **Download Speed.** The Data Transaction Report | Download Speed report displays the speed at which data was downloaded from the server (specified in the server policy) to SL1. The graph displays the speed at which data was downloaded from the specified server to SL1 for the selected duration.



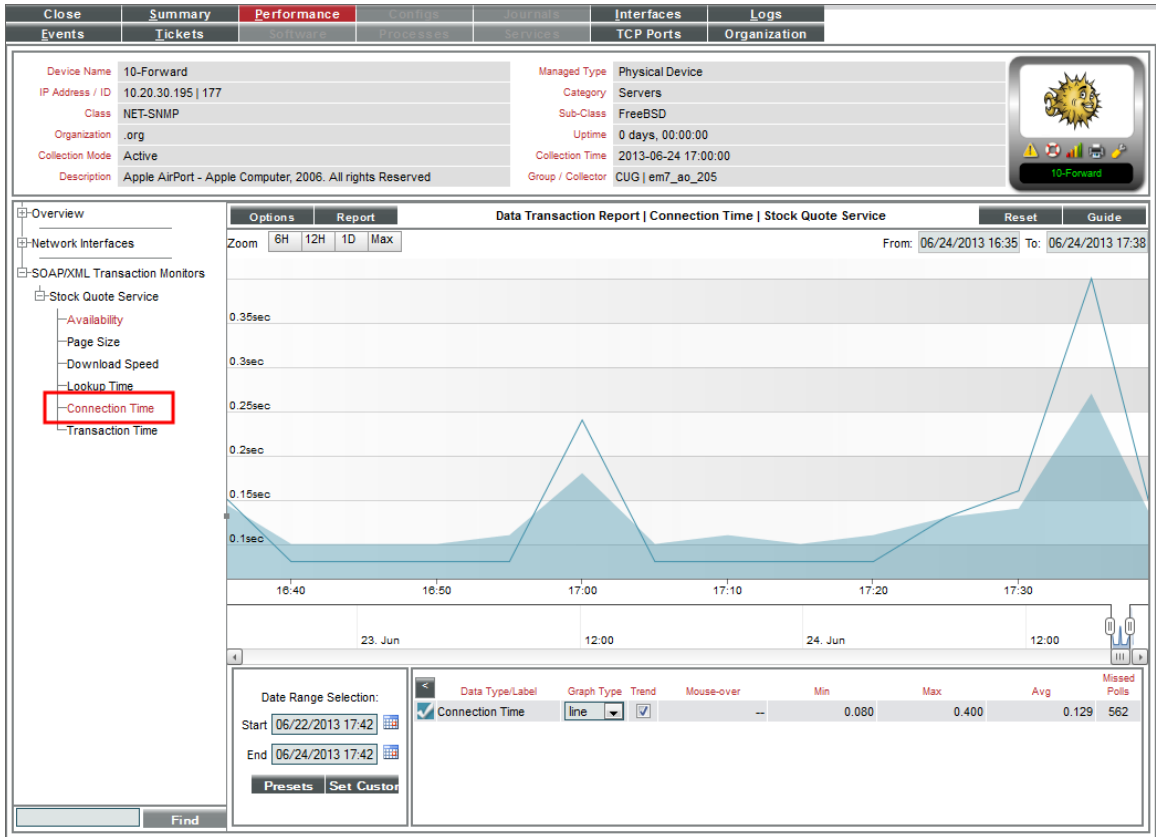
- The y-axis displays the speed at which data was downloaded from the server to SL1, in (bits per second) Bps.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).

- **Lookup Time.** The Data Transaction Report | Domain Lookup Time report displays the speed at which your DNS system was able to resolve the name of the server in the server policy. The graph displays the speed at which your DNS system was able to resolve the name of the server in the policy for the specified duration.



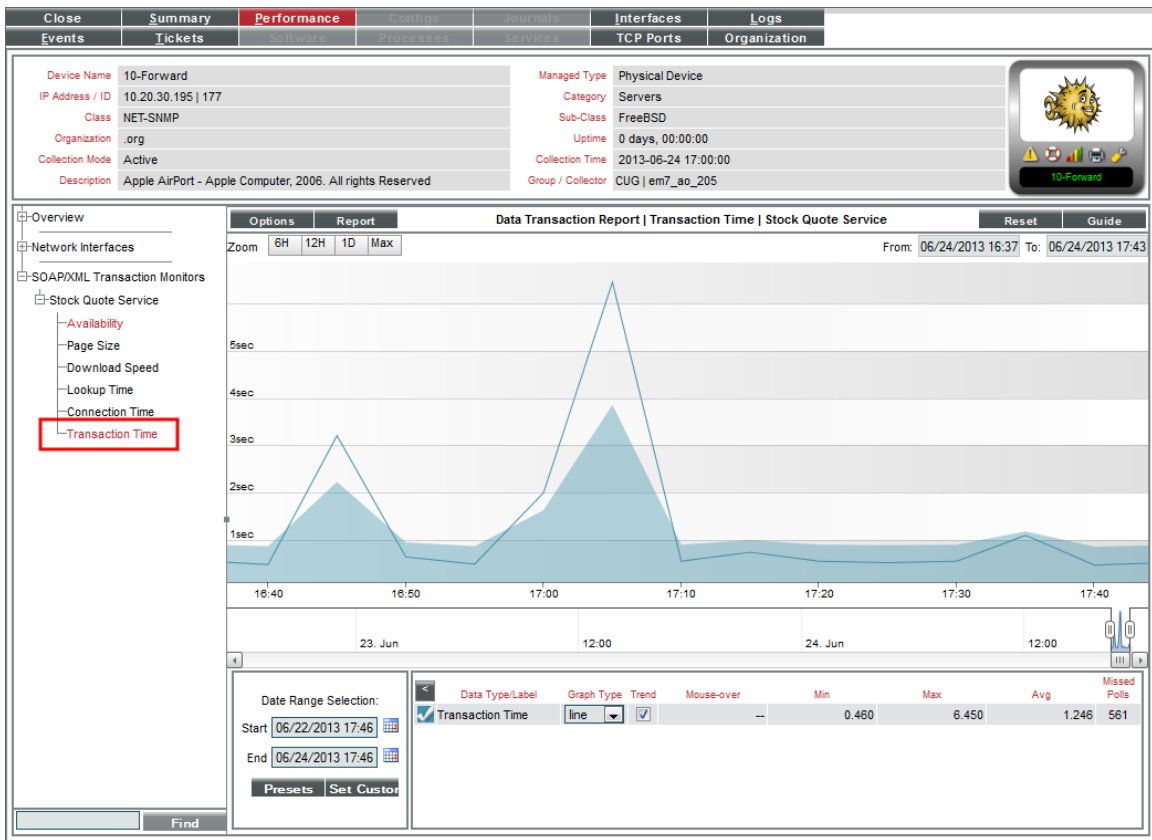
- The y-axis displays the speed at which your DNS system was able to resolve the name of the server, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

- **Connection Time.** The Data Transaction Report | Connection Time report displays the time it takes for SL1 to establish communication with the external server. In other words, the time it takes from the beginning of the HTTP request to the TCP/IP connection. The graph displays the speed at which SL1 was able to make a TCP/IP connection to the external server in the policy for the specified duration.



- The y-axis displays the speed at which SL1 was able to make a TCP/IP connection to the external server, in seconds.
- The y-axis displays the speed at which SL1 was able to make a TCP/IP connection to the external server, in seconds.

- **Transaction Time.** The Data Transaction Report | Transaction Time report displays the total time it took to make a connection to the external server, send the HTTP request, wait for the server to parse the request, receive the requested data from the server, and close the connection. The graph displays the total time for the entire transaction from SL1 to the external server and back to SL1 for the specified duration.



- The y-axis displays the speed of the entire transaction from SL1 to the external server and back to SL1, in seconds.
- The x-axis displays the speed of the entire transaction from SL1 to the external server and back to SL1, in seconds.

Viewing Availability Reports for a Single System Process on a Device

When you define a process monitoring policy, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

If the SL1 agent is installed on a device, data collected by the agent is used by default for process monitoring policies on that device. For more information about monitoring processes with the agent, see the **Monitoring Using the SL1 agent** manual.

For policies that monitor system processes, SL1 generates one or more of the following reports:

- The **Process Report** displays the availability of a single monitored process on the device and also displays the number of instances of that process running on the device.
- The **Process Availability Composite Report** displays the availability of all monitored processes on the device.

Availability means the process is running.


During polling, a process has two possible availability values:

- 100%. Process is up and running.
- 0%. Process is not up and running.

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 process was unavailable, the average would be 80% ($100 + 100 + 100 + 100 + 0 = 400$; $400/5 = 80$).


There are two ways to navigate to the reports for process monitoring:

1. From the **Device Manager** page (Devices > Device Manager):

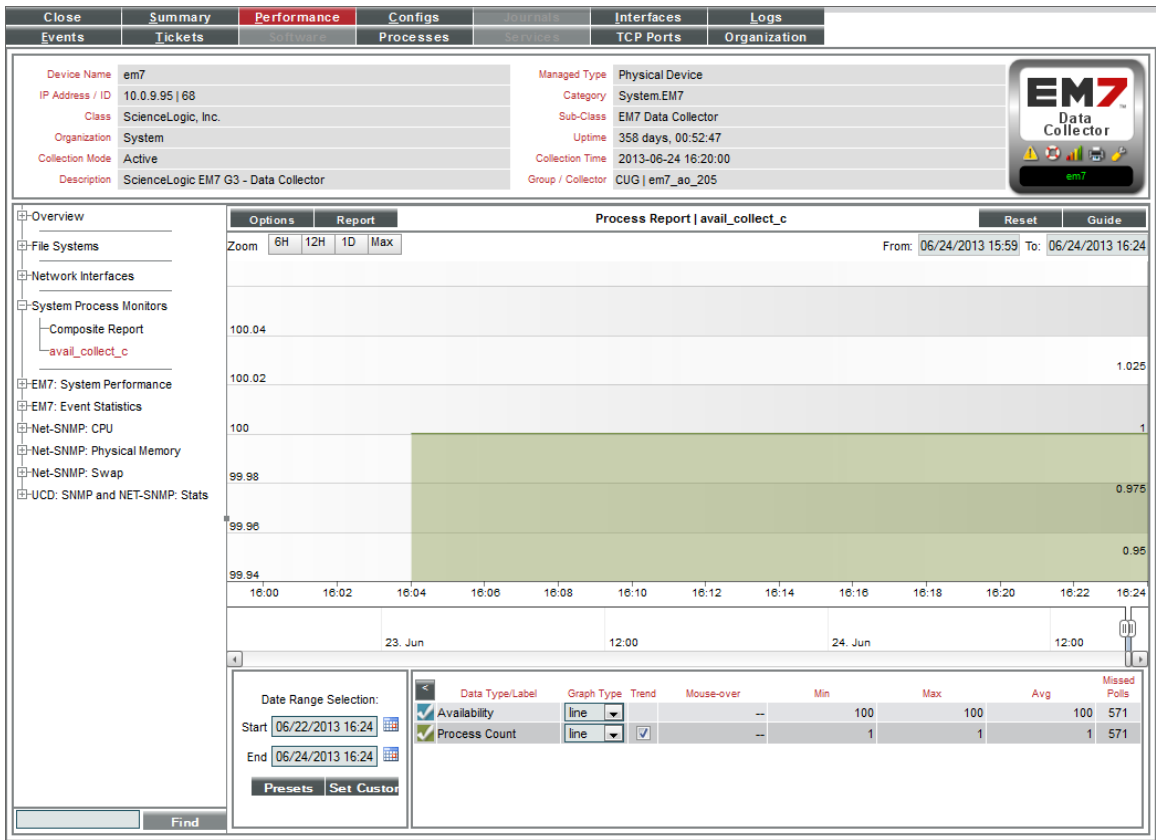
- In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
- In the **Device Reports** panel, select the **Performance** tab.
- In the NavBar, expand System Process Monitors and select the policy for which you want to view the report.

Or:

2. From the **System Process Monitoring** page (Registry > Monitors > System Processes):

- In the **System Process Monitoring** page, find the system process policy for which you want to see a report.
- Select its bar graph icon in the *Process Name* field ()

3. The **Device Performance** page appears, with the Process Report displayed.



4. The Process Report displays a color-coded line for the availability of the monitored process over time and another color-coded line that represents the number of instances of the process running on the device.

- The y-axis displays the availability of the process, in percent to the left and the number of processes to the right.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

5. If you have defined monitoring policies for multiple processes on a single device, you can also view the Process Availability Composite Report.

6. The Process Availability Composite Report displays the availability of all monitored processes on the device.

- The graph displays the availability of each monitored process. Each monitored process is represented with a color-coded line.
- The y-axis displays the availability of the process, in percent.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

Viewing Port Availability Reports for a Single Device

When you define a policy to monitor port availability, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

If the SL1 agent is installed on a device, data collected by the agent is used by default for policies that monitor port availability on that device. For more information about monitoring ports with the agent, see the **Monitoring Using the SL1 agent** manual.


The Port Availability Report displays the availability of a monitored port.

Availability means the port's ability to accept connections and data from the network. During polling, a port has two possible availability values:


- 100%. Port is up and running.
- 0%. Port 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 port was unavailable, the average would be 80% ($100 + 100 + 100 + 100 + 0 = 400$; $400/5 = 80$).

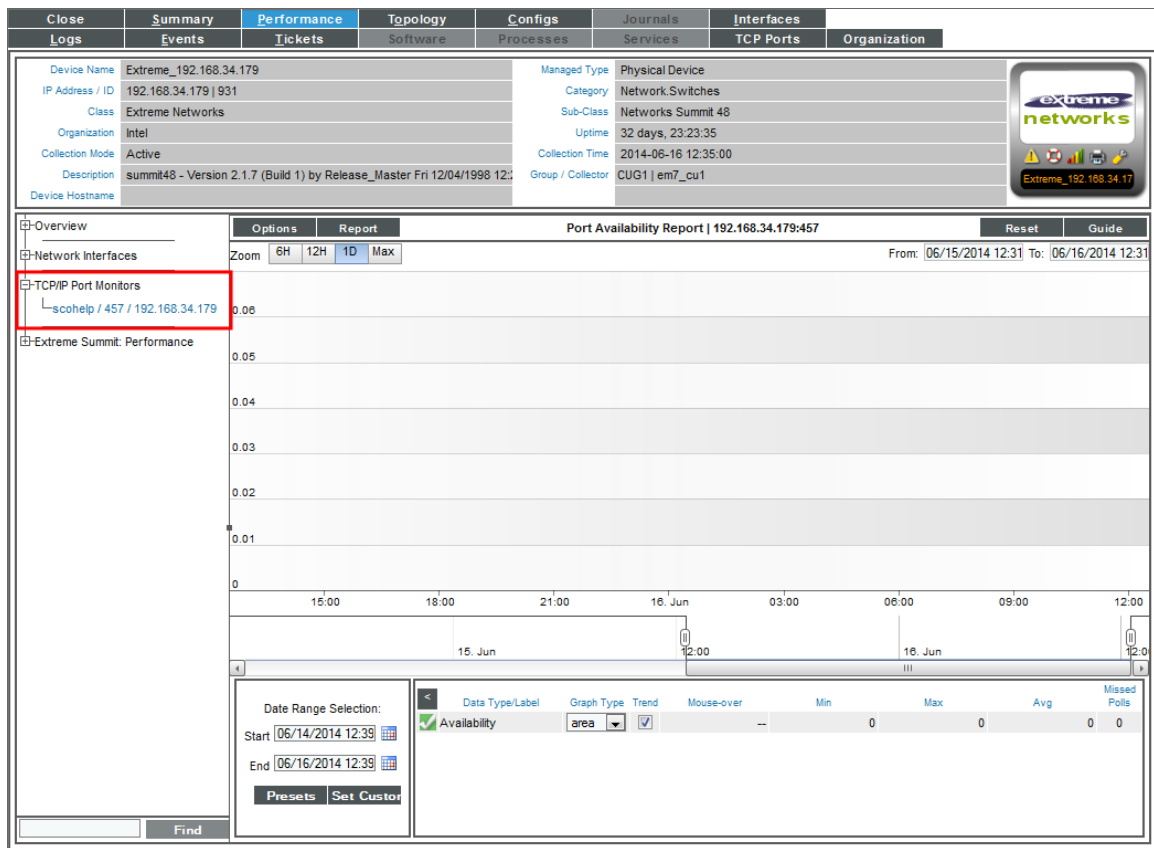
There are two ways to navigate to the reports for process monitoring:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
 - In the **Device Reports** panel, select the **Performance** tab.
 - In the NavBar, expand TCP/IP Port Monitors and select the policy for which you want to view the report.

Or:

2. From the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports):
 - In the **TCP/IP Port Monitoring** page, find the port policy for which you want to see a report.
 - Select its bar graph icon in the *Port Number* field()

3. The **Device Performance** page appears, with the Port Availability Report displayed.



4. The Port Availability Report displays the availability of a single monitored port over time.

- The y-axis displays the availability of the port , in percent.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).

Viewing Reports for a Web Content Policy


The Content Verification Reports display results from a Web Content policy. These reports display availability and other statistics about the website and its content.

Availability means whether or not the specified content was found on the website. During polling, a webserver has two possible availability values:


- 100%. Content was found.
- 0%. Content was not found.

However, you might see values other than 100 or 0 in the 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, the specified content was not found, the average would be 80% ($100 + 100 + 100 + 100 + 0 = 400$; $400/5 = 80$).

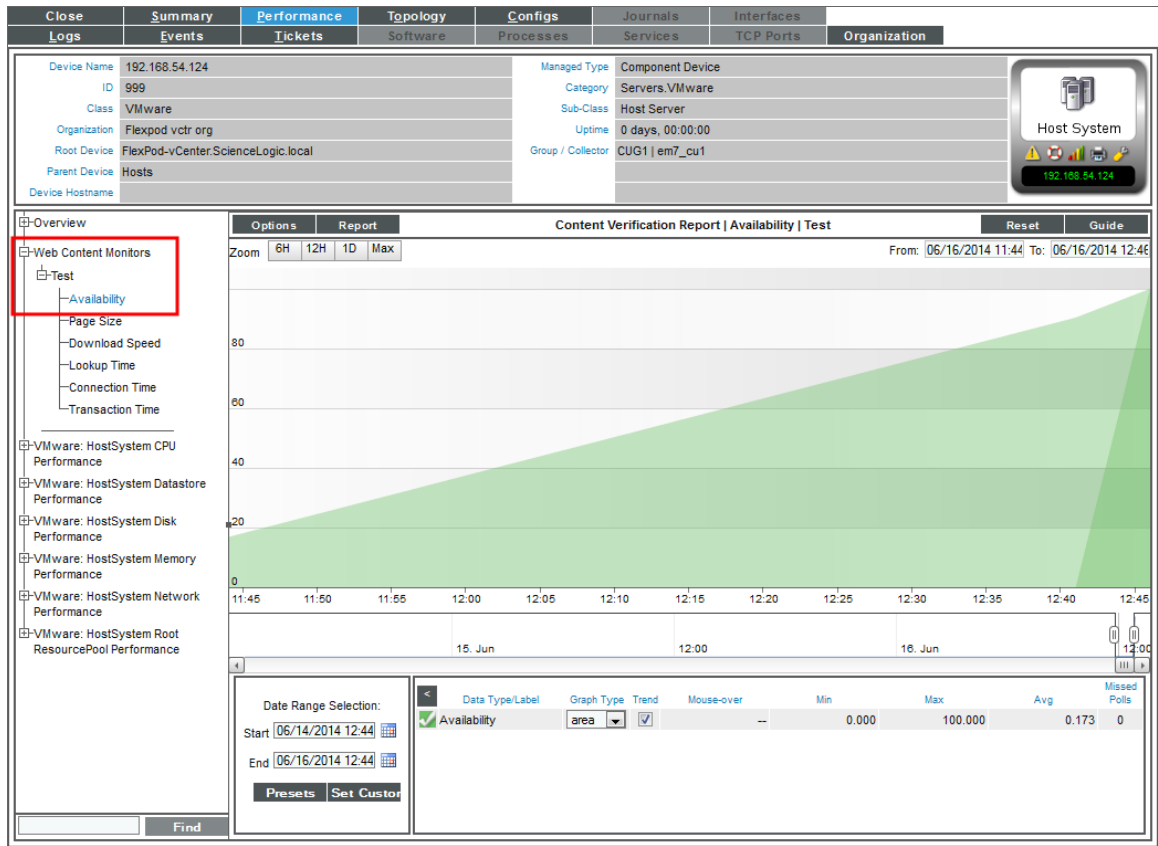
There are two ways to navigate to the reports for a web content policy:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
 - In the Device Reports panel, select the **Performance** tab.
 - In the NavBar, expand Web Content Monitors and select the policy for which you want to view the report.

Or:

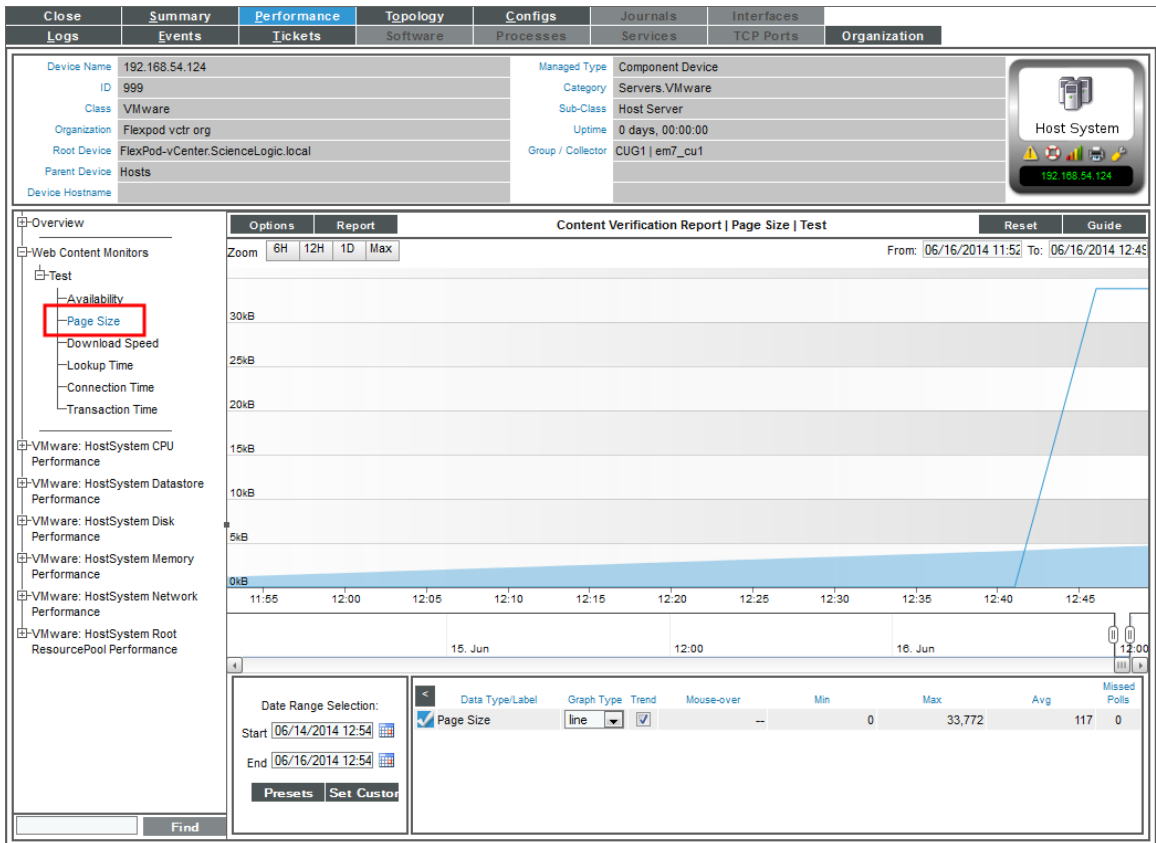
2. From the **Web Content Monitoring** page (Registry > Monitors > Web Content):
 - In the **Web Content Monitoring** page, find the policy for which you want to see a report.
 - Select its bar graph icon in the *Policy Name* field ()

- The **Device Performance** page appears, with the Content Verification Report | Availability report displayed.



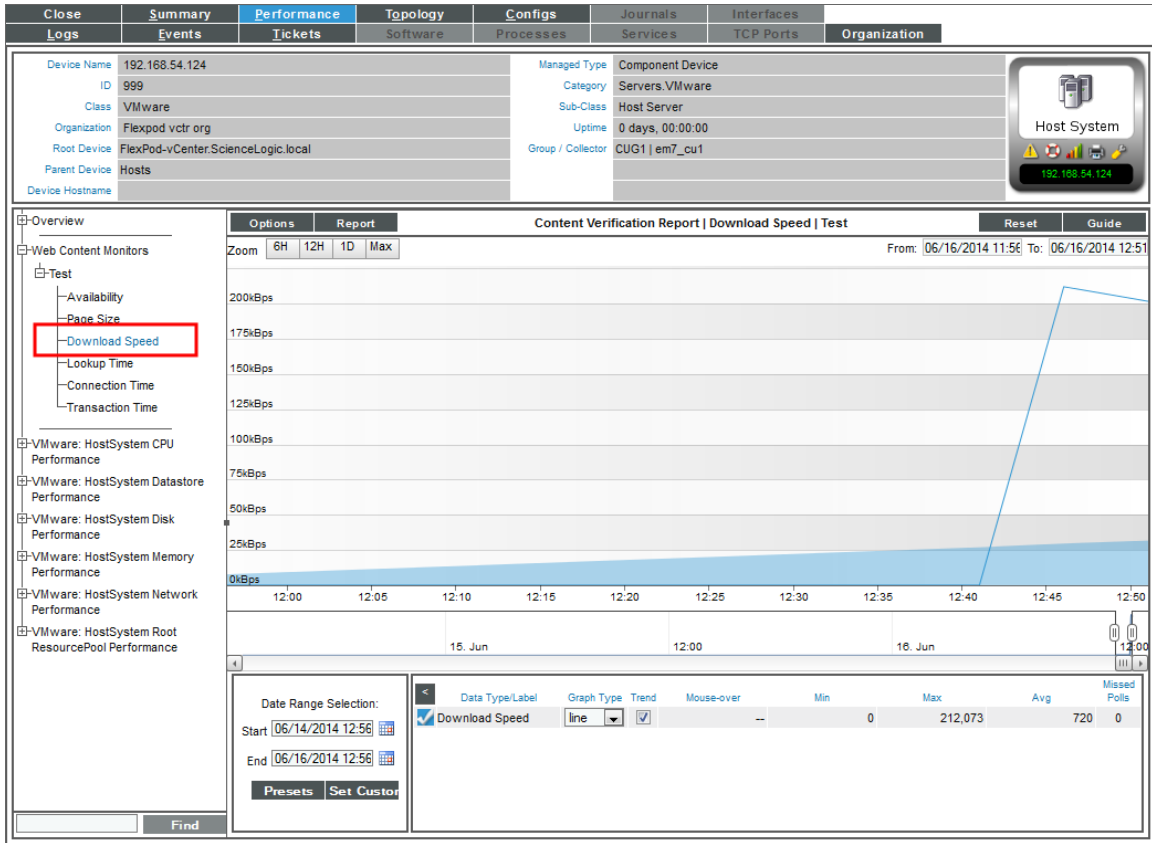
- The Content Verification Report | Availability report displays the availability of the specified content on the specified web-server for the selected duration.
 - The y-axis displays availability, in percent to the left.
 - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- For each Web Content policy, you can also view the following additional reports. To view them select the entries in the NavBar:

- **Page Size.** The Content Verification Report | Page Size report displays information about the size of the page specified in the URL of the policy. The graph displays the page size of the specified URL for the selected duration.



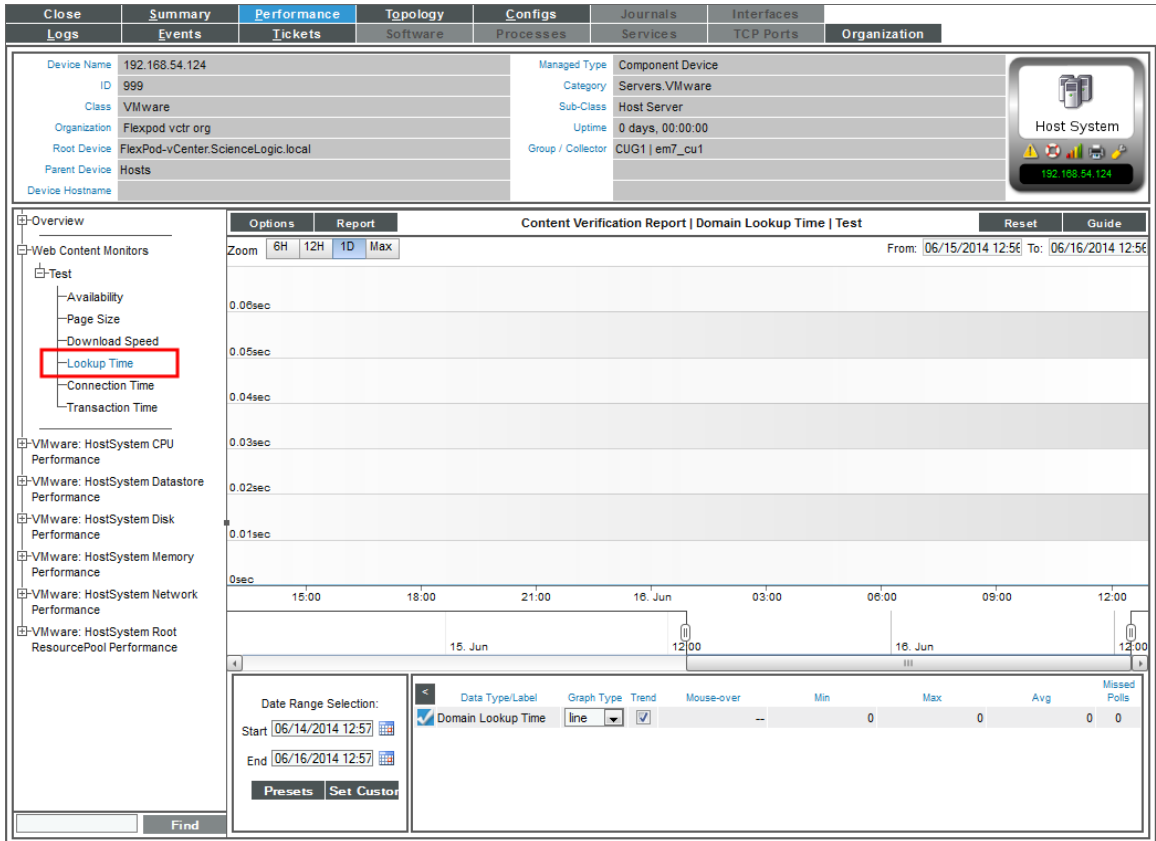
- The y-axis displays size in kilobytes (Kb).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

- **Download Speed.** The Content Verification Report | Download Speed report displays the speed at which data was downloaded from the website (specified in the policy) to SL1. The graph displays the speed at which data was downloaded from the specified website to SL1 for the selected duration.



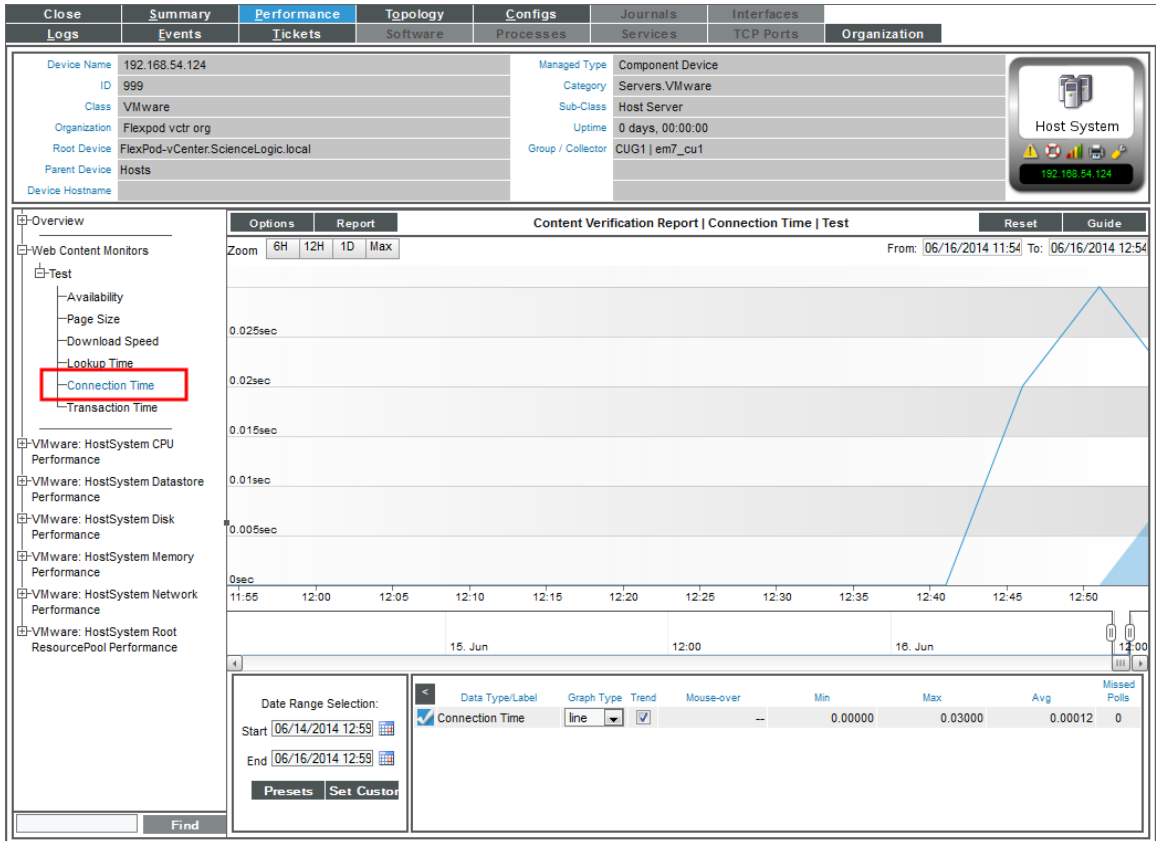
- The y-axis displays the speed at which data was downloaded from the website to SL1, in bits per second (Bps).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).

- **Lookup Time.** The Content Verification Report | Domain Lookup Time report displays the speed at which your DNS system was able to resolve the name of the website specified in the policy. The graph displays the speed at which your DNS system was able to resolve the name of the website for the specified duration.



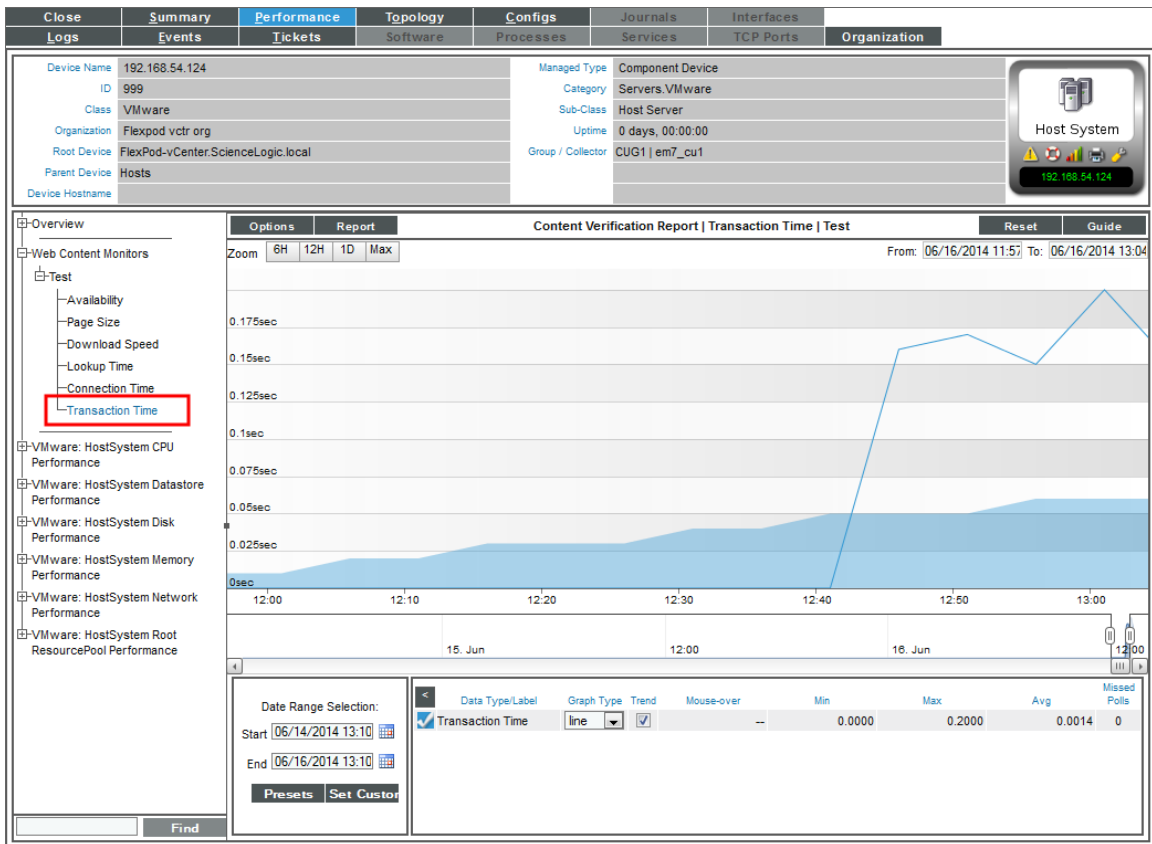
- The y-axis displays the speed at which your DNS system was able to resolve the name of the website, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

- **Connection Time.** The Content Verification Report | Connection Time report displays the time it takes for SL1 to establish communication with the external website. In other words, the time it takes from the beginning of the HTTP request to the TCP/IP connection. The graph displays the speed at which SL1 was able to make a TCP/IP connection to the external website for the specified duration.



- The y-axis displays the speed at which SL1 was able to make a TCP/IP connection to the external website, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

- **Transaction Time.** The Content Verification Report | Transaction Time report displays the total time it took to make a connection to the external website, send the HTTP request, wait for the website to parse the request, receive the requested data from the website, and close the connection. The graph displays the total time for the entire transaction from SL1 to the external website and back to SL1 for the specified duration.



- The y-axis displays the speed of the entire transaction from SL1 to the external website and back to SL1, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the [Options] menu) and the date range (from the **Date Range Selection** pane).

Viewing Availability Reports for a Single Windows Service on a Device

When you define a Windows service -monitoring policy, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

For policies that monitor Windows service, SL1 generates the following report:

- The **Service Report** displays the availability of a single monitored Windows Service on the device


During polling, a service has two possible availability values:

- 100%. Service is up and running.
- 0%. Service is not up and running

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 service was unavailable, the average would be 80% ($100 + 100 + 100 + 100 + 0 = 400$; $400/5 = 80$).


There are two ways to navigate to the reports for Windows Service monitoring:

1. From the **Device Manager** page (Devices > Device Manager):

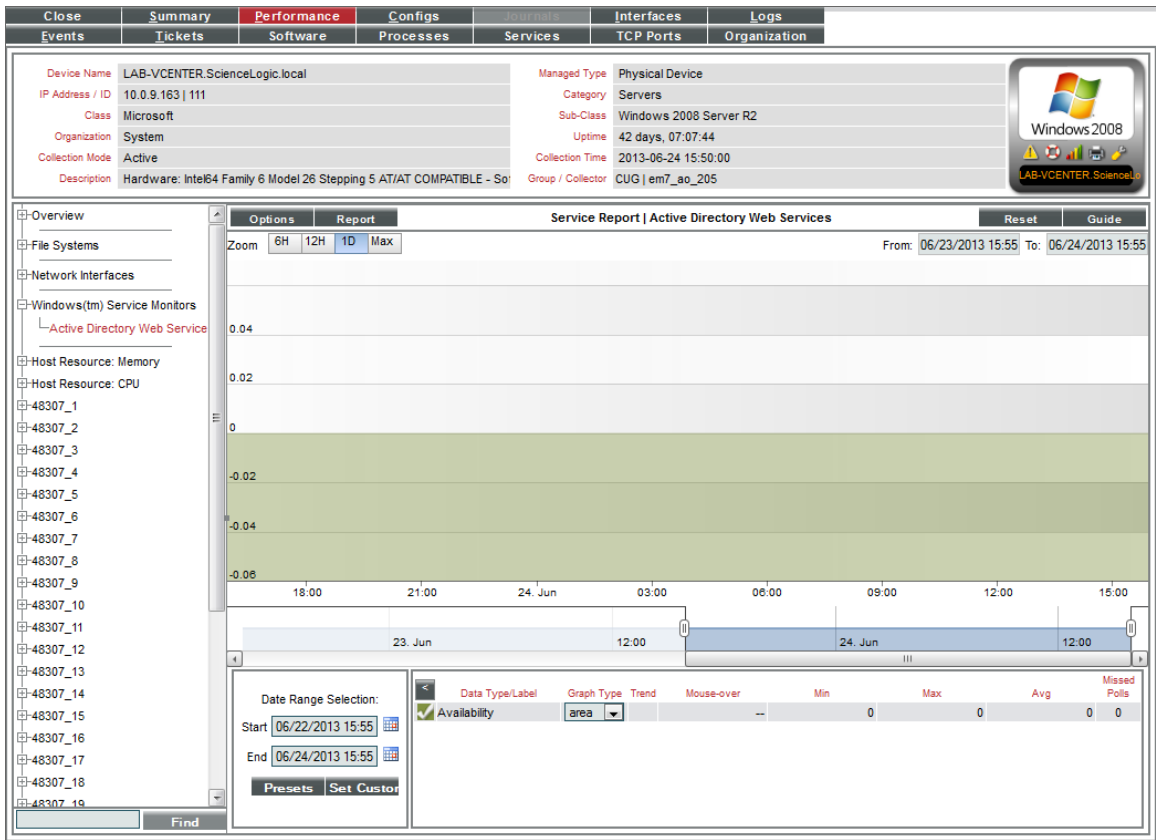
- In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon () for the device.
- In the **Device Reports** panel, select the **Performance** tab.
- In the NavBar, expand *Windows Service Monitors* and select the policy for which you want to view the report.

Or:

2. From the **Windows Service Monitoring** page (Registry > Monitors > Windows Services):

- In the **Windows Service Monitoring** page, find the policy for which you want to see a report.
- Select its bar graph icon in the *Windows Service* name field ()

3. The **Device Performance** page appears, with the Service Report displayed.



4. The Service Report displays a color-coded line for the availability of the monitored Windows service over time.



- The y-axis displays the availability of the service in percent to the left.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).

Viewing Configuration & Journal Data

Overview

This chapter describes how to view data collected by Dynamic Applications that collect configuration and journal data.

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:

<i>Configuration Dynamic Applications</i>	186
<i>Journal Dynamic Applications</i>	190

Configuration Dynamic Applications


The **Configuration Report** page displays data collected from the device by configuration Dynamic Applications. Usually, configuration data contains static information about hardware and configuration settings, such as serial numbers, version numbers, and hardware status.

NOTE: If you select the **Hide Object** checkbox for an object in the **Collection Objects** page (System > Manage > Dynamic Applications > Create/Edit), the object will not be included in the **Configuration Report** page.

For objects of type "enum," you can mouseover the object and view all the possible values for the object.

NOTE: The **Configuration Report** page does not display Dynamic Applications that have *Cache Results* selected in the **Caching** field in the **Dynamic Applications Properties Editor** page. Dynamic Applications that cache results are designed to collect data only for other Dynamic Applications and cannot be used to display data.

To view Configuration Dynamic Application information:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to view configuration Dynamic Application data. Select its bar graph icon (). In the **Device Administration** panel, select the **[Configs]** tab.

3. The **Device Configuration** page is displayed:

The screenshot displays the 'Device Configuration' page for a VMware host system. The top navigation bar includes tabs for Close, Summary, Performance, Topology, Configs (selected), Journals, Interfaces, Logs, Events, Tickets, Software, Processes, Services, TCP Ports, and Organization. The main content area is divided into several sections:

- Device Information:** Shows details like Device Name (192.168.54.124), ID (999), Class (VMware), Organization (Flexpod vctr org), Root Device (FlexPod-vCenter.ScienceLogic.local), Parent Device (Hosts), and Device Hostname.
- Managed Type:** Lists Component Device, Servers.VMware, Host Server, Uptime (0 days, 00:00:00), and Group / Collector (CUG1 | em7_cu1).
- Configuration Report | VMware: Hardware Monitoring Configuration:** Includes a Snap-Shot Date (2014-06-16 13:05:00) and a Rollup System Health section showing a Green status.
- Processor Health:** A table listing 14 items such as CPU1 Level-1 Cache, Memory Module 2, Processor 1 P1_PROCHOT, etc., all with a Green health state.
- Fan Health:** A table with columns for Description, Health State, and RPMs.
- Power Health:** A table listing 5 items like Processor 1 VCCP_P1_CUR_SENS, System Board 0 POWER_USAGE, etc., with columns for Description, Health State, Units, and Value.

Selecting Data to View

If one or more Dynamic Applications of type "configuration" are associated with the device, the **Configuration Report** page will display that list of Dynamic Applications in the left NavBar.

NOTE: The left navigation bar does not display Dynamic Applications that have *Cache Results* selected in the **Caching** field in the **Dynamic Applications Properties Editor** page. Dynamic Applications that cache results are designed to collect data only for other Dynamic Applications and cannot be used to display data.

Viewing Data

When you select a Dynamic Application in the left NavBar, the right pane displays data collected from the device by the Dynamic Application.

- Some objects may appear in a list at the top of the right pane. These are objects that are not grouped into a table. For each of these values, no values were specified in the **Group** field and the **Table Alignment** field, in the **Collection Objects** page. These are usually objects for which there is only one, non-changing value

(like model number, for example).

- Some objects may appear in tables. Tables work best for objects with multiple values, like RAM location. Each row represents one value from each collection object in the group, which all have the same index.
 - Each column heading is the name of an object. Mousing over the column heading displays a description of the object. To edit the description, click on the column heading. The **Collection Objects** page appears, populated with values from the appropriate object. You can edit the value in the *Description* field, and that value will appear when you mouseover the column heading in the **Configuration Report** page.
- Mousing over a value can display the following:
 - If the object is of type "enum", the mouseover text displays the list of all possible values for the object. For example, "0 unknown, 1 disabled, 2 enabled".
 - If change detection has not been enabled, displays the text "Change detection is disabled. No history available".
 - If change detection has been enabled, displays "Click to view change history". If you click, SL1 displays the **Change History** modal page, where you can view all the values collected from the device for the selected object.

Generating a Report of the Data

You can generate a report about the data in the **Configuration Report** page. To do so:

1. In the **Configuration Report** page, in the Navigation Bar (left pane), select the Dynamic Application you want to generate a report from.
2. In the **Configuration Report** page, select the **[Actions]** menu. Select *Print a Report*.
3. SL1 generates an HTML report that contains all the data from the **Configuration Report** page. You can view, print, or save the report.

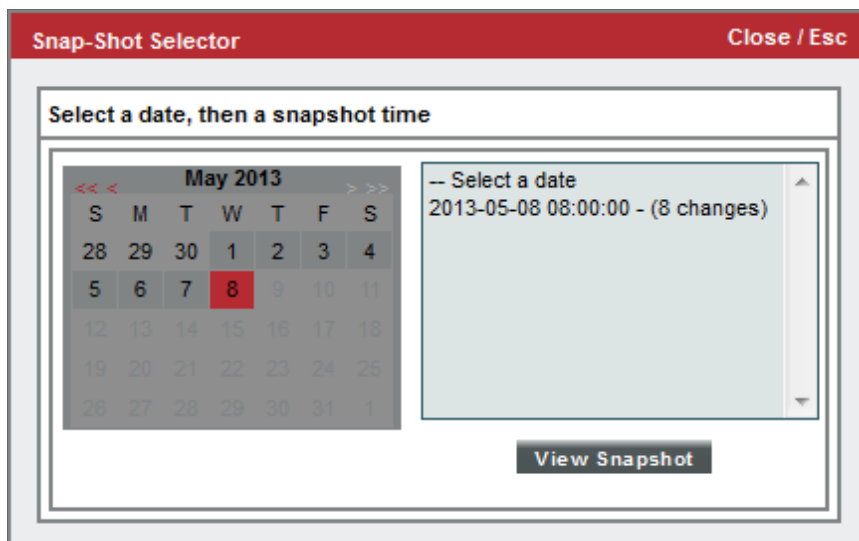
Viewing Historical Data

By default, the **Configuration Report** page displays data from the latest polling session. However, you can use the **Snap-Shot Selector** page to display data from a previous polling session in the **Configuration Report** page.

The **Snap-Shot Selector** page displays a list of polling sessions where a change was discovered in the configuration data. If none of the data in a Dynamic Application changes from one polling session to the next, then SL1 does not include an entry in the **Snap-Shot Selector** page.

To display data from a previous polling session in the **Configuration Report** page:

1. In the **Configuration Report** page, in the Navigation Bar (left pane), select the Dynamic Application for which you want to view historical data.
2. When the data is displayed in the right pane, select the **[Snap-Shots]** button.
3. The **Snap-Shot Selector** modal page appears. This page displays a calendar interface, in which you can select a date for which you want to view a list of Snap-Shots.



4. To select a date for a Snap-Shot, scroll through the calendar until you find the month that you are interested in. Click on the date you are interested in.
5. The pane to the right will display a list of all available Snap-Shots for the selected date. Each Snap-Shot is labeled with a date and time stamp and specifies how many objects had changed values. To select a Snap-Shot, click on it and select the **[View Snapshot]** button.

NOTE: If the pane to the right does not display one or more available Snap-Shots, this means that SL1 did not detect any changes to the objects on the selected date.

6. The data from the selected Snap-Shot is loaded and displayed in the **Configuration Report** page.

Editing the Application

From the **Configuration Report** page, you can edit the properties of a Dynamic Application. When you do so, you change the behavior of the Dynamic Application for all subscriber devices, not just the current device.

To edit a Dynamic Application from the **Configuration Report** page:


1. In the **Configuration Report** page, in the Navigation Bar (left pane), select the Dynamic Application you want to view and edit.
2. When the data from the Dynamic Application is displayed in the right pane, select the **[Actions]** menu and choose *Edit This Application*.
3. The **Collection Objects** page appears. In this page, you can edit how SL1 retrieves values for an object and how those values are displayed in the **Configuration Report** page. You can also access all the other tabs in the Dynamic Applications panel for the Dynamic Application.

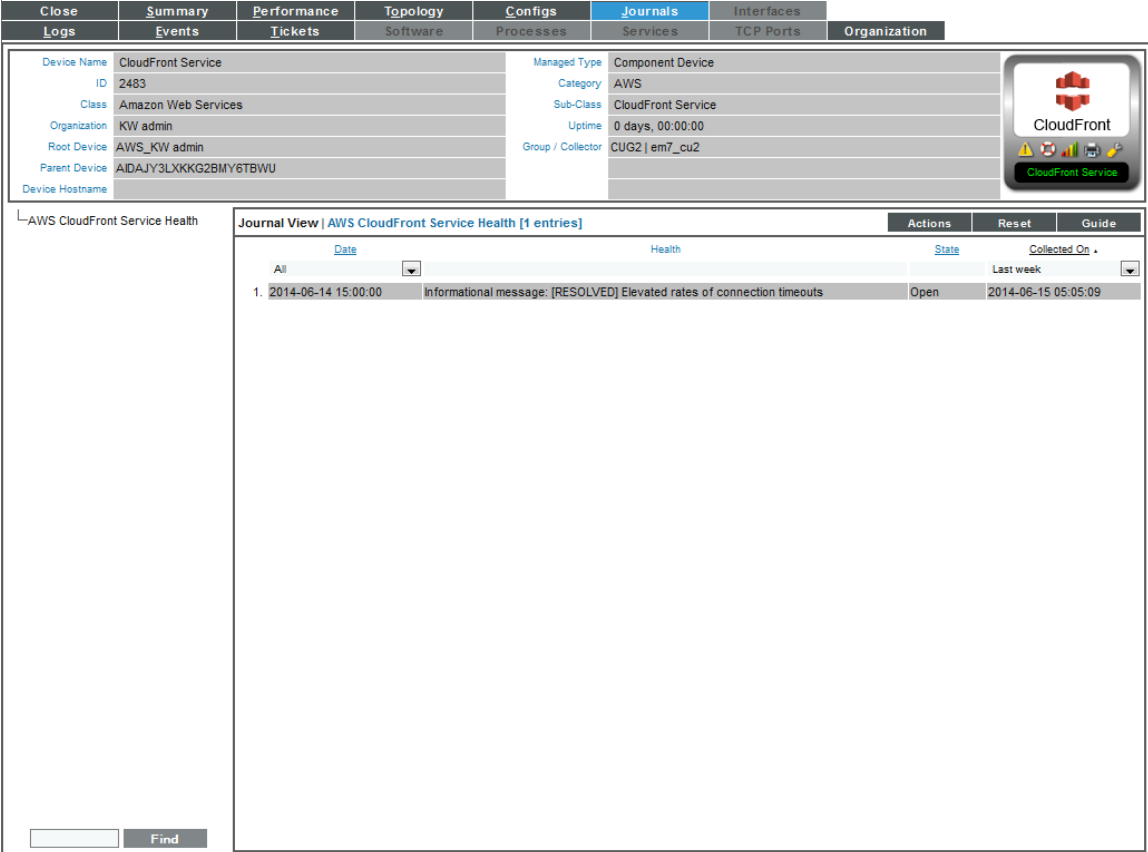
For information about editing Dynamic Applications, see the *Dynamic Application Development* manual.


Journal Dynamic Applications

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

To view journal Dynamic Application information:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to view journal Dynamic Application data. Select its bar graph icon () in the **Device Reports** panel, select the **[Journals]** tab.
3. The **Journal View** page is displayed:



Close	Summary	Performance	Topology	Configs	Journals	Interfaces	
Logs	Events	Tickets	Software	Processes	Services	TCP Ports	Organization
Device Name	CloudFront Service	Managed Type	Component Device				
ID	2483	Category	AWS				
Class	Amazon Web Services	Sub-Class	CloudFront Service				
Organization	KW admin	Uptime	0 days, 00:00:00				
Root Device	AWS_KW admin	Group / Collector	CUG2 em7_cu2				
Parent Device	AIDAJY3LXKKG2BMY6TBWU						
Device Hostname							
AWS CloudFront Service Health							
Journal View AWS CloudFront Service Health [1 entries]							
Actions Reset Guide							
Date Health State Collected On							
All					Last week		
1.	2014-06-14 15:00:00	Informational message: [RESOLVED] Elevated rates of connection timeouts	Open	2014-06-15 05:05:09			

Selecting Data to View

If one or more Dynamic Applications of type "journal" are associated with the device, the **Journal View** page will display that list of Dynamic Applications in the left NavBar.

When you select a Dynamic Application in the left NavBar, the right pane displays data collected from the device by the Dynamic Application.

Viewing Data

The **Journal View** page arranges collected journal entries in tabular format.

- The table contains a row for each journal entry.
- The table contains a column for each presentation object, plus the **State** and **Collected On** columns. Presentation objects define the text to display in each row in the column, including which collection values will be displayed. Presentation objects are defined in the **Presentation Objects** page for the Dynamic Application.

The **Journal View** page displays the following about each journal entry:

TIP: To sort by descending order, click the column heading again. To sort a column that contains presentation objects, sorting must be enabled in the **Presentation Objects** page (System > Manage > Dynamic Applications > Create/Edit). Date and time column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- **Presentation Objects.** One or more columns in the table of journal entries will be presentation objects defined in the Dynamic Application. The values in this column can be based on one or more collection objects, and can be a text string, a number, or a time and date value.
- **State.** Specifies the current state of the journal entry. Journal entries can have one of the following states:
 - Open
 - Closed
 - Abandoned
 - Error
 - Reopened
- **Collected On.** Specifies the last time the journal entry was updated.

Searching & Filtering the List of Data

You can filter the list on the **Journal View** page by one or more parameters. Only journal entries that meet all the filter criteria will be displayed in the **Journal View** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Journal View** page searches for journal entries 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:

- **Presentation Objects.** Each presentation object column has a filter. For columns that contain a text string or a numeric value, you can enter text to match, including special characters, and the **Journal View** page will display only journal entries that have a matching value for that presentation object. For each journal entry, the value that is matched for a presentation object is the value of the first collection object that appears in the presentation object text. For columns that contain a time and date, you can select a time span, and the **Journal View** page will display only journal entries that have a time and date value within the selected time span. Choices are:
 - *All.* Display all journal entries that match the other filters.
 - *Last Minute.* Display only journal entries that have been created within the last minute.
 - *Last Hour.* Display only journal entries that have been created within the last hour.
 - *Last Day.* Display only journal entries that have been created within the last day.
 - *Last Week.* Display only journal entries that have been created within the last week.
 - *Last Month.* Display only journal entries that have been created within the last month.
 - *Last Year.* Display only journal entries that have been created within the last year.
- **State.** You can enter text to match, including special characters, and the **Journal View** page will display only journal entries that have a matching state. Journal entries can have one of the following states:
 - Open
 - Closed
 - Abandoned
 - Error
 - Reopened
- **Collected On.** You can select a time span, and the **Journal View** page will display only journal entries that have been updated within that time period. Choices are:
 - *All.* Display all journal entries that match the other filters.
 - *Last Minute.* Display only journal entries that have been created within the last minute.
 - *Last Hour.* Display only journal entries that have been created within the last hour.
 - *Last Day.* Display only journal entries that have been created within the last day.
 - *Last Week.* Display only journal entries that have been created within the last week.
 - *Last Month.* Display only journal entries that have been created within the last month.
 - *Last Year.* Display only journal entries that have been created 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 contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^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!*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!^s*i!*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 "sXiXo" 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".

Generating a Report of the Data

You can generate a report about the data in the **Journal View** page.

To generate a report about the data in the **Journal View** page:


1. Go to Devices > Device Manager. Find the device for which you want to generate a report. Select its bar graph icon (). Select the **[Journals]** tab.

2. In the **Journal View** page, in the left NavBar, select the Dynamic Application you want to generate a report from.
3. You can filter the journal entries to include in the report. Using the search filters at the top of the table of journal entries, filter the list of journal entries so that only the journal entries you want to include on the report are displayed.
4. In the **Journal View** page, select the **[Actions]** menu. Select **Generate Report**.
5. The **Export current view as a report** page is displayed. Select the output format for the report, optionally select if SL1 must force the browser to save the file to disk, and then select the **[Generate]** button.

Editing the Application

From the **Journal View** page, you can edit the properties of a Dynamic Application. When you do so, you change the behavior of the Dynamic Application for all subscriber devices, not just the current device.

To edit a Dynamic Application from the **Journal View** page:

1. Go to Devices > Device Manager. Find the device for which you want to view data. Select its bar graph icon (). Select the **[Journals]** tab.
2. In the **Journal View** page, in the left NavBar, select the Dynamic Application you want to view and edit.
3. When the data from the Dynamic Application is displayed in the right pane, select the **[Actions]** menu and choose **Edit This Application**.
4. The **Collection Objects** page appears. In this page, you can edit how SL1 retrieves values for an object. You can also access all the other tabs in the Dynamic Applications panel for the Dynamic Application.

For information about editing Dynamic Applications, see the **Dynamic Application Development** manual.

Chapter

8

Network Interfaces



Overview

During discovery, SL1 discovers all interfaces on each discovered device. The list of all interfaces is displayed on the **Network Interfaces** page (Registry > Networks > Interfaces).

SL1 applies a default monitoring policy to every discovered interface (excluding loopback interfaces). The default policy collects inbound and outbound bandwidth statistics every 5 minutes.

The **Network Interfaces** page allows you to view a list of all interfaces, view details on each interface, edit the monitoring policy for an interface, and view bandwidth reports on each interface.

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:

Class-Based Quality of Service (CBQoS)	199
Viewing All Interfaces Discovered by the ScienceLogic Platform	199
Viewing Interfaces for a Single Device	203
Generating a Report for Multiple Network Interfaces	207
Generating a Report for a Single Network Interface	209
Monitoring Interfaces	211
Defining a Detailed Monitoring Policy for a Single Interface	211
Defining Monitoring Settings for Multiple Interfaces	217
Defining Thresholds for an Interface	222

Viewing the List of Discovered CBQoS Objects	226
Editing Thresholds for a Quality of Service (QoS) Object	229
Viewing Reports About Interfaces and Bandwidth	232
Global Settings that Affect Interfaces	232

Class-Based Quality of Service (CBQoS)

Class-Based Quality of Service (CBQoS) is a Cisco technology, available on Cisco devices. CBQoS allows you to manage and prioritize network traffic. SL1 can retrieve configuration information about CBQoS from Cisco devices that are configured to use CBQoS.

To collect CBQoS data about an interface, you must enable CBQoS monitoring in two places in SL1:

- In the **Behavior Settings** page (System > Settings > Behavior), enable the field **Enable CBQoS Collection**. This setting allows SL1 to collect configuration data from interfaces that are configured for CBQoS. SL1 will check for new CBQoS interfaces during initial discovery, during manual discovery, and once a day when the process **Data Collection: CBQoS Inventory** runs.
- In the **Network Interfaces** page (Registry > Networks > Interfaces) or the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon), enable CBQoS reporting for each interface for which you want to view CBQoS data. This setting allows SL1 to collect performance data for interfaces that are configured for CBQoS and generate performance graphs for those interfaces.

You must enable CBQoS for the SL1 system and also for each interface.

If both settings are enabled, the SL1 system will display the collected CBQoS configuration data in the reports in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) for the device that contains this interface.

Viewing All Interfaces Discovered by the ScienceLogic Platform

During discovery, SL1 discovers all interfaces on each discovered device. The list of all interfaces is displayed in the **Network Interfaces** page.

The **Network Interfaces** page allows you to view a list of all interfaces, view details on each interface, define a monitoring policy for an interface, and view bandwidth reports on each interface.

To view a list of all interfaces discovered by SL1:

1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).

2. The **Network Interfaces** page displays a list of all network interfaces discovered by SL1.

Device Name	Port/Sub	IF Name	Tags	Organization	Alias	MAC Address	IF Index	IF Type	Admin/Oper Status	Measure	Interface Speed	Alerting	Auto-Name Update	Collection Frequency	Collect Errors	Collect Disacts	Collect CSOOS	Collect Packets	Counter Settings	State
10.168.48.59	0/0112	Gig12		System		08.00.9f58.cc.8c.10112		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/1	V11		System	Link to WAN-R1	08.00.9f58.cc.8c.01		propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/0114	Gig14		System		08.00.9f58.cc.8c.10114		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/0115	Gig15		System		08.00.9f58.cc.8c.10115		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/0116	Gig16		System		08.00.9f58.cc.c2.10116		ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/5	V15		System		08.00.9f58.cc.c3.5		propVirtual	Down/Down	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/0118	Gig18		System		08.00.9f58.cc.92.10118		ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/0113	Gig13		System		08.00.9f58.cc.8c.10113		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/666	V666		System		08.00.9f58.cc.8c.666		propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10501	Nu0		System			10501	other	Up/Up	Mega	10 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	32	Enabled
10.168.48.59	0/0117	Gig17		System		08.00.9f58.cc.8c.10117		ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/99	V999		System		08.00.9f58.cc.c4.99		propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/999	V999		System	Link to WAN-R1	08.00.9f58.cc.c8.999		propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10101	Gig1		System		08.00.9f58.cc.c1.10101		ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10102	Gig2		System		08.00.9f58.cc.c2.10102		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10103	Gig3		System		08.00.9f58.cc.83.10103		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10104	Gig4		System		08.00.9f58.cc.84.10104		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10105	Gig5		System		08.00.9f58.cc.85.10105		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10106	Gig6		System		08.00.9f58.cc.86.10106		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10107	Gig7		System		08.00.9f58.cc.87.10107		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10108	Gig8		System		08.00.9f58.cc.88.10108		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10109	Gig9		System		08.00.9f58.cc.89.10109		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10110	Gig10		System		08.00.9f58.cc.8a.10110		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
10.168.48.59	0/10111	Gig11		System		08.00.9f58.cc.8b.10111		ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
76095-NPE3.000	0/1	Te3/1		System	connection CRS-1-P	00.24.14.4b.48.4.1		ethernetCsmacd	Up/Down	Mega	10 Gbps	Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled
76095-NPE3.000	0/2	Te3/2		System		00.24.14.4b.48.4.2		ethernetCsmacd	Up/Up	Mega		Yes	Yes	5 Min	No	No	Yes	Yes	64	Enabled

3. The **Network Interfaces** page displays the following for each interface:

TIP: To sort the list of interfaces, 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 where the interface resides.
- **Port/Sub.** Port and sub-port (if applicable) of the interface.
- **IF Name.** The name of the network interface. The auto-name, generated by SL1, is device_name:interface_number. Users can define a different name in the **Interface Properties** page.
- **Tags.** Displays a comma-delimited list of descriptive tags that have been manually defined for the interface. Interface tags are used to group interfaces in an IT service policy. To add or edit the tags for an interface, click its wrench icon (🔧). In the **Edit Network Interface Tags** modal page that appears, supply a comma-delimited list of tags in the **Tags** field, and then click the **[Save]** button.
- **Organization.** Organization associated with the network interface. This can be the organization associated with the device where the interface resides, or it can be an organization that has emissary rights to the interface.
- **Alias.** User-defined name assigned to the interface.
- **MAC Address.** Short for Media Access Control Address. A unique number that identifies the interface. MAC Addresses are defined by the hardware manufacturer.
- **IF Index.** A unique number (greater than zero) that identifies each interface on a device. These numbers are defined within the device.

- **IF Type.** A string that describes the type of interface, as defined by the standards group Internet Assigned Numbers Authority.
- **Status.** Two-part status:
 - *Administration Status.* Specifies how the network interface has been configured on the device. Can be one of the following:
 - Up. Network interface has been enabled (configured to be up and running).
 - Down. Network interface has been purposefully disabled.
 - *Operation 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.

NOTE: SL1 generates an event when a network interface has an administrative status of "up" and an operation status of "down".

- **Measure.** Unit of measurement for bandwidth reports for the interface. The choices are:
 - Mega
 - Giga
 - Kilo
 - Tera
 - Peta
- **Interface Speed.** The number of megabits per second that can pass through the network interface.
- **Alerting.** Specifies whether or not events will be generated for the selected interfaces.
 - Yes. SL1 monitors the network interface and generates events when the required conditions are met.
 - No. SL1 monitors the network interface, but events are not generated for the interface.
- **Auto-Name Update.** Specifies whether or not SL1 will update and/or over-write the interface name during auto-discovery.
 - Yes. SL1 can update and/or over-write the interface name during auto-discovery.
 - No. SL1 will not update and/or over-write the interface name during auto-discovery.

- **Collection Frequency.** When you define a monitoring policy for an interface, you must specify how frequently you want SL1 to collect data from the interface. Your choices are every:
 - 1 Minute
 - 5 Minutes
 - 10 Minutes
 - 15 Minutes
 - 30 Minutes
 - 60 Minutes
 - 120 Minutes

- **Collect Errors.** Specifies whether or not 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. Your choices are:
 - Yes. SL1 will collect data on packet errors that occur on the interface.
 - No. SL1 will not collect data on packet errors that occur on the interface.

- **Collect Discards.** Specifies whether or not SL1 will collect data on interface discards. Discards occur when an interface receives more traffic than it can handle (either 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. Your choices are:
 - Yes. SL1 will collect data on packet discards that occur on the interface.
 - No. SL1 will not collect data on packet discards that occur on the interface.

- **Collect CBQoS.** Specifies whether SL1 will collect CBQoS (Class-Based Quality-of-Service) data for this interface. This column appears only if you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior). If **Collect CBQoS** is enabled for an interface, SL1 will display the collected CBQoS data in Device Performance reports associated with the device that contains this interface. Choices are:
 - Yes. SL1 will collect CBQoS data for this interface.
 - No. SL1 will not collect CBQoS data for this interface.

- **Collect Packets.** Specifies whether SL1 will collect data for unicast, multicast, and broadcast traffic, in packets, for this interface. If **Collect Packets** is enabled for an interface, SL1 will display the collected data in Device Performance reports associated with the device that contains this interface. Choices are:
 - Yes. SL1 will collect packet data for this interface.
 - No. SL1 will not collect packet data for this interface.

- **Counter Setting.** Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface.

NOTE: If an interface has a status of "down" during initial discovery, SL1 will discover the interface but assign the interface the default Counter Setting of "32". During re-discovery or nightly auto-discovery, SL1 will update Counter Setting to "64" if applicable.



- **State.** This field can have one of two values:
 - *Enabled.* SL1 monitors the network interface and collects data on the network interface for reports.
 - *Disabled.* SL1 does not monitor the network interface or collect data on the network interface for reports.
- **Edit Date.** Date and time the monitoring policy for the interface was created or last edited. If the interface is using the default monitoring policy, the edit date reflects the date that the interface was discovered by SL1.

Viewing Interfaces for a Single Device

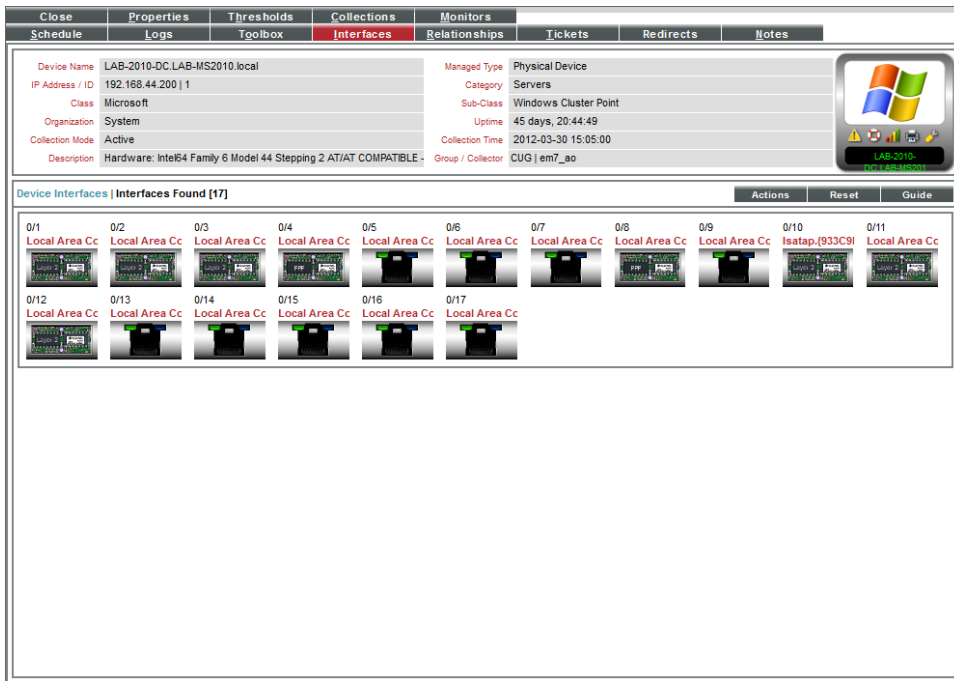
In the **Device Administration** panel for a device, you can view the **Device Interfaces** page. The **Device Interfaces** page displays detailed information about each network interface on the device and allows you to define monitoring policies for interfaces on the device. When you define a monitoring policy for an interface, SL1 will monitor the interface and gather usage data from the interface. SL1 uses the data retrieved from the interface to generate bandwidth reports for the interface.

In the **Device Reports** panel for a device, you can view the **Interfaces Found** page. The **Interfaces Found** page displays detailed information about each network interface on the device. The **Interfaces Found** page allows you to view a list of all interfaces on the device, view details about each interface, and view bandwidth usage reports for each interface.

To view details about the network interfaces on a device:

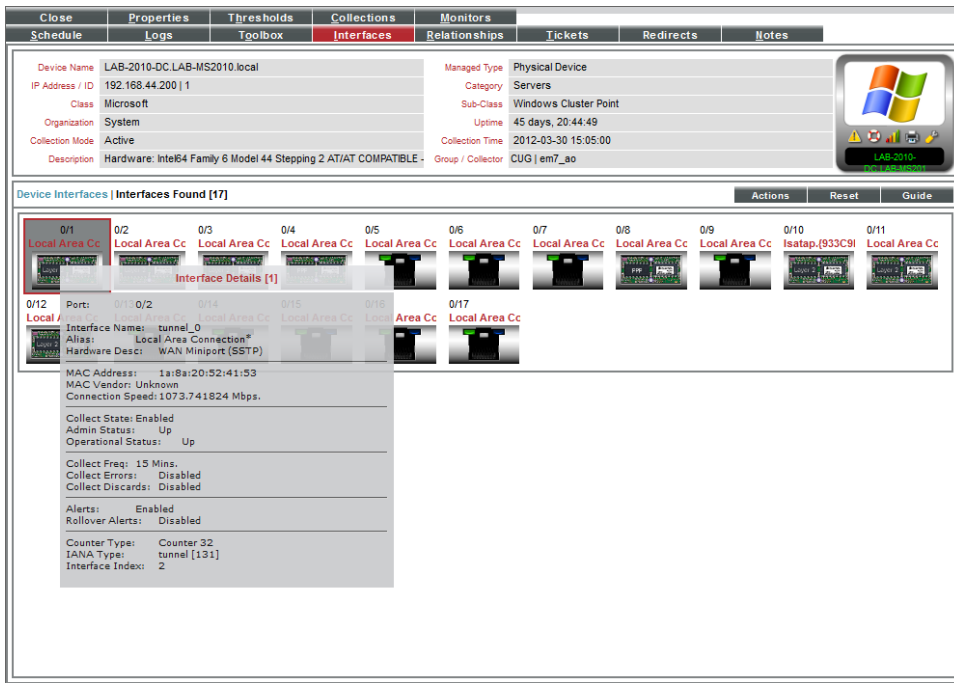
1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to view the list of network interfaces, then do one of the following:
 - Click its wrench icon () , followed by the **[Interfaces]** tab, to view the **Device Interfaces** page.
 - Click the bar graph icon () , followed by the **[Interfaces]** tab, to view the **Interfaces Found** page.

- Both pages display icons to represent the interfaces on the device:



- The page displays an icon for each interface on the device. Each icon provides a visual overview of the interface.
- For details on interface icons, click the **[Legend]** button, or in the **[Actions]** menu, select **Interface Legend**. The **Interface Legend** modal page displays each type of interface icon with explanatory callouts.

6. When you mouse over the icon for that interface, the **Interface Details** modal page appears. This page displays details about the interface and its current monitoring policy.



7. The **Interface Details** modal page displays the following about an interface:

- **Port / Sub.** Port and sub-port (if applicable) of the interface.
- **Interface Name.** The name of the network interface. The auto-name, generated by SL1, is device_name:interface_number.
- **Alias.** Easy-to-remember, human-readable name for the network interface.
- **Hardware Desc.** 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 network hardware. MAC Addresses are defined by the hardware manufacturer.
- **MAC Vendor.** Manufacturer of the network interface.
- **Connection Speed.** The amount of data per second that can pass through the network interface.
- **Collect State.** Specifies whether or not SL1 monitors the network interface and collects data from the network interface for reports.
- **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.
- **Collect Freq.** Frequency at which SL1 will poll the interface to collect data. Choices are 1 minute, 5 minutes, 10 minutes, 30 minutes, 60 minutes, and 120 minutes.
- **Collect Errors.** Specifies whether or not 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 or not 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 or not 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 or not SL1 will generate an event when the counter for the interface rolls over.

NOTE: Rollovers and **Rollover Alerts** apply only to 32-bit counters and not to 64-bit counters.

- **IP.** IP address and network mask assigned to the interface.
- **Counter Type.** Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface.

NOTE: If an interface has a status of "down" during initial discovery, SL1 will discover the interface but assign the interface the default **Counter Type** of "32". During re-discovery or nightly auto-discovery, SL1 will update the **Counter Type** to "64" if applicable.

- **IANA Type.** A string that describes the type of interface, as defined by the standards group Internet Assigned Numbers Authority.
 - **Interface Index.** A unique number (greater than zero) that identifies each interface on a device. These numbers are defined by the device.
8. In the **Device Interfaces** page, clicking on an interface icon leads to the **Interface Properties** page, where you can define a monitoring policy for an interface.
 9. In the **Interfaces Found** page, clicking on an interface icon leads to the Network Bandwidth Usage report in the **Device Performance** page.

Generating a Report for Multiple Network Interfaces

The Registry tab includes the **Network Interfaces** page. From the **Network Interfaces** page you can generate a report on all, multiple, or a single interface in SL1. The report will contain all the information displayed in the **Network Interfaces** page. The **Network Interfaces** page is located at Registry > Networks > Interfaces.

Network Interfaces Report generated by em7admin on 2016-05-27 14:20:22

Device Name	Port/Sub	IF Name	Alias	MAC Address	IF Index	IF Type	IF Status	Measure	Speed	Alerting	Name Update	Collect Rate	Errors	Discards	Counter	State	
1.	10.168.48.59	0/0112	Gi0/12		08:00:9f:58:cc:8c	10112	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
2.	10.168.48.59	0/1	V11	Link to WAN-R1	08:00:9f:58:cc:c0	1	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
3.	10.168.48.59	0/0114	Gi0/14		08:00:9f:58:cc:8e	10114	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
4.	10.168.48.59	0/0115	Gi0/15		08:00:9f:58:cc:8f	10115	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
5.	10.168.48.59	0/0116	Gi0/16		08:00:9f:58:cc:c2	10116	etherNetCsmacd	/	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
6.	10.168.48.59	0/5	V15		08:00:9f:58:cc:c3	5	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
7.	10.168.48.59	0/0118	Gi0/18		08:00:9f:58:cc:c2	10118	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
8.	10.168.48.59	0/0113	Gi0/13		08:00:9f:58:cc:8d	10113	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
9.	10.168.48.59	0/666	V1666		08:00:9f:58:cc:c5	666	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
10.	10.168.48.59	0/0501	Nu0		10501	other	/	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	32 bits	Enabled	
11.	10.168.48.59	0/0117	Gi0/17		08:00:9f:58:cc:92	10117	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
12.	10.168.48.59	0/99	V199		08:00:9f:58:cc:c4	99	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
13.	10.168.48.59	0/999	V1999	Link to WAN-R1	08:00:9f:58:cc:c6	999	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
14.	10.168.48.59	0/0101	Gi0/1		08:00:9f:58:cc:c1	10101	etherNetCsmacd	/	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
15.	10.168.48.59	0/0102	Gi0/2		08:00:9f:58:cc:c2	10102	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
16.	10.168.48.59	0/0103	Gi0/3		08:00:9f:58:cc:83	10103	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
17.	10.168.48.59	0/0104	Gi0/4		08:00:9f:58:cc:84	10104	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
18.	10.168.48.59	0/0105	Gi0/5		08:00:9f:58:cc:85	10105	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
19.	10.168.48.59	0/0106	Gi0/6		08:00:9f:58:cc:86	10106	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
20.	10.168.48.59	0/0107	Gi0/7		08:00:9f:58:cc:87	10107	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
21.	10.168.48.59	0/0108	Gi0/8		08:00:9f:58:cc:88	10108	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
22.	10.168.48.59	0/0109	Gi0/9		08:00:9f:58:cc:89	10109	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
23.	10.168.48.59	0/0110	Gi0/10		08:00:9f:58:cc:8a	10110	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
24.	10.168.48.59	0/0111	Gi0/11		08:00:9f:58:cc:8b	10111	etherNetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
25.	7609S-NPE3-cisco	0/1	Te3/1	connection CRS-1-P	00:24:14:4b:48:40	1	etherNetCsmacd	/	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
26.	7609S-NPE3-cisco	0/2	Te3/2		00:24:14:4b:48:40	2	etherNetCsmacd	/	Mega	-	Yes	Yes	5 Min.	No	No	64 bits	Enabled
27.	7609S-NPE3-cisco	0/3	Te3/3		00:24:14:4b:48:40	3	etherNetCsmacd	/	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
28.	7609S-NPE3-cisco	0/4	Te3/4	Connection to IXIA S	00:24:14:4b:48:40	4	etherNetCsmacd	/	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
29.	7609S-NPE3-cisco	0/5	Gi4/1		00:24:14:4b:48:40	5	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
30.	7609S-NPE3-cisco	0/6	Gi4/2		00:24:14:4b:48:40	6	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
31.	7609S-NPE3-cisco	0/7	Gi4/3	connection to CE-288	00:24:14:4b:48:40	7	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
32.	7609S-NPE3-cisco	0/8	Gi4/4		00:24:14:4b:48:40	8	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
33.	7609S-NPE3-cisco	0/9	Gi4/5		00:24:14:4b:48:40	9	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
34.	7609S-NPE3-cisco	0/10	Gi4/6	**Connection to 2951	00:24:14:4b:48:40	10	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
35.	7609S-NPE3-cisco	0/11	Gi4/7		00:24:14:4b:48:40	11	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
36.	7609S-NPE3-cisco	0/12	Gi4/8		00:24:14:4b:48:40	12	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
37.	7609S-NPE3-cisco	0/13	Gi4/9		00:24:14:4b:48:40	13	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
38.	7609S-NPE3-cisco	0/14	Gi4/10		00:24:14:4b:48:40	14	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
39.	7609S-NPE3-cisco	0/15	Gi4/11	connected to ASAS8	00:24:14:4b:48:40	15	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
40.	7609S-NPE3-cisco	0/16	Gi4/12		00:24:14:4b:48:40	16	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
41.	7609S-NPE3-cisco	0/17	Gi4/13		00:24:14:4b:48:40	17	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
42.	7609S-NPE3-cisco	0/18	Gi4/14		00:24:14:4b:48:40	18	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
43.	7609S-NPE3-cisco	0/19	Gi4/15		00:24:14:4b:48:40	19	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
44.	7609S-NPE3-cisco	0/20	Gi4/16		00:24:14:4b:48:40	20	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
45.	7609S-NPE3-cisco	0/21	Gi4/17		00:24:14:4b:48:40	21	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
46.	7609S-NPE3-cisco	0/22	Gi4/18		00:24:14:4b:48:40	22	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
47.	7609S-NPE3-cisco	0/23	Gi4/19		00:24:14:4b:48:40	23	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
48.	7609S-NPE3-cisco	0/24	Gi4/20		00:24:14:4b:48:40	24	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
49.	7609S-NPE3-cisco	0/25	Gi4/21		00:24:14:4b:48:40	25	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
50.	7609S-NPE3-cisco	0/26	Gi4/22		00:24:14:4b:48:40	26	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
51.	7609S-NPE3-cisco	0/27	Gi4/23		00:24:14:4b:48:40	27	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
52.	7609S-NPE3-cisco	0/28	Gi4/24		00:24:14:4b:48:40	28	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
53.	7609S-NPE3-cisco	0/29	Gi4/25		00:24:14:4b:48:40	29	etherNetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled

To view a report on all or multiple discovered interfaces:

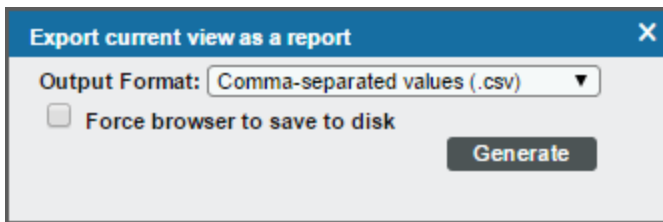
1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).

2. In the **Network Interfaces** page, click the **[Report]** button.

Name	Port/Sub-IF Name	Type	Organization	Alias	MAC Address	IF Index	IF Type	Admin/Oper Status	Measure	Interface Speed	Alerting	Auto-Status Update	Collection Frequency	Collected Errors	Collected Discards	Collected CSOOS	Collected Packets	Counter Settings	State
1	10.168.48.59	0/01012_Gi0/12	--	System	--	08.d0.9f58.cc.82.10112	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
2	10.168.48.59	0/01, V11	--	System	Link to WAN-R1	08.d0.9f58.cc.82.01	propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
3	10.168.48.59	0/01014_Gi0/14	--	System	--	08.d0.9f58.cc.82.10114	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
4	10.168.48.59	0/01015_Gi0/15	--	System	--	08.d0.9f58.cc.81.10115	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
5	10.168.48.59	0/01016_Gi0/16	--	System	--	08.d0.9f58.cc.82.10116	ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
6	10.168.48.59	0/05, V15	--	System	--	08.d0.9f58.cc.83.5	propVirtual	Down/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
7	10.168.48.59	0/01018_Gi0/18	--	System	--	08.d0.9f58.cc.82.10118	ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
8	10.168.48.59	0/01013_Gi0/13	--	System	--	08.d0.9f58.cc.82.10113	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
9	10.168.48.59	0/066, V666	--	System	--	08.d0.9f58.cc.83.666	propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
10	10.168.48.59	0/010501_Nu0	--	System	--	--	10501 other	Up/Up	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	32	Enabled
11	10.168.48.59	0/01017_Gi0/17	--	System	--	08.d0.9f58.cc.82.10117	ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
12	10.168.48.59	0/099, V99	--	System	--	08.d0.9f58.cc.84.99	propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
13	10.168.48.59	0/099, V999	--	System	Link to WAN-R1	08.d0.9f58.cc.83.999	propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
14	10.168.48.59	0/01001_Gi0/1	--	System	--	08.d0.9f58.cc.81.10101	ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
15	10.168.48.59	0/01002_Gi0/2	--	System	--	08.d0.9f58.cc.82.10102	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
16	10.168.48.59	0/01003_Gi0/3	--	System	--	08.d0.9f58.cc.83.10103	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
17	10.168.48.59	0/01004_Gi0/4	--	System	--	08.d0.9f58.cc.84.10104	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
18	10.168.48.59	0/01005_Gi0/5	--	System	--	08.d0.9f58.cc.85.10105	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
19	10.168.48.59	0/01006_Gi0/6	--	System	--	08.d0.9f58.cc.86.10106	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
20	10.168.48.59	0/01007_Gi0/7	--	System	--	08.d0.9f58.cc.87.10107	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
21	10.168.48.59	0/01008_Gi0/8	--	System	--	08.d0.9f58.cc.88.10108	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
22	10.168.48.59	0/01009_Gi0/9	--	System	--	08.d0.9f58.cc.89.10109	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
23	10.168.48.59	0/01010_Gi0/10	--	System	--	08.d0.9f58.cc.82.10110	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
24	10.168.48.59	0/01011_Gi0/11	--	System	--	08.d0.9f58.cc.83.10111	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
25	76099-NPE3.000	0/1, Te3/1	--	System	connection CRS-1-P	00.24.14.4b.48.4.1	ethernetCsmacd	Up/Down	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
26	76099-NPE3.000	0/2, Te3/2	--	System	--	00.24.14.4b.48.4.2	ethernetCsmacd	Up/Up	Mega	--	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled

NOTE: If you want to include only certain interfaces in the report, use the "search as you type" fields at the top of each column. You can filter the list by one or more column headings. You can then click the **[Report]** button, and only the interfaces displayed in the **Network Interfaces** page will appear in the report.

3. The **Export current view as a report** modal page appears.



4. In the **Export current view as a report** modal page, you must select the format in which SL1 will generate the report. Your choices are:

- Comma-separated values (.csv)
- Web page (.html)
- OpenDocument Spreadsheet (.ods)
- Excel spreadsheet (.xlsx)
- Acrobat document (.pdf)

- Click the **[Generate]** button. The report will contain all the information displayed in the **Network Interfaces** page. You can immediately view the report or save it to a file for later viewing.

Generating a Report for a Single Network Interface


From the **Network Interfaces** page, you can generate a text-based, bandwidth-usage report for a single interface. You can choose to generate a report on outbound traffic, inbound traffic, all traffic, errors, discards, or all.

Report Summary		
Device Name	35S.State	
Device Address	172.16.0.187	
Interface Name	Interface: NULL 0 Name: NULL 0 Type: other MAC: 00:00:00:00:00:00	
Interface Descr.	NULL 0	
Blade / Port / Sub	0/1107705856/0	
Measurement	Mbps.	
Report Duration	Last 24 Hours	

Interface Usage / Errors / Discards												
Date Time	Octets In	Octets Out	Octets Total	Mbps. In	Mbps. Out	Mbps. Total	Errors In	Errors Out	Errors Total	Discards In	Discards Out	Discards Total
406	339	745	745	1.1E-5	9.0E-6	2.0E-5	0	0	0	0	0	0
249	412	661	661	7.0E-6	1.1E-5	1.8E-5	0	0	0	0	0	0
525	501	1026	1026	1.4E-5	1.3E-5	2.7E-5	0	0	0	0	0	0
607	514	1121	1121	1.6E-5	1.4E-5	3.0E-5	0	0	0	0	0	0
452	303	755	755	1.2E-5	8.0E-6	2.0E-5	0	0	0	0	0	0
511	428	939	939	1.4E-5	1.1E-5	2.5E-5	0	0	0	0	0	0
313	435	748	748	8.0E-6	1.2E-5	2.0E-5	0	0	0	0	0	0
468	406	874	874	1.2E-5	1.1E-5	2.3E-5	0	0	0	0	0	0
572	446	1018	1018	1.5E-5	1.2E-5	2.7E-5	0	0	0	0	0	0
396	385	781	781	1.1E-5	1.0E-5	2.1E-5	0	0	0	0	0	0
364	379	743	743	1.0E-5	1.0E-5	2.0E-5	0	0	0	0	0	0
498	465	963	963	1.3E-5	1.2E-5	2.5E-5	0	0	0	0	0	0
476	366	842	842	1.3E-5	1.0E-5	2.3E-5	0	0	0	0	0	0
613	743	1356	1356	1.6E-5	2.0E-5	3.6E-5	0	0	0	0	0	0
424	420	844	844	1.1E-5	1.1E-5	2.2E-5	0	0	0	0	0	0
545	622	1167	1167	1.5E-5	1.7E-5	3.2E-5	0	0	0	0	0	0
272	460	732	732	7.0E-6	1.2E-5	1.9E-5	0	0	0	0	0	0

To generate the report:

- Go to **Network Interfaces** (Registry > Networks > Interfaces).

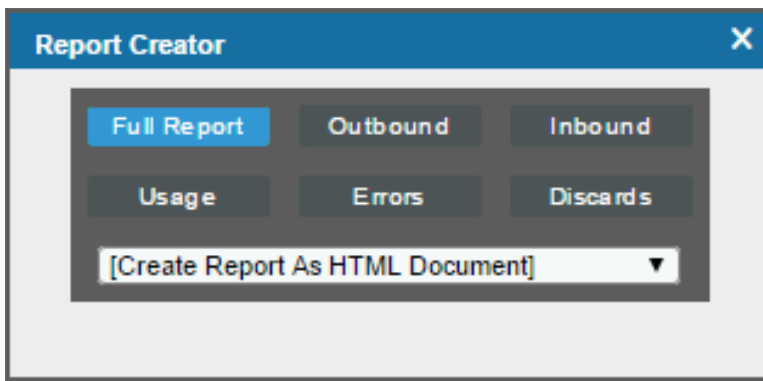
- In the **Network Interfaces** page, find the interface for which you want to generate a bandwidth report. Click its printer icon ().

Network Interfaces | Interfaces Found [130]

Details	Part/Sub IF Name	Tags	Organization	Alias	MAC Address	IF Index	IF Type	Admin/Oper Status	Message	Interface Speed	Auto-Configure	Collect Encountered	Collect Errors	Collect Discards	Collect Packets	Counter Status	State		
1	10.168.48.59	0/10112, Gi0/12	--	System	--	08.00.9f.58.cc.81.10112	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
2	10.168.48.59	0/1, V11	--	System	Link to WAN-R1	08.00.9f.58.cc.c0.1	propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
3	10.168.48.59	0/10114, Gi0/14	--	System	--	08.00.9f.58.cc.86.10114	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
4	10.168.48.59	0/10115, Gi0/15	--	System	--	08.00.9f.58.cc.81.10115	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
5	10.168.48.59	0/10116, Gi0/16	--	System	--	08.00.9f.58.cc.82.10116	ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
6	10.168.48.59	0/5, V5	--	System	--	08.00.9f.58.cc.c3.5	propVirtual	Down/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
7	10.168.48.59	0/10118, Gi0/18	--	System	--	08.00.9f.58.cc.92.10118	ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
8	10.168.48.59	0/10113, Gi0/13	--	System	--	08.00.9f.58.cc.86.10113	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
9	10.168.48.59	0/060, V660	--	System	--	08.00.9f.58.cc.c5.660	propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
10	10.168.48.59	0/10501, Nu0	--	System	--	--	10501 other	Up/Up	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	32	Enabled
11	10.168.48.59	0/10117, Gi0/17	--	System	--	08.00.9f.58.cc.91.10117	ethernetCsmacd	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
12	10.168.48.59	0/99, V99	--	System	--	08.00.9f.58.cc.84.99	propVirtual	Up/Down	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
13	10.168.48.59	0/999, V999	--	System	Link to WAN-R1	08.00.9f.58.cc.c8.999	propVirtual	Up/Up	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
14	10.168.48.59	0/10101, Gi0/1	--	System	--	08.00.9f.58.cc.c1.10101	ethernetCsmacd	Up/Up	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
15	10.168.48.59	0/10102, Gi0/2	--	System	--	08.00.9f.58.cc.82.10102	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
16	10.168.48.59	0/10103, Gi0/3	--	System	--	08.00.9f.58.cc.83.10103	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
17	10.168.48.59	0/10104, Gi0/4	--	System	--	08.00.9f.58.cc.84.10104	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
18	10.168.48.59	0/10105, Gi0/5	--	System	--	08.00.9f.58.cc.85.10105	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
19	10.168.48.59	0/10106, Gi0/6	--	System	--	08.00.9f.58.cc.86.10106	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
20	10.168.48.59	0/10107, Gi0/7	--	System	--	08.00.9f.58.cc.87.10107	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
21	10.168.48.59	0/10108, Gi0/8	--	System	--	08.00.9f.58.cc.88.10108	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
22	10.168.48.59	0/10109, Gi0/9	--	System	--	08.00.9f.58.cc.89.10109	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
23	10.168.48.59	0/10110, Gi0/10	--	System	--	08.00.9f.58.cc.8a.10110	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
24	10.168.48.59	0/10111, Gi0/11	--	System	--	08.00.9f.58.cc.8b.10111	ethernetCsmacd	Up/Down	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
25	70935-NPE3.csr6	0/1, Te3/1	--	System	connection CRS-1-P	00.24.14.4b.48.4.1	ethernetCsmacd	Up/Down	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled
26	70935-NPE3.csr6	0/2, Te3/2	--	System	--	00.24.14.4b.48.4.2	ethernetCsmacd	Up/Up	Mega	--	Yes	Yes	5 Min.	No	No	Yes	Yes	64	Enabled

[Viewing Page: 1]

- The **Report Creator** modal page is displayed.



- Select from the following list of formats to select a format in which to generate the report:

- 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

5. Select one of the following buttons to specify the information to include in the device report:
 - **[Full Report]**. Include all information about outbound data through the interface, inbound data through the interface, combined bandwidth through the interface, errors on the interface, and discards on the interface.
 - **[Outbound]**. Include all information about outbound data through the interface.
 - **[Inbound]**. Include all information about inbound data through the interface.
 - **[Usage]**. Include all information about inbound data and outbound data through the interface.
 - **[Errors]**. Include all information about errors on the interface.
 - **[Discards]**. Include all information about discards on the interface.
6. SL1 will generate the report. You can immediately view the report or save it to your local computer.

Monitoring Interfaces

A monitoring policy for an interface tells SL1 how frequently to poll the interface for data and which data to collect. SL1 uses this collected data to generate bandwidth reports and trigger events.

NOTE: *By default, SL1 monitors each discovered interface.* By default, SL1 will poll the interface every 15 minutes, will not collect data on errors, will not collect data on discards, enables alerting, and allows SL1 to update the interface name during discovery.

There are two ways to define monitoring policies for interfaces:

- Define a detailed policy for a single interface at a time.
- Define a single policy setting for multiple interfaces at a time.

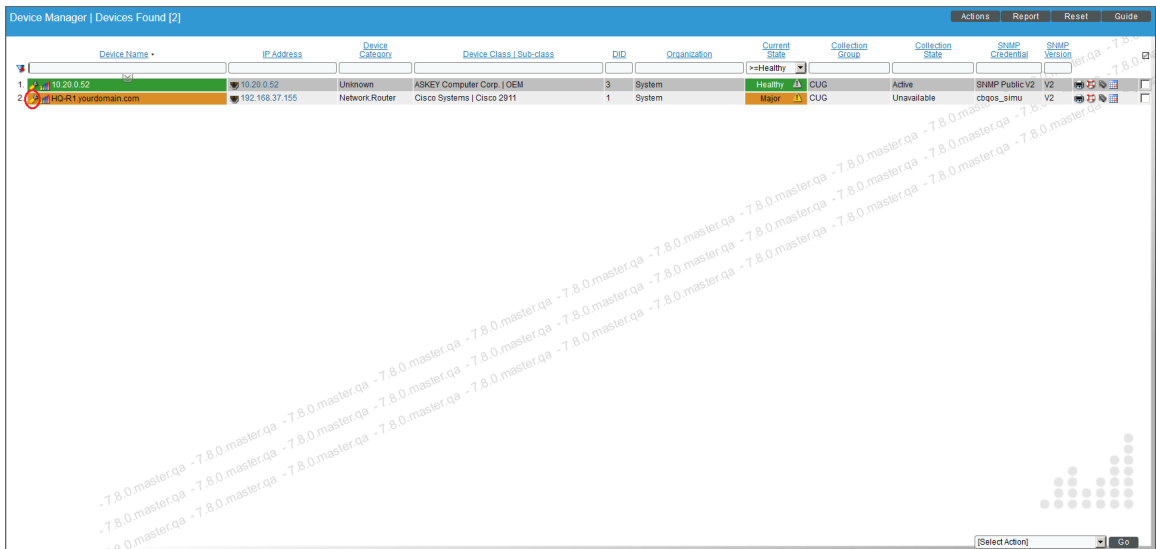
The following sections describe both methods.

Defining a Detailed Monitoring Policy for a Single Interface

To define a monitoring policy for one or more interfaces on a single device:

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

- In the **Device Manager** page, find the device for which you want to define interface monitoring. Click its wrench icon (🔧).



- In the **Device Administration** panel, click the **[Interfaces]** tab.



- In the **Device Interfaces** page, find the icon for the interface you want to monitor. Click on the icon.

- The **Interface Properties** page appears. In this page, you can define a detailed monitoring policy for the selected interface.

For Interface [12]

[Editing: ens160]

Report Purge Reset Guide

Properties Thresholds

Interface Name: ens160
 Port Description: ens160
 MAC Address: 00:50:56:85:C8:54 / Vmware
 IANA Type: ethernetCsmacd [6]
 Speed & Counter: 10000 Mbps. [Counter 64]
 Position & Ifindex: 2 / 2
 Admin/Oper Status: Up / Up
 TCP IP Address: 10.2.9.20 / 255.255.255.0 [10.2.9.0]

Interface Name: ens160 Disable Discovery Name Update
 Interface Event Display Name: ens160
 Interface Tags:
 Interface Speed: 10000000000 [Bits] Disable Interface Speed Update
 Linked-Device: [None]
 Linked-Interface:

Collect State / Frequency: [Enabled] / [5 Min.]
 Alerting / Rollovers: [Enabled] / [Disabled]
 Event Severity Adjust: [Default Severity]
 Errors / Discards: [Disabled] / [Disabled]
 Quality of Service: [Disabled]
 Packets: [Disabled]
 Measurement / Percentile: [Mega] / [Accumulative]
 Display on Summary:

Emissary: [SAC_Sanity_IC_Test]


Save

- To define a monitoring policy in the **Interface Properties** page, supply a value in each of the following fields in the **Monitoring Options** pane:

NOTE: For SL1 to monitor an interface, you must define **Collect State** as *Enabled*.

- Interface Name.** The name of the network interface. The auto-name, generated by SL1, is "device_name". You can supply a different name in this field.
- Disable Discovery Name Update.** When selected, prevents SL1 from updating and/or overwriting the interface name during auto-discovery.
- Interface Event Display Name.** The name of the network interface that you want to appear in events.

NOTE: If *Disable Discovery Name Update* is selected for an interface in its **Interface Properties** page, SL1 cannot change the interface name during nightly auto-discovery and during re-discovery, regardless of the settings in the *Interface Event Display Name* field. To apply a new naming convention to interfaces, you must first ensure that *Disable Discovery Name Update* is not selected for those interfaces. You can do this in the **Network Interfaces** page (Registry > Networks > Interfaces): select the interfaces you want to rename, select the **Select Actions** field (in the lower right), and choose *Auto-Name Update > Enable*.

- **Interface Tags.** Displays a comma-delimited list of descriptive tags that have been manually defined for this interface. Interface tags are used to group interfaces in an IT service policy. To add or edit the tags for this interface, click the wrench icon (). In the **Edit Network Interface Tags** modal page that appears, supply a comma-delimited list of tags in the **Tags** field, and then click the **[Save]** button.
- **Interface Speed.** The speed of the network interface reported by the device. If the device reported an incorrect speed, you can supply a different speed in this field. In the drop-down list to the right of this field, you can select the unit of measurement for the speed you specified.
- **Disable Interface Speed Update.** When selected, prevents SL1 from updating and/or overwriting the interface speed during nightly auto-discovery.
- **Linked Device.** Device to associate with this interface. You can select from the drop-down list of all devices in SL1.
- **Linked Interface.** Interface to be associated with this interface. You can select from a drop-down list of interfaces on the selected device (specified in the *Linked Device* field).

NOTE: The *Linked Device* and *Linked Interface* fields allow you to manually create relationships that will be reflected in the topology maps in the **[Views]** tab.

- **Collect State.** This field can have one of two values:
 - *Enabled:* SL1 monitors the network interface and collects data on the network interface for reports.
 - *Disabled:* SL1 does not monitor the network interface and collect data on the network interface for reports.
- **Frequency.** When you enable monitoring (collection) for an interface, you must specify how frequently you want SL1 to collect data from the interface. Your choices are every:
 - 1 Minute
 - 5 Minutes
 - 10 Minutes
 - 15 Minutes
 - 30 Minutes

- 60 Minutes
- 120 Minutes

The Network Interface reports will display the average incoming and outgoing bandwidth-usage for the current day in the time-intervals specified in the **Frequency** field.

- **Alerting**. Alerting for this interface can be enabled or disabled. When disabled, the interface is monitored, but events are not generated for the interface.
- **Rollovers**. Specifies whether or not SL1 will generate an event when the counter for the interface rolls over. This field does not affect the Network Usage graphs. This field is most helpful for interfaces that are busy and require frequent monitoring, but for which the device supports only 32-bit counters (instead of 64-bit counters). The counters on such interfaces roll over frequently.

NOTE: Rollovers and alerting for **Rollovers** apply only to 32-bit counters and not to 64-bit counters.

- **Event Severity Adjust**. Allows you to specify a severity for this interface. You can then configure one or more interface events to use this custom severity when creating events for this interface. For example, if this interface is part of a mission-critical operation, you might want all events associated with this interface to have a severity of "critical". Choices are:
 - Sev -3. Reduces the severity by 3.
 - Sev -2. Reduces the severity by 2.
 - Sev -1. Reduces the severity by 1.
 - *Default Severity*. Uses the default severity for each event.
 - Sev +1. Increases the severity by 1.
 - Sev +2. Increases the severity by 2.
 - Sev +3. Increases the severity by 3. The highest possible severity is "Critical".

NOTE: Event severities have the following numeric values:

5 = Healthy
 4 = Notice
 3 = Minor
 2 = Major
 1 = Critical

In the **Event Severity Adjust** field, you cannot change a severity of "Notice" or higher to a severity of "Healthy".
 In the **Event Severity Adjust** field, you also cannot change the severity of a "Healthy" event.

- **Errors**. Specifies whether or not 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. Choices are:

- *Enabled*. If **Errors** is enabled for an interface, the **Thresholds** tab for the interface will display thresholds for errors in and errors out. If **Errors** is enabled for an interface, SL1 will display the collected data in the **Device Performance** page (Registry > Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface.
- *Disabled*. SL1 will not collect data about errors for this interface.
- **Discards**. Specifies whether or not 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. Choices are:
 - *Enabled*. If **Discards** is enabled for an interface, the **Thresholds** tab for the interface will display thresholds for discards in and discards out. If **Discards** is enabled for an interface, SL1 will display the collected data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface.
 - *Disabled*. SL1 will not collect data about discards this interface. Disabled.
- **Quality of Service**. Specifies whether SL1 will collect CBQoS (Class-Based Quality-of-Service) configuration data for this interface. This option appears only if you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior). If **Collect CBQoS** is enabled for an interface, SL1 will display the collected CBQoS data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface. Choices are:
 - *Enable*. SL1 will collect CBQoS configuration data for this interface.
 - *Disable*. SL1 will not collect CBQoS configuration data for this interface.

NOTE: If you set **Collect CBQoS** to *Enable* for an interface that is not configured for CBQoS, SL1 will display an error message.

- **Packets**. Specifies whether SL1 will collect data for unicast, multicast, and broadcast traffic in packets, for this interface. Choices are:
 - *Enabled*. If **Packets** is enabled for an interface, the **Thresholds** tab for the interface will display thresholds for unicast, multicast, and broadcast traffic. If **Packets** is enabled for an interface, SL1 will display the collected data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface.
 - *Disabled*. SL1 will not collect data for unicast, multicast, and broadcast traffic, in packets, for this interface.
- **Measurement**. Unit of measurement for bandwidth reports for the interface. The choices are:
 - Mega
 - Giga

- Kilo
- Tera
- Peta
- **Percentile.** The basis for bandwidth billing for this interface. The choices are:
 - *Accumulative.* Customer is billed for total inbound and outbound bandwidth for all applicable interfaces. Billing is at the specified percentile point.
 - *Inbound.* Customer is billed for the total inbound bandwidth for all applicable interfaces. Billing is at the specified percentile point.
 - *Outbound.* Customer is billed for the total outbound bandwidth for all applicable interfaces. Billing is at the specified percentile point.
 - *Highest Poll.* Customer is billed for either the total inbound or total outbound, whichever is highest, for each applicable interface. Billing is at the specified percentile point.
- **Display on Summary.** If selected, a usage graph for this interface will appear in the **Device Summary** page.

NOTE: Only one interface per device can be displayed on the **Device Summary** page.

7. In the **Emissary** pane, you can allow all users in another organization to view reports about the current interface and view bandwidth billing policies associated with the interface.
 - **Emissary.** This field allows a user to define an emissary interface. Select an organization to allow the users in that organization to view this interface. When you click the **[Save]** button, the members of the selected organization will be able to view reports about the interface, include the interface in dashboards, and view bandwidth billing policies associated with the interface.

Defining Monitoring Settings for Multiple Interfaces

In the **Network Interfaces** page, the **Select Actions** drop-down menu (in the lower right corner of the page) allows you to apply or change the monitoring settings for one, multiple, or all interfaces in the **Network Interfaces** page.

To apply a monitoring option to one or more interfaces:

1. Go to the **Network Interfaces** page (Registry > Networks > Interfaces).
2. In the **Network Interfaces** page, find each interface to which you want to apply a monitoring option and select its checkbox.

3. To select all checkboxes, select the red checkbox icon (☑) in the column heading.

The screenshot shows a table titled "Network Interfaces | Interfaces Found [130]". The table has columns for Device Name, Port/Sub-IF Name, Type, Organization, Alias, MAC Address, IF Index, IF Type, Admin/Oper Status, Measure, Interface Speed, Alerting, Auto-Update, Collection Frequency, Collect Errors, Collect Discards, Collect CBOoS, Collect Packets, Counter Settings, and State. A red checkbox icon is visible in the "Select Action" column header. A dropdown menu is open over the "Enabled" column header, showing options like "Every 120 Min", "Collection Status", "L_Disabled", "Collect Errors", "Collect Discards", "Collect CBOoS", "Collect Packets", and "Collection Counter Settings".

4. In the **Select Action** drop-down, select the option you want to apply to the checked interfaces. Your choices are:

- **Report Measurement.** Unit of measurement for bandwidth reports for the interface. The choices are:
 - Mega
 - Giga
 - Kilo
 - Tera
 - Peta
- **Interface Alerting.** Specifies whether or not events should be generated for the selected interfaces. Choices are:
 - *Enabled.* SL1 monitors the network interface and generates events when the required conditions are met.
 - *Disabled.* SL1 monitors the network interface, but events are not generated for the interface.

- **Rollover Alerting.** This checkbox is for interfaces that are busy and require frequent monitoring, but for which the device supports only 32-bit counters (instead of 64-bit counters). The counters on such interfaces roll over frequently. If enabled, each time the counter rolls over (is set back to zero), SL1 will generate an event. Choices are:
 - *Enabled.* SL1 monitors the network interface and generates an event when the counter rolls over and is reset to zero.
 - *Disabled.* SL1 monitors the network interface, but does not generate an event when the counter rolls over and is reset to zero.

NOTE: Rollovers and **Rollover Alerting** apply only to 32-bit counters and not to 64-bit counters.

- **Auto-Name Update.** Specifies whether or not events should be generated for the selected interfaces. Choices are:
 - *Enabled.* SL1 can update and/or overwrite the interface name during auto-discovery.
 - *Disabled.* SL1 will not update and/or overwrite the interface name during auto-discovery.
- **Tags.** For each interface in SL1, you can manually define a comma-delimited list of descriptive tags. Interface tags are used to group interfaces in an IT service policy. The following options allow you to manage interface tags:
 - *Clear all Tags.* Removes all existing tags from the selected interfaces.
 - *Remove Tags.* Displays the **Bulk Remove Network Interface Tags** modal page, where you can remove one or more tags from the selected interfaces. In the **Bulk Remove Network Interface Tags** modal page, select the checkbox for each tag that you want to remove, and then click the **[Remove]** button.
 - *Add Tags.* Displays the **Bulk Add Network Interface Tags** modal page, where you can add one or more tags to the selected interfaces. In the **Bulk Add Network Interface Tags** modal page, select the checkbox for each existing tag that you want to add and/or supply a comma-delimited list of new tags, and then click the **[Save]** button.
- **Collection Frequency.** When you define a monitoring policy for an interface, you must specify how frequently you want SL1 to collect data from the interface. Your choices are every:
 - 1 Minute
 - 5 Minutes
 - 10 Minutes
 - 15 Minutes
 - 30 Minutes
 - 60 Minutes
 - 120 Minutes

- **Collection State.** Specifies whether collection should be active or disabled. Choices are:
 - *Enabled.* SL1 monitors the network interface and collects data on the network interface for reports.
 - *Disabled.* SL1 does not monitor the network interface and collect data on the network interface for reports.

NOTE: For SL1 to monitor an interface, you must define **Collect State** as enabled.

- **Collection Errors.** Specifies whether or not 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. Choices are:
 - *Enabled.* SL1 will collect data on packet errors that occur on the interface.
 - *Disabled.* SL1 will not collect data on packet errors that occur on the interface.
- **Collection Discards.** Specifies whether or not 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. Choices are:
 - *Enabled.* SL1 will collect data on packet discards that occur on the interface.
 - *Disabled.* SL1 will not collect data on packet discards that occur on the interface.
- **Collect CBQoS.** Specifies whether SL1 will collect CBQoS (Class-Based Quality-of-Service) data for this interface. This option appears only you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior). If **Collect CBQoS** is enabled for an interface, SL1 will display the collected CBQoS data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) for the device that contains this interface. Choices are:
 - *Enable.* SL1 will collect CBQoS data for this interface.
 - *Disable.* SL1 will not collect CBQoS data for this interface.

NOTE: If you set **Collect CBQoS** to *Enable* for an interface that is not configured for CBQoS, SL1 will display an error message.

- **Packets.** Specifies whether SL1 will collect data for unicast, multicast, and broadcast traffic, in packets, for this interface. If **Collect Packets** is enabled for an interface, SL1 will display the collected data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface. Choices are:
 - *Enabled* . SL1 will collect data for unicast, multicast, and broadcast traffic, in packets, for this interface.
 - *Disabled*. SL1 will not collect data for unicast, multicast, and broadcast traffic, in packets, for this interface.

- **Collection Counter Setting.** Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface. During auto-discovery, SL1 automatically discovers which type of counter is associated with each interface. A 32-bit counter will roll-over (restart at 0) after about four billion octets (bytes) have passed through the interface. A 64-bit counter will roll-over after 1.85 x 10¹⁶ octets (bytes) have passed through the interface. Most high-speed interfaces use a 64-bit counter to measure bandwidth on the interface. If a 64-bit counter is available, SL1 will use it by default. Choices are:
 - *Counter 32*. Specify that the interface uses a 32-bit counter.
 - *Counter 64*. Specify that the interface uses a 64-bit counter.

- **Percentile Factor.** Many service providers use a percentile bandwidth measure when billing customers for bandwidth usage. In this field, you can select the percentile factor, and SL1 will perform the calculations for you at billing time. For example, if a provider chose the percentile factor "95", SL1 would collect bandwidth data every 5 minutes for an entire month. At billing time, the highest 5% of readings are dropped. The customer is charged for the 95% highest reading. This prevents customers from being billed for unusual spikes. Choices are:
 - 100% - 1%, in increments of 1%.

- **Event Severity Adjust.** Allows you to specify a severity for this interface. You can then configure one or more interface events to use this custom severity when creating events for this interface. For example, if this interface is part of a mission critical operation, you might want all events associated with this interface to have a severity of "critical". Choices are:
 - *Sev -3*. Reduces the severity by 3.
 - *Sev -2*. Reduces the severity by 2.
 - *Sev -1*. Reduces the severity by 1.
 - *Default Severity*. Uses the default severity for each event.
 - *Sev +1*. Increases the severity by 1.
 - *Sev +2*. Increases the severity by 2.
 - *Sev +3*. Increases the severity by 3. The highest possible severity is "Critical".

NOTE: Event severities have the following numeric values:

- 5 = Healthy
- 4 = Notice
- 3 = Minor
- 2 = Major
- 1 = Critical

In the **Event Severity Adjust** field, you cannot change a severity of "Notice" or higher to a severity of "Healthy".
In the **Event Severity Adjust** field, you also cannot change the severity of a "Healthy" event.

5. Click the **[Go]** button.
6. You can repeat these steps to change another monitoring option for the selected interface or for a different group of interfaces.

Defining Thresholds for an Interface


The **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) allows you to define custom thresholds for the monitored interface. If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. SL1 will use either the global thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) or the custom threshold you define for a specific interface in the **Thresholds** tab. When the values for an interface exceed one or more thresholds, SL1 will generate an event.

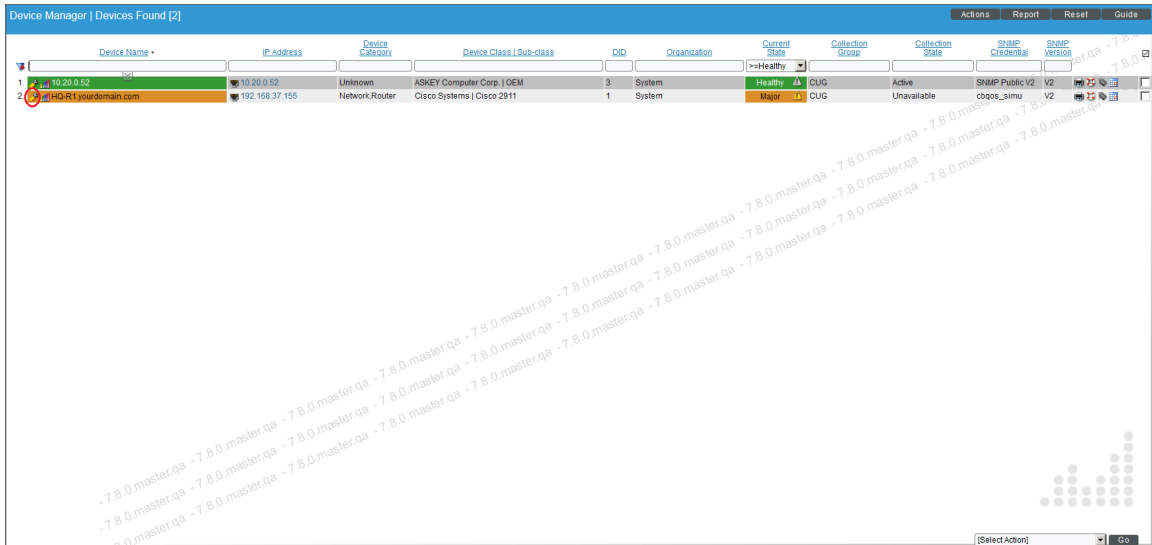
NOTE: The thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) determine which thresholds will appear in this page. For a list of all possible thresholds that can appear in this page, see the section on [Global Settings that Affect Interfaces](#).

NOTE: The thresholds defined for a specific interface in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) override the global thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface).

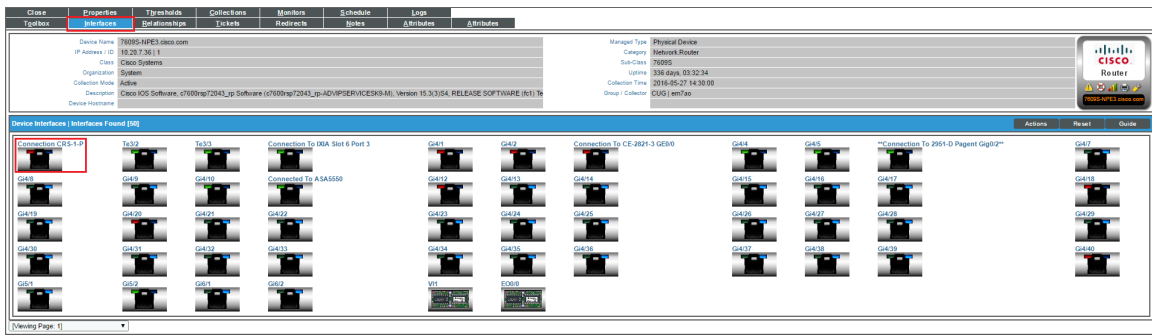
To define custom thresholds for an interface:

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

- In the **Device Manager** page, find the device for which you want to define custom interface thresholds. Click its wrench icon ().



- In the **Device Administration** panel, click the **[Interfaces]** tab.



- In the **Device Interfaces** page, find the icon for the interface you want to monitor. Click on the icon.

5. The **Interface Properties** page appears.

The screenshot shows the 'Interface Properties' configuration page for interface 'ens160'. The page is divided into two tabs: 'Properties' and 'Thresholds'. The 'Properties' tab is active, displaying various interface settings. A small image of a network switch is visible on the right side of the page.

Property	Value
Interface Name	ens160
Port Description	ens160
MAC Address	00:50:56:85:C8:54 / Vmware
IANA Type	ethernetCsmacd [6]
Speed & Counter	10000 Mbps. [Counter 64]
Position & Ifindex	2 / 2
Admin/Oper Status	Up / Up
TCP IP Address	10.2.9.20 / 255.255.255.0 [10.2.9.0]

Below the read-only fields, there are several configuration options:

- Interface Name: ens160 (with a 'Disable Discovery Name Update' checkbox)
- Interface Event Display Name: ens160
- Interface Tags: (empty field)
- Interface Speed: 10000000000 [Bits] (with a 'Disable Interface Speed Update' checkbox)
- Linked-Device: [None]
- Linked-interface: (empty field)
- Collect State / Frequency: [Enabled] / [5 Min.]
- Alerting / Rolovers: [Enabled] / [Disabled]
- Event Severity Adjust: [Default Severity]
- Errors / Discards: [Disabled] / [Disabled]
- Quality of Service: [Disabled]
- Packets: [Disabled]
- Measurement / Percentile: [Mega] / [Accumulative]
- Display on Summary: (checkbox)
- Emissary: [SAC_Sanity_IC_Test]

A 'Save' button is located at the bottom of the page.

6. Click the **Thresholds** tab.

The screenshot shows the 'Thresholds' configuration page for interface 'Ethernet0'. The page is divided into two tabs: 'Properties' and 'Thresholds'. The 'Thresholds' tab is active, displaying a table of metrics and their corresponding thresholds. A 'Metric' input field is at the top, and a 'Default Overridden' indicator is present. The 'Set All to Defaults' button is also visible.

Metric	Value	Defaults	Defaults in Use
Utilization % In	Inbound Percent: 65.000	65.000	Enable All [Enabled]
Utilization % Out	Outbound Percent: 65.000	65.000	Enable All [Enabled]
Bandwidth In	Inbound Bandwidth: 0.000	0.000	Enable All [Disabled]
Bandwidth Out	Outbound Bandwidth: 0.000	0.000	Enable All [Disabled]

A 'Save' button is located at the bottom of the page.

7. The following global thresholds are defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) and also appear in the **Thresholds** tab:

NOTE: You can specify the unit of measure for all the metrics in **Bandwidth In** and **Bandwidth Out**. You can select *bps*, *kpbs*, *Mbps* (the default), or *Gbps*.

Threshold	Default Value	Default Status
<i>Utilization % In > Inbound Percent</i>	65.000	Enabled
<i>Utilization % Out > Outbound Percent</i>	65.000	Enabled
<i>Bandwidth In > Inbound Bandwidth</i>	0.000	Disabled
<i>Bandwidth Out > Outbound Bandwidth</i>	0.000	Disabled
<i>Errors % In > Inbound Error Percent</i>	1.000	Enabled
<i>Errors % Out > Outbound Error Percent</i>	1.000	Enabled
<i>Errors In > Inbound Errors</i>	1000.000	Enabled
<i>Errors Out > Outbound Errors</i>	1000.000	Enabled
<i>Discard % In > Inbound Discard Percent</i>	1.000	Enabled
<i>Discards % Out > Outbound Discard Percent</i>	1.000	Enabled
<i>Discards In > Inbound Discards</i>	1000.000	Enabled
<i>Discards Out > Outbound Discards</i>	1000.000	Enabled
<i>Multicast % In > Rising Medium</i>	30.000	Disabled
<i>Multicast % In > Rising Low</i>	20.000	Disabled
<i>Broadcast % Out > Rising Medium</i>	30.000	Disabled
<i>Broadcast % Out > Rising Low</i>	20.000	Disabled

NOTE: To edit thresholds for errors in and errors out, you must enable **Errors** in [the Properties tab](#) for the interface. To edit thresholds for discards, you must enable **Discards** in [the Properties tab](#) for the interface. To edit thresholds for unicast, multicast, and broadcast traffic, you must enable **Packets** in [in the Properties tab for](#) the interface.

8. For each threshold in the **Thresholds** tab, you can edit the following:
- **Value.** The value at which the threshold will trigger an event.

- For thresholds that include the word *Rising*, when a value exceeds the specified value, SL1 triggers an event.
- For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers an event.
- For thresholds that do not include the word *Rising* or *Falling*, when a value exceeds the specified value, SL1 triggers an event.
- **Status.** Specifies whether the threshold is active and whether the threshold will appear in the **Thresholds** tab of the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). Choices are:
 - *Enabled.* The threshold is applied to the interface and is monitored by SL1.
 - *Disabled.* The threshold appears in the **Thresholds** tab but it not monitored by SL1.
- **Unit of Measure.** For all the metrics under **Bandwidth In** and **Bandwidth Out**, you can edit the unit of measure. Choices are:
 - bps
 - kbps
 - Mbps
 - Gbps

Viewing the List of Discovered CBQoS Objects

The **Quality of Service (QoS)** page displays a list of all Class-Based Quality of Service (CBQoS) classes and policies that are aligned with devices and interfaces discovered by SL1.

SL1 collects CBQoS data only if you have enabled the field **Enable CBQoS Collection** in the **Behavior Settings** page (System > Settings > Behavior).

If **Quality of Service** is enabled for an interface in the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon), SL1 will display:

- graphs about the collected CBQoS data in the **Device Performance** page (Devices > Device Manager > bar-graph icon > Performance) associated with the device that contains this interface.
- a list all CBQoS classes and policies that are aligned with the interface in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service).

To view the list of all CBQoS classes and policies that are aligned with devices and interfaces discovered by SL1:

1. Go to the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service).

Quality of Service Object	Index	Policy	Type	Device Name	IF Name	IF Alias
Match	327681	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	327682	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	131073	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	65539	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue 524290	524290	--	Queueing	7609S-NPE3.cisco.com	--	--
queue 196612	196612	--	Queueing	7609S-NPE3.cisco.com	--	--
CE-IN	1	inbound	PolicyMap	7609S-NPE3.cisco.com	--	--
wred 131077	131077	--	WRED	7609S-NPE3.cisco.com	--	--
--	0	--	REDValue	7609S-NPE3.cisco.com	--	--
--	1	--	REDValue	7609S-NPE3.cisco.com	--	--
--	2	--	REDValue	7609S-NPE3.cisco.com	--	--
Match	196609	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	383219	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	65538	--	MatchStatement	7609S-NPE3.cisco.com	--	--
PREC-0	456752	--	ClassMap	7609S-NPE3.cisco.com	--	--
queue 327684	327684	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	383219	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	327681	--	MatchStatement	7609S-NPE3.cisco.com	--	--
policing 131076	131076	--	Policing	7609S-NPE3.cisco.com	--	--
Match	262145	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue 262148	262148	--	Queueing	7609S-NPE3.cisco.com	--	--
PREC-0	456752	--	ClassMap	7609S-NPE3.cisco.com	--	--
queue 131076	131076	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	196609	--	MatchStatement	7609S-NPE3.cisco.com	--	--
class-default	524288	--	ClassMap	7609S-NPE3.cisco.com	--	--
Match	456755	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue 327684	327684	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	456754	--	MatchStatement	7609S-NPE3.cisco.com	--	--

2. The **Quality of Service (QoS)** page displays the following for each QoS object:

TIP: To sort the list of QoS objects, 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.

- **Quality of Service Object.** Name of the CBQoS class or policy. Can be the name of a class map, policing policy, sets policy, match statement, queuing policy, traffic shaping policy, WRED policy, or RED value.
- **Index.** Index value for the CBQoS object on a specific device. This value is generated by the CISCO-CLASS-BASED-QOS-MIB.
- **Policy.** Name of the parent CBQoS policy.
- **Type.** CBQoS object type. Possible values are:
 - ClassMap
 - MatchStatement
 - Policing
 - PolicyMap
 - Queueing
 - REDValue
 - Set

- TrafficShaping
- WRED
- **Device Name.** Name of the device where SL1 found the CBQoS object.
- **IF Name.** If applicable, name of the interface where SL1 found the CBQoS object.
- **IF Alias.** If applicable, alias for the interface where SL1 found the CBQoS object.

Filtering the List of Quality of Service (QoS) Objects

You can filter the list on the **Quality of Service (QoS)** page by one or more parameters. Only CBQoS objects that meet all the filter criteria will be displayed in the **Quality of Service (QoS)** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Quality of Service (QoS)** page searches for CBQoS objects 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:

- **Quality of Service Object.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects with a matching name.
- **Index.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects with a matching index value.
- **Policy.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects aligned with a matching policy.
- **Type.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects of the specified type.
- **Device Name.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects aligned with the specified device.
- **IF Name.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects aligned with the specified interface name.
- **IF Alias.** You can enter text to match, including special characters, and the **Quality of Service (QoS)** page will display only CBQoS objects aligned with the specified interface alias.

Editing Thresholds for a Quality of Service (QoS) Object

From the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service), you can access the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon) and edit the thresholds for a CBQoS object. The threshold will apply to that specific CBQoS object on a specific device and specific interface.

If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. For interfaces that are part of a CBQoS class, SL1 will use either the global CBQoS thresholds defined in the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) or the custom threshold you define in the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon). When the values for an interface exceed one or more thresholds, SL1 will generate an event.

NOTE: The thresholds defined in the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) determine which thresholds will appear in **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon). For a list of all possible thresholds that can appear in this page, see the section on [Global Settings that Affect Interfaces](#).

NOTE: The thresholds defined in the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon) for a specific interface override the global thresholds defined in the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service).

To edit the interface thresholds for a CBQoS object on a specific device and specific interface:

1. Go to the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service).

The screenshot shows the 'Quality of Service (QoS)' configuration page. The table lists various QoS objects with their indices, policies, types, device names, and interface names. A red circle highlights the 'PREC-0' object in row 15.

Quality of Service Object	Index	Policy	Type	Device Name	IF Name	IF Alias
Match	327681	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	327682	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	131073	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	65539	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue-524290	524290	--	Queueing	7609S-NPE3.cisco.com	--	--
queue-196612	196612	--	Queueing	7609S-NPE3.cisco.com	--	--
GE-IN	1	inbound	PolicyMap	7609S-NPE3.cisco.com	--	--
wred-131077	131077	--	WRED	7609S-NPE3.cisco.com	--	--
--	0	--	REDValue	7609S-NPE3.cisco.com	--	--
--	1	--	REDValue	7609S-NPE3.cisco.com	--	--
--	2	--	REDValue	7609S-NPE3.cisco.com	--	--
Match	196609	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	383219	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	65538	--	MatchStatement	7609S-NPE3.cisco.com	--	--
PREC-0	458752	--	ClassMap	7609S-NPE3.cisco.com	--	--
queue-327684	327684	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	383219	--	MatchStatement	7609S-NPE3.cisco.com	--	--
Match	327681	--	MatchStatement	7609S-NPE3.cisco.com	--	--
policing-131076	131076	--	Policing	7609S-NPE3.cisco.com	--	--
Match	262145	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue-262148	262148	--	Queueing	7609S-NPE3.cisco.com	--	--
PREC-0	458752	--	ClassMap	7609S-NPE3.cisco.com	--	--
queue-131076	131076	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	196609	--	MatchStatement	7609S-NPE3.cisco.com	--	--
class-default	524288	--	ClassMap	7609S-NPE3.cisco.com	--	--
Match	458755	--	MatchStatement	7609S-NPE3.cisco.com	--	--
queue-327684	327684	--	Queueing	7609S-NPE3.cisco.com	--	--
Match	458754	--	MatchStatement	7609S-NPE3.cisco.com	--	--

2. Find the CBQoS object for which you want to edit interface thresholds.

- Click the wrench icon (🔧).

PREC-0 | 458752 | 7609S-NPE3 cisco.com Reset Guide

Thresholds

Metric: Default Overridden Set All to Defaults

Category	Metric	Unit	Defaults	Default Status
Drop Rate	Rising High	bps	1.000	[Disabled]
	Rising Medium	bps	0.500	[Disabled]
Violation Rate	Rising High	bps	1.000	[Disabled]
	Rising Medium	bps	0.500	[Disabled]
Pre-Policy Inbound Utilization	Rising High	%	60.000	[Disabled]
	Rising Medium	%	40.000	[Disabled]
Post-Policy Outbound Utilization	Rising High	%	60.000	[Disabled]
	Rising Medium	%	40.000	[Disabled]
Discard Rate	Rising High	Bps	1.000	[Disabled]
	Rising Medium	Bps	0.500	[Disabled]

Save

- The **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon) appears. On this page, you can edit one or more thresholds, which are applied to the interfaces aligned with the CBQoS object. SL1 examines the thresholds in the **Quality of Service Object Thresholds** page and generates events when the thresholds are exceeded.

NOTE: The thresholds defined in the **Quality of Service Object Thresholds** page (System > Settings > Thresholds > Quality of Service) determine which thresholds will appear in this page. For a list of all possible thresholds that can appear in this page, see the section on [Global Settings that Affect Interfaces](#).

- The following global thresholds are defined in the **Quality of Service Object Thresholds** page (System > Settings > Thresholds > Quality of Service) and also appear in the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon):

Threshold	Default Value	Default Status
<i>Drop Rate > Rising High</i>	1.000	Disabled

Threshold	Default Value	Default Status
<i>Drop Rate > Rising Medium</i>	0.500	Disabled
<i>Violation Rate > Rising High</i>	1.000	Disabled
<i>Violation Rate > Rising Medium</i>	0.500	Disabled
<i>Pre-Policy Inbound Utilization % > Rising High</i>	60.000	Disabled
<i>Pre-Policy Inbound Utilization % > Rising Medium</i>	40.000	Disabled
<i>Pre-Policy Outbound Utilization % > Rising High</i>	60.000	Disabled
<i>Pre-Policy Outbound Utilization % > Rising Medium</i>	40.000	Disabled
<i>Discard Rate > Rising High</i>	1.000	Disabled
<i>Discard Rate > Rising Medium</i>	0.500	Disabled

6. For each threshold in the **Thresholds** tab, you can edit the following:

- **Value.** The value at which the threshold will trigger an event.
 - For thresholds that include the word *Rising*, when a value exceeds the specified value, SL1 triggers an event.
 - For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers an event.
 - For thresholds that do not include the word *Rising* or *Falling*, when a value exceeds the specified value, SL1 triggers an event.
- **Status.** Specifies whether the threshold is active. Choices are:
 - *Enabled.* The threshold is applied to the interface and is monitored by SL1.
 - *Disabled.* The threshold appears in the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon) but it not monitored by SL1.

Viewing Reports About Interfaces and Bandwidth

See the chapter on [Viewing Performance Graphs](#) for information about and examples of reports about interfaces and bandwidth.

Global Settings that Affect Interfaces

The following pages contain settings that affect interfaces:

Behavior Settings

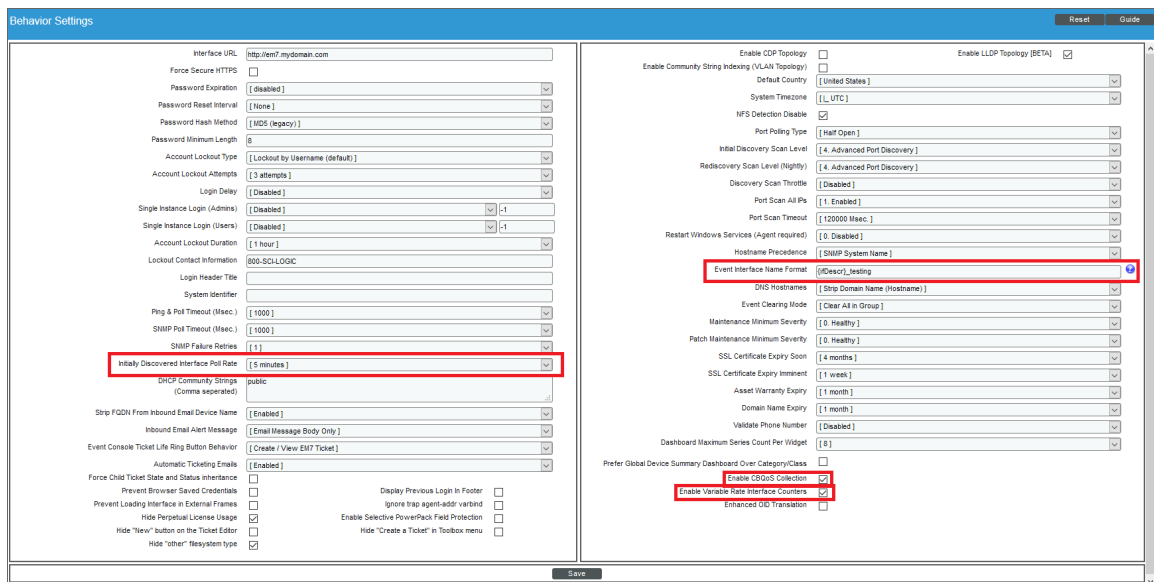
The **Behavior Settings** page (System > Settings > Behavior) allows you to define global parameters that affect:

- User Logins
- Discovery
- Data collection
- Settings that affect the display and behavior of the user interface
- Expiration warnings for asset warranties and SSL certificates

The parameters in the **Behavior Settings** page affect all pages, devices, and discovery functionality in SL1. For most settings, you can define a one-time, manual override in the affected page. You can also override many of these settings per device. For example, you can define global parameters for nightly discovery in this page, but in a device's **Device Properties** page (Devices > Device Manager > wrench icon), you can override these settings for a specific device.

To define or edit the settings in the **Behavior Settings** page:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).



2. In the **Behavior Settings** page, the following fields affect how SL1 manages interfaces:

- **Initially Discovered Interface Poll Rate.** This field specifies the frequency with which SL1 will poll newly discovered interfaces. This setting does not affect interfaces that have been previously discovered with a different value in this field or interfaces for which the **Frequency** field has been manually edited in the **Interface Properties** page. Choices in this field are:
 - 1 min. SL1 will poll the newly discovered interfaces every minute.

- *5 mins.* SL1 will poll the newly discovered interfaces every five minutes. This is the default value for this field.
 - *10 mins.* SL1 will poll the newly discovered interfaces every 10 minutes.
 - *15 mins.* SL1 will poll the newly discovered interfaces every 15 minutes.
 - *30 mins.* SL1 will poll the newly discovered interfaces every 30 minutes.
 - *60 mins.* SL1 will poll the newly discovered interfaces every 60 minutes.
 - *120 mins.* SL1 will poll the newly discovered interfaces every 120 minutes.
- **Event Interface Name Format.** Specifies the format of the network interface name that you want to appear in events. If you selected *Interface Alias* for the deprecated **Interface Name Precedence** field in a previous release of SL1, the format for existing interfaces is set to {alias}. If you selected “Interface Name” for the deprecated **Interface Name Precedence** field in a previous release of SL1, the format for existing interfaces is set to {name}. The default format is {name}.
 - **Enable CBQoS Collection.** If selected, SL1 will collect configuration data about Class-Based Quality-of-Service (CBQoS) from interfaces that are configured for CBQoS. If selected, you can enable collection of CBQoS metrics per-interface. The collected CBQoS metrics are displayed in Device Performance reports associated with the device that contains those interfaces. This setting is disabled by default. (For more information about Device Performance reports, see the chapter in the **Device Management** manual.)
 - **Enable Variable Rate Interface Counters.** If selected, enables more accurate collection of data from interfaces. If enabled, when SL1 retrieves data from an interface, that data is stored in the ScienceLogic database along with the timestamp associated with the exact collection time. Before normalization occurs, SL1 applies an interpolation function that spaces the data at regular time intervals. For example, suppose you have specified that SL1 should collect interface data every five minutes. However, due to network traffic across the Data Collectors, SL1 might collect data from an interface at 13:01 and then 13:05. Because the ScienceLogic normalization process expects data that has been collected every five minutes, SL1 first applies an interpolation to the data to prepare the data for normalization.

3. Click the **[Save]** button to save any changes in this page.

Interface Threshold Defaults

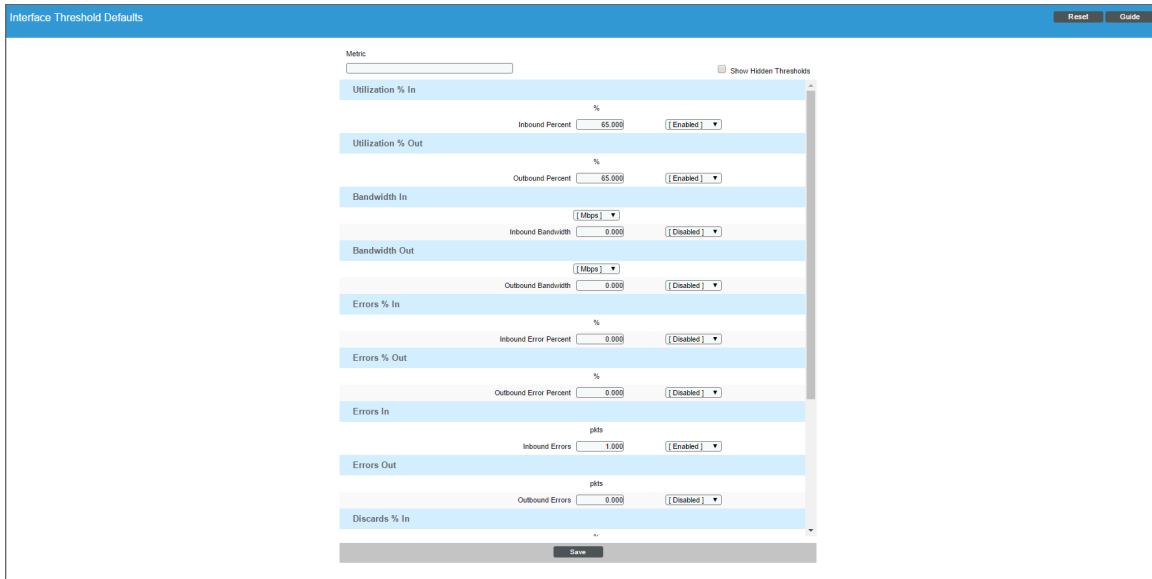
The **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) allows you to define global thresholds for interfaces.

The settings in the **Interface Thresholds Defaults** page apply to all interfaces. However, you can override these system settings on a case-by-case basis for each interface in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).

If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. SL1 will use either the default thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) or the custom threshold you define in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). When the values for an interface exceed one or more thresholds, SL1 will generate an event.

To define global thresholds for interfaces:

1. Go to **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface).



2. The following global thresholds are defined by default in the **Interface Thresholds Defaults** page:

NOTE: You can specify the unit of measure for all the metrics in **Bandwidth In** and **Bandwidth Out**. You can select *bps*, *kpbs*, *Mbps* (the default), or *Gbps*.

Threshold	Default Value	Default Status
<i>Utilization % In > Inbound Percent</i>	65.000	Enabled
<i>Utilization % Out > Outbound Percent</i>	65.000	Enabled
<i>Bandwidth In > Inbound Bandwidth</i>	0.000	Disabled
<i>Bandwidth Out > Outbound Bandwidth</i>	0.000	Disabled
<i>Errors % In > Inbound Error Percent</i>	1.000	Enabled
<i>Errors % Out > Outbound Error Percent</i>	1.000	Enabled
<i>Errors In > Inbound Errors</i>	1000.000	Enabled
<i>Errors Out > Outbound Errors</i>	1000.000	Enabled
<i>Discard % In > Inbound Discard Percent</i>	1.000	Enabled
<i>Discards % Out > Outbound Discard Percent</i>	1.000	Enabled
<i>Discards In > Inbound Discards</i>	1000.000	Enabled

Threshold	Default Value	Default Status
<i>Discards Out > Outbound Discards</i>	1000.000	Enabled
<i>Multicast % In > Rising Medium</i>	30.000	Disabled
<i>Multicast % In > Rising Low</i>	20.000	Disabled
<i>Broadcast % Out > Rising Medium</i>	30.000	Disabled
<i>Broadcast % Out > Rising Low</i>	20.000	Disabled

3. Selecting the **Show Hidden Thresholds** checkbox displays the following default thresholds:

NOTE: You can specify the unit of measure for all the metrics in **Bandwidth In** and **Bandwidth Out**. You can select **bps**, **kbps**, **Mbps** (the default), or **Gbps**.

Threshold	Default Value	Default Status
<i>Utilization % In > Rising High</i>	0.000	Hidden
<i>Utilization % In > Rising Medium</i>	0.000	Hidden
<i>Utilization % In > Rising Low</i>	0.000	Hidden
<i>Utilization % In > Falling Low</i>	0.000	Hidden
<i>Utilization % In > Falling Medium</i>	0.000	Hidden
<i>Utilization % In > Falling High</i>	0.000	Hidden
<i>Utilization % In > Inbound Percent</i>	65.000	Enabled
<i>Utilization % Out > Rising High</i>	0.000	Hidden
<i>Utilization % Out > Rising Medium</i>	0.000	Hidden
<i>Utilization % Out > Rising Low</i>	0.000	Hidden
<i>Utilization % Out > Falling Low</i>	0.000	Hidden
<i>Utilization % Out > Falling Medium</i>	0.000	Hidden
<i>Utilization % Out > Falling High</i>	0.000	Hidden
<i>Utilization % Out > Outbound Percent</i>	65.000	Enabled
<i>Bandwidth In > Rising High</i>	0.000	Hidden
<i>Bandwidth In > Rising Medium</i>	0.000	Hidden
<i>Bandwidth In > Rising Low</i>	0.000	Hidden
<i>Bandwidth In > Falling Low</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Bandwidth In > Falling Medium</i>	0.000	Hidden
<i>Bandwidth In > Falling High</i>	0.000	Hidden
<i>Bandwidth In > Inbound Bandwidth</i>	0.000	Disabled
<i>Bandwidth Out > Rising High</i>	0.000	Hidden
<i>Bandwidth Out > Rising Medium</i>	0.000	Hidden
<i>Bandwidth Out > Rising Low</i>	0.000	Hidden
<i>Bandwidth Out > Falling Low</i>	0.000	Hidden
<i>Bandwidth Out > Falling Medium</i>	0.000	Hidden
<i>Bandwidth Out > Falling High</i>	0.000	Hidden
<i>Bandwidth Out > Outbound Bandwidth</i>	0.000	Disabled
<i>Errors % In > Rising High</i>	0.000	Hidden
<i>Errors % In > Rising Medium</i>	0.000	Hidden
<i>Errors % In > Rising Low</i>	0.000	Hidden
<i>Errors % In > Falling Low</i>	0.000	Hidden
<i>Errors % In > Falling Medium</i>	0.000	Hidden
<i>Errors % In > Falling High</i>	0.000	Hidden
<i>Errors % In > Inbound Error Percent</i>	1.000	Enabled
<i>Errors % Out > Rising High</i>	0.000	Hidden
<i>Errors % Out > Rising Medium</i>	0.000	Hidden
<i>Errors % Out > Rising Low</i>	0.000	Hidden
<i>Errors % Out > Falling Low</i>	0.000	Hidden
<i>Errors % Out > Falling Medium</i>	0.000	Hidden
<i>Errors % Out > Falling High</i>	0.000	Hidden
<i>Errors % Out > Outbound Error Percent</i>	1.000	Enabled
<i>Errors In > Rising High</i>	0.000	Hidden
<i>Errors In > Rising Medium</i>	0.000	Hidden
<i>Errors In > Rising Low</i>	0.000	Hidden
<i>Errors In > Falling Low</i>	0.000	Hidden
<i>Errors In > Falling Medium</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Errors In > Falling High</i>	0.000	Hidden
<i>Errors In > InboundErrors</i>	1000.000	Enabled
<i>Errors Out > Rising High</i>	0.000	Hidden
<i>Errors Out > Rising Medium</i>	0.000	Hidden
<i>Errors Out > Rising Low</i>	0.000	Hidden
<i>Errors Out > Falling Low</i>	0.000	Hidden
<i>Errors Out > Falling Medium</i>	0.000	Hidden
<i>Errors Out > Falling High</i>	0.000	Hidden
<i>Errors Out > Outbound Errors</i>	1000.000	Enabled
<i>Discards % In > Rising High</i>	0.000	Hidden
<i>Discards % In > Rising Medium</i>	0.000	Hidden
<i>Discards % In > Rising Low</i>	0.000	Hidden
<i>Discards % In > Falling Low</i>	0.000	Hidden
<i>Discards % In > Falling Medium</i>	0.000	Hidden
<i>Discards % In > Falling High</i>	0.000	Hidden
<i>Discards % In > Inbound Discard Percent</i>	1.000	Enabled
<i>Discards % Out > Rising High</i>	0.000	Hidden
<i>Discards % Out > Rising Medium</i>	0.000	Hidden
<i>Discards % Out > Rising Low</i>	0.000	Hidden
<i>Discards % Out > Falling Low</i>	0.000	Hidden
<i>Discards % Out > Falling Medium</i>	0.000	Hidden
<i>Discards % Out > Falling High</i>	0.000	Hidden
<i>Discards % Out > Outbound Discard Percent</i>	1.000	Enabled
<i>Discards In > Rising High</i>	0.000	Hidden
<i>Discards In > Rising Medium</i>	0.000	Hidden
<i>Discards In > Rising Low</i>	0.000	Hidden
<i>Discards In > Falling Low</i>	0.000	Hidden
<i>Discards In > Falling Medium</i>	0.000	Hidden
<i>Discards In > Falling High</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Discards In > Inbound Discards</i>	1000.000	Enabled
<i>Discards Out > Rising High</i>	0.000	Hidden
<i>Discards Out > Rising Medium</i>	0.000	Hidden
<i>Discards Out > Rising Low</i>	0.000	Hidden
<i>Discards Out > Falling Low</i>	0.000	Hidden
<i>Discards Out > Falling Medium</i>	0.000	Hidden
<i>Discards Out > Falling High</i>	0.000	Hidden
<i>Discards Out > Outbound Discards</i>	1000.000	Enabled
<i>Broadcast % In > Rising High</i>	0.000	Hidden
<i>Broadcast % In > Rising Medium</i>	30.000	Disabled
<i>Broadcast % In > Rising Low</i>	20.000	Disabled
<i>Broadcast % In > Falling Low</i>	0.000	Hidden
<i>Broadcast % In > Falling Medium</i>	0.000	Hidden
<i>Broadcast % In > Falling High</i>	0.000	Hidden
<i>Broadcast % Out > Rising High</i>	0.000	Hidden
<i>Broadcast % Out > Rising Medium</i>	30.000	Disabled
<i>Broadcast % Out > Rising Low</i>	20.000	Disabled
<i>Broadcast % Out > Falling Low</i>	0.000	Hidden
<i>Broadcast % Out > Falling Medium</i>	0.000	Hidden
<i>Broadcast % Out > Falling High</i>	0.000	Hidden
<i>Broadcast In > Rising High</i>	0.000	Hidden
<i>Broadcast In > Rising Medium</i>	0.000	Hidden
<i>Broadcast In > Rising Low</i>	0.000	Hidden
<i>Broadcast In > Falling Low</i>	0.000	Hidden
<i>Broadcast In > Falling Medium</i>	0.000	Hidden
<i>Broadcast In > Falling High</i>	0.000	Hidden
<i>Broadcast Out > Rising High</i>	0.000	Hidden
<i>Broadcast Out > Rising Medium</i>	0.000	Hidden
<i>Broadcast Out > Rising Low</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Broadcast Out > Falling Low</i>	0.000	Hidden
<i>Broadcast Out > Falling Medium</i>	0.000	Hidden
<i>Broadcast Out > Falling High</i>	0.000	Hidden
<i>Multicast % In > Rising High</i>	0.000	Hidden
<i>Multicast % In > Rising Medium</i>	00.000	Hidden
<i>Multicast % In > Rising Low</i>	00.000	Hidden
<i>Multicast % In > Falling Low</i>	0.000	Hidden
<i>Multicast % In > Falling Medium</i>	0.000	Hidden
<i>Multicast % In > Falling High</i>	0.000	Hidden
<i>Multicast % Out > Rising High</i>	0.000	Hidden
<i>Multicast % Out > Rising Medium</i>	00.000	Hidden
<i>Multicast % Out > Rising Low</i>	00.000	Hidden
<i>Multicast % Out > Falling Low</i>	0.000	Hidden
<i>Multicast % Out > Falling Medium</i>	0.000	Hidden
<i>Multicast % Out > Falling High</i>	0.000	Hidden
<i>Multicast In > Rising High</i>	0.000	Hidden
<i>Multicast In > Rising Medium</i>	0.000	Hidden
<i>Multicast In > Rising Low</i>	0.000	Hidden
<i>Multicast In > Falling Low</i>	0.000	Hidden
<i>Multicast In > Falling Medium</i>	0.000	Hidden
<i>Multicast In > Falling High</i>	0.000	Hidden
<i>Multicast Out > Rising High</i>	0.000	Hidden
<i>Multicast Out > Rising Medium</i>	0.000	Hidden
<i>Multicast Out > Rising Low</i>	0.000	Hidden
<i>Multicast Out > Falling Low</i>	0.000	Hidden
<i>Multicast Out > Falling Medium</i>	0.000	Hidden
<i>Multicast Out > Falling High</i>	0.000	Hidden
<i>Unicast % In > Rising High</i>	0.000	Hidden
<i>Unicast % In > Rising Medium</i>	00.000	Hidden

Threshold	Default Value	Default Status
<i>Unicast % In > Rising Low</i>	00.000	Hidden
<i>Unicast % In > Falling Low</i>	0.000	Hidden
<i>Unicast % In > Falling Medium</i>	0.000	Hidden
<i>Unicast % In > Falling High</i>	0.000	Hidden
<i>Unicast % Out > Rising High</i>	0.000	Hidden
<i>Unicast % Out > Rising Medium</i>	00.000	Hidden
<i>Unicast % Out > Rising Low</i>	00.000	Hidden
<i>Unicast % Out > Falling Low</i>	0.000	Hidden
<i>Unicast % Out > Falling Medium</i>	0.000	Hidden
<i>Unicast % Out > Falling High</i>	0.000	Hidden
<i>Unicast In > Rising High</i>	0.000	Hidden
<i>Unicast In > Rising Medium</i>	0.000	Hidden
<i>Unicast In > Rising Low</i>	0.000	Hidden
<i>Unicast In > Falling Low</i>	0.000	Hidden
<i>Unicast In > Falling Medium</i>	0.000	Hidden
<i>Unicast In > Falling High</i>	0.000	Hidden
<i>Unicast Out > Rising High</i>	0.000	Hidden
<i>Unicast Out > Rising Medium</i>	0.000	Hidden
<i>Unicast Out > Rising Low</i>	0.000	Hidden
<i>Unicast Out > Falling Low</i>	0.000	Hidden
<i>Unicast Out > Falling Medium</i>	0.000	Hidden
<i>Unicast Out > Falling High</i>	0.000	Hidden

4. For each threshold, you can edit the following:

- **Value.** The value at which the threshold will trigger an event.
 - For thresholds that include the word *Rising*, when a value exceeds the specified value, SL1 triggers an event.
 - For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers an event.
 - For thresholds that do not include the word *Rising* or *Falling*, when a value exceeds the specified value, SL1 triggers an event.

- **Status.** Specifies whether the threshold is active and whether the threshold will appear in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). Choices are:
 - *Enabled.* The threshold is applied to all interfaces and is monitored by SL1. The threshold appears in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). Users can edit the **Value** and **Status** of the threshold.
 - *Disabled.* The threshold is applied to all interfaces but is not monitored by SL1. The threshold appears in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) with a status of *Disabled*. In the **Thresholds** tab on the **Interface Properties** page, users can edit the **Value** and **Status** of the threshold.
 - *Hidden.* The threshold is not applied to all interfaces, and is not monitored by SL1. The threshold does not appear in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).
- **Unit of Measure.** For all the metrics under **Bandwidth In** and **Bandwidth Out**, you can select the unit of measure. Choices are:
 - bps
 - kbps
 - Mbps
 - Gbps

Quality of Service Threshold Defaults

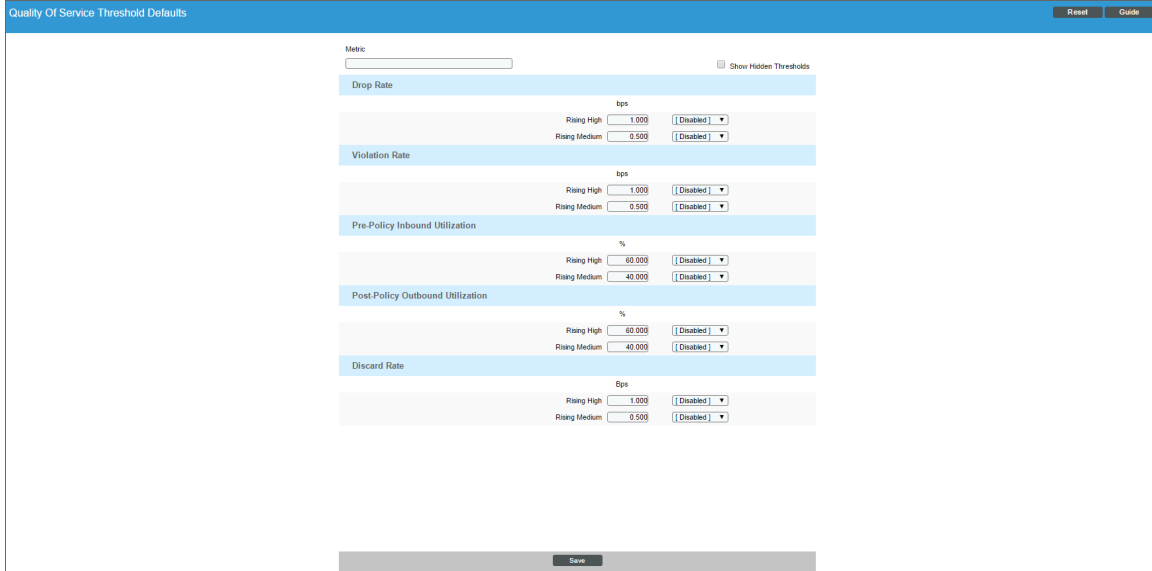
The **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) allows you to define global thresholds for CBQoS objects.

The settings in the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) apply to all CBQoS objects. However, you can override these system settings on a case-by-case basis for each interface in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service).

If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. For interfaces that are part of a CBQoS class, SL1 will use either the global CBQoS thresholds defined in the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) or the custom threshold you define in the **Quality of Service Object Thresholds** page (Registry > Network > Quality of Service (QoS) > wrench icon). When the values for an interface exceed one or more thresholds, SL1 will generate an event.

To edit the global thresholds for a CBQoS object:

1. Go to the **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service).



2. The following global thresholds are defined by default in **Quality of Service Threshold Defaults** page:

Threshold	Default Value	Default Status
<i>Drop Rate > Rising High</i>	1.000	Disabled
<i>Drop Rate > Rising Medium</i>	0.500	Disabled
<i>Violation Rate > Rising High</i>	1.000	Disabled
<i>Violation Rate > Rising Medium</i>	0.500	Disabled
<i>Pre-Policy Inbound Utilization % > Rising High</i>	60.000	Disabled
<i>Pre-Policy Inbound Utilization % > Rising Medium</i>	40.000	Disabled
<i>Pre-Policy Outbound Utilization % > Rising High</i>	60.000	Disabled
<i>Pre-Policy Outbound Utilization % > Rising Medium</i>	40.000	Disabled
<i>Discard Rate > Rising High</i>	1.000	Disabled
<i>Discard Rate > Rising Medium</i>	0.500	Disabled

3. Selecting the **Show Hidden Thresholds** checkbox displays the following default thresholds:

Threshold	Default Value	Default Status
<i>Pre-Policy Rate > Rising High</i>	0.000	Hidden
<i>Pre-Policy Rate > Rising Medium</i>	0.000	Hidden
<i>Pre-Policy Rate > Rising Low</i>	0.000	Hidden
<i>Pre-Policy Rate > Falling Low</i>	0.000	Hidden
<i>Pre-Policy Rate > Falling Medium</i>	0.000	Hidden
<i>Pre-Policy Rate > Falling High</i>	0.000	Hidden
<i>PostPolicy Rate > Rising High</i>	0.000	Hidden
<i>Post-Policy Rate > Rising Medium</i>	0.000	Hidden
<i>Post-Policy Rate > Rising Low</i>	0.000	Hidden
<i>Post-Policy Rate > Falling Low</i>	0.000	Hidden
<i>Post-Policy Rate > Falling Medium</i>	0.000	Hidden
<i>Post-Policy Rate > Falling High</i>	0.000	Hidden
<i>Drop Rate > Rising High</i>	1.000	Disabled
<i>Drop Rate > Rising Medium</i>	0.500	Disabled
<i>Drop Rate > Rising Low</i>	0.000	Hidden
<i>Drop Rate > Falling Low</i>	0.000	Hidden
<i>Drop Rate > Falling Medium</i>	0.000	Hidden
<i>Drop Rate > Falling High</i>	0.000	Hidden
<i>Conforming Rate > Rising High</i>	0.000	Hidden
<i>Conforming Rate > Rising Medium</i>	0.000	Hidden
<i>Conforming Rate > Rising Low</i>	0.000	Hidden
<i>Conforming Rate > Falling Low</i>	0.000	Hidden
<i>Conforming Rate > Falling Medium</i>	0.000	Hidden
<i>Conforming Rate > Falling High</i>	0.000	Hidden
<i>Non-Conforming Rate > Rising High</i>	0.000	Hidden
<i>Non-Conforming Rate > Rising Medium</i>	0.000	Hidden
<i>Non-Conforming Rate > Rising Low</i>	0.000	Hidden
<i>Non-Conforming Rate > Falling Low</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Non-Conforming Rate > Falling Medium</i>	0.000	Hidden
<i>Non-Conforming Rate > Falling High</i>	0.000	Hidden
<i>Violation Rate > Rising High</i>	1.000	Disabled
<i>Violation Rate > Rising Medium</i>	0.500	Disabled
<i>Violation Rate > Rising Low</i>	0.000	Hidden
<i>Violation Rate > Falling Low</i>	0.000	Hidden
<i>Violation Rate > Falling Medium</i>	0.000	Hidden
<i>Violation Rate > Falling High</i>	0.000	Hidden
<i>Current Queue Depth > Rising High</i>	0.000	Hidden
<i>Current Queue Depth > Rising Medium</i>	0.000	Hidden
<i>Current Queue Depth Current Queue Depth > Rising Low</i>	0.000	Hidden
<i>Current Queue Depth > Falling Low</i>	0.000	Hidden
<i>Current Queue Depth > Falling Medium</i>	0.000	Hidden
<i>Current Queue Depth > Falling High</i>	0.000	Hidden
<i>Pre-Policy Inbound Utilization > Rising High</i>	60.000	Disabled
<i>Pre-Policy Inbound Utilization > Rising Medium</i>	40.000	Disabled
<i>Pre-Policy Inbound Utilization > Rising Low</i>	0.000	Hidden
<i>Pre-Policy Inbound Utilization > Falling Low</i>	0.000	Hidden
<i>Pre-Policy Inbound Utilization > Falling Medium</i>	0.000	Hidden
<i>Pre-Policy Inbound Utilization > Falling High</i>	0.000	Hidden
<i>Post-Policy Inbound Utilization > Rising High</i>	60.000	Disabled
<i>Post-Policy Inbound Utilization > Rising Medium</i>	40.000	Disabled
<i>Post-Policy Inbound Utilization > Rising Low</i>	0.000	Hidden
<i>Post-Policy Inbound Utilization > Falling Low</i>	0.000	Hidden
<i>Post-Policy Inbound Utilization > Falling Medium</i>	0.000	Hidden
<i>Post-Policy Inbound Utilization > Falling High</i>	0.000	Hidden
<i>Discard Rate > Rising High</i>	1.000	Disabled
<i>Discard Rate > Rising Medium</i>	0.500	Disabled
<i>Discard Rate Discard Rate > Rising Low</i>	0.000	Hidden

Threshold	Default Value	Default Status
<i>Discard Rate > Falling Low</i>	0.000	Hidden
<i>Discard Rate > Falling Medium</i>	0.000	Hidden
<i>Discard Rate > Falling High</i>	0.000	Hidden

4. For each threshold, you can edit the following:

- **Value.** The value at which the threshold will trigger an event.
 - For thresholds that include the word *Rising*, when a value exceeds the specified value, SL17 triggers an event.
 - For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers an event.
 - For thresholds that do not include the word *Rising* or *Falling*, when a value exceeds the specified value, SL1 triggers an event.
- **Status.** Specifies whether the threshold is active and whether the threshold will appear in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service) page. Choices are:
 - *Enabled.* The threshold is applied to all CBQoS-enabled interfaces and is monitored by SL1. The threshold appears in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service). Users can edit the **Value** and **Status** of the threshold.
 - *Disabled.* The threshold is applied to all CBQoS-enabled interfaces but is not monitored by SL1. The threshold appears in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service) with a status of *Disabled*. In the **Quality of Service (QoS)** page, users can edit the **Value** and **Status** of the threshold.
 - *Hidden.* The threshold is not applied to all interfaces, and is not monitored by SL1. The threshold does not appear in the **Quality of Service (QoS)** page (Registry > Networks > Quality of Service).

Chapter

9



Monitoring Networks

Overview

During discovery, SL1 discovers all IP networks. The list of all networks is displayed in the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).

The **IPv4 Networks** page allows you to view a list of all networks, manage networks and IPs, view devices and interfaces in each network, and view maps and reports for each network.

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:

IPv4 Networks	248
Viewing the List of IPv4 Networks	249
Browsing a Network	251
Viewing Used and Unused IP Addresses in a Network	251
Viewing Devices Aligned with a Network	252
Viewing Interfaces Aligned with a Network	252
Viewing a Map of a Network	252
Generating a Report for a Network	253
Defining a New Network	254
Merging One or More Networks	255
Synchronizing One or More Networks	256

<i>Editing a Network's Properties</i>	257
<i>Performing Dynamic Discovery for a Network</i>	257
<i>Creating a Ticket About a Network</i>	258
<i>Deleting One or More IPv4 Networks</i>	259

IPv4 Networks

The **IPv4 Networks** page (Registry > Networks > IPv4 Networks) lists all networks and subnets detected by ScienceLogic auto-discovery and all manually defined (new) networks.

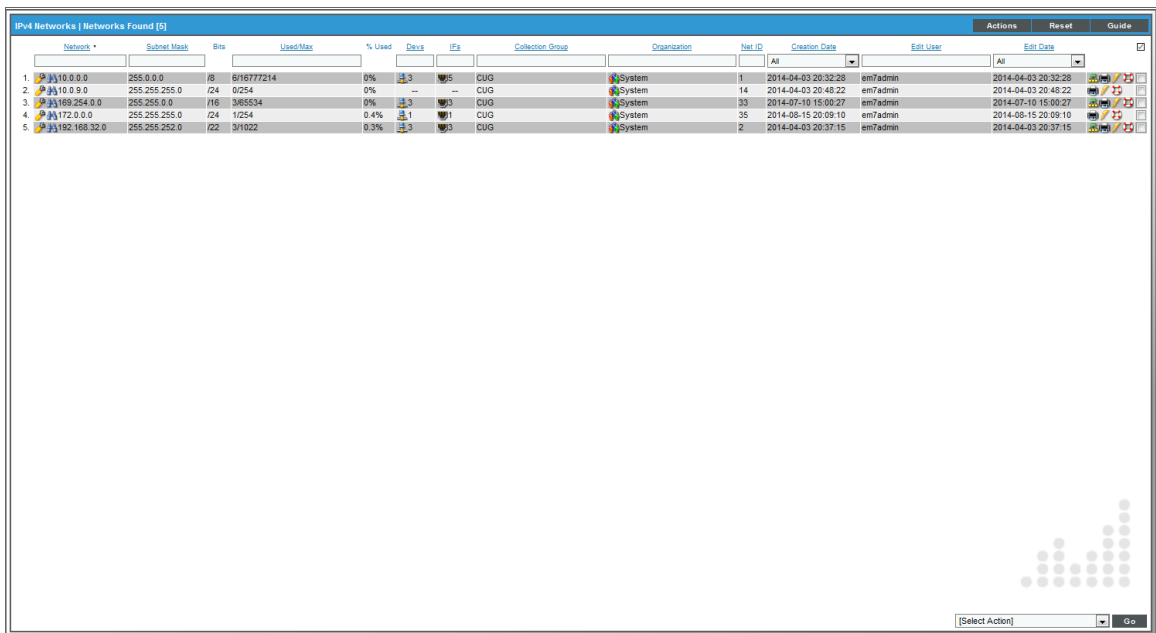
The **IPv4 Networks** page allows you to easily manage networks and IP addresses. From the **IPv4 Networks** page, you can view detailed data about the network, keep records of subnets, and determine which IP addresses are in use and which IP addresses are available.

NOTE: Users of type "user" can view only IPv4 networks that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all IPv4 networks.

Viewing the List of IPv4 Networks

The table in the **IPv4 Networks** page (Registry > Networks > IPv4 Networks) contains an entry for each network managed by SL1:

NOTE: Users of type "user" can view only IPv4 networks that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all IPv4 networks.












The screenshot displays a web interface titled "IPv4 Networks | Networks Found [5]". It features a table with the following columns: Network, Subnet Mask, Bits, Used/Max, % Used, Days, I/Fs, Collection Group, Organization, Net ID, Creation Date, Edit User, and Edit Date. The table contains five rows of network data. At the bottom right of the interface, there is a "[Select Action]" dropdown menu and a "Go" button.

Network	Subnet Mask	Bits	Used/Max	% Used	Days	I/Fs	Collection Group	Organization	Net ID	Creation Date	Edit User	Edit Date
1. 10.0.0.0	255.0.0.0	/8	616777214	0%	13	5	CUG	System	1	2014-04-03 20:32:28	em7admin	2014-04-03 20:32:28
2. 10.0.9.0	255.255.255.0	/24	0/254	0%	--	--	CUG	System	14	2014-04-03 20:48:22	em7admin	2014-04-03 20:48:22
3. 189.254.0.0	255.255.0.0	/16	368534	0%	13	3	CUG	System	33	2014-07-10 15:00:27	em7admin	2014-07-10 15:00:27
4. 172.0.0.0	255.255.255.0	/24	1/254	0.4%	11	1	CUG	System	35	2014-03-15 20:09:10	em7admin	2014-03-15 20:09:10
5. 192.168.32.0	255.255.252.0	/22	3/1022	0.3%	13	3	CUG	System	2	2014-04-03 20:37:15	em7admin	2014-04-03 20:37:15

The **IPv4 Networks** page displays the following about each managed network:

TIP: To sort the list of networks, 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.

- **Network.** IP address of the entire network.
- **Subnet Mask.** Subnet mask for the subnet.
- **Bits.** The number of bits used for the network address.
- **Used/Max.** Number of IP addresses discovered and monitored by SL1 and the maximum number of IP addresses allowed in the subnet.

- **% Used**. Percentage of total addresses in the network that have been discovered and monitored by SL1. In the **Account Preferences** page, you can specify whether or not you want to include empty networks (networks with no devices or interfaces) in the list of networks. These networks will have 0% in the % Used column.
- **Devs**. Number of devices in the subnet.
- **IFs**. Number of interfaces in the subnet.
- **Collection Group**. The collector group associated with the network. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).
- **Organization**. Organization associated with the network.
- **Net ID**. Unique network ID, assigned by SL1.
- **Creation Date**. Date the network was discovered or manually defined.
- **Edit User**. User who created or last edited the network's properties.
- **Edit Date**. Date the network was created or last edited, whichever is later.
- **Tools**. For each network in the table, the following tools are available:
 - **View/Edit Network Properties** (). Displays the **Network Properties** modal page, where you can view and edit the basic properties of an IPv4 network.
 - **Browse Network** (). Leads to the **Network Browser** page. From this page, you can view a list of IP addresses (used and unused) included in a network, a list of devices included in a network, and a list of interfaces included in a network.
 - **View/Edit Aligned Devices** (). Leads to the **Network Browser** page, where you can view a list of devices associated with a network.
 - **View/Edit Aligned Interfaces** (). Leads to the **Network Browser** page, where you can view a list of interfaces associated with a network.
 - **View/Edit Organization** (). Leads to the **Organizational Summary** page, where you can view and edit information associated with the organization.
 - **View Network Map** (). Leads to the **Layer-2 Maps** page, where you can view and edit a graphical representation of a layer-2 network.
 - **View a Network Report** (). Opens the **Report Creator** modal page, where you can specify information to include in the report and the format in which to generate the report.
 - **Add Network to Dynamic Discovery** (). Adds the network to the dynamic-discovery queue. SL1 will perform dynamic-discovery on all of the IP addresses in the network and gather information about any devices and interfaces in the network. Leads to the **Discovery Control Panel** page, with the selected network as the value in the discovery list.
 - **Create a Ticket** (). Leads to the **Ticket Editor** page, where you can create a ticket that will be associated with the selected network.

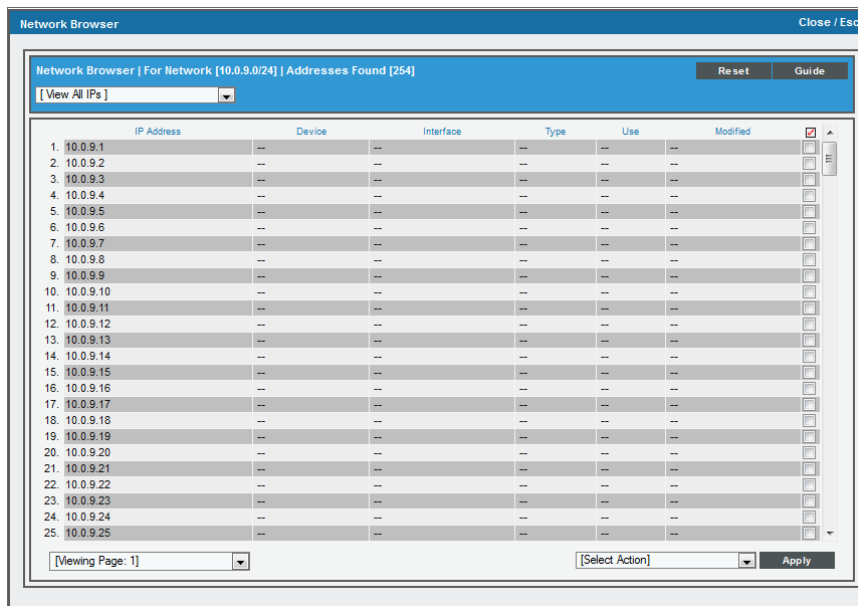
- **Delete** (🗑️). To delete the network, select this checkbox and then click the **[Delete]** button. To select all the checkboxes, click the large red check icon.

Browsing a Network

From the **IPv4 Networks** page, you can browse a network and view the IPs, devices, and interfaces within the network. To do this:

NOTE: Users of type "user" can view only devices that are aligned with the same organization(s) to which the user is aligned. Users of type "administrator" can view all devices. Users of type "user" can view only interfaces that are aligned with the same organization(s) to which the user is aligned or have been emissaried to the user's organization(s). Users of type "administrator" can view all interfaces.


1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to browse.
3. Click the binocular icon (🔍) for that network.
4. The **Network Browser** page appears.



5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.


Viewing Used and Unused IP Addresses in a Network

From the **IPv4 Networks** page, you can view a list of all IP addresses, used and unused, in a network. To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.
3. Click the binocular icon () for that network.
4. The **Network Browser** page appears.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.


Viewing Devices Aligned with a Network

From the **IPv4 Networks** page, you can view a list of all devices in a network To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.
3. Click the devices icon () for that network.
4. The **Network Browser** page appears and displays the list of devices in the network.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.


Viewing Interfaces Aligned with a Network

From the **IPv4 Networks** page, you can view a list of all interfaces in a network To do this:

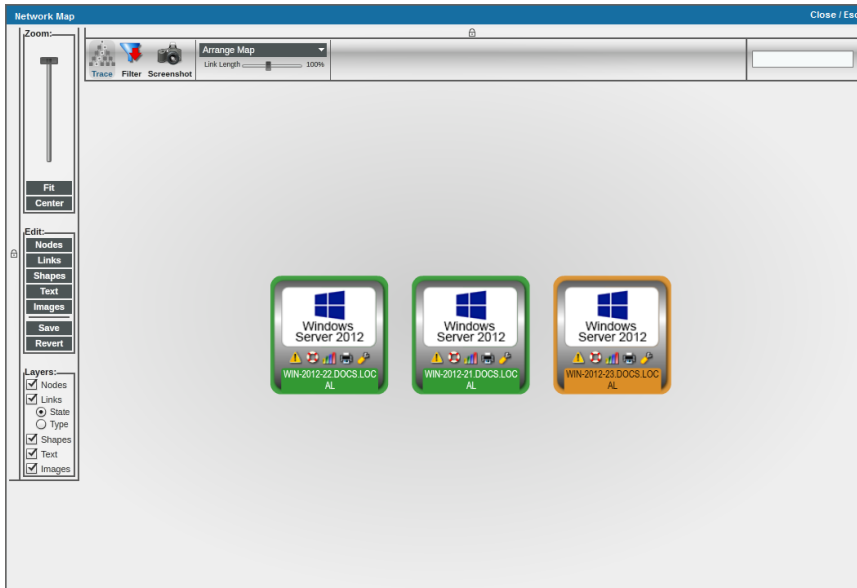
1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to view.
3. Click the interface icon () for that network.
4. The **Network Browser** page appears and displays the list of interface in the network.
5. In the drop-down menu in the upper left, you can choose to view all IP addresses in the network, all devices in the network, or all interfaces in the network.

Viewing a Map of a Network

From the **IPv4 Networks** page, you can view a layer-2 topology map of the network. To view a network map for a particular network:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network for which you want to view a map.
3. Click the map icon () for that network.

4. The **Layer-2 Maps** page appears, with the current network displayed.

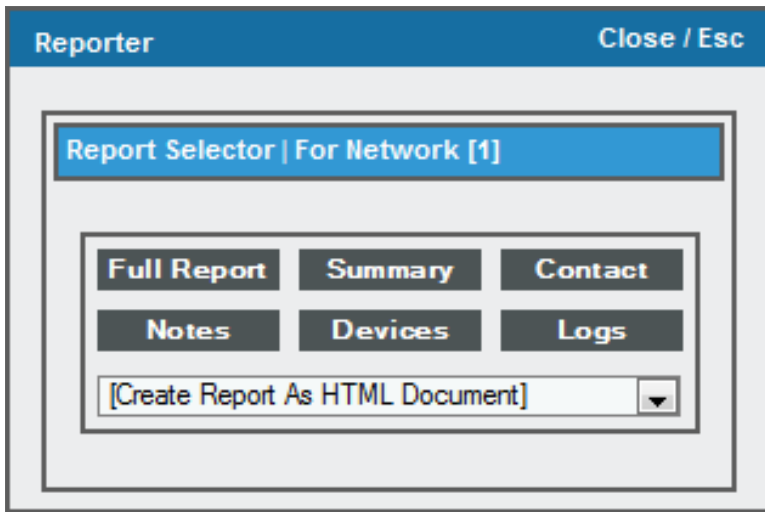


Generating a Report for a Network

To generate a report for a network:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network for which you want to view a map.
3. Click the printer icon (🖨️) for that network.

4. The **Report Creator** modal page appears. In this page, you can specify information to include in the report and the format in which to generate the report.



Defining a New Network

In the **IPv4 Networks** page, you can manually define a network. To do this:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, click the **[Actions]** button and select *Create*.
3. The **Network Properties** modal page appears.
4. In the **Network Properties** modal page, supply values in the following fields:

The image shows a modal window titled "Create new IPv4 Network" with a "Close / Esc" button in the top right corner. Inside the modal, there is a header bar that says "Network Properties | New Network". Below this header, there are several input fields and dropdown menus:

- Network:
- Subnet Mask / Bits:
- Description:
- Organization:
- Network Type:
- Network Usage:

At the bottom of the modal, there is a "Save" button.

- **Network.** IP address of the entire network (first IP). This field is read-only.

- **Description**. Description of the new network. This field is read-only.
- **Subnet Mask**. The subnet mask for the network, in use standard dotted-decimal format and the number of bits used for the network address.
- **Organization**. Select from the drop-down list. The drop-down contains a list of all organizations in SL1.
- **Network Type**. Description of the network type. Choices are:
 - ARIN Registered Public
 - Private Admin Network
 - Private Backup Network
 - Private NAT to ARIN Public
 - Provider Leased Public
- **Network Usage**. Description of how the network will be used. The entries in this drop-down can be edited in the **Select Objects Editor** page (System > Customize > Selected Objects). The default values are:
 - DHCP Block
 - DNS Servers
 - Email/Messaging Servers
 - File Server
 - Firewalls
 - Printers
 - Web Servers

5. Click the **[Save]** button to save the new network.

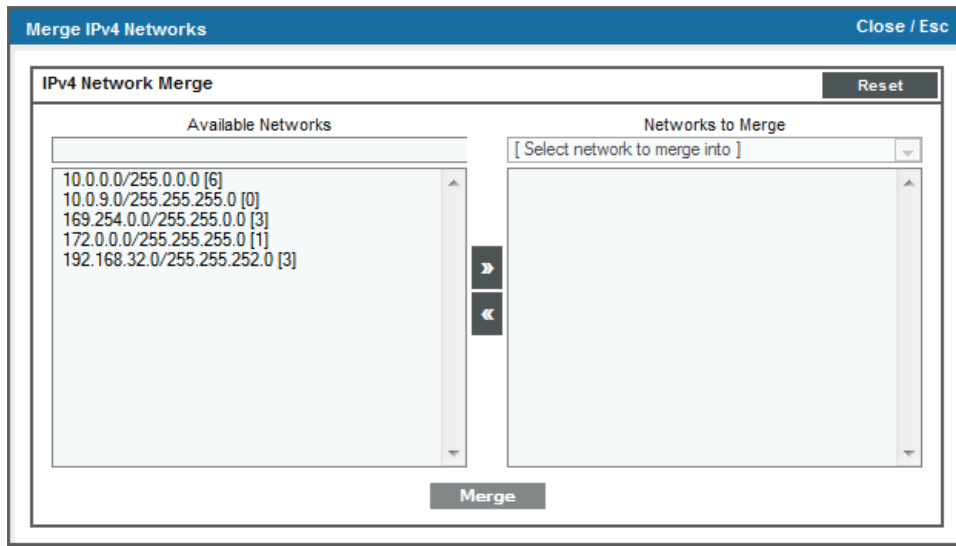
Merging One or More Networks

From the **IPv4 Networks** page, you can merge two or more networks. To merge networks, select a network to merge into and then select networks to add to the "merge into" network. When you merge networks, all devices in each selected network will become part of the "merge into" network. In the future, SL1 will automatically move any devices from the selected networks to the "merge into" network.

To merge networks:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, click the **[Actions]** button and select *Merge*.
3. The **IPv4 Network Merge** modal page appears.

4. In the **IPv4 Network Merge** modal page, supply a value in the following fields:



- **Available Networks.** Select one or more networks that you want to merge. Use the arrow button [**>>**] to add each network to the list of Networks to Merge.
- **Select network to merge into.** From the list of networks in the Networks to Merge list, you must select one network to be the "merge into" network. The other networks in the Networks to Merge list will be added to the "merge into" network.

5. Click the [**Merge**] button to save the newly merged network.

Synchronizing One or More Networks

When you synchronize a network, you remove any duplicate IPs from the network. The synchronize tool will remove only duplicate IPs from a single subnet where all the devices use the same Data Collector or Collector Group. To remove duplicate IPs:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, click the [**Actions**] button and select *Synchronize*.

- Text appears in the upper left of the page detailing how many networks were searched and how many addresses were synchronized.

Network	Subnet Mask	Bits	Used/Max	% Used	Devs	IFA	Collection Group	Organization	Net ID	Creation Date	Edit User	Edit Date
1. 10.0.0.0	255.0.0.0	18	6/16777214	0%	3	5	CUG	System	1	2014-04-03 20:32:28	em7admin	2014-04-03 20:32:28
2. 10.0.0.0	255.255.255.0	/24	0/254	0%	--	--	CUG	System	14	2014-04-03 20:48:22	em7admin	2014-04-03 20:48:22
3. 109.254.0.0	255.255.0.0	/16	3/85534	0%	3	3	CUG	System	33	2014-07-10 15:00:27	em7admin	2014-07-10 15:00:27
4. 172.0.0.0	255.255.255.0	/24	1/254	0.4%	1	1	CUG	System	35	2014-08-15 20:09:10	em7admin	2014-08-15 20:09:10
5. 192.168.32.0	255.255.252.0	/22	3/1022	0.3%	3	3	CUG	System	2	2014-04-03 20:37:15	em7admin	2014-04-03 20:37:15

Editing a Network's Properties

In the **IPv4 Networks** page, you can edit the basic properties of a network. To do this:

- Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
- In the **IPv4 Networks** page, find the network you want to edit.
- Click the wrench icon (🔧) for that network. The **Network Properties** modal page appears.
- In the **Network Properties** modal page, you can edit the *values for one or more parameters*.
- To save your changes to the network, click the **[Save]** button.

Performing Dynamic Discovery for a Network

You can perform dynamic discovery for a selected network. SL1 will then use Dynamic Applications to retrieve information about each device and application in the network. To manually trigger dynamic discovery for a network:


- Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
- In the **IPv4 Networks** page, find the network for which you want to perform dynamic discovery. Click the lightning bolt icon (⚡) for that network.

- The **Discovery Control Panel** page appears, with the field IP Address Discovery List already populated with the IP range from the selected network.

Session Name	IP/Hostname List	Collector	Organization	Pings	Rediscovery	User	Last Edit
1 VMware	10.100.100.46	em7_ao	System	Yes	Disabled	em7admin	2014-07-20 13:05:05
2 Support EM7	192.168.33.50 - 192.168.33.52	em7_ao	System	No	Disabled	em7admin	2014-07-20 18:52:11
3 KVM	10.100.100.40	em7_ao	System	Yes	Disabled	em7admin	2014-07-28 18:31:31
4 Windows Servers	10.100.100.21,10.100.100.22,10.100.100.23	em7_ao	System	Yes	Disabled	em7admin	2014-07-10 15:10:01
5 NetApp	10.0.9.45	em7_ao	Intel	Yes	Disabled	em7admin	2014-05-21 17:52:32
6 NetApp	10.100.100.20	em7_ao	Intel	Yes	Disabled	em7admin	2014-05-21 17:52:32
7 SUSE 11	10.100.100.30 - 10.100.100.34	em7_ao	Intel	Yes	Disabled	em7admin	2014-05-16 17:08:23
8 Extreme Switch	192.168.34.179	em7_ao	Intel	No	Disabled	em7admin	2014-05-16 17:08:03
9 EM7 System	10.100.100.13,10.100.100.15,10.100.100.17	em7_ao	System	No	Disabled	em7admin	2014-05-16 17:07:35
10 Cisco Switch	10.0.0.1	em7_ao	Intel	Yes	Disabled	em7admin	2014-05-16 17:07:25
11 SUSE 10	10.100.100.35 - 10.100.100.40	em7_ao	Intel	Yes	Disabled	em7admin	2014-05-16 17:07:14

Creating a Ticket About a Network

From the **IPv4 Networks** page, you can create a ticket about a network (the ticket's element will be the selected network). To do this:

- Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
- In the **IPv4 Networks** page, find the network for which you want to create a ticket.
- Click the ticket icon () for that network.
- The **Ticket Editor** page appears.

5. To create a ticket, supply a value in each field. Click the **[Save]** button to save the new ticket.

The screenshot shows the 'Ticket Editor | New Ticket' interface. At the top, there are tabs for 'Properties', 'Logs', 'Automation', 'Message', and 'Test'. The 'Properties' tab is active, showing a 'Description' field with '(New Ticket)' and an 'Import Template' dropdown set to '(No template)'. Below this, the 'Organization' is set to '[System]' and the 'Element' is 'System'. The 'Ticket Properties' section contains several dropdown menus: 'Ticket Description' (TICKET FOR ORGANIZATION: System | ID: 0), 'Ticket State' (Open), 'Status' (Open), 'Severity' (Sev 4 / Notice), 'Category' (Abuse), 'Source' (Automated), 'Queue' (Asset Management), and 'Assigned User' (em7admin). There is also an 'Example Custom' field. The 'Notes & Attachments' section has a 'Maximize', 'Descending', and 'New Note' button. It contains a rich text editor with a toolbar and a text area that says 'Start typing or drop image here ...'. A 'Save' button is located at the bottom of the form.

Deleting One or More IPv4 Networks

You can delete one or more networks from the **IPv4 Networks** page. When you delete a network, the devices and interfaces associated with the network still remain in SL1 and are unchanged. When you delete a network from the **IPv4 Networks** page, only the information in the **IPv4 Networks** page and related pages is deleted; the network itself and the devices and interfaces are not affected.

To delete one or more networks from the **IPv4 Networks** page:

1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to delete from the page.
3. Select the checkbox () for the network.
4. Repeat steps 2-3 for each network you want to delete.
5. From the **Select Action** field (in the lower right), choose *Delete Monitors*. Click the **[Go]** button.
6. Each selected network will be deleted from the **IPv4 Networks** page.

Chapter



10

Hardware and Software

Overview

The **Device Hardware** page (Devices > Hardware) displays a list of all hardware components discovered by SL1. The list includes hardware components from all devices that have been discovered by SL1. The **Software Titles** page (Devices > Software) displays a list of all software on all devices discovered by SL1. From this page, you can view the list of software titles, generate an Excel report on all discovered software, or generate an exclusion report.

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:

<i>Viewing the List of All Discovered Hardware Components</i>	261
<i>Filtering the List of Hardware Components</i>	262
<i>Generating a Report for Multiple Hardware Components on Multiple Devices</i>	263
<i>Hiding a File System</i>	264
<i>Changing Thresholds for One or More File Systems</i>	266
<i>Viewing the List of All Discovered Software Titles</i>	266
<i>Filtering the List of Software Titles</i>	267
<i>Viewing a List of Software Titles for a Single Device</i>	268
<i>Generating a Report on All Software on All Devices</i>	270
<i>Generating an Exclusion Report for a Single Software Title</i>	273

Viewing the List of All Discovered Hardware Components

The **Device Hardware** page allows you to easily view details on device components and generate reports on device components. The **Device Hardware** page can display information about the following types of components:

- CPU
- Disk
- File system
- Memory
- Virtual Memory
- Components

To view a list of hardware components in the **Device Hardware** page:



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

Device Name	Organization	IP Address	Device Class / Device Subclass	Comp Type	Description	Type	Size	Hidden	Comp ID
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/	Other	10,230 MB	No	27
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/var	Other	6,134 MB	No	28
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/var/log	Other	9,206 MB	No	29
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/var/log/audit	Other	2,038 MB	No	30
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/home	Other	509 MB	No	31
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/tmp	Other	18,422 MB	No	32
10-64-171-130-CDB	East Coast	10.64.171.130	ScienceLogic, Inc EM7 Database	File System	/data.local/ob	Other	803,847 MB	No	33
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/	Other	9,118 MB	No	63
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/var	Other	6,134 MB	No	64
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/var/log	Other	5,110 MB	No	65
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/var/log/audit	Other	2,038 MB	No	66
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/home	Other	509 MB	No	67
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/tmp	Other	2,038 MB	No	68
AA-AIO-33-177	System	192.168.33.177	ScienceLogic, Inc EM7 All-in-One	File System	/data.local/ob	Other	9,122 MB	No	69
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/	Other	10,230 MB	No	207
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/var	Other	6,134 MB	No	208
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/var/log	Other	5,110 MB	No	209
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/var/log/audit	Other	2,038 MB	No	210
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/home	Other	509 MB	No	211
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/tmp	Other	3,960 MB	No	212
esupekar-aio-62	System	10.2.15.62	ScienceLogic, Inc EM7 All-in-One	File System	/data.local/ob	Other	41,404 MB	No	213
Automation-system1-110	System	10.2.15.110	ScienceLogic, Inc EM7 All-in-One	File System	/	Other	10,230 MB	No	532
Automation-system1-110	System	10.2.15.110	ScienceLogic, Inc EM7 All-in-One	File System	/var	Other	6,134 MB	No	534

3. The **Device Hardware** page displays the following for each hardware component:

TIP: To sort the list of hardware, 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 associated with the hardware component.
- **Organization.** Name of the organization associated with the hardware component.

- **IP Address.** IP address of the device or of the hardware component, if applicable.
- **Device-Class / Device Sub-class.** The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during auto-discovery, at the same time as the Category.
- **Comp Type.** Description of the hardware component. The choices are:
 - CPU
 - Disk
 - File system
 - Memory
 - Swap
 - Components
- **Description.** Description of the hardware component.
- **Type.** Further categorization of the hardware component.
- **Size.** If applicable, the size of the hardware component.
- **Hidden.** For file systems, specifies whether or not the component is "hidden", meaning "not monitored" by SL1.
- **Comp ID.** Unique, numeric ID assigned to the component by SL1.
- **Tools.** For each hardware component, one or more of the following tools are available:
 - *Report of all hardware inventory for this device* (). Leads to the **Hardware Profile Report** page, where you can view information about all the hardware and components for a selected 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.
 - *Checkbox* (). Applies the action in the **[Select Actions]** drop-down to the hardware component. To select all the checkboxes, select the check icon above the list of hardware components.

Filtering the List of Hardware Components

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

To filter by parameter, enter text into the desired filter-while-you-type field. The **Device Hardware** page searches for hardware components 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 **Device Hardware** page will display only hardware components that have a matching policy name.
- **Organization.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching organization.
- **IP Address.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching IP address.
- **Device-Class / Device Sub-class.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components from devices that have a matching device class.
- **Comp Type.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching component type. Choices are: *CPU, Disk, File System, Memory, Swap, Components*.
- **Description.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching description.
- **Type.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching sub-type.
- **Size.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching size.
- **Hidden.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching value. This column applies to file systems. Choices are: *Yes, No, and null*.
- **Comp ID.** You can enter text to match, including special characters, and the **Device Hardware** page will display only hardware components that have a matching ID. SL1 automatically assigns this unique, numeric ID to each hardware component.

Generating a Report for Multiple Hardware Components on Multiple Devices

The **Device Hardware** page allows you to generate an Excel report that contains all the information on the **Device Hardware** page. You can immediately view the information or save it to a file for later viewing.

The linked image cannot be displayed. The file may have been moved.

Device Hardware Report
April 17, 2015, 3:53 am

Search Results										
Device	Device ID	IP Address	Device Class	Sub-Class	Component Type	Description	Type	Size (KB)	Hidden	Component ID
MS-2008-SPPND_0.185	50	172.16.0.185	RHEL	Redhat 5.5	0.0				No	161576
MS-2008-SPPND_0.185	50	172.16.0.185	RHEL	Redhat 5.5	0.0				No	161577
MS-2008-SPPND_0.185	50	172.16.0.185	RHEL	Redhat 5.5	0.0				No	161578
MS-2008-SPPND_0.185	50	172.16.0.185	RHEL	Redhat 5.5	0.0				No	161579
MS-2008-SPPND_0.185	50	172.16.0.185	RHEL	Redhat 5.5	0.0				No	478523
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM					No	478717
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM					No	478718
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM			18480772		No	478719
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM					No	478720
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM					No	478721
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM			37046888		No	478722
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM	/data/	Other	89863300		No	478723
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM	/usr	LinuxExt2	4061540		No	478724
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM	/	LinuxExt2	2030736		No	478725
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM	/var	LinuxExt2	6892388		No	478726
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM	/home	LinuxExt2	505604		No	478727
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/	LinuxExt2	24914564		No	478784
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/proc	Other	0	Yes	478785	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/sys	Unknown	0	Yes	478786	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/dev/pts	Unknown	0	Yes	478787	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/common	LinuxExt2	88093440	No	478788	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/dev/shm	Other	2008368	Yes	478789	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/grub	LinuxExt2	256665	No	478790	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/partB	LinuxExt2	25316476	No	478791	
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (BM)	/proc/sys/fs/binfmt_misc	Unknown	0	Yes	478792	

To generate a report on all hardware components in SL1:

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

Device Hardware | Records Found [679]

Report Reset Guide

Device Name	Organization	IP Address	Device Class	Device Subclass	Comp Type	Description	Type	Size	Hidden	Comp ID
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Swap	--	--	--	--	480480
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Swap	--	--	2,371 MB	--	480482
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Memory	--	--	--	--	480484
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	File System	C:\	NTFS	30,618 MB	No	480500
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	CPU	0.0	--	--	--	480479
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Swap	--	--	--	--	480481
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Memory	--	--	--	--	480483
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	Memory	--	--	1,024 MB	--	480485
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	File System	A:\	--	0 MB	Yes	480489
ACME - DB-MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft	MSSQL Server	File System	D:\	FAT	0 MB	Yes	480501
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	CPU	0.0	--	--	--	480486
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Swap	--	--	--	--	480488
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Memory	--	--	--	--	480490
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Memory	--	--	1,024 MB	--	480492
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	File System	A:\	--	9 MB	Yes	480496
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	File System	D:\	FAT	0 MB	Yes	480498
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Swap	--	--	--	--	480487
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Swap	--	--	2,048 MB	--	480489
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	Memory	--	--	--	--	480491
ACME - DB-MSSQL - WebApp	ACME	192.168.32.112	Microsoft	Windows Server 2008 R2	File System	C:\	NTFS	30,618 MB	No	480497
ACME - Middleware Server 1	ACME	172.16.0.164	Linux	Tomcat Server	CPU	0.0	--	--	--	480942
ACME - Middleware Server 1	ACME	172.16.0.164	Linux	Tomcat Server	File System	/	LinuxExt2	995 MB	No	479002
ACME - Middleware Server 1	ACME	172.16.0.164	Linux	Tomcat Server	Swap	--	--	--	--	479026
ACME - Middleware Server 1	ACME	172.16.0.164	Linux	Tomcat Server	Memory	--	--	--	--	479028
ACME - Middleware Server 1	ACME	172.16.0.164	Linux	Tomcat Server	Memory	--	--	2,007 MB	--	479030

3. In the **Device Hardware** page, select the **[Report]** button.
4. When prompted, specify whether you want to save the report to your local computer or open the report immediately.

Hiding a File System

When you hide a file system, SL1 stops collecting information about the file system. When you hide a file system:

- SL1 does not generate events about the file system.
- SL1 does not monitor the file system for thresholds (defined in the **Device Thresholds** and **Global Threshold Settings** pages).
- SL1 does not include the file system in the **Device Summary** page.
- SL1 does not include the file system in file system reports in the **Device Performance** page.

The following rules are applied during discovery to automatically hide file systems:

- If the **NFS Detection Disable** checkbox is selected in the **Behavior Settings** page (System > Settings > Behavior), NFS file systems are automatically hidden during discovery.
- File systems of type "iso9660" are automatically hidden during discovery.
- File systems for which the storage size is not reported or the storage size is less than 1024 KB are automatically hidden during discovery.
- File systems of type "Other" are automatically hidden during discovery.

NOTE: If the type of a discovered file system changes, the auto-hide rules are re-applied to that file system. For example, suppose a Windows drive letter is initially discovered as a removable disk and auto-hidden. If that drive-letter is later re-used for a fixed drive, this change will cause the file system to be automatically un-hidden.

To manually hide one or more file systems:

1. Go to the **Device Hardware** page (Devices > Hardware).
2. Filter the list to display only **Comp Type** of "file system".
3. Select the checkbox for one or more file systems you would like to hide.
4. From the **Select Actions** field (in the lower right), select *Hide File Systems*.
5. Click the **[Go]** button.
6. Each selected file system will be hidden in SL1.

To manually unhide one or more file systems:

1. Go to the **Device Hardware** page (Devices > Hardware).
2. Filter the list to display only **Comp Type** of "file system".
3. Select the checkbox for one or more file systems you would like to unhide.
4. From the **Select Actions** field (in the lower right), select *Unhide File Systems*.
5. Click the **[Go]** button.
6. SL1 will resume collection for each selected file system and will include each selected file system in the **Device Summary** and **Device Performance** pages.

Changing Thresholds for One or More File Systems

From the **Device Hardware** page (Devices > Hardware), you can change the **Major** and **Critical** thresholds for one or more file systems. These thresholds appear on the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds). Changes made to file system thresholds from the **Device Hardware** page update the settings in the **Device Thresholds** page. Changes made to file system thresholds in the **Device Thresholds** page override thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

- **Major Threshold.** This threshold will trigger a "low disk space" event. The default threshold is 85%. When a file system 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, set the threshold to 0% (zero percent). When you disable a threshold, SL1 does not generate an event for the threshold.
- **Critical Threshold.** This threshold will trigger a "low disk space" event. The default threshold is 95%. When a file system 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, set the threshold to 0% (zero percent). When you disable a threshold, SL1 does not generate an event for the threshold.

To change a **Major** file system threshold:

1. Find the file system for which you want to change the Major threshold. Select its checkbox .
2. Select the checkbox for each additional file system for which you want to change the Major threshold.
3. In the **Select Action** drop-down list, find *Change Major Threshold* and select a new threshold (between 0 - 100).
4. Select the **[Go]** button.
5. SL1 will change the Major threshold for each selected file system.

To change a **Critical** file system threshold:

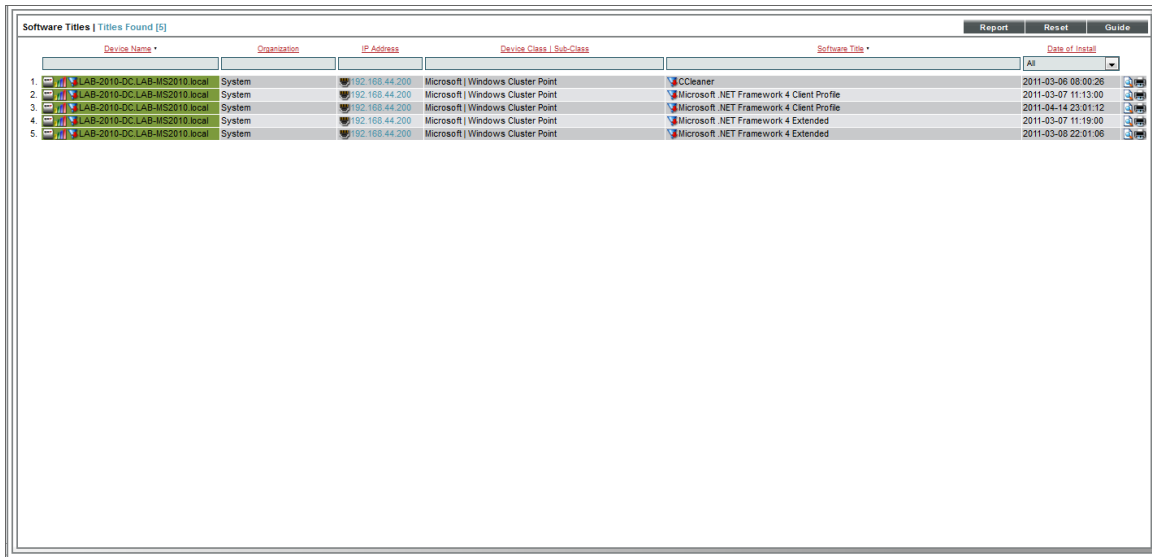
1. Find the file system for which you want to change the Critical threshold. Select its checkbox .
2. Select the checkbox for each additional file system for which you want to change the Critical threshold.
3. In the **Select Action** drop-down list, find *Change Critical Threshold* and select a new threshold (between 0 - 100).
4. Select the **[Go]** button.
5. SL1 will change the Critical threshold for each selected file system.

Viewing the List of All Discovered Software Titles

The **Software Titles** page displays a list of all software on all devices discovered by SL1. From this page, you can view the list of software titles, generate an Excel report on all discovered software, or generate an exclusion report (that is, a report for a single software title that specifies devices where the software is installed and devices where the software is not installed.)

To view a list of all software discovered on all devices:

1. Go to the **Software Titles** page (Devices > Software).



The screenshot shows a web interface titled "Software Titles | Titles Found [5]". It features a table with columns for Device Name, Organization, IP Address, Device Class / Sub-Class, Software Title, and Date of Install. The table contains five rows of data, all for devices with IP address 192.168.44.200. The software titles listed are CCleaner, Microsoft .NET Framework 4 Client Profile, Microsoft .NET Framework 4 Extended, and Microsoft .NET Framework 4 Client Profile.

Device Name	Organization	IP Address	Device Class / Sub-Class	Software Title	Date of Install
LAB-2010-DC.LAB-HIS2010.local	System	192.168.44.200	Microsoft Windows Cluster Point	CCleaner	2011-03-06 09:00:26
LAB-2010-DC.LAB-HIS2010.local	System	192.168.44.200	Microsoft Windows Cluster Point	Microsoft .NET Framework 4 Client Profile	2011-03-07 11:13:00
LAB-2010-DC.LAB-HIS2010.local	System	192.168.44.200	Microsoft Windows Cluster Point	Microsoft .NET Framework 4 Client Profile	2011-04-14 23:01:12
LAB-2010-DC.LAB-HIS2010.local	System	192.168.44.200	Microsoft Windows Cluster Point	Microsoft .NET Framework 4 Extended	2011-03-07 11:19:00
LAB-2010-DC.LAB-HIS2010.local	System	192.168.44.200	Microsoft Windows Cluster Point	Microsoft .NET Framework 4 Extended	2011-03-06 22:01:08

2. The **Software Titles** page displays the following about each installed software title:

TIP: To sort the list of software, 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 where the software title is installed. 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.
- **Organization.** Organization associated with the software.
- **IP Address.** IP address of the device where the software is installed.
- **Device Class / Sub-Class.** The manufacturer (device class) and type of device (sub-class). The Device Class/Sub-Class is automatically assigned during auto-discovery.
- **Software Title.** Name of the software.
- **Date of Install.** Date the software was installed.

Filtering the List of Software Titles

You can filter the list on the **Software Titles** page by one or more parameters. Only software titles that meet all the filter criteria will be displayed in the **Software Titles** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Software Titles** page searches for software titles 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 (comma, ampersand, and exclamation mark), and the **Software Titles** page will display only software titles installed on a matching device name.
- **Organization.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Software Titles** page will display only software titles that have a matching organization.
- **IP Address.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Software Titles** page will display only software titles installed on a device with a matching IP address.
- **Device Class.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Software Titles** page will display only software titles installed on devices with a matching device class.
- **Software Title.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Software Titles** page will display only software titles that have a matching name.
- **Date of Install.** Only those software titles that match all the previously selected fields and have the specified install date will be displayed. The choices are:
 - *All.* Display software titles with all installed dates.
 - *Last Minute.* Display only software titles that have been installed within the last minute.
 - *Last Hour.* Display only software titles that have been installed within the last hour.
 - *Last Day.* Display only software titles that have been installed within the last day.
 - *Last Week.* Display only software titles that have been installed within the last week.
 - *Last Month.* Display only software titles that have been installed within the last month.
 - *Last Year.* Display only software titles that have been installed within the last year.

Viewing a List of Software Titles for a Single Device


The **Software Packages** page displays a list of all the software installed on the device. If possible, the installation date is also displayed.

To view the list of software installed on a single device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device for which you want to view the list of installed software. Select the bar graph icon () for that device.

Device Manager (Devices Found [1293])													Actions	Report	Reset	Guide
Device Name	Device Hostname	IP Address	Device Gateway	Device Class / Sub-class	DIG	Orientation	Current State	Collection Status	Collection State	SNMP Credentials	SNMP Access					
1	10.100.100.40	10.100.100.40	Pingable	Ping / ICMP	274	System	Healthy	CUG	User-Disabled	--	--					
2	10.100.100.46	10.100.100.46	Pingable	FreeBSD / ICMP	294	Johto	Healthy	CUG	User-Disabled	--	--					
3	10.7.11.188	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2					
4	10.7.11.186	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2					
5	10.7.11.188	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2226	System	Notice	CUG	Active	SNMP Public V2	V2					
6	10.7.11.186.5951	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1430	System	Healthy	CUG	Active	SNMP Public V2	V2					
7	10.7.11.186.8222	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1204	System	Healthy	CUG	Active	SNMP Public V2	V2					
8	10.7.11.186.7706	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1951	System	Healthy	CUG	Active	SNMP Public V2	V2					
9	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2					
10	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2					
11	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2					
12	10.7.11.187.4289	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1952	System	Healthy	CUG	Active	SNMP Public V2	V2					
13	10.7.11.187.5996	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1206	System	Healthy	CUG	Active	SNMP Public V2	V2					
14	10.7.11.187.5080	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1431	System	Healthy	CUG	Active	SNMP Public V2	V2					
15	10.7.11.188	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2080	System	Healthy	CUG	Active	SNMP Public V2	V2					
16	10.7.11.188	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2					
17	10.7.11.188.8992	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	3658	System	Notice	CUG	Active	SNMP Public V2	V2					
18	10.7.11.188.8992	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	2102	System	Healthy	CUG	Active	SNMP Public V2	V2					
19	10.7.11.188.7340	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1391	System	Healthy	CUG	Active	SNMP Public V2	V2					
20	10.7.11.188.7881	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	855	System	Healthy	CUG	Active	SNMP Public V2	V2					
21	10.7.11.237	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2					
22	10.7.11.237.7659	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1423	System	Healthy	CUG	Active	SNMP Public V2	V2					
23	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2633	System	Notice	CUG	Active	SNMP Public V2	V2					
24	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2					
25	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2					
26	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2					
27	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2651	System	Healthy	CUG	Active	SNMP Public V2	V2					
28	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2					
29	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2					
30	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2					
31	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2					
32	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2652	System	Healthy	CUG	Active	SNMP Public V2	V2					
33	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2					
34	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2					
35	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2					
36	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2					
37	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2					
38	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2					
39	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2					
40	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2					
41	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2					
42	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2					
43	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2					

3. In the **Device Reports** panel, select the **Software** tab. The **Software Packages** page appears.

Close	Summary	Performance	Topology	Configs	Journals	Interfaces		
Logs	Events	Tickets	Software	Processes	Services	TCP Ports	Organization	
Device Name	224371-58.lou01.hosting.com			Managed Type	Physical Device			
IP Address / ID	10.20.0.250 106			Category	Network Application			
Class	F5 Networks, Inc.			Sub-Class	BIG-IP 1600			
Organization	System			Uptime	355 days, 23:43:20			
Collection Mode	Active			Collection Time	2014-06-16 14:25:00			
Description	Linux 224371-58.lou01.hosting.com 2.6.18-164.11.1.eIS.1.0.f5app #1			Group / Collector	CUG2 em7_cu2			
Device Hostname								
								
Software Packages Packages Found [483]								
Filter:							Guide	Refresh
Software Package Name							Install Date	
1.	acctd-10.2.4-577.0						--	
2.	aceagentsdk-6.1-577.0						--	
3.	aced-10.2.4-577.0						--	
4.	alertd-10.2.4-577.0						--	
5.	alertd-config-10.2.4-577.0						--	
6.	anacron-2.3-45.eIS.17.0						--	
7.	aom-firmware-1.4-10.1.10.100.6.0						--	
8.	aom-software-1.0.F5-10.1.10.100.6.0						--	
9.	apache_auth_token_mod-10.2.4-577.0						--	
10.	apd-10.2.4-577.0						--	
11.	apr-1.2.7-11.1.17.0						--	
12.	apr-util-1.2.7-7.eIS_3.2.17.0						--	
13.	audit-1.7.13-2.eIS_3.17.0						--	
14.	audit-libs-1.7.13-2.eIS_3.17.0						--	
15.	audit-libs-python-1.7.13-2.eIS_3.17.0						--	
16.	audit_forwarder-10.2.4-577.0						--	
17.	auto-letshop-app-10.2.4-577.0						--	
18.	basesystem-8.0-5.1.1.eIS.17.0						--	
19.	bash-3.2-24.eIS.17.0						--	
20.	bcm56xxd-10.2.4-591.0						--	
21.	bcm56xxd-modules-5.9.3-577.0						--	
22.	bdeccrypt-4.1.2-10.1.1.17.0						--	
23.	bigd-10.2.4-577.0						--	
24.	bigdb-10.2.4-577.0						--	
25.	bigdbd-10.2.4-577.0						--	
26.	bigstart-10.2.4-577.0						--	
27.	bigtop-10.2.4-577.0						--	
28.	bind-9.6.4.ESV.R5.P6-577.0						--	
29.	bind-utils-9.6.4.ESV.R5.P6-577.0						--	
30.	binutils-2.17.50.0.6.12.eIS.17.0						--	

4. For each installed software title, the **Software Packages** page displays the following information:

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

Filtering the List of Software

You can filter the list of software titles in the **Software Packages** page. The list dynamically updates as you enter the regular expression to use as a filter.

- In the **Filter** field, you must enter a regular expression. SL1 will search for software package names that match the regular expression. You can use the following special characters in each filter:
 - * Match zero or more characters preceding the asterisk. For example:
"dell*" would match "dell", "dell2650", "dell7250" and "dell1700N".
"*dell*" would match "mydell", "dell", "dell2650", "dell7250" and "dell1700N".
 - % Match zero or more characters preceding the percent. This special character behaves in the same way as the asterisk.

Generating a Report on All Software on All Devices

From the **Software Titles** page (Devices > Software) you can generate a report on all, multiple, or a single software title in SL1. The report will contain all the information displayed in the **Software Titles** page.

Software Titles Report generated by banderton on 2015-04-17 03:50:56						
Devices that have [Array] installed						
	Device Name	Organization	IP Address	Device Class Sub-Class	Software Title	Date of Install
0	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	BOINC	2012-10-05 05:52:20
1	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft Application Error Reporting	2012-10-03 17:49:50
2	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
3	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
4	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Native Client	2012-10-04 07:04:48
5	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 RsFx Driver	2012-10-04 07:08:14
6	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Setup (English)	2012-10-03 17:54:38
7	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 Setup Support Files	2012-10-04 07:06:10
8	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server System CLR Types (x64)	2012-10-04 07:04:56
9	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server VSS Writer	2012-10-04 07:04:54
10	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:06
11	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:12
12	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:46
13	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:30
14	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:07:34
15	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:06:20
16	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:38
17	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:32
18	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:06:30
19	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:07:40
20	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:44
21	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:04
22	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:08
23	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:00
24	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Sql Server Customer Experience Improvement	2012-10-04 07:04:56
25	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft Application Error Reporting	2012-10-03 17:49:50
26	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
27	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
28	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 Native Client	2012-10-04 07:04:48
29	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 RsFx Driver	2012-10-04 07:08:14
30	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 Setup (English)	2012-10-03 17:54:38
31	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 Setup Support Files	2012-10-04 07:06:10
32	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server System CLR Types (x64)	2012-10-04 07:04:56
33	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server VSS Writer	2012-10-04 07:04:54
34	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:06
35	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:12
36	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:46

To generate a report on all or multiple software titles in SL1:

1. Go to the **Software Titles** page (Devices > Software).

- In the **Software Titles** page, select the **[Report]** button.

Software Titles | Titles Found [6331]

Device Name	Organization	IP Address	Device Class Sub-Class	Software Title	Date of Install	
1	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	BONIC	2012-10-05 05:52:20
2	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft Application Error Reporting	2012-10-03 17:49:50
3	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
4	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
5	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Native Client	2012-10-04 07:04:48
6	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 RsFx Driver	2012-10-04 07:08:14
7	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Setup (English)	2012-10-03 17:54:36
8	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 Setup Support Files	2012-10-04 07:05:10
9	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server System CLR Types (x64)	2012-10-04 07:04:56
10	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server VSS Writer	2012-10-04 07:04:54
11	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:06
12	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:12
13	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:46
14	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:30
15	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:07:24
16	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:06:20
17	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:38
18	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:32
19	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:06:30
20	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:07:40
21	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:44
22	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:04
23	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:08
24	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:00
25	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Sql Server Customer Experience Improvement Program	2012-10-04 07:04:56

NOTE: If you want to include only certain software titles in the report, use the "find while you type" fields at the top of each column. You can filter the list by one or more column headings. You can then select the **[Report]** button, and only the software titles displayed in the **Software Titles** page will appear in the report.

- The **Export current view as a report** modal page appears.

Export current view as a report

Output Format: Comma-separated values (.csv)

Force browser to save to disk

Generate

- In the **Export current view as a report** page, you must select the format in which SL1 will generate the report. Your choices are:
 - Comma-separated values (.csv)
 - Web page (.html)
 - OpenDocument Spreadsheet (.ods)
 - Excel spreadsheet (.xlsx)
 - Acrobat document (.pdf)
- Select the **[Generate]** button. The report will contain all the information displayed in the **Software Titles** page. You can immediately view the report or save it to a file for later viewing.

Generating an Exclusion Report for a Single Software Title

From the **Software Titles** page you can generate Software Exclusion Reports. These reports can help administrators manage patches and software versions. Software Exclusions Reports are generated in .XLSX format.

Software Exclusion Report generated by banderton on 2015-04-17 03:45:57		
Report Summary [Microsoft SQL Server 2008 R2 (64-bit)]		
Total Devices		102
Unique Device Categories		3
Unique Device Classes		1
Titles Found		6
Titles Not Found		96

Software Exclusion Report generated by banderton on 2015-04-17 03:45:57						
Devices that have [Microsoft SQL Server 2008 R2 (64-bit)] installed						
	Device Name	Organization	IP Address	Device Class Sub-Class	Software Title	Date of Install
0	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
1	ACME - DB MSSQL 2 - W\ACME		192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
2	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
3	ACME - DB-MSSQL - W\ACME		192.168.32.112	Microsoft Windows Server 2008 R2	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
4	DEMO-SP-01	HQ Data Center	192.168.41.108	Microsoft Windows Server 2012	Microsoft SQL Server 2008 R2 (64-bit)	2014-12-17 05:01:44
5	DEMO-SP-01	HQ Data Center	192.168.41.108	Microsoft Windows Server 2012	Microsoft SQL Server 2008 R2 (64-bit)	2014-12-17 05:01:44

Software Exclusion Report generated by banderton on 2015-04-17 03:45:57						
Devices that do not have [Microsoft SQL Server 2008 R2 (64-bit)] installed						
	Device Name	Organization	IP Address	Device Class Sub-Class	Software Title	Date of Install
0	ACME - WEB IIS 2 - W\ACME		192.168.32.110	Microsoft Windows Server 2008 R2	BOINC	2012-10-05 07:01:42
1	ACME - WEB-IIS-1 - W\ACME		192.168.32.111	Microsoft Windows Server 2008 R2	BOINC	2012-10-05 10:06:00
2	DEMO-AP-01.demo.scie	HQ Data Center	192.168.41.107	Microsoft Windows Server 2012	None	--
3	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft Help Viewer 1.1	2014-08-28 14:07:48
4	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft SQL Server 2012 (64-bit)	2014-08-28 14:10:16
5	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft SQL Server 2012 (64-bit)	2014-08-28 14:10:16
6	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft SQL Server 2012 Native Client	2014-08-28 14:10:18
7	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft SQL Server 2012 Transact-SQL Com	2014-08-28 14:10:26
8	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft Visual C++ 2010 x64 Redistributable	2014-08-27 12:48:54
9	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Microsoft VSS Writer for SQL Server 2012	2014-08-28 14:10:30
10	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	None	2014-08-28 14:10:02
11	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	Service Pack 2 for SQL Server 2012 (KB29584	2014-09-12 10:21:34
12	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Common Files	2014-08-28 14:15:50
13	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Common Files	2014-08-28 14:13:10
14	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Data quality client	2014-08-28 14:15:54
15	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Data quality service	2014-08-28 14:16:44
16	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Data quality service	2014-08-28 14:16:46
17	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Data quality service	2014-09-12 10:12:04
18	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Database Engine Services	2014-08-28 14:16:30
19	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Database Engine Services	2014-09-12 10:11:22
20	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Database Engine Shared	2014-08-28 14:16:20
21	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Distributed Replay	2014-08-28 14:15:48
22	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Distributed Replay	2014-08-28 14:15:46
23	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Full text search	2014-08-28 14:16:42
24	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Integration Services	2014-08-28 14:15:56
25	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Integration Services	2014-08-28 14:15:30
26	DEMO-SQL-01.demo.scie	HQ Data Center	192.168.41.109	Microsoft Windows Server 2012	SQL Server 2012 Management Studio	2014-08-28 14:19:58

A Software Exclusions Report displays the following:

- Name of the software title and the date the report was generated.
- List of all devices in SL1 that have the software installed.
- List of all devices in SL1 that don't have the software installed. SL1 includes only appropriate servers in this report. For example, Solaris servers would not appear in a report for a Windows 2000 patch.
- The last row in the report displays:
 - Total number of devices in report.

- Total number of device categories included in the report.
- Total number of device classes included in the report.
- Number of devices where software is installed.
- Number of devices where software is not installed.

To generate a software exclusion report:

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

Device Name	Organization	IP Address	Device Class Sub-Class	Software Title	Date of Install
1 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	BOINC	2012-10-05 05:52:20
2 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft Application Error Reporting	2012-10-03 17:49:50
3 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
4 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 (64-bit)	2012-10-04 07:06:20
5 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Native Client	2012-10-04 07:04:48
6 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 RsFx Driver	2012-10-04 07:06:14
7 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 R2 Setup (English)	2012-10-03 17:54:36
8 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server 2008 Setup Support Files	2012-10-04 07:06:10
9 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server System CLR Types (x64)	2012-10-04 07:04:56
10 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Microsoft SQL Server VSS Writer	2012-10-04 07:04:54
11 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:06
12 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Analysis Services	2012-10-04 07:08:12
13 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:46
14 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Client Tools	2012-10-04 07:07:30
15 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:07:34
16 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Common Files	2012-10-04 07:06:20
17 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:38
18 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Services	2012-10-04 07:08:32
19 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:06:30
20 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Database Engine Shared	2012-10-04 07:07:40
21 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:44
22 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Management Studio	2012-10-04 07:07:04
23 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:06
24 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server 2008 R2 Reporting Services	2012-10-04 07:11:00
25 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Sqj Server Customer Experience Improvement Program	2012-10-04 07:04:56

2. In the **Software Titles** page, find an instance of the software title you want to generate an exclusion report for. Select its printer icon (🖨️)
3. You will be prompted to save or view the generated report.



Chapter

11

Device Logs

Overview

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 Logs for a Device	275
Viewing Events Associated with a Log Entry	277
Creating an Event Policy from a Log Entry	278
Viewing Logs for All Devices	279

Viewing Logs for a Device


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

To access the **Device Logs & Messages** page 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 view the device logs. Select its wrench icon (.

Device Name	Device Hostname	IP Address	Device Category	Device Class / Subclass	CID	Organization	Current State	Collocated Device	Collocation State	SNMP Credentials	SNMP Version	Report	Reset	Guide
1	10.100.100.40	--	Pingable	FreeBSD / ICMP	274	System	Healthy	CUG	User-Disabled	--	--			
2	10.100.100.46	--	Pingable	FreeBSD / ICMP	294	System	Healthy	CUG	User-Disabled	--	--			
3	10.100.7.11.188	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2			
4	10.100.7.11.188	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2			
5	10.100.7.11.188	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2			
6	10.100.7.11.188.5651	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1430	System	Healthy	CUG	Active	SNMP Public V2	V2				
7	10.100.7.11.188.5922	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1204	System	Healthy	CUG	Active	SNMP Public V2	V2				
8	10.100.7.11.188.7705	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1951	System	Healthy	CUG	Active	SNMP Public V2	V2				
9	10.100.7.11.187	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2			
10	10.100.7.11.187	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2			
11	10.100.7.11.187	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2840	System	Healthy	CUG	Active	SNMP Public V2	V2			
12	10.100.7.11.187.2309	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1952	System	Healthy	CUG	Active	SNMP Public V2	V2				
13	10.100.7.11.187.5995	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1206	System	Healthy	CUG	Active	SNMP Public V2	V2				
14	10.100.7.11.187.5995	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1431	System	Healthy	CUG	Active	SNMP Public V2	V2				
15	10.100.7.11.189	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2080	System	Healthy	CUG	Active	SNMP Public V2	V2			
16	10.100.7.11.189	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2002	System	Notice	CUG	Active	SNMP Public V2	V2			
17	10.100.7.11.189	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2			
18	10.100.7.11.189.6952	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 2122	System	Healthy	CUG	Active	SNMP Public V2	V2				
19	10.100.7.11.189.7340	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1931	System	Healthy	CUG	Active	SNMP Public V2	V2				
20	10.100.7.11.189.7881	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 855	System	Healthy	CUG	Active	SNMP Public V2	V2				
21	10.100.7.11.237	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3032	System	Notice	CUG	Active	SNMP Public V2	V2			
22	10.100.7.11.237.7639	--	Network App	F5 Networks, Inc. BIG-IP LTM Pool Mem 1423	System	Healthy	CUG	Active	SNMP Public V2	V2				
23	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2			
24	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2179	System	Healthy	CUG	Active	SNMP Public V2	V2			
25	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2138	System	Healthy	CUG	Active	SNMP Public V2	V2			
26	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2			
27	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2081	System	Healthy	CUG	Active	SNMP Public V2	V2			
28	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2			
29	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2			
30	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2			
31	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2			
32	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2062	System	Healthy	CUG	Active	SNMP Public V2	V2			
33	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2			
34	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2			
35	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2079	System	Notice	CUG	Active	SNMP Public V2	V2			
36	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2			
37	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2			
38	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2			
39	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2368	System	Healthy	CUG	Active	SNMP Public V2	V2			
40	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2			
41	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2454	System	Notice	CUG	Active	SNMP Public V2	V2			
42	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	3208	System	Healthy	CUG	Active	SNMP Public V2	V2			
43	10.100.7.12.125	--	Network App	F5 Networks, Inc. BIG-IP LTM Node	2386	System	Notice	CUG	Active	SNMP Public V2	V2			

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

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes																														
<p>Device Name: storeboard-rest-prd.nike.net_80 ID: 418 Class: F5 Networks, Inc. Organization: System Root Device: lb440d.ussac1 Parent Device: BIG-IP LTM Service Device Hostname: </p>					<p>Managed Type: Component Device Category: Network Application Sub-Class: BIG-IP LTM Virtual Server Uptime: 0 days, 00:00:00 Group / Collector: CUG em7_ao</p>																																					
<p>Device Logs & Messages Messages Found [5]</p> <p>[Search All Messages] where Message is like [Search]</p> <table border="1"> <thead> <tr> <th>Date Time</th> <th>Source</th> <th>Event ID</th> <th>Priority</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>2014-10-09 18:00:52</td> <td>Internal</td> <td>38964</td> <td>--</td> <td>New child component device found: storeboard-rest-prd.nike.net_8080 (Class: F5 Networks, Inc. BIG-IP LTM Pool)</td> </tr> <tr> <td>2014-10-09 17:56:08</td> <td>Internal</td> <td>--</td> <td>--</td> <td>Component device record created (Class: F5 Networks, Inc. BIG-IP LTM Virtual Server) F5 Networks, Inc. BIG-IP LTM Virtual Server</td> </tr> <tr> <td>2014-10-09 17:56:08</td> <td>Internal</td> <td>38148</td> <td>--</td> <td>Added dynamic application for device: BIG-IP: LTM: Virtual Server Configuration</td> </tr> <tr> <td>2014-10-09 17:56:08</td> <td>Internal</td> <td>38149</td> <td>--</td> <td>Added dynamic application for device: BIG-IP: LTM: Virtual Server Performance</td> </tr> <tr> <td>2014-10-09 17:56:08</td> <td>Internal</td> <td>38150</td> <td>--</td> <td>Added dynamic application for device: BIG-IP: LTM: Virtual Server Pool Discovery</td> </tr> </tbody> </table>													Date Time	Source	Event ID	Priority	Message	2014-10-09 18:00:52	Internal	38964	--	New child component device found: storeboard-rest-prd.nike.net_8080 (Class: F5 Networks, Inc. BIG-IP LTM Pool)	2014-10-09 17:56:08	Internal	--	--	Component device record created (Class: F5 Networks, Inc. BIG-IP LTM Virtual Server) F5 Networks, Inc. BIG-IP LTM Virtual Server	2014-10-09 17:56:08	Internal	38148	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Configuration	2014-10-09 17:56:08	Internal	38149	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Performance	2014-10-09 17:56:08	Internal	38150	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Pool Discovery
Date Time	Source	Event ID	Priority	Message																																						
2014-10-09 18:00:52	Internal	38964	--	New child component device found: storeboard-rest-prd.nike.net_8080 (Class: F5 Networks, Inc. BIG-IP LTM Pool)																																						
2014-10-09 17:56:08	Internal	--	--	Component device record created (Class: F5 Networks, Inc. BIG-IP LTM Virtual Server) F5 Networks, Inc. BIG-IP LTM Virtual Server																																						
2014-10-09 17:56:08	Internal	38148	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Configuration																																						
2014-10-09 17:56:08	Internal	38149	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Performance																																						
2014-10-09 17:56:08	Internal	38150	--	Added dynamic application for device: BIG-IP: LTM: Virtual Server Pool Discovery																																						


4. The **Device Logs & Messages** page displays the following about each log entry:

- **Date Time.** The date and time the entry was made in the log.
- **Source.** The entity or process that generated the message.

- *Syslog*. Entry was generated from standard system log generated by device.
- *Internal*. Entry was generated by SL1.
- *Trap*. Entry was generated by an SNMP trap.
- *Dynamic*. Entry was generated by a Dynamic Application.
- *API*. Entry was generated by another application.
- *Email*. Entry was generated by an email message from a third-party application to SL1.
- **Event ID**. If an event was created, a unique event ID, generated by SL1. If the log entry is not associated with an event, no ID appears in this column.
- **Priority**. If applicable, specifies the priority of the syslog message.
 - *Info*. An error occurred.
 - *Notice*. An error has not occurred. Entry denotes normal system activity.
 - *N / A*. Not applicable. Entry was not generated by syslog.
- **Message**. Text of the log entry, color coded to match event severity (if applicable).

Viewing Events Associated with a Log Entry

From the **Device Logs & Messages** page you can view the event generated by each log entry. To do so:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device whose log you want to view. Select its wrench icon ()
3. In the **Device Administration** panel, select the Logs tab.

Close	Properties	Thresholds	Collections	Monitors	Tickets	Redirects	Notes
Schedule	Logs	Toolbox	Interfaces	Relationships			
Device Name	10.7.12.125:5391	Managed Type	Component Device				
ID	1606	Category	Network.Application				
Class	F5 Networks, Inc.	Sub-Class	BIG-IP LTM Pool Member				
Organization	System	Uptime	0 days, 00:00:00				
Root Device	lb440d.ussac1	Group / Collector	CUG em7_a0				
Parent Device	ori-niketown.nike.com_8013						
Device Hostname							

Device Logs & Messages Messages Found [31]					Actions	Reset	Guide
[Search All Messages] where Message is like					Search		
Date Time	Source	Event ID	Priority	Message			
1. 2014-10-20 17:11:29	Dynamic	54443	--	BIG-IP: LTM: Pool Member State: Not Available (message repeats 167 times)			
2. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaBytesOut (id: 4248)			
3. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaCurConns (id: 4249)			
4. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaPktsIn (id: 4250)			
5. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaPktsOut (id: 4251)			
6. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaTotConns (id: 4252)			
7. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerBytesIn (id: 4253)			
8. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerBytesOut (id: 4254)			
9. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerCurConns (id: 4255)			
10. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerPktsIn (id: 4256)			
11. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerPktsOut (id: 4257)			
12. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerTotConns (id: 4258)			
13. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatTotPvaAssistConn (id: 4259)			
14. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatTotRequests (id: 4260)			
15. 2014-10-13 15:01:50	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatServerMaxConns (id: 4261)			
16. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatConnqAgeEdm (id: 4238)			
17. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatConnqAgeEma (id: 4239)			
18. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatConnqAgeHead (id: 4240)			
19. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatConnqDepth (id: 4241)			
20. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatConnqServiced (id: 4242)			
21. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatCurrentConnsPerSec (id: 4243)			
22. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatCurrPvaAssistConn (id: 4244)			
23. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatCurSessions (id: 4245)			
24. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatDurationRateExceeded (id: 4246)			
25. 2014-10-13 15:01:49	Internal	53321	--	Dynamic app. object collection disabled: BIG-IP: LTM: Pool Member Performance - ItmPoolMemberStatPvaBytesIn (id: 4247)			
26. 2014-10-13 10:27:06	Internal	50868	--	New child component device found: 10.7.12.125 (Class: F5 Networks, Inc. BIG-IP LTM Node)			

- In the **Device Logs & Messages** page, find the log entry you are interested in. Select its event icon ().
- The **Viewing Events** page appears for the device and displays the event associated with the selected log entry. For details on events, see the manual **Events**.

Creating an Event Policy from a Log Entry

From the **Device Logs & Messages** page, you can create a new event policy based on a log entry. If a log entry does not have an event policy already associated with it, the pencil icon () will appear next to the entry. You can click on this icon to create a new event policy. After you create an event policy, each time this log entry is generated for a device, SL1 will trigger an event in the **Events** page.


For devices on which the SL1 agent is installed, you can also define a Log File Monitoring policy. Log File Monitoring policies specify the log files the agent should monitor, as well as the log files the agent should send to the platform. You can define event policies to trigger an event based on Log File Monitoring policies. For more information about Log File Monitoring policies, see the Monitoring Using the Agent manual.

To create an event policy from a log entry:

- Go to the **Device Manager** page (Devices > Device Manager).
- In the **Device Manager** page, find the device whose log you want to view. Select its wrench icon ().

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

Date Time	Source	Event ID	Priority	Message
2014-10-21 11:21:47	Trap	--	--	Trap Received (No name found for this Trap OID) Trap Detail: (Trap OID: .1.2.3.4.5.6)
2014-10-21 11:20:04	Dynamic	6806	--	Physical Memory has exceeded threshold: (80%) currently (84%)
2014-10-21 11:15:04	Dynamic	6806	--	Physical Memory has exceeded threshold: (80%) currently (90%) (message repeats 2 times)
2014-10-21 11:00:09	Dynamic	--	--	Physical Memory has exceeded threshold: (80%) currently (85%)
2014-10-21 10:56:16	Internal	--	--	Completed application discovery on device
2014-10-21 10:56:16	Internal	--	--	Completed TCP/IP port scan
2014-10-21 10:56:16	Internal	--	--	Completed scan for SSL certificates
2014-10-21 10:56:16	Internal	--	--	Completed IP address classification
2014-10-21 10:56:16	Internal	--	--	Completed detailed discovery session
2014-10-21 10:55:51	Internal	--	--	Started detailed discovery session (message repeats 1 time)
2014-10-21 10:55:15	Dynamic	--	--	Physical Memory has exceeded threshold: (80%) currently (83%)
2014-10-21 10:55:02	Internal	--	--	Completed IP address classification
2014-10-21 10:55:02	Internal	--	--	Completed detailed discovery session
2014-10-21 10:55:01	Internal	6795	--	Added dynamic application for device: EM7: System Performance
2014-10-21 10:55:01	Internal	6796	--	Added dynamic application for device: EM7: Event Statistics
2014-10-21 10:55:01	Internal	6797	--	Added dynamic application for device: Net-SNMP: CPU
2014-10-21 10:55:01	Internal	6798	--	Added dynamic application for device: Net-SNMP: Physical Memory
2014-10-21 10:55:01	Internal	6799	--	Added dynamic application for device: Net-SNMP: Swap
2014-10-21 10:55:01	Internal	6800	--	Added dynamic application for device: EM7: Asset Information
2014-10-21 10:55:01	Internal	6801	--	Added dynamic application for device: Host Resource: CPU Config
2014-10-21 10:55:01	Internal	6802	--	Added dynamic application for device: Host Resource: Memory Config
2014-10-21 10:55:01	Internal	6803	--	Added dynamic application for device: Support: File System
2014-10-21 10:55:01	Internal	--	--	Completed application discovery on device
2014-10-21 10:55:01	Internal	--	--	Completed TCP/IP port scan
2014-10-21 10:55:01	Internal	--	--	Completed scan for SSL certificates
2014-10-21 10:54:47	Internal	--	--	Device record created (Class: ScienceLogic, Inc. EM7 All-In-One) ScienceLogic, Inc. EM7 All-In-One

4. In the **Device Logs & Messages** page, find the log entry from which you want to create an event policy. Select its pencil icon ()
5. The **Event Policy Editor** page appears, with some of the fields automatically populated with values from the selected log entry. For details on defining event policies, see the manual **Events**.

Viewing Logs for All Devices

The **Audit Logs** page (System > Monitor > Audit Logs) displays a list of all actions that have occurred on all devices.

For details on the **Audit Logs** page, see the manual **System Administration**.

Chapter

12

Device Relationships

Overview of 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.

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 Relationships	281
Filtering the List of Device Relationships	284
Viewing the Relationships for a Single Device	285
The Device View Page	287
Event Correlation	288
Defining Device Relationships	289
Device Categories that Don't Support Parent-Child Devices	290
Events that May Not Be Displayed in the Events Page	291
Defining Event Correlation	291
Layer-2 Topology Collection	294
CDP Topology Collection	295
LLDP Topology Collection	296
Layer-3 Topology Collection	298

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	Child IP	Child Interface	Child Phys Addr	Child IF Manufacturer	Parent	Parent Interface	Parent IF Alias	Parent Phys Addr	Parent IF Manufacturer	Type
Topology Device 3	10.40.40.6	HP Network T 00:09:97:c0:e2:99		NortelNetw	Topology Switch 0	Fab010	--	00:00:b1:1b:9d:2c	Sonicwall	Layer 2
Topology Device 4	10.40.40.7	HP Network T 00:0a:08:ab:65:51		SipuraTech	Topology Switch 0	Fab011	--	00:00:b1:1b:9d:2d	Sonicwall	Layer 2
Topology Switch 0	--	Fab012	00:00:b1:1b:9d:04	Sonicwall	Topology Switch 0	V1.1	--	00:00:00:01:3c:33	Heidelberg	Layer 2

- **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 the Relationships 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.

Device Relationships Relationships Found (3)										Trace	Reset	Guide
Child	Child IP	Child Interface	Child Phys Addr	Child IF Manufacturer	Parent	Parent Interface	Parent IF Alias	Parent Phys Addr	Parent IF Manufacturer	Type		
1. Topology Device 3	10.40.40.6	HP Network T	00:09:97:c0:a2:99	NortelNetw	Topology Switch B	Fa0/10	--	00:06:b1:1b:9d:2c	Sonicwall	Layer 2		
2. Topology Device 4	10.40.40.7	HP Network T	00:0e:00:aa:05:51	SiguroTech	Topology Switch B	Fa0/11	--	00:06:b1:1b:9d:2d	Sonicwall	Layer 2		
3. Topology Switch B	--	Fa0/12	00:06:b1:1b:9d:2e	Sonicwall	Topology Switch A	VL1	--	00:50:80:81:3c:33	TandbergTe	Layer 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:

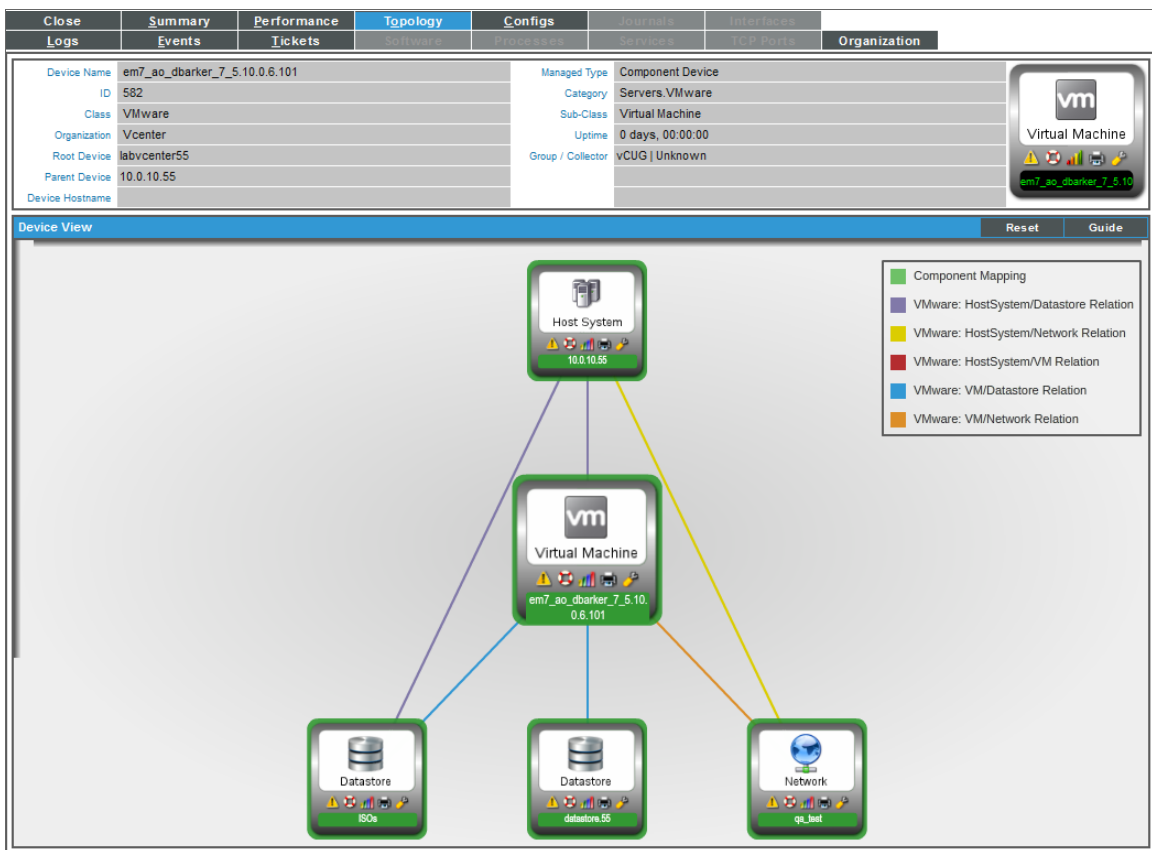
- **Type of relationship.** Possible values are:
 - *Layer 2.* Layer-2 devices and their clients.
 - *Layer 3.* Layer-3 devices and layer-2 devices.
 - *VMware.* Hypervisors and their virtual machines.
 - *CDP.* Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as 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**.

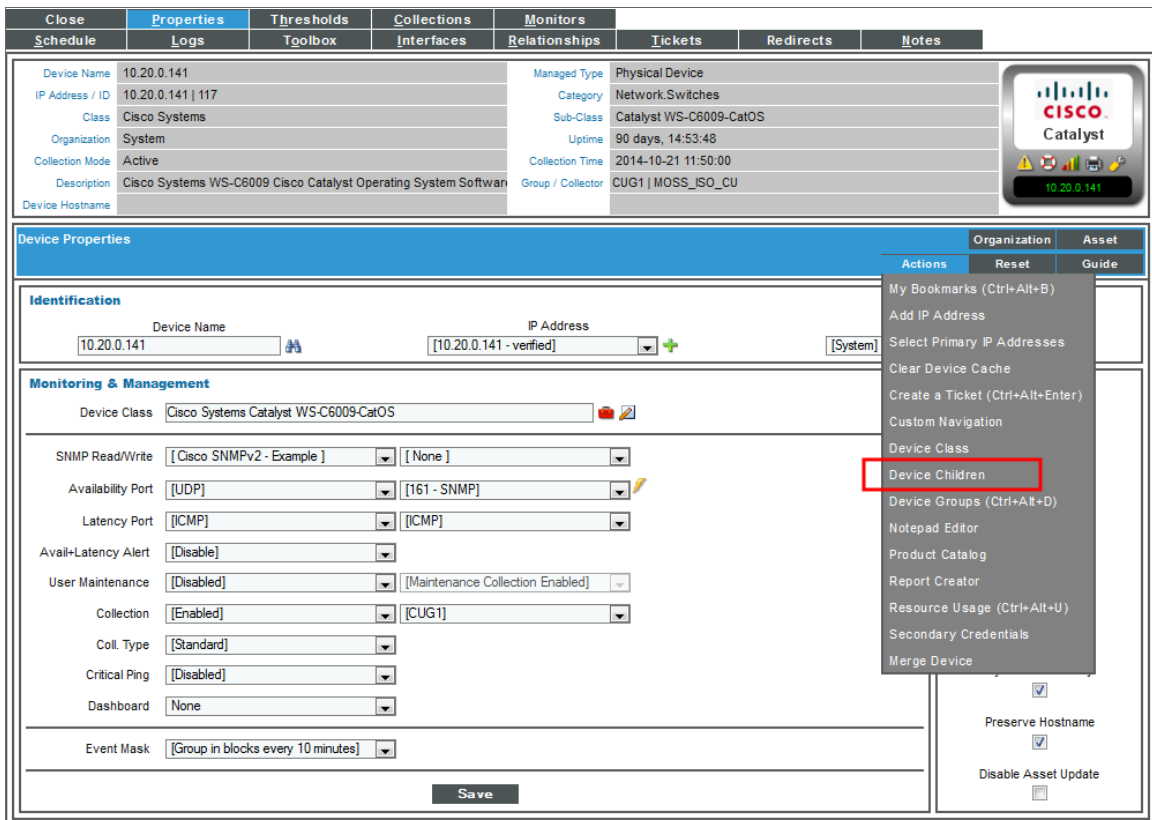
Defining Device Relationships

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:

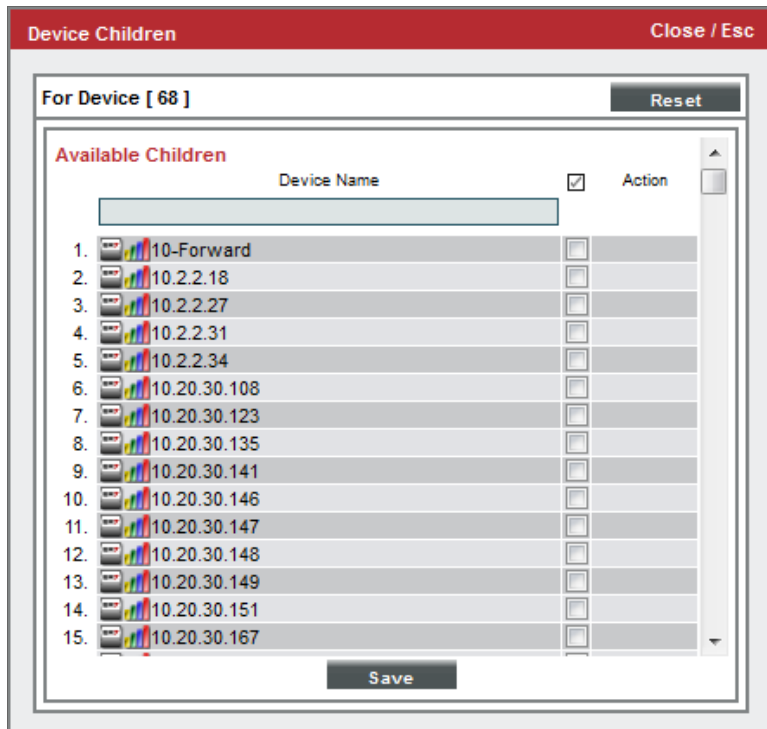
1. Go to the **Device Manager** page (Devices > Device Manager).
2. In the **Device Manager** page, find the device for which you want to add children devices. Select the wrench icon (🔧) for that device.
3. The **Device Properties** page appears:

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, you must define two types of events:

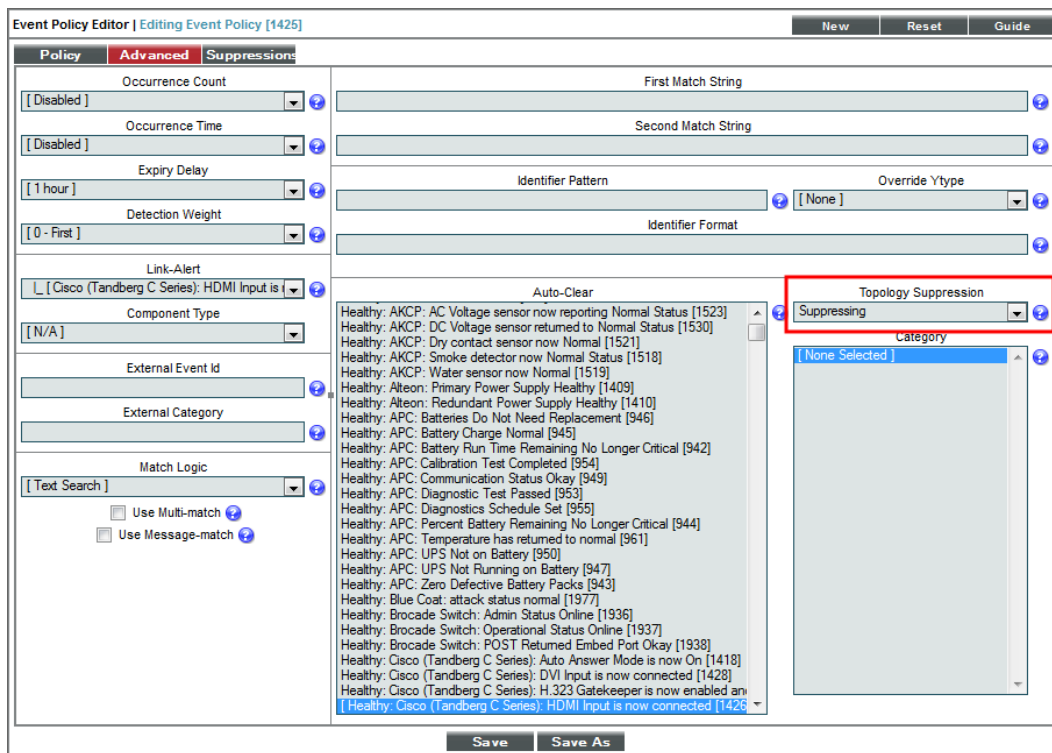
- **Suppressing events.** If this event occurs on a parent device, SL1 will search all related children devices for **suppressible** events. On the children devices, all suppressible events will be suppressed. Only the suppressing event will appear in the **Events** page. The suppressible events will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

- **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:

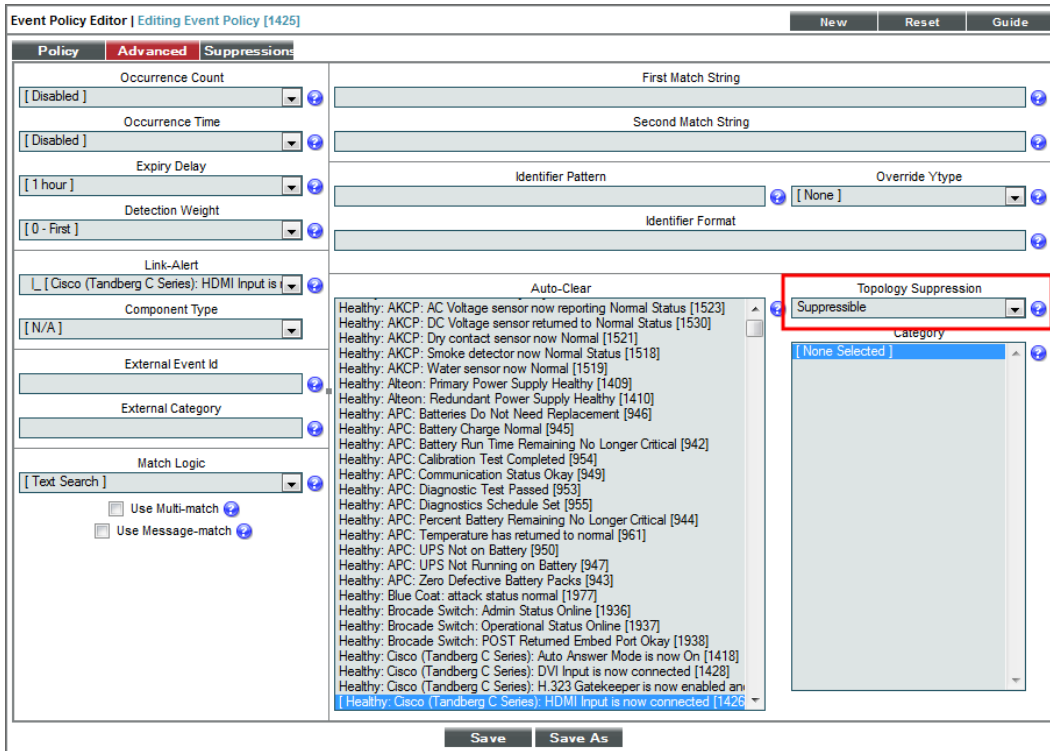
1. Go to the **Event Policy Manager** page (Events > Event Policies).
2. On the **Event Policy Manager** page, select the wrench icon (🔧) of the event that you want to define as the **suppressing** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]**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

1. Go to the **Event Policy Manager** page (Events > Event Policies).
2. On the **Event Policy Manager** page, select 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, select 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, 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.

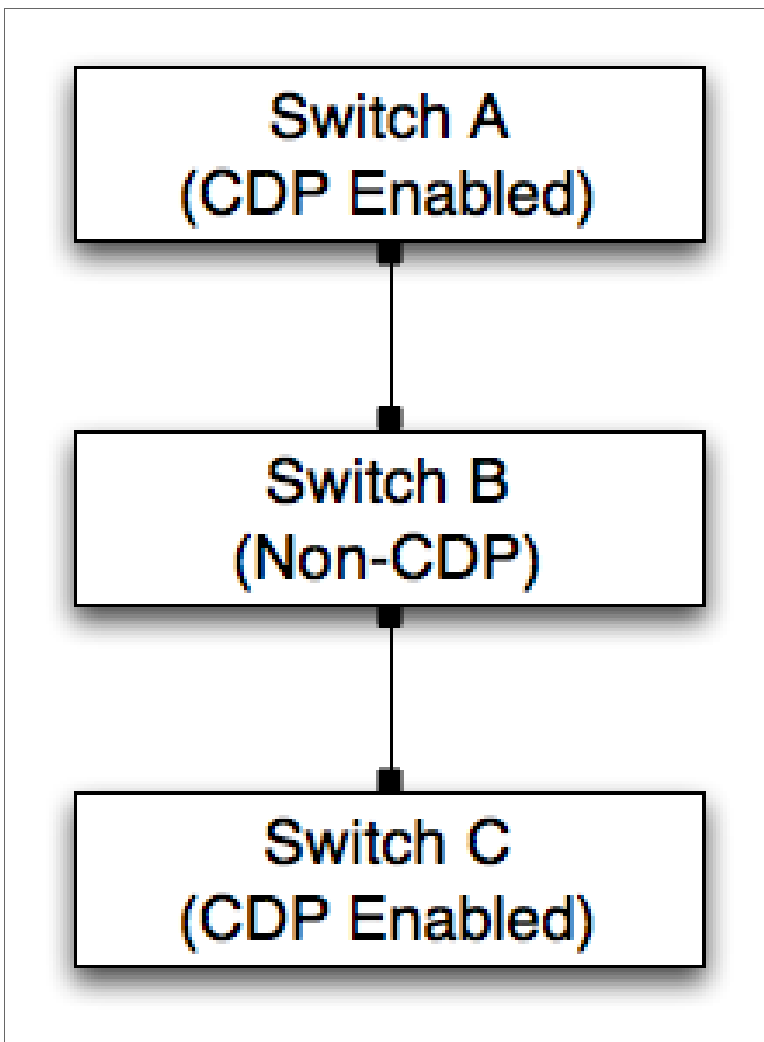
The information collected from the Bridge-MIB does not explicitly indicate which devices are directly connected to a network switch or bridge; switches and bridges will report forwarding information for MAC addresses that are several network hops away from the switch or bridge. A second "crunch" process 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.

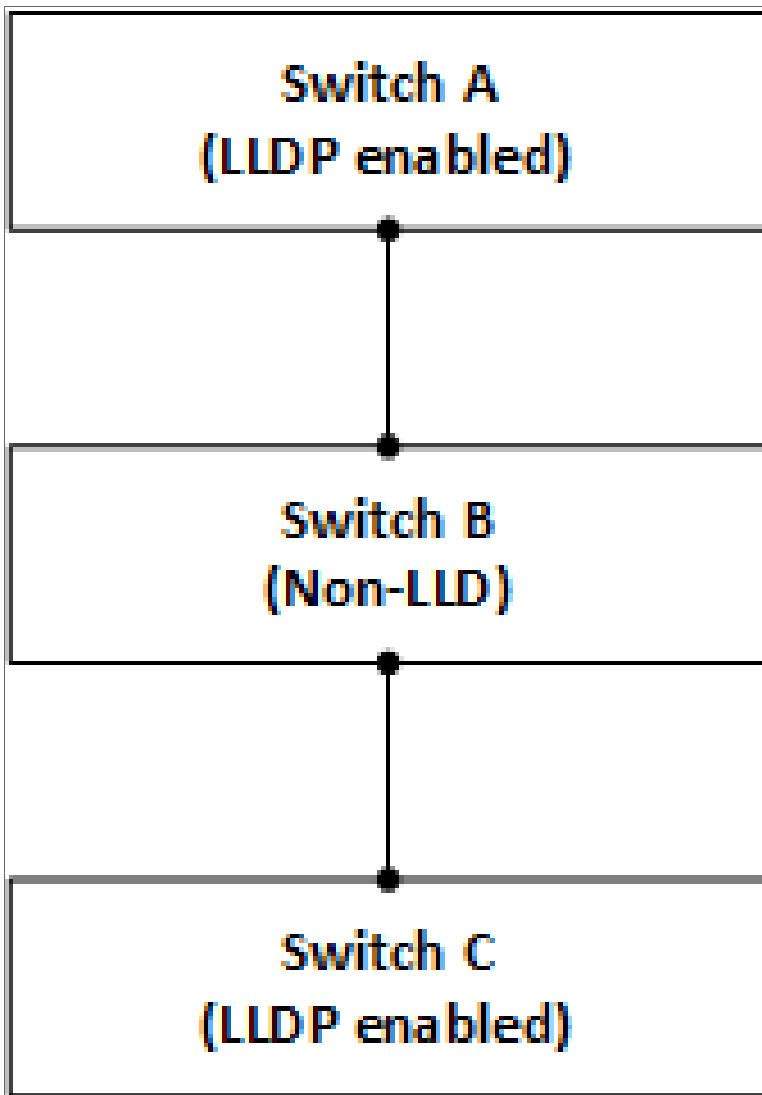
To view CDP maps, go to the **Subnet Map (CDP)** page (Views > Topology Maps > CDP). For details on viewing CDP maps, see the **Views** manual.

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

13

SSL Certificates

Overview

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:

<i>Monitoring SSL Certificates</i>	300
<i>System Settings that Affect SSL Certificates in the ScienceLogic Platform</i>	301
<i>Viewing the List of SSL Certificates</i>	302
<i>Filtering the List of SSL Certificates</i>	304

Monitoring SSL Certificates

Secure Sockets Layer (SSL) is a cryptographic protocol that provide security and data integrity for communications over TCP/IP networks such as the Internet. SSL allows client/server applications to communicate across a network in a way that prevents eavesdropping, tampering, and message forgery.

SSL uses certificates to verify communication and encrypt message. The certificate issuer (also known as the certificate authority or CA) is an organization that issues digital certificates (digital IDs). These digital IDs (called keys) authenticate the identity of people and organizations over a public system such as the Internet. These keys also allow senders and receivers to encrypt messages and un-encrypt replies.

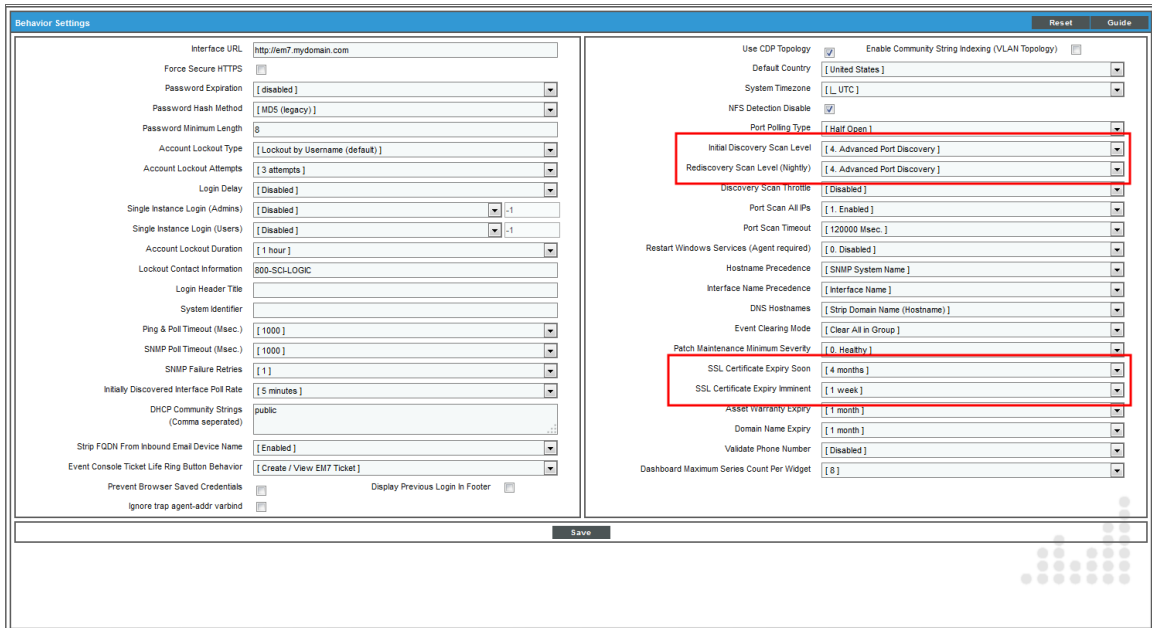
During discovery and nightly auto-discovery, SL1 can search for all SSL certificates. If you specify a discovery level and/or a rediscovery level of "3" or greater (in the **Behavior Settings** page), SL1 will then collect information about each discovered SSL certificate. You can specify values in the **Asset & SSL Certificate Expiry fields** (also in the **Behavior Settings** page), and SL1 will generate the following events to remind you when an SSL certificate is about to expire or has expired:

- SSL Certificate due to expire soon. This event will be launched at the time specified in the **Behavior Settings** page, in the **SSL Certificate Expiry Soon** field.
- SSL Certificate due to expire imminently. This event will be launched at the time specified in the **Behavior Settings** page, in the **SSL Certificate Expiry Imminent** field.
- SSL certificate has expired.
- SSL certificate has been renewed. This event will be launched when an SSL certificate has been renewed.

In the **SSL Certificate Monitoring** page (Registry > Monitors > SSL Certificates) you can view a list of all discovered SSL certificates and their expiration dates.

System Settings that Affect SSL Certificates in the ScienceLogic Platform

In the **Behavior Settings** page (System > Settings > Behavior), the following settings affect how SL1 monitors SSL Certificates:



- **Initial Discovery Scan Level.** Specifies the data to be gathered during the discovery session. The options are:

- *0. Model Device Only*. Discovery tool will discover if 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.
- *1. Initial Population of Apps*. Discovery tool will search for Dynamic Applications to associate with the device. Discovery will also perform "0. Model Device Only" discovery.
- *2. Discover SSL Certificates*. Discovery tool will search for SSL certificates and retrieve SSL data. Discovery tool will also perform "1. Initial Population of Apps", and "0. Model Device Only".
- *3. Discover Open Ports*. Discovery tool will search for open ports. Discovery tool will also perform "2. Discover SSL Certificates", "1. Initial Population of Apps", and "0. Model Device Only".

NOTE: If your system includes a firewall and you select option 4, discovery may be blocked and/or may be taxing to your network.

- *4. Advanced Port Discovery*. Discovery tool will search for open ports, using a faster TCP/IP connection method. Discovery tool will also perform "2. Discover SSL Certificates", "1. Initial Population of Apps", and "0. Model Device Only".
- *5. Deep discovery*. Discovery tool will perform advanced OS/service fingerprinting on detected open ports.

NOTE: If your system includes a firewall and you select option 4, some auto-discovered devices may 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.

- **Rediscovery Scan Level (Nightly)**. Specifies the data to be gathered/updated each night during the rediscovery process. The Rediscovery process will find any changes to previously discovered devices and will also find any new devices added to the network. The options are the same as those described for **Initial Discovery Scan Level**.
- **SSL Certificate Expiry Soon**. Specifies when SL1 should notify the user that the SSL Certificate is about to expire soon. The choices range from 1 day to 9 months. When the time between the current date and the expiry date of an SSL Certificate is less than the selected value, SL1 will generate an event with a severity of *Minor*. The event message will say "SSL certificate due to expire soon." When you renew the certificate, SL1 will generate a healthy event which will clear the outstanding SSL expiration event(s).
- **SSL Certificate Expiry Imminent**. Specifies when SL1 should send a more urgent notification to the user that the SSL Certificate is about to expire imminently. The choices range from 1 day to 9 months. When the time between the current date and the expiry date of an SSL Certificate is less than the selected value, SL1 will generate an event with a severity of *Major*. The event message will say "SSL certificate due to expire imminently." When you renew the certificate, SL1 will generate a healthy event which will clear the outstanding SSL expiration event(s).

Viewing the List of SSL Certificates

To view the list of discovered SSL certificates:

1. Go to the **SSL Certificate Monitoring** page (Registry > Monitors > SSL Certificates).
2. The **SSL Certificate Monitoring** page displays a list of all SSL Certificates discovered by SL1.

	Certificate Organization	Expiration Date	Cert ID	Device Name	IP Address	Device Category	Organization
1	ScienceLogic, Inc.	2024-08-10 21:34:38	295	em7_ap_100	10.0.9.100	System	Hoenn
2	ScienceLogic, Inc.	2024-07-04 14:18:32	293	2pov2_em7_db	10.0.9.91	System	Hoenn
3	ScienceLogic, Inc.	2024-07-02 21:13:38	292	em7_db	10.0.9.90	System	Hoenn
4	ScienceLogic, Inc.	2024-04-15 21:40:43	291	Snthl_AJO	10.0.9.93	System	Hoenn
5	ScienceLogic, Inc.	2024-08-07 15:54:19	289	Global_Manager_AJO	10.0.9.92	System	Hoenn
6	ScienceLogic, Inc.	2024-07-21 23:12:38	280	em7_ap_89	10.0.9.89	System	Hoenn
7	ScienceLogic, LLC.	2018-07-03 01:35:10	282	em7_db	10.0.9.92	System	Hoenn
8	ScienceLogic, LLC.	2018-07-03 01:35:10	105	em7_73db_mysql	192.168.33.50	System	System
9	ScienceLogic, LLC.	2018-07-03 01:35:10	31	--	--	--	--
10	ScienceLogic, LLC.	2018-07-03 01:35:10	30	--	--	--	--
11	ScienceLogic, LLC.	2018-07-03 01:35:10	17	--	--	--	--
12	ScienceLogic, LLC.	2018-07-03 01:35:10	16	--	--	--	--
13	SomeOrganization	2015-07-10 16:25:07	172	10.100.100.40	10.100.100.40	Pingable	System
14	VMware Installer	2022-04-12 07:24:07	190	10.100.100.46	10.100.100.46	Pingable	John
15	VMware Installer	2025-09-22 14:45:08	13	--	--	--	--
16	VMware Installer	2024-11-15 12:30:55	12	--	--	--	--
17	VMware, Inc.	2023-06-23 20:10:58	18	--	--	--	--

3. For each discovered SSL certificate, the **SSL Certificate Monitoring** page displays the following information:

TIP: To sort the list of SSL certificates, 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 **Expiration Date** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- **Certificate Organization.** Name of the certificate issuer. If the certificate does not include this information, this field will display "Not Specified".
- **Expiration Date.** Date and time at which the SSL certificate expires. To continue to use the SSL certificate, you must renew it before this date and time.
- **Cert ID.** Unique, numeric ID, assigned to the monitoring policy automatically by SL1.
- **Device Name.** Name of the device associated with the SSL certificate.
- **IP Address.** IP address of the device associated with the SSL certificate. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the SSL certificate.
- **Organization.** Organization for the device associated with the SSL certificate.

Filtering the List of SSL Certificates

You can filter the list on the **SSL Certificate Monitoring** page by one or more parameters. Only SSL certificates that meet all the filter criteria will be displayed in the **SSL Certificate Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **SSL Certificate Monitoring** page searches for SSL certificates 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:

- **Certificate Organization**. The organization that issued the certificate. This is sometimes called a Certificate Authority.
- **Expiration Date**. Only those SSL certificates that have the specified expiration date will be displayed. The choices are:
 - *All*. Display all SSL certificates that match the other filters.
 - *Past*. Display only SSL certificates that have already expired.
 - *Next Week*. Display only SSL certificates that will expire within the next week.
 - *Next Month*. Display only SSL certificates that will expire within the next month.
 - *Next Six Months*. Display only SSL certificates that will expire within the next six months.
 - *Next Year*. Display only SSL certificates that will expire within the next year.
- **Cert ID**. You can enter text to match, including special characters, and the **SSL Certificate Monitoring** page will display only SSL certificates that have a matching cert ID.
- **Device Name**. You can enter text to match, including special characters, and the **SSL Certificate Monitoring** page will display only SSL certificates aligned with a device with a matching device name.
- **IP Address**. You can enter text to match, including special characters, and the **SSL Certificate Monitoring** page will display only SSL certificates aligned with a device with a matching IP address.
- **Device Category**. You can enter text to match, including special characters, and the **SSL Certificate Monitoring** page will display only SSL certificates aligned with a device with a matching device category.
- **Organization**. You can enter text to match, including special characters, and the **SSL Certificate Monitoring** page will display only SSL certificates that have a matching organization.

Chapter

14

Device Processes

Overview

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

There are two methods for monitoring processes:

- For devices monitored using SNMP, SL1 automatically collects a list of all processes running every two hours.
- For devices monitored using the SL1 agent, SL1 automatically collects a list of all processes running every five minutes.

SL1 allows you to create policies that monitor system processes every five minutes:

- If a device is not monitored using the SL1 agent, the policy collection is performed using SNMP.
- If a device is monitored using the SL1 agent, the policy collection is performed by the agent.

For each monitored process, you can create a policy that specifies:

- Whether or not to generate an event if the process is running.
- How much memory each instance of a process can use.
- How many instances of a process can run simultaneously.
- If policy collection is performed by the agent, how much memory all instances of a process can use in total.
- If policy collection is performed by the agent, how much CPU all instances of a process can use in total.

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:

<i>Viewing the List of Device Processes</i>	306
<i>Filtering the List of Device Processes</i>	308
<i>Viewing a List of System Processes on a Single Device</i>	309
<i>Generating a Report on Multiple System Processes</i>	311
<i>Generating an Exclusion Report for a Single System Process</i>	313
<i>Viewing the System Process Monitoring Policies</i>	315
<i>Filtering the List of System Process Monitoring Policies</i>	315
<i>Defining a Monitoring Policy for a System Process</i>	316
<i>Editing a Monitoring Policy for a System Process</i>	319
<i>Executing a System Process Monitoring Policy</i>	320
<i>Example Policy for System Process</i>	321
<i>Viewing Reports for a System Process Policy</i>	321
<i>Deleting a System Process Monitoring Policy</i>	321

Viewing the List of Device Processes

The **Device Processes** page displays a list of all processes discovered by SL1 on all devices.

To view the list of all processes running on all discovered devices:

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

NOTE: Run states are defined by a device's operating system and/or installed agents. Run states may differ between devices.

- **Monitored.** Specifies whether or not SL1 monitors the process:
 - Yes. SL1 currently monitors this process.
 - No. SL1 does not currently monitor this process.

Filtering the List of Device Processes

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

To filter by parameter, enter text into the desired filter-while-you-type field. The **Device Processes** page searches for processes 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 (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching device name.
- **Organization.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching organization.
- **IP Address.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching IP address.
- **Device Class.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching device class.
- **Process.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching process name.
- **PID.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching process ID.
- **Memory.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching amount of memory currently used/reserved for the process.

- **Run State.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching run state.
- **Monitored.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Device Processes** page will display only processes that have a matching monitoring status.

Viewing a List of System Processes on a Single Device

The **System Processes** page displays a list of all of the processes that are running on a single device. The **System Processes** page displays a combined list of processes collected via SNMP and the agent, where applicable.

To view the list of processes on a single device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device where you want to view the list of processes. Select the bar graph icon () for that device.

Device Manager Devices Found (1293)											Actions		Report	Reset	Guide	
Device Name	Device Hostname	IP Address	Device Category	Device Class / Sub-class	OID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version					
1	10.100.100.40	10.100.100.40	Pingable	Ping ICMP	274	System	Healthy	CUG	User-Disabled	--	--					
2	10.100.100.40	10.100.100.40	Pingable	FreeSO1 CIMP	294	System	Healthy	CUG	User-Disabled	--	--					
3	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2					
4	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2					
5	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2					
6	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1430	System	Healthy	CUG	Active	SNMP Public V2	V2					
7	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1204	System	Healthy	CUG	Active	SNMP Public V2	V2					
8	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1951	System	Healthy	CUG	Active	SNMP Public V2	V2					
9	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2					
10	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2					
11	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2					
12	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1952	System	Healthy	CUG	Active	SNMP Public V2	V2					
13	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1206	System	Healthy	CUG	Active	SNMP Public V2	V2					
14	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1431	System	Healthy	CUG	Active	SNMP Public V2	V2					
15	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2688	System	Healthy	CUG	Active	SNMP Public V2	V2					
16	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2902	System	Notice	CUG	Active	SNMP Public V2	V2					
17	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2					
18	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	2102	System	Healthy	CUG	Active	SNMP Public V2	V2					
19	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1391	System	Healthy	CUG	Active	SNMP Public V2	V2					
20	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	655	System	Healthy	CUG	Active	SNMP Public V2	V2					
21	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2					
22	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Pool Mem1	1423	System	Healthy	CUG	Active	SNMP Public V2	V2					
23	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2					
24	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2					
25	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2196	System	Healthy	CUG	Active	SNMP Public V2	V2					
26	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2					
27	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2					
28	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2					
29	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2					
30	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2					
31	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2					
32	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2662	System	Healthy	CUG	Active	SNMP Public V2	V2					
33	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2					
34	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2					
35	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2					
36	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2					
37	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2					
38	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2					
39	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2					
40	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2					
41	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2					
42	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2					
43	10.7.12.125	--	Network App F5 Networks, Inc.	IGP-PLTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2					

3. In the **Device Reports** panel, select the Processes tab. The **System Processes** page appears.

Process	Argument(s)	Path / User	PID	Memory	Run State	Monitored
1. "aio/0"	--	"/aio/0"	170	0 kB	Runnable	No
2. "aio/1"	--	"/aio/1"	171	0 kB	Runnable	No
3. "alertd"	"-f"	"/usr/sbin/alertd"	3531	6332 kB	Runnable	No
4. "ata/0"	--	"/ata/0"	329	0 kB	Runnable	No
5. "ata/1"	--	"/ata/1"	330	0 kB	Runnable	No
6. "ata_aux"	--	"/ata_aux"	331	0 kB	Runnable	No
7. "audispd"	--	"/sbin/audispd"	2949	568 kB	Runnable	No
8. "audtd"	--	"/audtd"	2947	700 kB	Runnable	No
9. "audt_forwarder"	--	"/usr/bin/audt_forwarder"	2174	9232 kB	Runnable	No
10. "bash"	--	"/bash"	28070	1448 kB	Runnable	No
11. "bcm56xxd"	"-f"	"/usr/bin/bcm56xxd"	3481	34340 kB	Runnable	No
12. "big3d"	--	"/shared/bin/big3d"	3498	2228 kB	Runnable	No
13. "bigd"	--	"/usr/bin/bigd"	3513	30260 kB	Runnable	No
14. "bigpipe"	"shell"	"/bigpipe"	28213	11388 kB	Runnable	No
15. "cbrd"	"--threads=2 --host-memory=134217728 --umu_threshold=90 --pending_trans=5000 --"	"/usr/share/cbr/bin/cbrd"	3518	10548 kB	Runnable	No
16. "chmand"	"-f"	"/usr/bin/chmand"	3492	9052 kB	Runnable	No
17. "cqueue/0"	--	"/cqueue/0"	107	0 kB	Runnable	No
18. "cqueue/1"	--	"/cqueue/1"	108	0 kB	Runnable	No
19. "crond"	--	"/crond"	3283	924 kB	Runnable	No
20. "cssd"	"-f"	"/usr/bin/cssd"	3457	1584 kB	Runnable	No
21. "csyncd"	--	"/usr/bin/csyncd"	3476	8828 kB	Runnable	No
22. "eventd"	"-f"	"/usr/bin/eventd"	3533	4528 kB	Runnable	No
23. "events/0"	--	"/events/0"	8	0 kB	Runnable	No
24. "events/1"	--	"/events/1"	9	0 kB	Runnable	No
25. "fpdd"	--	"/usr/bin/fpdd"	3489	9236 kB	Runnable	No

4. For each process, the **System Processes** page displays the following information:

TIP: To sort the list of processes, 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.

- **Process.** The name of the process. A single process name can have multiple entries.
- **Argument(s).** The arguments with which the process was invoked.
- **Path/User.** The path where the process executable resides. The value in this field varies, depending on the device's operating system and installed agents.
- **PID.** A unique ID for the process. The device's operating system assigns this value.
- **Memory.** The amount of memory currently being used/reserved for the process.
- **Run State.** The current state of the process. This can be one of the following:
 - *Runnable.* Process is ready to run as needed.
 - *Running.* Process is currently running.

- *Not Running*. Process is in a "waiting" state.
- *Invalid*. Process is part of an operation that failed. Process was not ended gracefully.

NOTE: Run states are defined by a device's operating system and/or installed agents. Run states may differ between devices.

- **Monitored**. Specifies whether or not SL1 is monitoring this process.

Generating a Report on Multiple System Processes

From the **Device Processes** page (Devices > Processes) you can generate a report on all, multiple, or a single process in SL1.

The report will contain all the columns displayed in the **Device Processes** page (Devices > Processes).

Device Processes Report generated by banderton on 2015-04-17 03:47:25

Device Name	Organization	IP Address	Device Class Sub-Class	Process	PID	Memory	Run State	Monitored
0. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	boinc.exe	2140	4952 kB	Running	No
1. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	boincmgr.exe	2888	5850 kB	Running	No
2. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	conhost.exe	2668	116 kB	Running	No
3. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	csrss.exe	296	680 kB	Running	No
4. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	csrss.exe	348	664 kB	Running	No
5. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	csrss.exe	1220	544 kB	Running	No
6. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	dwm.exe	1040	284 kB	Running	No
7. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	explorer.exe	2648	3200 kB	Running	No
8. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	LogonUI.exe	704	6576 kB	Running	No
9. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	lsass.exe	452	5148 kB	Running	No
10. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	lsm.exe	464	1920 kB	Running	No
11. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	msdtc.exe	2432	156 kB	Running	No
12. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	msmdsrv.exe	1080	6320 kB	Running	No
13. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	rdpclip.exe	2084	352 kB	Running	No
14. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	ReportingServicesService.exe	1140	64212 kB	Running	No
15. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	services.exe	444	4760 kB	Running	No
16. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	smss.exe	216	80 kB	Running	No
17. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	snmp.exe	1460	3624 kB	Running	No
18. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	spoolsv.exe	272	1148 kB	Running	No
19. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	sppsvc.exe	2496	2992 kB	Running	No
20. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	sqlservr.exe	1052	36984 kB	Running	No
21. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	sqlwriter.exe	1484	88 kB	Running	No
22. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	552	3072 kB	Running	No
23. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	824	3628 kB	Running	No
24. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	712	6388 kB	Running	No
25. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	764	19972 kB	Running	No
26. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	804	5296 kB	Running	No
27. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	844	1176 kB	Running	No
28. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	884	6140 kB	Running	No
29. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	980	3496 kB	Running	No
30. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	1108	80 kB	Running	No
31. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	1832	2632 kB	Running	No
32. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	1864	108 kB	Running	No
33. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	svchost.exe	2248	100 kB	Running	No
34. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	System	4	48 kB	Running	No
35. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	System Idle Process	1	24 kB	Running	No
36. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	taskhost.exe	2704	3304 kB	Running	No
37. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	wininit.exe	368	80 kB	Running	No
38. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	winlogon.exe	384	280 kB	Running	No
39. ACME - DB-MSSQL-2 - WebACME		192.168.32.113	Microsoft MSSQL Server	winlogon.exe	1664	80 kB	Running	No
40. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	csrss.exe	296	844 kB	Running	No
41. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	csrss.exe	348	452 kB	Running	No
42. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	csrss.exe	1676	564 kB	Running	No
43. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	dwm.exe	2272	512 kB	Running	No
44. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	explorer.exe	2340	4080 kB	Running	No
45. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	LogonUI.exe	704	1592 kB	Running	No
46. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	lsass.exe	452	6460 kB	Running	No
47. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	lsm.exe	460	2156 kB	Running	No
48. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	msdtc.exe	1276	1516 kB	Running	No
49. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	msmdsrv.exe	1128	7260 kB	Running	No
50. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	Oobe.exe	2472	17408 kB	Running	No
51. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	rdpclip.exe	536	560 kB	Running	No
52. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	services.exe	444	5864 kB	Running	No
53. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	smss.exe	216	316 kB	Running	No
54. ACME - DB-MSSQL - WebACME		192.168.32.112	Microsoft Windows Server 2008 R2	snmp.exe	1408	3916 kB	Running	No

Page 1

To generate a report on all or multiple device processes in SL1:

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

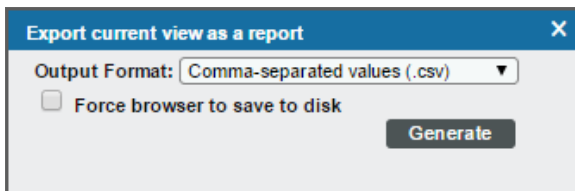
2. In the **Device Processes** page, select the **[Report]** button.

The screenshot shows the 'Device Processes' page with a table of processes. The 'Report' button is highlighted in a red box in the top right corner. The table has the following columns: Device Name, Organization, IP Address, Device Class | Sub-Class, Process, PID, Memory, Run State, and Monitored. The table contains 25 rows of data, each representing a process running on a device.

Device Name	Organization	IP Address	Device Class Sub-Class	Process	PID	Memory	Run State	Monitored
1. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	boinc.exe	2140	4952 kB	Running	No
2. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	boincmgr.exe	2888	5860 kB	Running	No
3. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	conhost.exe	2688	116 kB	Running	No
4. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	296	680 kB	Running	No
5. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	348	664 kB	Running	No
6. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	1220	544 kB	Running	No
7. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	dim.exe	1040	284 kB	Running	No
8. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	explorer.exe	2648	3200 kB	Running	No
9. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	LogonUI.exe	704	6576 kB	Running	No
10. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	lsass.exe	452	5148 kB	Running	No
11. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	lsm.exe	464	1920 kB	Running	No
12. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	msdtc.exe	2432	156 kB	Running	No
13. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	msmsdsv.exe	1080	6320 kB	Running	No
14. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	rdpclip.exe	2084	352 kB	Running	No
15. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	ReportingServicesService.exe	1140	64212 kB	Running	No
16. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	services.exe	444	4760 kB	Running	No
17. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	smss.exe	216	80 kB	Running	No
18. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	snmp.exe	1460	3624 kB	Running	No
19. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	spoolv.exe	272	1148 kB	Running	No
20. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	sppsvc.exe	2496	2992 kB	Running	No
21. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	sqlservr.exe	1052	36884 kB	Running	No
22. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	sqlwriter.exe	1484	88 kB	Running	No
23. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	552	3072 kB	Running	No
24. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	624	3628 kB	Running	No
25. ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	712	6388 kB	Running	No

NOTE: If you want to include only certain processes in the report, use the "search as you type" fields at the top of each column. You can filter the list by one or more column headings. You can then select the **[Report]** button, and only the processes displayed in the **Device Processes** page will appear in the report.

3. The **Export current view as a report** modal page appears.



4. In the **Export current view as a report** modal page, you must select the format in which SL1 will generate the report. Your choices are:

- Comma-separated values (.csv)
- Web page (.html)
- OpenDocument Spreadsheet (.ods)
- Excel spreadsheet (.xlsx)
- Acrobat document (.pdf)

- Click **[Generate]**. The report will contain all the information displayed in the **Device Processes** page. You can immediately view the report or save it to a file for later viewing.

Generating an Exclusion Report for a Single System Process

From the **Device Processes** page (Devices > Processes), you can generate an exclusion report for a process. SL1 will generate the report in MS Word format. An exclusion report specifies all devices where the selected process is running and all devices where the selected process is not running. SL1 lists only appropriate servers in this report. For example, Linux servers would not appear in a report for Windows-based processes.


























EM7 TM Management Systems		Windows Service Exclusion Report <i>April 17, 2015, 3:49 am</i>	
Devices That Have [ReportingServicesService.exe] Service Installed			
Device	IP Address	Device Class / Sub-Class	Service
			Run State
			Report Summary
			Total Devices 0
			Unique Device Categories 0
			Unique Device Classes 0
			Services Found [on + off]
			Services Not Found 0
			Report Created By ScienceLogic EM7 TM


A Process Exclusion Report displays the following:

- Name of the process.
- List of all devices in SL1 where the process is running.
- List of all devices in SL1 where the process is not running. SL1 includes only appropriate servers in this report. For example, Solaris servers would not appear in a report for a Windows 2000 patch.
- The last row in the report displays:
 - Total number of devices in report.
 - Total number of device categories included in the report.
 - Total number of device classes included in the report.
 - Total number of devices where process is running
 - Total number of devices where process is not running.

To generate an exclusion report about a process:

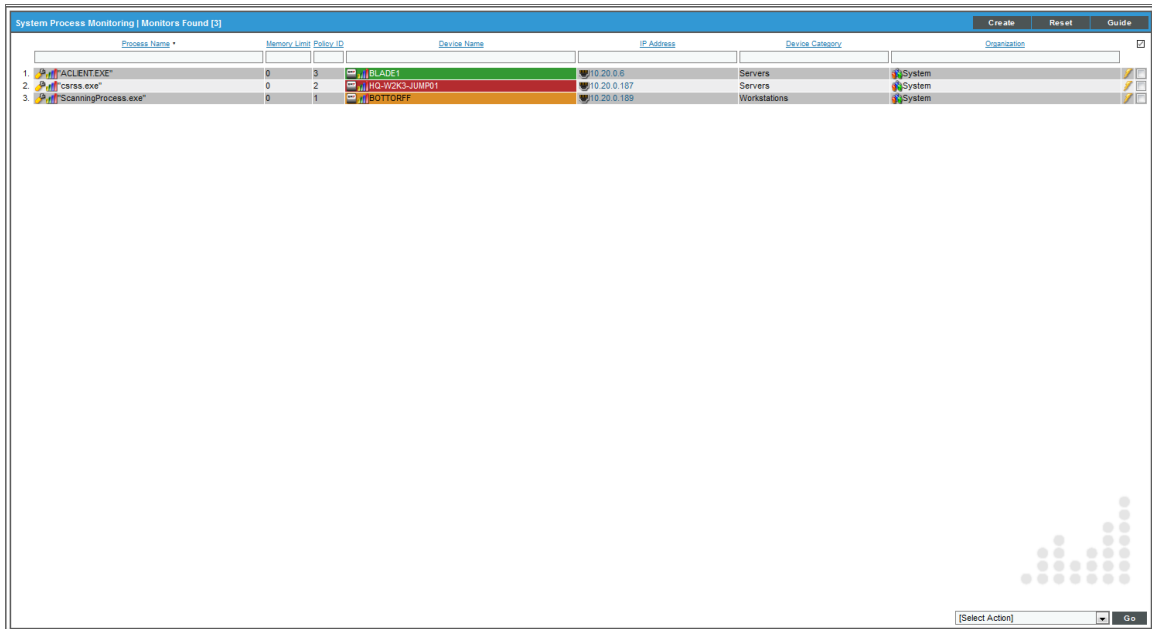
1. Go to the **Device Processes** page (Devices > Processes).

Device Name	Organization	IP Address	Device Class Sub-Class	Process	PID	Memory	Run State	Monitored
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	boinc.exe	2140	4952 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	boincmgr.exe	2888	5860 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	conhost.exe	2668	116 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	296	680 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	348	664 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	csrss.exe	1220	544 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	divm.exe	1640	294 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	explorer.exe	1640	3200 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	LogonUI.exe	704	6576 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	lsass.exe	452	5148 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	lsim.exe	464	1920 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	msdtc.exe	2432	156 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	msmdsrv.exe	1060	6320 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	rdpclip.exe	2094	352 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	ReportingServicesService.exe	1140	64212 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	services.exe	444	4760 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	smss.exe	216	80 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	snmp.exe	1460	3624 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	spoolsv.exe	272	1148 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	spssvc.exe	2496	2992 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	sqlservr.exe	1052	36884 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	sqlwfltr.exe	1484	88 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	552	3072 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	624	3628 kB	Running	No 
ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	svchost.exe	712	6388 kB	Running	No 

2. In the **Device Processes** page, find an instance of the process you want to generate an exclusion report for. Select its printer icon ().
3. You will be prompted to save or view the generated report.

Viewing the System Process Monitoring Policies

You can view a list of system process monitoring policies from the **System Process Monitoring** page (Registry > Monitors > System Processes). The **System Process Monitoring** page displays the following information about each system process:



The screenshot shows a window titled "System Process Monitoring | Monitors Found [3]". It contains a table with the following columns: Process Name, Memory Limit, Policy ID, Device Name, IP Address, Device Category, and Organization. There are three rows of data:

Process Name	Memory Limit	Policy ID	Device Name	IP Address	Device Category	Organization
1. "ACCLIENT.EXE"	0	3	BLADE1	10.20.0.6	Servers	System
2. "csrss.exe"	0	2	10-WORK3-JUMP01	10.20.0.187	Servers	System
3. "ScanningProcess.exe"	0	1	BOTTORFF	10.20.0.189	Workstations	System

At the bottom right of the window, there is a "[Select Action]" dropdown menu and a "Go" button.

- **Process Name.** Name of the policy.
- **Memory Limit.** The maximum amount of memory that can be used or reserved by a single instance of the process, as specified in the process policy.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of System Process Monitoring Policies

You can filter the list on the **System Process Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **System Process Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **System Process Monitoring** page searches for policies 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:

- **Process Name.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies that monitor a process that has a matching process name.
- **Memory Limit.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies that contain a matching per-process memory limit.
- **Policy ID.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies that have a matching policy ID.
- **Device Name.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Category.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies aligned with a device with a matching device category.
- **Organization.** You can enter text to match, including special characters, and the **System Process Monitoring** page will display only policies that have a matching organization.

Defining a Monitoring Policy for a System Process


You can define a process monitoring policy in the **System Process Policy** modal page. You can access the **System Process Policy** page either from the **Device Manager** page (Devices > Device Manager) or from the **System Process Monitoring** page (Registry > Monitors > System Processes).

To access the **System Process Policy** modal page from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Device Manager)
2. In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
3. In the **Device Administration** panel for the device, select the **[Monitors]** tab.
4. From the **[Create]** menu in the upper right, select **Create System Process Policy**.
5. The **System Process Policy** modal page appears.

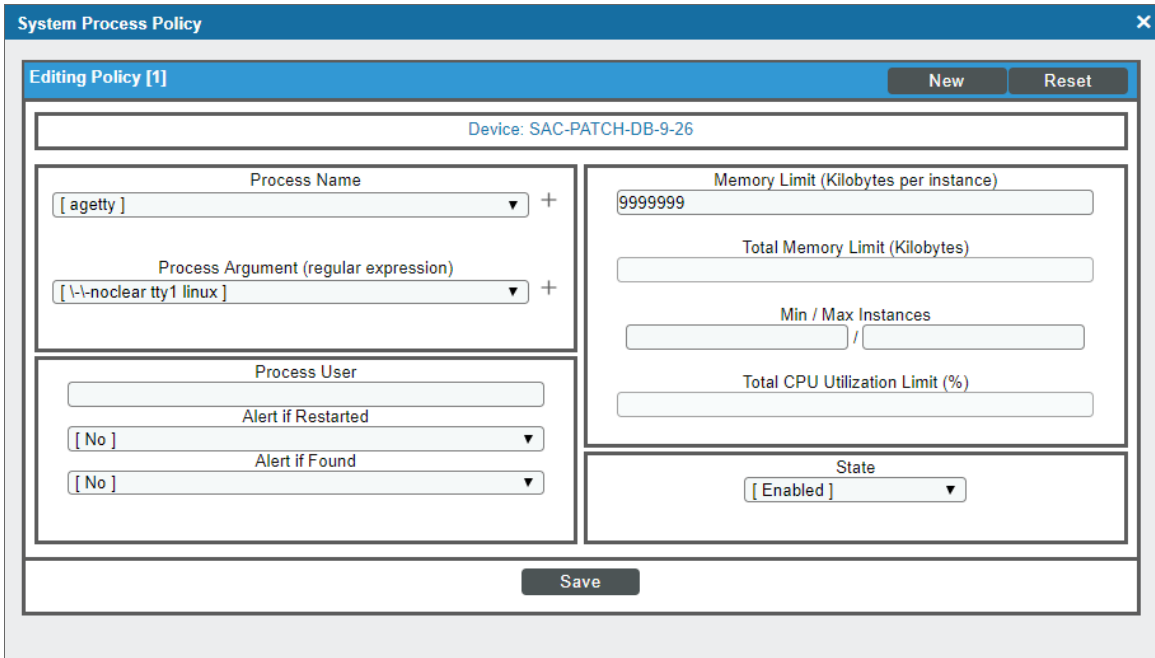
To access the **System Process Policy** modal page from the **System Process Monitoring** page:

1. Go to the **System Process Monitoring** page (Registry > Monitors > System Processes).
2. Select the **[Create]** button.

3. Click the device icon () for the device you want to align to policy with.
4. The **System Process Policy** modal page appears.

To define a process monitoring policy in the **System Process Policy** modal page:

1. In the **System Process Policy** modal page, supply a value in each of the following fields:



- **Process Name.** The name of the process. You can either:
 - Select from a list of all processes running on this device.
 - Click on the "+" icon and manually enter the name of a process.
- **Process Argument (regular expression).** The arguments with which the process is invoked. This field includes a drop-down list of all arguments currently in use by the current device for the specified process (specified in the **Process Name** field). If you don't want to use an argument from the drop-down, you can manually enter a valid regular expression in this field. If you want to include special characters in this regular expression, be sure to escape those special characters. The **Create System Process Policy** modal page will display an error message if the regular expression is not valid. SL1 will match the policy to a process if the value in this field appears anywhere in the argument string for that process. For example "win" would match arguments for "windows" and "win2k".
- **Process User.** Search for the following process user or process owner when the process is running. This field is helpful for finding processes running as root or su which should not be.

NOTE: Some hardware includes information about a process user or owner for each process in the SNMP data; some does not. Do not specify a value in the **Process User** field if the device does not include process user or process owner information in its SNMP data. If you specify a process user, and a device does not include process user in its SNMP data, SL1 will not generate an alert, even if it finds this process running

- **Alert if Restarted.** You can use this field to generate an alert in the Device Log if a system process restarts. Your choices are:
 - Yes. Use this setting to check for system processes that have restarted. SL1 checks every 5 minutes to determine if a system process has restarted. If SL1 finds a restarted system process, it will generate an alert in the Device Log.
 - No. Use this setting if you do not want SL1 to check for system processes that have restarted.

NOTE: When a system process has been restarted, it receives a new process ID number. It might take up to 2 hours for this new ID to appear on the **Process Manager** page (System > Settings > Processes).

NOTE: In some cases, this alert might appear if a device is restarted.

- **Alert if Found.** You can use this field in one of two ways: generate an event when a required system process is not running or generate an event when an illicit system process is running. Your choices are:
 - Yes. Use this setting to look for illicit processes.
 - If SL1 finds the illicit process (specified in the **Process Name** field), SL1 will generate an event.
 - If SL1 does not find the illicit process running, SL1 will not generate an event.
 - No. Use this setting to ensure that a required process is running.
 - If SL1 finds the required (specified in the **Process Name** field) running, SL1 does not generate an event.
 - If SL1 does not find the required process running, SL1 generates an event.
- **Memory Limit (Kilobytes per instance).** The amount of memory, in kilobytes, you will allow each instance of the process to use. This is an optional field.
- **Total Memory Limit (Kilobytes).** This setting is available only if the SL1 agent is installed on the selected device. The amount of memory, in kilobytes, you will allow all instances of the process to use in total. This is an optional field.
- **Min Instances.** The minimum number of instances of the process that should be running. If the minimum instances are not running, SL1 generates an event. The event will be of severity "major" and will say "too few processes running."



- **Max Instances.** The maximum number of instances of the process you will allow to run. If the maximum number of instances is exceeded, SL1 generates an event. The event will be of severity "major" and will say "too many processes process running."
- **Total CPU Utilization Limit (%).** This setting is available only if the SL1 agent is installed on the selected device. The amount of overall CPU you will allow all instances of the process to use in total. This is an optional field.
- **State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Admin Processes) for the **Data Collection: OS Process Check** process.
 - *Disabled.* SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.

2. Click **[Save]**.


NOTE: If you want to change the aligned device, click on the link for **Change Selected Device** before you clicked **[Save]**. After you clicked **[Save]**, you cannot edit the aligned device.

Editing a Monitoring Policy for a System Process

There are two places in SL1 from which you can edit a monitoring policy for a system process:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ()

Or:

2. From the **System Process Monitoring** page (Registry > Monitors > System Processes):
 - In the **System Process Monitoring** page, find the policy you want to edit and select its wrench icon ()

3. The **System Process Policy** modal page appears.

The screenshot shows the 'System Process Policy' modal page. The window title is 'System Process Policy'. The header bar contains 'Editing Policy [1] | Click Save to commit changes' and buttons for 'New' and 'Reset'. The main content area is for 'Device: SAC-PATCH-DB-9-26'. It contains several sections: 'Process Name' (dropdown with 'crond'), 'Process Argument (regular expression)' (dropdown with '[*-n]'), 'Process User' (text input), 'Alert if Restarted' (dropdown with '[No]'), and 'Alert if Found' (dropdown with '[No]'). On the right, there are 'Memory Limit (Kilobytes per instance)', 'Total Memory Limit (Kilobytes)', 'Min / Max Instances' (two text inputs), and 'Total CPU Utilization Limit (%)' (text input). At the bottom right is a 'State' dropdown with '[Enabled]'. A 'Save' button is at the bottom center.

4. In the **System Process Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining a Monitoring Policy for System Processes](#).
5. To save your changes to the policy, select the **[Save]** button.

Executing a System Process Monitoring Policy

After creating or editing a system process monitoring policy, you can manually execute the policy and view detailed logs of each step during the execution.

NOTE: After you define a system process monitoring policy and enable the policy, SL1 will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.

To execute a system process monitoring policy:

1. In the **System Process Monitoring** page (Registry > Monitors > System Processes), find the policy you want to run manually.
2. Select the lightning bolt icon (⚡) to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Example Policy for System Process

The screenshot shows a configuration window for a system process policy. The window title is "System Process Policy". The main area is titled "Editing Policy [1] | Click Save to commit changes" and includes "New" and "Reset" buttons. The device is identified as "SAC-PATCH-DB-9-26". The configuration includes a "Process Name" dropdown set to "crond", a "Process Argument (regular expression)" dropdown set to "[\n]", a "Process User" text field, "Alert if Restarted" and "Alert if Found" dropdowns both set to "[No]", and a "State" dropdown set to "[Enabled]". There are also fields for "Memory Limit (Kilobytes per instance)", "Total Memory Limit (Kilobytes)", "Min / Max Instances", and "Total CPU Utilization Limit (%)", all of which are currently empty. A "Save" button is located at the bottom center.

- This policy monitors a system process on the device "em7ao".
- The policy looks for the process "crond".
- If the process is not found running on the device, SL1 generates an event.

Viewing Reports for a System Process Policy

See the chapter on [Viewing Performance Graphs](#) in the *Discovery and Credentials* manual for information and examples of reports for system processes.

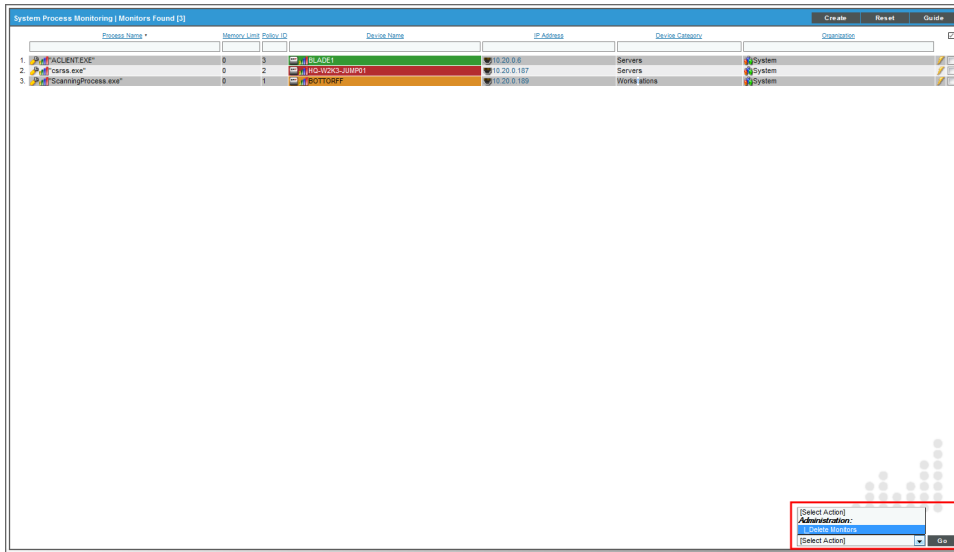
Deleting a System Process Monitoring Policy

You can delete a system process monitoring policy from the **System Process Monitoring** page. You can delete individual, multiple, or all existing policies. When you delete a system process monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

To delete a system process policy:

1. Go to the **System Process Monitoring** page (Registry > Monitors > System Processes).
2. In the **System Process Monitoring** page, select the checkbox(es) for each system process policy you want to delete. Click the checkmark icon (☑) to select all of the system process policies.

3. In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.



4. Click **[Go]**.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Chapter

15

Windows Services

Overview

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.

During discovery, SL1 retrieves information about Windows Services from discovered devices. When SL1 assigns a device class to a discovered device, SL1 examines the definition of that device class to determine how to retrieve information about Windows Services. SL1 looks at the **Service Collection** field in the definition of the device class. The **Service Collection** field specifies one of the following:

- This is not a Windows device class.
- Use the Windows MIB to gather information about Windows services.
- Use the WMI Informant MIB to gather information about Windows services.

SL1 allows you to create policies that monitor Windows Services. A service policy tells SL1 to monitor the device and look for the service. You can define a service policy so that:

- SL1 generates an event if the service is not running or SL1 generates an event if the service is running.
- Optionally, SL1 starts, pauses, or restarts the service.
- Optionally, SL1 reboots or shuts down the device.
- Optionally, SL1 triggers the execution of a script (script must reside on the device).

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.

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 Windows Services	324
Filtering the List of Windows Services	326
Viewing a List of Windows Services on a Single Device	326
Generating a Report on Multiple Windows Services	330
Generating an Exclusion Report for a Single Windows Service	332
Viewing the Windows Service Monitoring Policies	333
Filtering the List of Windows Service Monitoring Policies	334
Defining a Policy to Monitor Windows Services	335
Executing a Monitoring Policy for a Windows Service	340
Editing a Monitoring Policy for a Windows Service	340
Example Policy for Windows Service	342
Viewing Reports about Windows Services	342
Deleting a Windows Service Policy	342

Viewing the List of Windows Services

The **Windows Services** page displays a list of all services discovered by SL1. These services are running on devices that have been discovered by SL1. The **Windows Services** page also allows you to define service monitoring for multiple services running on multiple devices and to generate reports on services.

To view the list of all Windows services running on all devices:




1. Go to the **Windows Services** page (Devices > Services).

Windows™ Services Services Found (871)						Report	Reset	Guide
Device Name	Organization	IP Address	Device Class Sub-Class	Service	Monitored			
1	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Application Experience Lookup Service	Yes		
2	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVCacheRay	No		
3	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVCMgr	No		
4	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVDrChangeWriter	No		
5	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVDSAD	No		
6	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVDSGlobalCatalog	No		
7	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVSvc	No		
8	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVIMProxySvr	No		
9	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVMsgStoreMonitorSvr	No		
10	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVNotifierMgr	No		
11	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVAppSvc	No		
12	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVSqlChangeWriter	No		
13	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVTlsSvr	No		
14	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	AVUARSynSvc	No		
15	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CasOblityProxy	No		
16	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	COM+ Event System	No		
17	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	COM+ System Application	No		
18	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Computer Browser	No		
19	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Cryptographic Services	No		
20	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CsHspConnector	No		
21	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CsEmisSvc	No		
22	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CuDohMgr	No		
23	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CuMDBStoreMonitor	No		
24	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	CuMessageAgentSvr	No		
25	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	DCOM Server Process Launcher	No		
26	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	DHCP Client	No		
27	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Distributed Link Tracking Client	No		
28	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Distributed Transaction Coordinator	No		
29	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	DNS Client	No		
30	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Error Reporting Service	No		
31	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Event Log	No		
32	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	FTP Publishing Service	No		
33	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Help and Support	No		
34	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HD Input Service	No		
35	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HP ProLiant Remote Monitor Service	No		
36	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HP ProLiant System Shutdown Service	No		
37	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HP System Management Homepage	No		
38	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HP Version Control Agent	No		
39	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	HTTP SSL	No		
40	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	IS Admin Service	No		
41	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	IPSEC Services	No		
42	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Logical Disk Manager	No		
43	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Message Queuing	No		
44	AZUNITY	System	10.4.1.14	Microsoft Windows 2003 Server	Microsoft Exchange Management	No		

2. The **Windows Services** page displays the following about each process:

TIP: To sort the list of services, 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 where the service resides. 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.
- **Organization.** Organization associated with the device.
- **IP Address.** IP address of the device where the service is located.
- **Device Class | Sub-Class.** The manufacturer (device class) and type of device (sub-class). The **Device Class | Sub-Class** is automatically assigned during auto-discovery, at the same time as the **Category**.
- **Service.** The name of the service. A single service name can have multiple entries.
- **Monitored.** Specifies whether or not SL1 is monitoring the service. The choices are:
 - Yes. SL1 is currently monitoring this service.
 - No. SL1 is not currently monitoring this service.
- **Tools.** For each service, the following tools are available:
 - *Locate all services on device* (📁). Leads to the **Services Found** page, where you can view a list of all services that reside on the device.

- *Print exclusion report* (). Generates a detailed service report, in MS Word format. This report specifies all devices where the selected service is running and all devices where the selected service is not running. SL1 lists only appropriate devices in this report. For example, Solaris servers would not appear in a report for a Microsoft service.
- *Edit monitoring of this service* (). Leads to the **Monitoring Policies** page, where you can edit the properties of the monitoring policy.
- *Checkbox* (). The checkbox applies the action from the **Select Action** drop-down list to the service. To select all the checkboxes, select the large red check icon.

Filtering the List of Windows Services

You can filter the list on the **Windows Services** page by one or more parameters. Only services that meet all the filter criteria will be displayed in the **Windows Services** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Windows Services** page searches for services 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 (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching device name.
- **Organization**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching organization.
- **IP Address**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching IP address.
- **Device Class**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching device class.
- **Service**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching service name.
- **Monitored**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Windows Services** page will display only services that have a matching monitoring status.

Viewing a List of Windows Services on a Single Device

The **Windows Services** page displays a list of all of the Windows services that are running on a single device.

To view the list of Windows services on a single device:


1. Go to the **Device Manager** page (Devices > Services).
2. Find the device where you want to view the list of Windows services. Select the bar graph icon () for that device.

Device Manager Devices Found (1293)											Actions	Report	Reset	Guide	
Device Name	Device Hostname	IP Address	Device Subclass	Device Class / Sub-class	OID	Organisation	Current State	Collection Status	Collection Rate	SNMP Credentials	SNMP Message				
1	10.100.100.40	10.100.100.40	Pingable	Ping ICMP	274	System	Healthy	CUG	User-Disabled	--	--				
2	10.100.100.46	10.100.100.46	Pingable	FreeBSD ICMP	294	John	Healthy	CUG	User-Disabled	--	--				
3	10.7.11.186	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2				
4	10.7.11.186	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2				
5	10.7.11.186	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2				
6	10.7.11.188-8222	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1430	System	Healthy	CUG	Active	SNMP Public V2	V2				
7	10.7.11.188-8222	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1204	System	Healthy	CUG	Active	SNMP Public V2	V2				
8	10.7.11.188-7706	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1951	System	Healthy	CUG	Active	SNMP Public V2	V2				
9	10.7.11.187	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2				
10	10.7.11.187	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2291	System	Healthy	CUG	Active	SNMP Public V2	V2				
11	10.7.11.187	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2				
12	10.7.11.187-4269	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1952	System	Healthy	CUG	Active	SNMP Public V2	V2				
13	10.7.11.187-5996	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1206	System	Healthy	CUG	Active	SNMP Public V2	V2				
14	10.7.11.187-6848	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1431	System	Healthy	CUG	Active	SNMP Public V2	V2				
15	10.7.11.189	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2690	System	Healthy	CUG	Active	SNMP Public V2	V2				
16	10.7.11.189	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2				
17	10.7.11.189	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	3058	System	Notice	CUG	Active	SNMP Public V2	V2				
18	10.7.11.189-6662	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	2102	System	Healthy	CUG	Active	SNMP Public V2	V2				
19	10.7.11.189-7240	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1391	System	Healthy	CUG	Active	SNMP Public V2	V2				
20	10.7.11.189-7881	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	855	System	Healthy	CUG	Active	SNMP Public V2	V2				
21	10.7.11.237	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2				
22	10.7.11.237-7659	--	Network App F5 Networks, Inc.	IGMP-PLTM Pool Mem	1423	System	Healthy	CUG	Active	SNMP Public V2	V2				
23	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2433	System	Notice	CUG	Active	SNMP Public V2	V2				
24	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2				
25	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2				
26	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2				
27	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2				
28	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2				
29	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2				
30	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2281	System	Healthy	CUG	Active	SNMP Public V2	V2				
31	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2				
32	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2652	System	Healthy	CUG	Active	SNMP Public V2	V2				
33	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2				
34	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2				
35	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2				
36	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2				
37	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2				
38	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2				
39	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2				
40	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2				
41	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2				
42	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2				
43	10.7.12.125	--	Network App F5 Networks, Inc.	IGMP-PLTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2				

3. In the **Device Reports** panel, select the Services tab. The **Windows Services** page appears.

Close	Summary	Performance	Topology	Configs	Journals	Interfaces	
Logs	Events	Tickets	Software	Processes	Services	TCP Ports	Organization

Device Name	BOTTORFF	Managed Type	Physical Device
IP Address / ID	10.20.0.189 39	Category	Workstations
Class	Microsoft	Sub-Class	Windows XP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2014-06-16 14:45:00
Description	Hardware: x86 Family 15 Model 79 Stepping 2 AT/AT COMPATIBLE - Soft	Group / Collector	CUG2 em7_cu2
Device Hostname			



Windows Services Services Found [49]		Guide	Refresh
Service Name		Search	Search
ID	Service Name	Run State	Monitored
1.	Automatic Updates	Running	No
2.	Background Intelligent Transfer Service	Running	No
3.	CachemanXP	Running	No
4.	COM+ Event System	Running	No
5.	Computer Browser	Running	No
6.	Cryptographic Services	Running	No
7.	DCOM Server Process Launcher	Running	No
8.	DHCP Client	Running	No
9.	Distributed Link Tracking Client	Running	No
10.	DNS Client	Running	No
11.	Error Reporting Service	Running	No
12.	Event Log	Running	No
13.	Fast User Switching Compatibility	Running	No
14.	Help and Support	Running	No
15.	IPSEC Services	Running	No
16.	Logical Disk Manager	Running	No
17.	lxct_device	Running	No
18.	Network Connections	Running	No
19.	Network Location Awareness (NLA)	Running	No
20.	NVIDIA Display Driver Service	Running	No
21.	Plug and Play	Running	No
22.	Print Spooler	Running	No
23.	Protected Storage	Running	No
24.	Remote Procedure Call (RPC)	Running	No
25.	Remote Registry	Running	No

[Viewing Page: 1]

4. For each Windows service, the **Windows Services** page displays the following information:

TIP: To sort the list of Windows services, 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.

- **Service Name.** Name of the Windows service.
- **ID.** If you have defined a monitoring policy for the Windows service, SL1 generates a unique numeric ID for the service.
- **Run State.** The current state of the process. This can be one of the following:
 - *Runnable.* Service is ready to run as needed.
 - *Running.* Service is currently running.
 - *Not Running.* Service is in a "waiting" state.
 - *Invalid.* Service is part of an operation that failed. Service was not ended gracefully.

NOTE: Run states are defined by a device's operating system and/or installed agents. Run states may differ between devices.

- **Monitored.** Specifies whether or not SL1 is monitoring this Windows service.

Generating a Report on Multiple Windows Services

From the **Windows Services** page (Devices > Services) you can generate a report on all, multiple, or a single service in SL1. The **Windows Services** page allows you to generate a report that contains all the information displayed in the **Windows Services** page.

Windows™ Services Report generated by banderton on 2015-04-17 03:41:16

	Device Name	Organization	IP Address	Device Class Sub-Class	Service	Monitored
0.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Base Filtering Engine	No
1.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Certificate Propagation	No
2.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	COM+ Event System	No
3.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Cryptographic Services	No
4.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	DCOM Server Process Launcher	No
5.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Desktop Window Manager Session Man	No
6.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	DHCP Client	No
7.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic Policy Service	No
8.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic System Host	No
9.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Link Tracking Client	No
10.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Transaction Coordinator	No
11.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	DNS Client	No
12.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Group Policy Client	No
13.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	IKE and AuthIP IPsec Keying Modules	No
14.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	IP Helper	No
15.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	IPsec Policy Agent	No
16.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Network Connections	No
17.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Network List Service	No
18.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Network Location Awareness	No
19.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Network Store Interface Service	No
20.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Plug and Play	No
21.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Power	No
22.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Print Spooler	No
23.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Configuration	No
24.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Services	No
25.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Services UserMode Po	No
26.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Procedure Call (RPC)	No
27.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Registry	No
28.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	RPC Endpoint Mapper	No
29.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Security Accounts Manager	No
30.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Server	No
31.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Shell Hardware Detection	No
32.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SNMP Service	No
33.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Software Protection	No
34.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SPP Notification Service	No
35.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server (MSSQLSERVER)	No
36.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server Analysis Services (MSSQLS	No
37.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server Reporting Services (MSSQL	No
38.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	SQL Server VSS Writer	No
39.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	System Event Notification Service	No
40.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Task Scheduler	No
41.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	TCP/IP NetBIOS Helper	No
42.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	User Profile Service	No
43.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Event Log	No
44.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Firewall	No
45.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Font Cache Service	No
46.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Installer	No
47.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Management Instrumentation	No
48.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Modules Installer	No
49.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Remote Management (WS-Ma	No
50.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Time	No
51.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Windows Update	No
52.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	WinHTTP Web Proxy Auto-Discovery Se	No
53.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	WMI Performance Adapter	No
54.	ACME - DB MSSQL 2 - We	ACME	192.168.32.113	Microsoft MSSQL Server	Workstation	No

Page 1

To generate a report on all or multiple Windows services in SL1 :

1. Go to the **Windows Services** page (Devices > Services).

- In the **Windows Services** page, select the **[Report]** button.

Windows™ Services | Services Found [1514]

Device Name *	Organization	IP Address	Device Class Sub-Class	Service	Monitored	
1	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Base Filtering Engine	No
2	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Certificate Propagation	No
3	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	COM+ Event System	No
4	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Cryptographic Services	No
5	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DCOM Server Process Launcher	No
6	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Desktop Window Manager Session Manager	No
7	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DHCP Client	No
8	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic Policy Service	No
9	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic System Host	No
10	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Link Tracking Client	No
11	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Transaction Coordinator	No
12	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DNS Client	No
13	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Group Policy Client	No
14	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IKE and AuthIPsec Keying Modules	No
15	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IP Helper	No
16	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IPsec Policy Agent	No
17	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Connections	No
18	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network List Service	No
19	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Location Awareness	No
20	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Store Interface Service	No
21	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Plug and Play	No
22	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Power	No
23	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Print Spooler	No
24	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Configuration	No
25	ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Services	No

NOTE: If you want to include only certain services in the report, use the "search as you type" fields at the top of each column. You can filter the list by one or more column headings. You can then select the **[Report]** button, and only the services displayed in the **Windows Services** page will appear in the report.

- The **Export current view as a report** modal page appears.

Export current view as a report

Output Format: Comma-separated values (.csv)

Force browser to save to disk

Generate

- In the **Export current view as a report** modal page, you must select the format in which SL1 will generate the report. Your choices are:
 - Comma-separated values (.csv)
 - Web page (.html)
 - OpenDocument Spreadsheet (.ods)
 - Excel spreadsheet (.xlsx)
 - Acrobat document (.pdf)
- Select the **[Generate]** button. The report will contain all the information displayed in the **Windows Services** page. You can immediately view the report or save it to a file for later viewing.

Generating an Exclusion Report for a Single Windows Service

From the **Windows Services** page, you can generate an exclusion report for a service. SL1 will generate the report in MS Word format. An exclusion report specifies all devices where the selected Windows service is running and all devices where the selected Windows service is not running. SL1 lists only appropriate devices in this report. For example, Solaris servers would not appear in a report for Windows services.

EM7™ Management Systems		Windows Service Exclusion Report <i>April 17, 2015, 3:56 am</i>			
Devices That Have [Desktop Window Manager Session Manager] Service Installed					
Device	IP Address	Device Class / Sub-Class	Service	Run State	
ACME - DB MSSQL 2 - WebA	192.168.32.113	Microsoft MSSQL Server	Desktop Window Manager Session Manager	On	
ACME - DB-MSSQL - WebApp	192.168.32.112	Microsoft Windows Server 2008 R2	Desktop Window Manager Session Manager	On	
ACME - WEB IIS 2 - WebAp	192.168.32.110	Microsoft Windows Server 2008 R2	Desktop Window Manager Session Manager	On	
ACME - WEB-IIS-1 - WebAp	192.168.32.111	Microsoft Windows Server 2008 R2	Desktop Window Manager Session Manager	On	
LAB-2007-DC.silodev07.io	172.16.0.181	Microsoft Windows NT 4.0 Workstation	Desktop Window Manager Session Manager	On	
MS-2008-SPFND 0.185	172.16.0.185	RHEL Redhat 5.5	Desktop Window Manager Session Manager	On	
VPM Equinix Server	172.16.0.238	Forte Networks Inc. OEM	Desktop Window Manager Session Manager	On	
WIN-DEMO-EX2010.demo2.sc	192.168.41.122	Microsoft Windows Server 2008 R2	Desktop Window Manager Session Manager	On	
Report Summary					
Total Devices	8				
Unique Device Categories	3				
Unique Device Classes	5				
Services Found	8 [8 on + off]				
Services Not Found	0				
Report Created By ScienceLogic EM7™					

A Windows Services Exclusion Report displays the following:

- Name of the Windows service.
- List of all devices in SL1 where the Windows service is running.
- List of all devices in SL1 where the Windows service is not running. SL1 includes only appropriate servers in this report. For example, Solaris servers would not appear in a report for Windows services.
- The last row in the report displays:
 - Total number of devices in report.
 - Total number of device categories included in the report.
 - Total number of device classes included in the report.
 - Total number of devices where Windows service is running.
 - Total number of devices where Windows service is not running.

To generate an exclusion report about a Windows service:

1. Go to the **Windows Services** page (Devices > Services).

Device Name	Organization	IP Address	Device Class Sub-Class	Service	Monitored
1 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Base Filtering Engine	No
2 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Certificate Propagation	No
3 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	COM+ Event System	No
4 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Cryptographic Services	No
5 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DCOM Server Process Launcher	No
6 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Desktop Window Manager Session Manager	No
7 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DHCP Client	No
8 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic Policy Service	No
9 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Diagnostic System Host	No
10 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Link Tracking Client	No
11 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Distributed Transaction Coordinator	No
12 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	DNS Client	No
13 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Group Policy Client	No
14 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IKE and AuthIPsec Keying Modules	No
15 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IP Helper	No
16 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	IPsec Policy Agent	No
17 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Connections	No
18 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network List Service	No
19 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Location Awareness	No
20 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Network Store Interface Service	No
21 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Plug and Play	No
22 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Power	No
23 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Print Spooler	No
24 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Configuration	No
25 ACME - DB MSSQL 2 - WebApp	ACME	192.168.32.113	Microsoft MSSQL Server	Remote Desktop Services	No

2. In the **Windows Services** page, find an instance of the Windows service you want to generate an exclusion report for. Select its printer icon (🖨️).
3. You will be prompted to save or view the generated report.

Viewing the Windows Service Monitoring Policies

You can view the list of windows service monitoring policies from the **Windows Service Monitoring** page (Registry > Monitors > Windows Services). The **Windows Service Monitoring** page displays the following information about each windows service monitoring policy:

Service Name	Policy ID	Device Name	IP Address	Device Category	Organization
1 Application Experience	Start Service 22	IPBOLD	192.168.1.107	System	System
2 Application Experience	Start Service 1	IPALMAYACCPOLA	192.168.1.204	System	System
3 Application Experience Lookup Service	Start Service 18	IPBURNHOUSE	192.2.13	System	System
4 Application Experience Lookup Service	Start Service 4	IPBLADET	192.1.186	System	System Test Org
5 Automatic Updates	Start Service 7	IPBOTTORFF	192.1.87	Workstations	Test
6 Automatic Updates	Start Service 3	IPBURNHOUSE	192.1.186	System	System
7 Backup Exec Remote Agent for Windows Servers	Start Service 5	IPBLADET	192.20.38.17	System	System
8 Base Filtering Engine	Start Service 2	IPBURNHOUSE	192.1.186	System	System
9 Calendar	Start Service 21	IPSCENEL-CCEPFTT	192.8.242	Workstations	System
10 Client-Level System	Start Service 8	IPBOTTORFF	192.1.91	Workstations	Test
11 Connect To Work Folders	Start Service 16	IPBLADET	192.20.38.185	System	System
12 Computer Browser	Start Service 6	IPBLADET	192.20.38.1	System	System Test Org
13 DCOM Server	Start Service 15	IPBURNHOUSE	192.188.20.21	System	System Test Org
14 Distributed File System	Start Service 12	IPBURNHOUSE	192.188.20.21	System	System
15 Distributed Link Tracking Client	Start Service 17	IPBURNHOUSE	192.188.20.21	System	System
16 DNS Client	Start Service 23	IPBURNHOUSE	192.188.20.21	System	System
17 Group Policy Service	Start Service 14	IPBURNHOUSE	192.188.20.21	System	System
18 Plug and Play	Start Service 9	IPBOTTORFF	192.1.90	Workstations	Test
19 Remote Storage	Start Service 13	IPBURNHOUSE	192.188.20.21	System	System
20 Remote Registry	Start Service 19	IPALMAYACCPOLA	192.168.1.10	System	System
21 Security Accounts Manager	Start Service 10	IPBOTTORFF	192.1.90	Workstations	Test
22 System Center Services	Start Service 11	IPBOTTORFF	192.20.38.159	Workstations	Test
23 Task Scheduler	Start Service 20	IPBURNHOUSE	192.188.20.21	System	System

- **Windows Service Name.** Name of the service that is monitored by the policy.
- **Service Action.** On their local devices, Windows services can be defined with a startup-type of "automatic." This means that the service is started automatically when the local device is booted. Generally, critical services are defined with a startup-type of "automatic" to ensure that the service is always available. If a service with a startup-type of "automatic" fails on a device, SL1 can automatically restart the service. If an unwanted service is running on a device, SL1 can automatically stop the service. For a Windows service-policy, SL1 can perform one or more of the following service actions:
 - *Stop Service.* SL1 stops the service.
 - *Start Service.* SL1 starts the service.
 - *Pause Service.* SL1 pauses the service.
 - *Restart Service.* SL1 restarts the service.
 - *Reboot System.* SL1 reboots the computer.
 - *Shutdown System.* SL1 shuts down the computer.
 - *Action Script.* SL1 triggers the execution of a script on the device. The script must reside on the managed device, in the directory "c:/program files/snmp informant/operating_system/spawn". For example, you might want to execute a script if a service has crashed; the script could execute the steps required to cleanup any problems before restarting the service.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of Windows Service Monitoring Policies

You can filter the list on the **Windows Service Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed on the Windows Service Monitoring page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Windows Service Monitoring** page searches for policies 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:

- **Windows Service Name.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies with a matching name.

- **Service Action.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies that perform actions that match the text.
- **Policy ID.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies that have a matching policy ID.
- **Device Name.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Category.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies aligned with a device with a matching device category.
- **Organization.** You can enter text to match, including special characters, and the **Windows Service Monitoring** page will display only policies that have a matching organization.

Defining a Policy to Monitor Windows Services

Before you can define a Windows service policy that performs action on the external device, you must perform some required configuration in SL1 and on the external server.

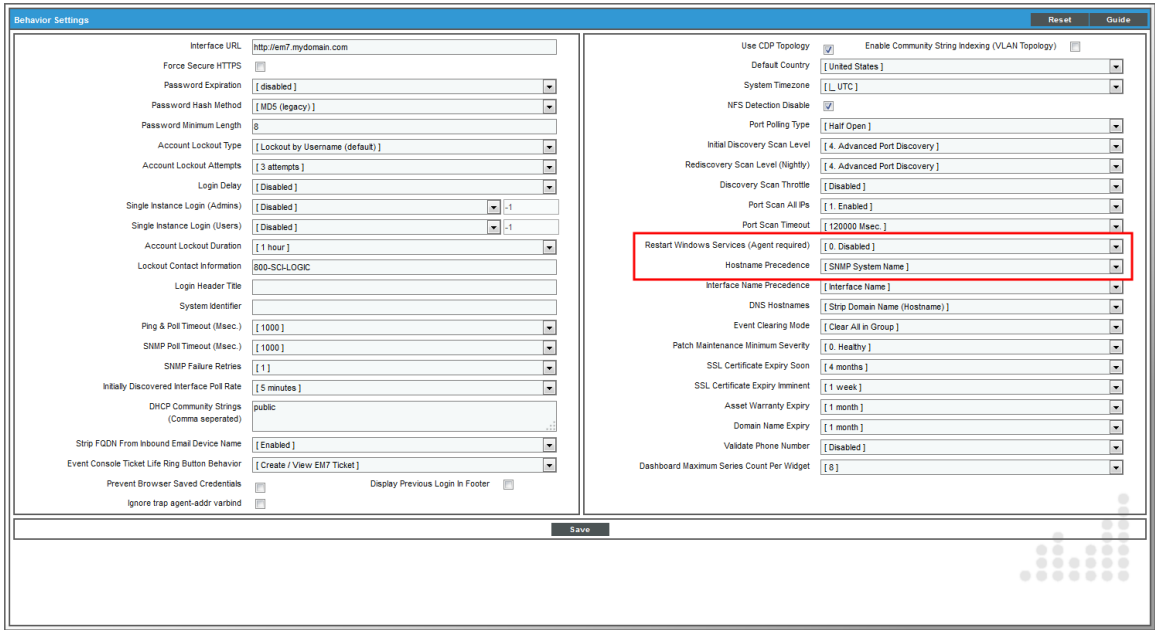
Optional Settings in the ScienceLogic Platform

If you do not define a Windows monitoring policy, SL1 will still detect the services that are running on Windows devices. You can configure SL1 to automatically monitor all services of type "automatic" and restart those services if they fail, without creating a Windows monitoring policy.

You can specify whether SL1 will automatically restart failed Windows services in the **Behavior Settings** page (System > Settings > Behavior). In the **Behavior Settings** page, you can define the following options in the *Restart Windows Services* page:

- *0. Disabled.* SL1 will not automatically restart failed services that have been defined on the device with a startup type of "automatic".
- *1. Enabled.* SL1 will automatically restart failed services that have been defined on the device with a startup type of "automatic".

NOTE: The following services have a startup type of "automatic", but run only when explicitly called. Therefore, these services will not be restarted automatically if they are not found running: **ATI HotKey Poller, Distributed Transaction Coordinator, Performance Logs and Alerts, Removable Storage, TPM Base Services, Windows Service Pack Installer update service, and VSS.** If you would like to include an additional service in this exclusion list, please contact ScienceLogic customer care.

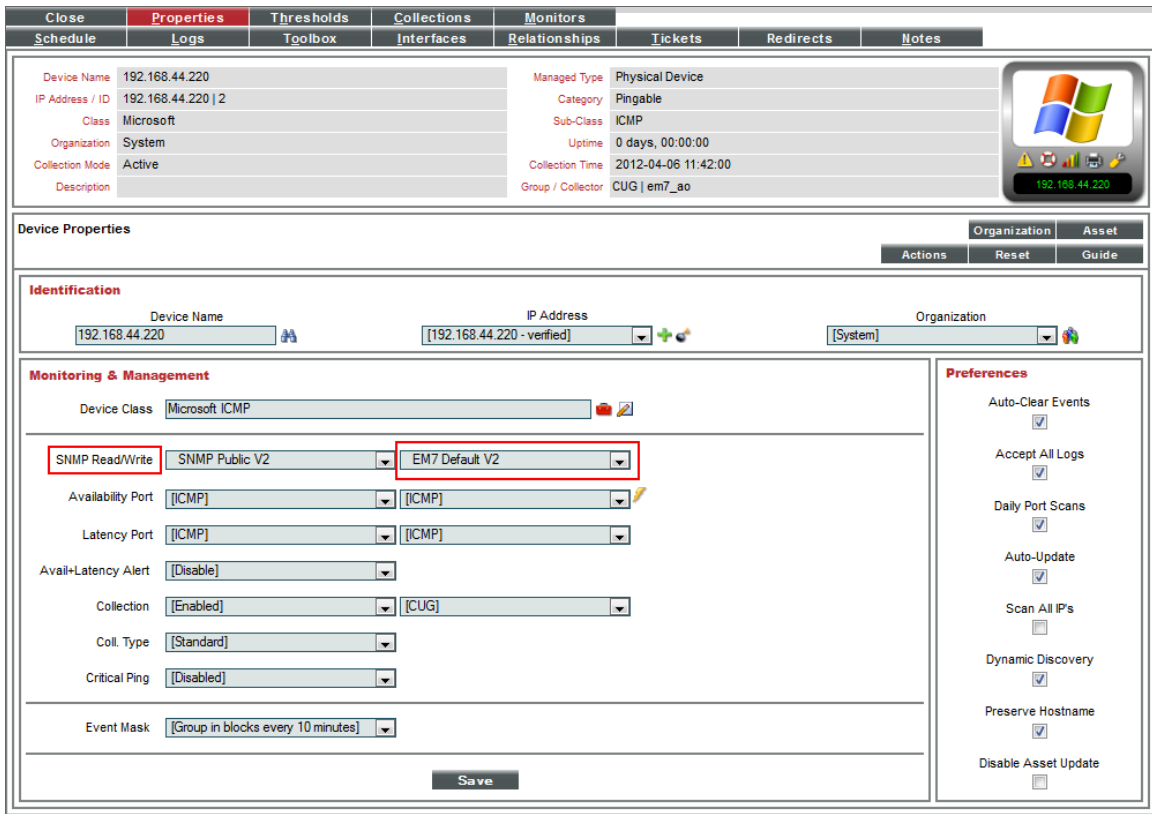


Required Configuration

For SL1 to automatically monitor services of type "automatic" and/or execute an action for a Windows Service Policy for a device, the device must:

- Be running the SNMP Informant, WMI Edition agent.
- Be aligned to a device class that has "WMI Informant" configured in the *Service Collection* field.

- Have an SNMP Write credential defined in the **Device Properties** page (Devices> Device Manager > wrench icon).



Additionally, to configure SL1 to execute a script on the external device in response to a Windows Service policy, the script must reside on the external device, in the directory:

c:/program files/snmp informant/operating_system/spawn.

Required Configuration on External Device


To include any of the optional actions in a Windows service policy, the external device must meet these requirements:

- The external device must be running the WMI agent.
- To execute a script on the external device for monitoring policies, the script must reside on the external device, in the directory:

c:/program files/snmp informant/operating_system/spawn.

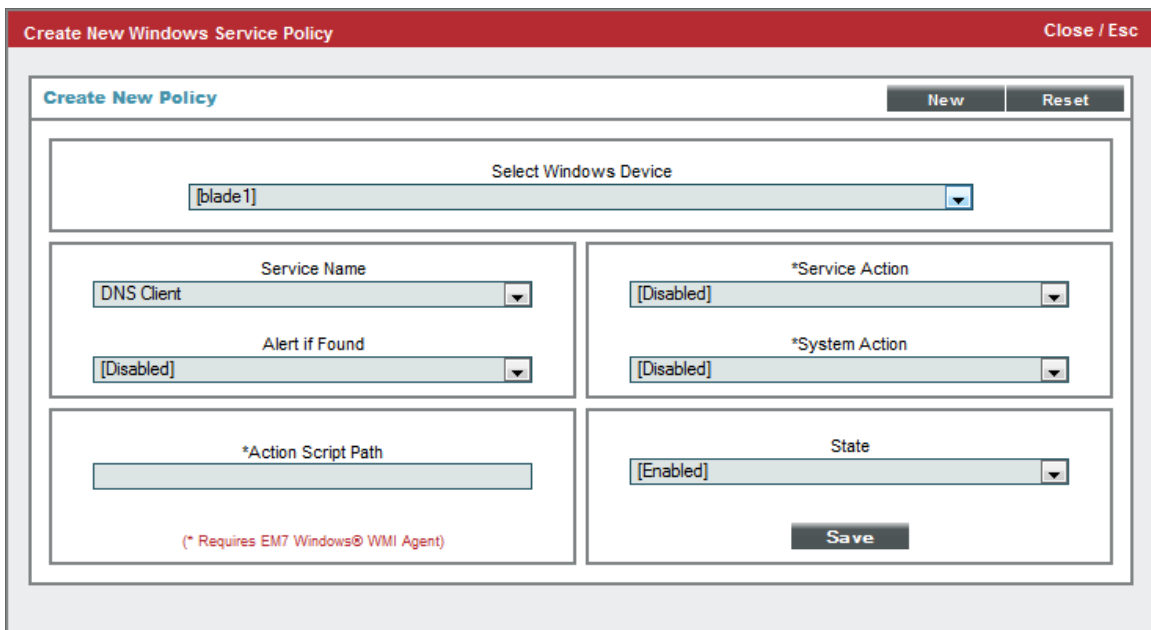
Defining the Policy

There are two places in SL1 from which you can define a monitoring policy for a system process:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - From the **[Create]** menu in the upper right, select **Create Windows Services Policy**.

Or:

2. From the **Windows Service Monitoring** page (Registry > Monitors > Windows Services):
 - In the **Windows Service Monitoring** page, select the **[Create]** button.
3. The **Windows Service Policy** modal page appears.



4. In the **Windows Service Policy** modal page, supply a value in each of the following fields:
 - **Select Device.** Select a device to align with this policy. If you accessed this page through the **Device Administration** panel, the current device is selected in this field by default. This field displays only devices that belong to a device class where the **Service Collection** field contains either *Windows Basic* or *WMI Informant*.

- **Service Name.** Service to be monitored by the policy. Select from a list of all Windows services discovered in the network by SL1.
- **Alert if Found.** You can use this field in one of two ways: Generate an event when a required Windows Service is not found or generate an event when an illicit Windows service is found. Your choices are:
 - Yes. Use this setting to look for an illicit service.
 - If SL1 finds the illicit service (specified in the **Service Name** field), SL1 will generate an event.
 - If SL1 does not find the illicit service, SL1 will not generate an event.
 - No. Use this setting to ensure that a required service is running.
 - If SL1 finds the required service, (specified in the **Service Name** field, SL1 does not generate an event.
 - If SL1 does not find the required service, SL1 generates an event.
- **Service Action.** If the device is a Windows computer running a WMI agent, you can define some automated actions, based on the condition specified in the **Alert if Found** field.
 - *Disabled.* The **Service Action** field is disabled and no automated actions are performed.
 - *Stop Service.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, stop the service.
 - *Start Service.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, start the service.
 - *Pause Service.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, pause the service.
 - *Restart Service.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, restart the service.
- **System Action.** If the device is a Windows computer running a WMI agent, you can define some automated actions, based on the condition specified in the **Alert if Found** field.
 - *Disabled.* The **System Action** field is disabled and no automated actions are performed.
 - *Reboot System.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, reboot the computer.
 - *Shutdown System.* If SL1 has generated an event based on the condition specified in the **Alert if Found** field, shut down the computer.
- **Action Script Path.** If the device is a Windows computer running a WMI agent, you can execute a script on the computer. If SL1 has generated an event based on the condition specified in the **Alert if Found** field, SL1 can then execute the action script. For example, you might want to execute a script if a service crashed; the script could execute the steps required to cleanup any problems before

restarting the service. In this field, you can specify the script to execute. The script must reside on the managed device, in the directory "c:/program files/snmp informant/operating_system/spawn".


- **State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Admin Processes) for the **Data Collection: OS Service Check** process.
 - *Disabled.* SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.

5. To save the new policy, select the **[Save]** button.

Executing a Monitoring Policy for a Windows Service



After creating or editing a Windows service monitoring policy, you can manually execute the policy and view detailed logs of each step during the execution. To do so:

NOTE: After you define a Windows service monitoring policy and enable the policy, SL1 will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.


1. In the **Windows Service Monitoring** page (Registry > Monitors > Windows Services), find the policy you want to run manually.
2. Select the lightning bolt icon () to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

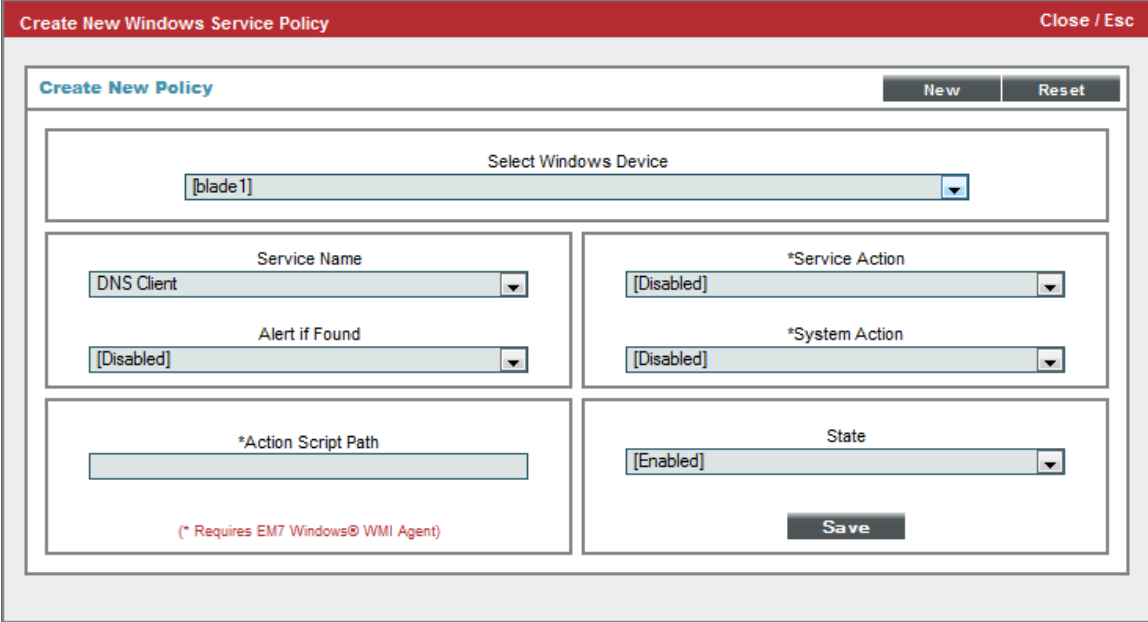
Editing a Monitoring Policy for a Windows Service

There are two places in SL1 from which you can edit a monitoring policy for a Windows service:

1. From the **Device Manager** (Devices > Device Manager) page:
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ().

Or:

- From the **Windows Service Monitoring** page (Registry > Monitors > Windows Services):
 - In the **Windows Service Monitoring** page, find the policy you want to edit and select its wrench icon ().
- The **Windows Service Policy** modal page appears.



The screenshot shows a modal window titled "Create New Windows Service Policy" with a "Close / Esc" button in the top right corner. The main content area is titled "Create New Policy" and contains several fields and buttons:

- Select Windows Device:** A dropdown menu with "blade1" selected.
- Service Name:** A dropdown menu with "DNS Client" selected.
- Alert if Found:** A dropdown menu with "[Disabled]" selected.
- *Service Action:** A dropdown menu with "[Disabled]" selected.
- *System Action:** A dropdown menu with "[Disabled]" selected.
- *Action Script Path:** A text input field.
- State:** A dropdown menu with "[Enabled]" selected.

Buttons for "New" and "Reset" are located in the top right corner. A "Save" button is located at the bottom right. A red note at the bottom left states "* Requires EM7 Windows® WMI Agent".

- In the **Windows Service Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining a Policy to Monitor Windows Services](#).
- To save your changes to the policy, select the **[Save]** button.

Example Policy for Windows Service

The screenshot shows a 'Create New Windows Service Policy' dialog box. The title bar is red and contains the text 'Create New Windows Service Policy' and 'Close / Esc'. Below the title bar is a 'Create New Policy' section with 'New' and 'Reset' buttons. The main area contains several fields: 'Select Windows Device' with a dropdown menu showing 'blade1'; 'Service Name' with a dropdown menu showing 'DNS Client'; 'Alert if Found' with a dropdown menu showing '[Disabled]'; '*Service Action' with a dropdown menu showing '[Disabled]'; '*System Action' with a dropdown menu showing '[Disabled]'; '*Action Script Path' with an empty text box; and 'State' with a dropdown menu showing '[Enabled]'. A red note at the bottom left says '* Requires EM7 Windows® WMI Agent'. A 'Save' button is at the bottom right.

- This policy monitors a Windows service on the device "blade1".
- This policy ensures that the Windows service "DNS Client" is running.
- The policy expects that the service "DNS Client" is running. If it is not, SL1 generates an event.

Viewing Reports about Windows Services

See the chapter on [Viewing Performance Graphs](#) for information and examples of reports for Windows services.

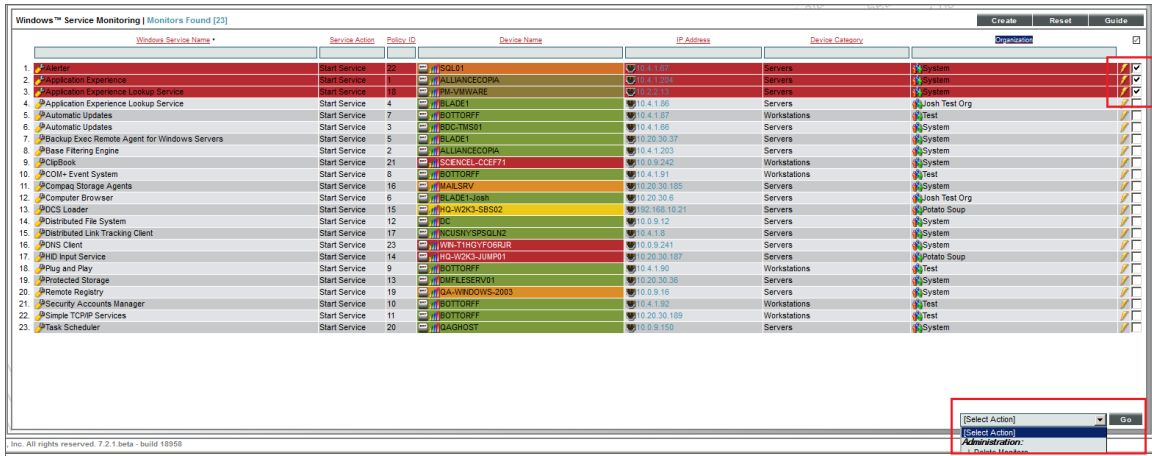
Deleting a Windows Service Policy

You can delete a Windows Service monitoring policy from the **Windows Service Monitoring** page. You can delete individual, multiple, or all existing policies. When you delete a Windows Service monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

To delete a Windows service process policy:

1. Go to the **Windows Service Monitoring** page (Registry > Monitors > Windows Services).
2. In the **Windows Service Monitoring** page, select the checkbox(es) for each system service policy you want to delete. Click the checkmark icon (☑) to select all of the service policies.

- In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.



- Select the **[Go]** button to delete the Windows service policies.
- The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.



Chapter

16

TCP Ports

Overview

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:

<i>What is a Port?</i>	345
<i>Port Security</i>	345
<i>Port Availability</i>	345
<i>Viewing a List of All Open Ports on All Devices</i>	346
<i>Filtering the List of IP Ports</i>	347
<i>Viewing a List of All Open Ports on a Single Device</i>	348
<i>System Settings for Monitoring Port Availability</i>	350
<i>Viewing the TCP/IP Port Monitoring Policies</i>	351
<i>Filtering the List of TCP/IP Port Monitoring Policies</i>	352
<i>Defining a Monitoring Policy for Port Availability</i>	352
<i>Editing a Monitoring Policy for a TCP/IP Port</i>	354
<i>Executing a TCP-IP Port Monitoring Policy</i>	355
<i>Example Policy for TCP/IP Port Availability</i>	356
<i>Viewing Reports for a Port-Availability Policy</i>	356

What is a Port?

Ports are used to route packets on a server to the appropriate application. Ports are like an apartment number in an apartment building; the street address (IP address) gets the message to the right building, and the apartment number (port number) gets the message to the right person. For example, port 80 is the standard port number for HTTP traffic, and port 80 packets are processed by a Web server.

Ports can use the UDP protocol or the TCP protocol. UDP does not include a handshake, does not ensure packets are sent in a particular order, does not return error messages, and will not automatically try to resend or re-receive a packet; TCP will do all these things. Commonly used UDP ports include port 53 for DNS and port 161 for SNMP. Commonly used TCP ports include port 80 for HTTP, port 25 for SMTP, and port 20 for FTP.

Ports 0-1023 are used by common Internet applications such as HTTP, FTP, and SMTP. Ports 1024-49151 can be registered by vendors for proprietary applications.

Port Security

The **Port Security** page (Devices > Device Manager > bar-graph icon > Performance) displays a list of all open ports on a device.

For SNMP and pingable devices, SL1 scans each device's TCP ports using NMAP.

For devices monitored using the SL1 agent, the agent reports open TCP and UDP ports. By default, the list of discovered ports is then automatically updated in SL1 every 5 minutes per agent.

The **Port Security** page displays open port information collected using NMAP and the SL1 agent, where applicable.

For SNMP and pingable devices, SL1 scans all the ports of each managed device every day. If any new ports are opened, SL1 updates the **Port Security** page and creates an event to notify users. You can explicitly ask that a device not be scanned nightly using NMAP, but if you do, SL1 will not notify you of newly opened ports on the device.

Port Availability

SL1 can monitor ports for availability. When a port monitor is created, SL1 monitors the port for availability every five minutes. You can choose whether a policy is executed by SL1 using NMAP or locally on the device by the agent.

During polling, a port has two possible availability values:

- 100%. Port is up and running.
- 0%. Port is not accepting connections and data from the network.

The data gathered by the port monitor is used to create port-availability reports.

If a port is not available, SL1 creates an event with the message "port not responding to connection".

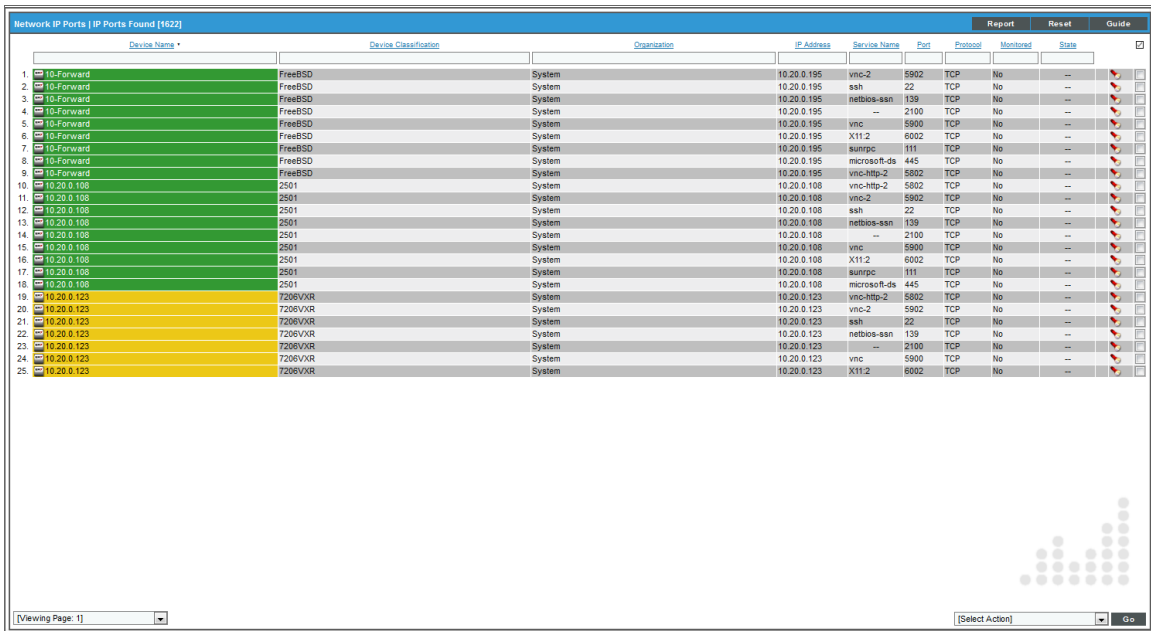
Viewing a List of All Open Ports on All Devices

The **Network IP Ports** page displays a list of all open ports on all devices discovered by SL1 using NMAP and the SL1 agent.

NOTE: Users of type "user" can view only IP ports that are aligned with the same organization(s) to which the user is aligned. This means that the device associated with the port(s) must be aligned with one of the organizations to which the user is aligned. Users of type "administrator" can view all IP ports.

To view the **Network IP Ports** page:

1. Go to the **Network IP Ports** page (Registry > Networks > IP Ports).



The screenshot shows the 'Network IP Ports | IP Ports Found [1622]' page. It features a table with columns for Device Name, Device Classification, Organization, IP Address, Service Name, Port, Protocol, Monitored, and State. The table lists 25 rows of data, including ports for devices like 10-Forward, 10.20.0.108, and 10.20.0.123. The table is sorted by IP Address in ascending order. At the bottom, there are controls for viewing page 1 and a 'Go' button.

Device Name	Device Classification	Organization	IP Address	Service Name	Port	Protocol	Monitored	State
10-Forward	FreeBSD	System	10.20.0.195	vnc-2	5902	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	ssh	22	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	netbios-ssn	139	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	--	2100	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	vnc	5900	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	X11-2	6002	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	sunrpc	111	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	microsoft-ds	445	TCP	No	--
10-Forward	FreeBSD	System	10.20.0.195	vnc-hdp-2	5802	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	vnc-hdp-2	5802	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	vnc-2	5802	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	ssh	22	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	netbios-ssn	139	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	--	2100	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	vnc	5900	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	X11-2	6002	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	sunrpc	111	TCP	No	--
10.20.0.108	2501	System	10.20.0.108	microsoft-ds	445	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	vnc-hdp-2	5802	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	vnc-2	5802	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	ssh	22	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	netbios-ssn	139	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	--	2100	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	vnc	5900	TCP	No	--
10.20.0.123	7206VXR	System	10.20.0.123	X11-2	6002	TCP	No	--

2. The **Network IP Ports** page displays a list of all discovered ports. For each port, the **Network IP Ports** page displays the following:

TIP: To sort the list of ports, 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 where the port resides. 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 Classification.** The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during auto-discovery, at the same time as the Category.
- **Organization.** The Organization associated with the device and port.
- **IP Address.** IP address associated with the open port.
- **Service Name.** The service accessed through the port.
- **Port.** The port number.
- **Protocol.** Either TCP or UDP.
- **Monitored.** Specifies whether SL1 is monitoring this port for availability.
- **State.** This column has a value only if a port-monitoring policy has been defined for the port. This field can have one of two values:
 - *Enabled.* The port-monitoring policy has been activated. SL1 monitors the port and collects availability data about the port.
 - *Disabled.* The port-monitoring policy has not been activated. SL1 will not monitor the port and does not collect availability data about the port.

Filtering the List of IP Ports

You can filter the list of discovered IP ports on the **Network IP Ports** page by one or more parameters. Only IP ports that meet all the filter criteria will be displayed in the **Network IP Ports** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Network IP Ports** page searches for IP ports 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 (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that are associated with a matching device name.
- **Device Classification.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that are associated with a matching device class.
- **Organization.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that are associated with a matching organization.



- **IP Address.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that are associated with a matching IP address.
- **Service Name.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that have a matching service name.
- **Port.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that have a matching port number.
- **Protocol.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that have a matching protocol.
- **Monitored.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that have a matching value for **Monitored**. Choices are *Yes* and *No*.
- **State.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Network IP Ports** page will display only IP ports that have a matching value for policy **State**. Choices are *Enabled* and *Disabled*.

Viewing a List of All Open Ports on a Single Device

NOTE: Users of type "user" can view only IP ports that are aligned with the same organization(s) to which the user is aligned. This means that the device associated with the port(s) must be aligned with one of the organizations to which the user is aligned. Users of type "administrator" can view all IP ports.

The **Port Security** page displays a list of all open ports on a single device.

To view the **Port Security** page for a device:

1. There are two ways to view the **Port Security** page:
 - Go to the **Device Manager** page (Devices > Device Manager). Find the device where you want to view the **Port Security** page. Select the bar graph icon () for that device.
 - Go to the **Network IP Ports** page (Registry > Networks > IP Ports). Find the device for which you want to view the **Port Security** page. Select the flashlight icon () for that device.

2. In the **Device Reports** panel, select the **[TCP/UDP Ports]** tab. The **Port Security** page appears.

The screenshot displays the 'Port Security | Port Scan Results' page. At the top, there are navigation tabs: Close, Summary, Performance, Topology, Configs, Journals, Interfaces, Logs, Events, Tickets, Software, Processes, Services, TCP/UDP Ports, and Organization. The 'TCP/UDP Ports' tab is selected.

Below the tabs, there is a summary section for device 'em7ao'. It includes fields for Device Name, IP Address / ID (10.64.68.20 | 1), Class (ScienceLogic, Inc.), Organization (System), Collection Mode (Active), Description (ScienceLogic EM7 G3 - All-In-One), Device Hostname, Managed Type (Physical Device), Category (System:EM7), Sub-Class (EM7 All-In-One), Uptime (0 days, 08:23:57), Collection Time (2016-11-22 14:00:09), and Group / Collector (CUG | em7ao).

The main part of the page is a table titled 'Port Security | Port Scan Results'. The table has columns for Interface IP, Port Number, Service, Protocol, Certificate Issuer, and Cert Expiration. The table lists 27 rows of scan results, including ports for SSH, SMTP, HTTP, SNMP, HTTPS, and Syslog.

	Interface IP	Port Number	Service	Protocol	Certificate Issuer	Cert Expiration
1.	0.0.0.0	0		TCP	--	--
2.	::	0		UDP	--	--
3.	::	0		TCP	--	--
4.	0.0.0.0	0		UDP	--	--
5.	10.64.68.20	22	ssh	TCP	--	--
6.	::	22	ssh	TCP	--	--
7.	0.0.0.0	22	ssh	TCP	--	--
8.	10.64.68.20	25	smtp	TCP	--	--
9.	0.0.0.0	25	smtp	TCP	--	--
10.	::	25	smtp	TCP	--	--
11.	127.0.0.1	80	http	TCP	--	--
12.	10.64.68.20	80	http	TCP	--	--
13.	0.0.0.0	80	http	TCP	--	--
14.	0.0.0.0	161	snmp	UDP	--	--
15.	0.0.0.0	162	snmptrap	UDP	--	--
16.	127.0.0.1	199	smux	TCP	--	--
17.	127.0.0.1	323		UDP	--	--
18.	::1	323		UDP	--	--
19.	0.0.0.0	443	https	TCP	--	--
20.	10.64.68.20	443	https	TCP	Silo	2017-06-08 14:50:04
21.	0.0.0.0	514	syslog	UDP	--	--
22.	::	514	shell	TCP	--	--
23.	0.0.0.0	5000	UPnP	TCP	--	--
24.	10.64.68.20	5000	UPnP	TCP	--	--
25.	127.0.0.1	5001	complex-link	TCP	--	--
26.	0.0.0.0	7700		TCP	--	--
27.	::ffff:127.0.0.1	7700		TCP	--	--

3. For each open port on the device, the **Port Security** page displays the following information:

- **Interface IP.** IP address through which SL1 communicates with the device.
- **Port Number.** The ID number of the port.
- **Service.** The service accessed through the port.
- **Protocol.** Either TCP or UDP.
- **Certificate Issuer.** If the service on this port uses a certificate, this column contains the name of the certificate authority.

NOTE: Certificates are used by secure services like HTTPS, SSL, SSH, and SFTP to verify communication and encrypt message. The certificate issuer (also known as the certificate authority or CA) is an organization that issues digital certificates (digital IDs). These digital IDs (called keys) authenticate the identity of people and organizations over a public system such as the Internet. These keys also allow senders and receivers to encrypt messages and un-encrypt replies.

- **Cert. Expiration.** The expiration date of the certificate.

System Settings for Monitoring Port Availability

Although you are not required to define system settings for port availability, you might find it useful to understand how these settings affect port monitoring.

The **Behavior Settings** page (System > Settings > Behavior) includes the following settings that affect policies for port availability:

The screenshot shows the 'Behavior Settings' page with various configuration options. The 'Port Polling Type' dropdown menu is highlighted with a red box, showing the options 'Half Open' and 'Full Connect'. The 'NFS Detection Disable' checkbox is also checked. The 'Save' button is located at the bottom center of the form.

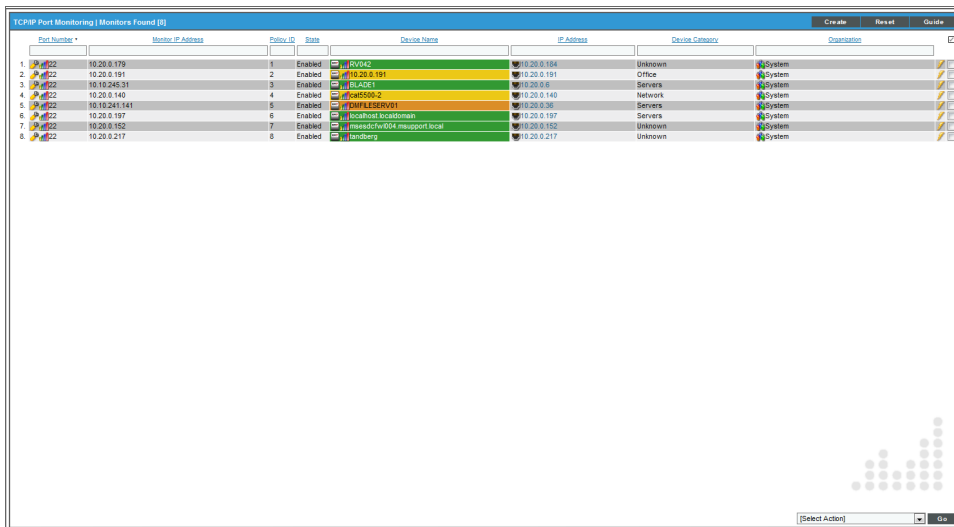
- **Port Polling Type.** Specifies how SL1 should poll ports for availability using NMAP. The choices are:
 - *Half Open.* Uses a faster TCP/IP connection method (a TCP SYN scan, `nmap -sS`) and does not appear on device's logs.
 - *Full Connect.* Uses the standard TCP/IP connection (`TCP connect()` scan, `nmap -sT`) to detect open ports.

Viewing the TCP/IP Port Monitoring Policies

You can view a list of TCP/IP port monitoring policies from the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).

The **TCP/IP Port Monitoring** page displays the following information for each TCP/IP port monitoring policy:

NOTE: Users of type "user" can view only IP ports that are aligned with the same organization(s) to which the user is aligned. This means that the device associated with the port(s) must be aligned with one of the organizations to which the user is aligned. Users of type "administrator" can view all IP ports.



Port Number	Monitor IP Address	Policy ID	Status	Device Name	IP Address	Device Category	Organization	Disabling
1. IP:22	10.20.0.179	1	Enabled	RD42	10.20.0.184	Unknown	System	
2. IP:22	10.20.0.191	2	Enabled	10.20.0.191	10.20.0.191	Office	System	
3. IP:22	10.10.245.31	3	Enabled	BLACCT	10.20.0.6	Servers	System	
4. IP:22	10.20.0.140	4	Enabled	10.20.0.140	10.20.0.140	Network	System	
5. IP:22	10.10.241.141	5	Enabled	DMLESERVER01	10.20.0.36	Servers	System	
6. IP:22	10.20.0.197	6	Enabled	localhost.localdomain	10.20.0.197	Servers	System	
7. IP:22	10.20.0.192	7	Enabled	localhost.localdomain	10.20.0.192	Helpdesk	System	
8. IP:22	10.20.0.217	8	Enabled	landberg	10.20.0.217	Unknown	System	

- **TCP/IP Port Number.** Port number of the port to be monitored.
- **Monitor IP Address.** IP address associated with the port to be monitored. For devices with multiple IP addresses, the IP address for the port policy might be different than the IP address used by SL1 to communicate with the device.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of TCP/IP Port Monitoring Policies

You can filter the list of discovered port monitoring policies on the **TCP/IP Port Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **TCP/IP Port Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **TCP/IP Port Monitoring** page searches for policies 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:

- **Port Number.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies that monitor ports with matching port number.
- **Monitor IP Address.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies that monitor a port with a matching IP address.
- **Policy ID.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies that have a matching policy ID.
- **State.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies that have a matching state (enabled or disabled).
- **Device Name.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Category.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies aligned with a device with a matching device category.
- **Organization.** You can enter text to match, including special characters, and the **TCP/IP Port Monitoring** page will display only policies that have a matching organization.

Defining a Monitoring Policy for Port Availability

NOTE: Users of type "user" can view only IP ports that are aligned with the same organization(s) to which the user is aligned. This means that the device associated with the port(s) must be aligned with one of the organizations to which the user is aligned. Users of type "administrator" can view all IP ports.

You can define a port monitoring policy in the **TCP/IP Port Policy** modal page. You can access the **TCP/IP Port Policy** page either from the **Device Manager** page (Devices > Device Manager) or from the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).

To access the **TCP/IP Port Policy** modal page from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Device Manager)
2. In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon (🔧) for the device.
3. In the **Device Administration** panel for the device, select the **[Monitors]** tab.
4. From the **[Create]** menu in the upper right, select **Create TCP/IP Port Policy**.
5. The **TCP/IP Port Policy** modal page appears.

To access the **TCP/IP Port Policy** modal page from the **TCP/IP Port Monitoring** page:

1. Go to the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).
2. Select the **[Create]** button.
3. The **TCP/IP Port Policy** modal page appears.

To define a port monitoring policy:

1. Navigate to the **TCP/IP Port Policy** modal page. See the procedures above for more information.
2. In the **TCP/IP Port Policy** modal page, supply a value in each of the following fields:

The screenshot shows a modal window titled "Create New TCP/IP Port Policy". At the top right are "New" and "Reset" buttons. The main form area contains several fields:

- "Select IP Device" dropdown menu with "[Select Device]" as the placeholder.
- "Device IP Address" dropdown menu.
- "Port / Service" dropdown menu with "1 / tcpmux" selected.
- "Monitor Method" dropdown menu with "Port Scan (NMAP)" selected.
- "Monitor State" dropdown menu with "[Enabled]" selected.
- "Critical Poll" dropdown menu with "[Disabled]" selected.
- "Timeout (ms)" text input field with the value "5000".

 A "Save" button is located at the bottom right of the form area.

- **Select Device.** Select a device from this drop-down list to align with this policy. By default, the current device is selected in this field.
- **Device IP Address.** IP address through which SL1 communicates with the device.
- **Port/Service.** Port number and the corresponding service running on the port.
- **Monitor Method.** Select whether the policy will be executed using NMAP or using the agent. This option is available only if you selected a device on which the agent is installed.
- **Monitor State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Processes) for the **Data Collection: TCP Port Monitor** process.

- *Disabled*. SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.
- **Critical Poll**. Frequency with which SL1 should "ping" the device. If the device does not respond, SL1 creates an event. The choices are:
 - *Disabled*. SL1 will not ping the device.
 - *Enabled*. SL1 will ping the device every 15, 30, 60, or 120 seconds, as specified.



NOTE: SL1 uses **Critical Poll** data to create events when mission-critical ports are not available. SL1 does not use this critical poll data to create port-availability reports. SL1 will continue to collect port availability only every five minutes.

3. Click **[Save]**.


Editing a Monitoring Policy for a TCP/IP Port

You can edit a port monitoring policy on the **TCP/IP Port Policy** modal page. You can access the **TCP/IP Port Policy** modal page either from the **Device Manager** page (Devices > Device Manager) or from the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).

To access the **TCP/IP Port Policy** modal page from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Device Manager)
2. In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon () for the device.
3. In the **Device Administration** panel, select the **[Monitors]** tab.
4. In the **Monitoring Policies** page, find the port policy you want to edit and select its wrench icon ()
5. The **TCP/IP Port Policy** modal page appears.

To access the **TCP/IP Port Policy** modal page from the **TCP/IP Port Monitoring** page:

1. Go to the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).
2. Find the device and port for which you want to edit the monitoring policy. Select the wrench icon () for the port.
3. The **TCP/IP Port Policy** modal page appears.

To edit a port monitoring policy:

1. If you have not done so already, navigate to the **TCP/IP Port Policy** modal page. See the procedures above for more information.

2. In the **TCP/IP Port Policy** modal page, edit the values in one or more of the fields.

The screenshot shows a modal window titled "TCP/IP Port Policy" with a subtitle "Editing Policy [1]". At the top right of the modal are "New" and "Reset" buttons. The main content area is divided into several sections. At the top is a "Select Device" dropdown menu with "em7ao" selected. Below this are three columns of settings. The first column contains "Device IP Address" (10.64.68.20) and "Port / Service" (22 / ssh). The second column contains "Monitor Method" (Port Scan (NMAP)), "Monitor State" (Enabled), and "Critical Poll" (Disabled). The third column contains a "Timeout (ms)" field set to 5000. A "Save" button is located at the bottom right of the modal.

3. Click **[Save]** when done.

Executing a TCP-IP Port Monitoring Policy

After creating or editing a TCP-IP port monitoring policy, you can manually execute the policy and view detailed logs of each step during the execution. To do so:

NOTE: After you define a TCP-IP port monitoring policy and enable the policy, SL1 or the SL1 agent will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.

1. In the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports), find the policy you want to run manually.
2. Select the lightning bolt icon (⚡) to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is helpful for diagnosing possible problems with a policy.

Example Policy for TCP/IP Port Availability

The screenshot shows a configuration window for a TCP/IP Port Policy. The window has a title bar 'TCP/IP Port Policy' and a subtitle 'Editing Policy [1]'. At the top right of the subtitle bar are 'New' and 'Reset' buttons. The main content area is divided into several sections. At the top is a 'Select Device' dropdown menu with 'em7ao' selected. Below this are three columns of settings. The first column contains 'Device IP Address' (10.64.68.20) and 'Port / Service' (22 / ssh). The second column contains 'Monitor Method' (Port Scan (NMAP)), 'Monitor State' (Enabled), and 'Critical Poll' (Disabled). The third column contains 'Timeout (ms)' (5000). At the bottom right of the main content area is a 'Save' button.

- This policy monitors a TCP/IP port on the device "cisco_10.2.1.29", at IP address 10.1.0.205.
- The policy will monitor port 22 for availability.

Viewing Reports for a Port-Availability Policy

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for port availability.

Deleting a TCP/IP Port Monitoring Policy

You can delete a port monitoring policy from the **TCP/IP Port Monitoring** page. You can delete individual, multiple, or all existing port monitoring policies. When you delete a TCP/IP Port Monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

To delete a port monitoring policy:

1. Go to the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).
2. In the **TCP/IP Port Monitoring** page, select the checkbox(es) for each port monitoring policy you want to delete. Click the checkmark icon (☑) to select all of the system process policies.

- In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.



Row Number	Monitor IP Address	Subnet ID	State	Device Name	IP Address	Device Category	Organization
1	10.20.0.178	1	Enabled	RV942	10.20.0.184	Unknown	System
2	10.20.0.191	2	Enabled	10.20.0.191	10.20.0.191	Office	System
3	10.10.0.531	3	Enabled	10.10.0.531	10.20.0.92	Server	System
4	10.20.0.140	4	Enabled	fcall506-2	10.20.0.140	Network	System
5	10.10.241.141	5	Enabled	10.10.241.141	10.20.0.246	Server	System
6	10.20.0.197	6	Enabled	10.20.0.197	10.20.0.197	Server	System
7	10.20.0.152	7	Enabled	msekdtw004.msupport.local	10.20.0.152	Unknown	System
8	10.20.0.217	8	Enabled	linburg	10.20.0.217	Unknown	System

- Click **[Go]** to delete the port monitoring policy.
- The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Monitoring Domain Servers and DNS Records

Overview

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:

<i>Monitoring Domain Names</i>	358
<i>Viewing the List of Domain Name Monitoring Policies</i>	360
<i>Filtering the List of Domain-Name Monitoring Policies</i>	360
<i>Defining a Monitoring Policy for a Domain Name</i>	361
<i>Editing a Monitoring Policy for a Domain Name</i>	363
<i>Example Policy for Domain Name</i>	364
<i>Executing the Domain-Name Monitoring Policy</i>	365
<i>Viewing Reports for a Domain-Name Monitoring Policy</i>	365
<i>Deleting a Domain-Name Policy</i>	365

Monitoring Domain Names

Domain-name monitoring policies allow you to monitor the availability and lookup time for a specific domain-name server and a specific record on a domain name server.

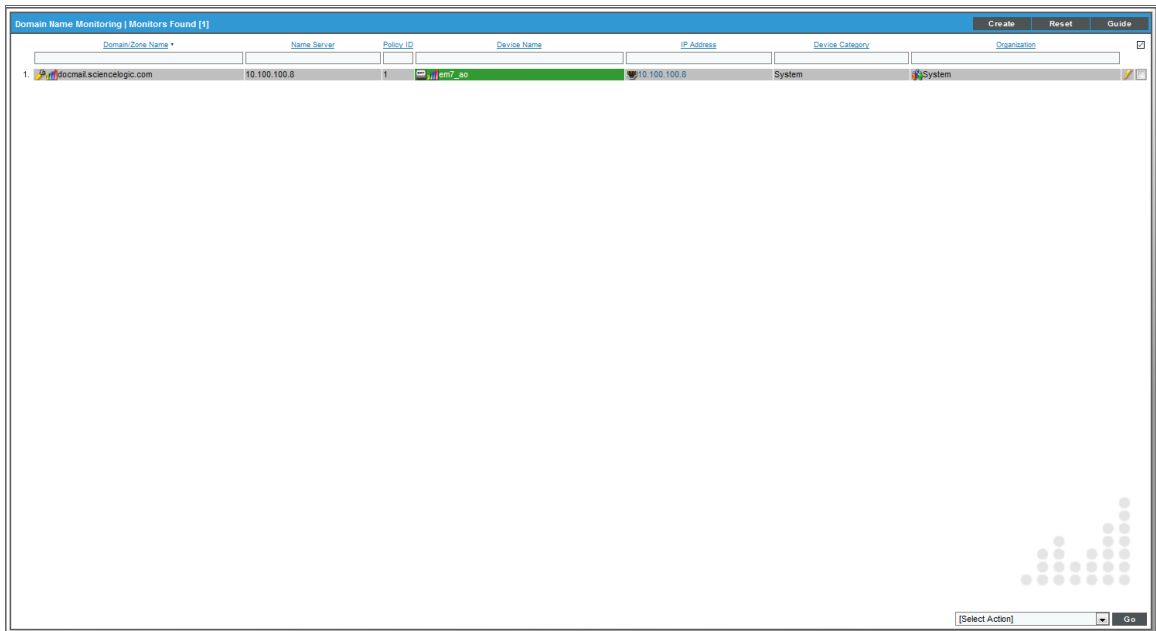
SL1 will send a request to the domain-name server asking the domain-name server to search a specified DNS record for the specified text string. If the domain-name server responds, SL1 considers the server as "available".

SL1 also monitors the amount of time it takes for the domain-name server to respond and collects this data to calculate and graph lookup time.

For each domain name policy, SL1 will collect data and create trend reports.

Viewing the List of Domain Name Monitoring Policies

You can view a list of domain name policies from the **Domain Name Monitoring** page (Registry > Monitors > Domain Name). The **Domain Name Monitoring** page displays the following about each domain name monitoring policy:



The screenshot shows a web interface titled "Domain Name Monitoring | Monitors Found [1]". It features a table with the following columns: Domain/Zone Name, Name Server, Policy ID, Device Name, IP Address, Device Category, and Organization. A single row is displayed with the following data: Domain/Zone Name: scienceologic.com, Name Server: 10.100.100.8, Policy ID: 1, Device Name: em7_ao, IP Address: 10.100.100.8, Device Category: System, and Organization: System. The table has a search bar at the top and a "Go" button at the bottom right.

Domain/Zone Name	Name Server	Policy ID	Device Name	IP Address	Device Category	Organization
scienceologic.com	10.100.100.8	1	em7_ao	10.100.100.8	System	System

- **Domain/Zone Name.** Domain or zone name of the domain being monitored by the policy.
- **Name Server.** Name server being monitored by the policy.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of Domain-Name Monitoring Policies

You can filter the list of policies on the Domain Name Monitoring page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **Domain Name Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Domain Name Monitoring** page searches for policies 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:

- **Domain/Zone Name.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies that act upon a matching domain name or zone name.
- **Name Server.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies that act upon a matching name server.
- **Policy ID.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies that have a matching policy ID.
- **Device Name.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Class.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies aligned with a device with a matching device class.
- **Organization.** You can enter text to match, including special characters, and the **Domain Name Monitoring** page will display only policies that have a matching organization.

Defining a Monitoring Policy for a Domain Name

There are two places in SL1 from which you can define a monitoring policy for a domain name:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - From the **[Create]** menu in the upper right, select **Create Domain Name Policy**.

Or:

2. From the **Domain Name Monitoring** page (Registry > Monitors > Domain Name):
 - Go to the **Domain Name Monitoring** page.
 - Select the **[Create]** button.

3. The **Create Domain Name Policy** modal page appears:

The screenshot shows a modal window titled "Create New Domain Name Policy" with a red header bar. The header contains the title on the left and "Close / Esc" on the right. Below the header is a sub-section titled "Create New Policy" with "New" and "Reset" buttons. The main form area is divided into several sections: a "Select Device" dropdown menu showing "[device 1]"; a "Domain Name" text input field containing "docmail.sciencelogic.com"; a "Name Server IP Address" text input field containing "192.168.10.21"; a "Record Type" dropdown menu showing "A - Address Record"; a "Timeout" dropdown menu showing "[10 sec.]"; a "Result Match" text input field containing "192.168.10.201"; an "Alert if Found" dropdown menu showing "[No]"; and a "State" dropdown menu showing "[Enabled]". A "Save" button is located at the bottom right of the form area.

4. In the **Create Domain Name Policy** modal page, supply a value in each of the following fields:

- **Select Device.** Select a device from the drop-down list to align with this policy. By default, the current device is selected in this field.

NOTE: Before you can define a domain-name policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the domain-name server you will be monitoring with the policy, but you aren't required to do so. The requests to the domain name server will be sent from a SL1 appliance, but you must still associate the policy with a device.



- **Domain Name.** Name of the domain you want to monitor with this policy.
- **Name Server IP Address.** IP address of the name-server device you want to monitor with this policy. SL1 will use this IP address to communicate with the name-server.
- **Record Type.** Type of DNS record you want to check for availability and lookup speed.
- **Timeout.** Number of seconds SL1 should wait for a response from the domain-name server. If SL1 does not receive a response message after the specified number of seconds, SL1 generates an event.
- **Result Match.** Text string to search for. SL1 will search the selected DNS record for this string. You can enter either a string that should always appear in the specified record or you can enter a string that you do not want to appear in this record (that is, a string that indicates an illicit entry).
- **Alert if Found.** You can use this field in one of two ways: generate an event when the normal content is not found in a record or generate an event when illicit content is found in a record. The resulting event is of severity "Major" and has the message "DNS expression match failure". Your choices are:

- Yes. Use this setting to look for illicit content in a DNS record.
 - If SL1 finds the illicit string (specified in the **Result Match** field), SL1 will generate an event.
 - If SL1 does not find the illicit string (specified in the **Result Match** field), SL1 will not generate an event.
- No. Use this setting to ensure that a DNS record contains the expected content.
 - If SL1 finds the expected string (specified in the **Result Match** field), SL1 does not generate an event.
 - If SL1 does not find the expected string (specified in the **Result Match** field), SL1 generates an event.
- **State**. Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled*. SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Admin Processes) for the **Data Collection: DNS Policy Monitoring** process.
 - *Disabled*. SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.


5. To save the new policy, select the **[Save]** button.

Editing a Monitoring Policy for a Domain Name

There are two places in SL1 from which you can edit a monitoring policy for a domain name:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ()

Or:

2. From the **Domain Name Monitoring** page (Registry > Monitors > Domain Name):
 1. In the **Domain Name Monitoring** page, find the policy you want to edit and select that policy's wrench icon ()

2. The **Domain Name Policy** modal page appears.

The screenshot shows a modal window titled "Create New Domain Name Policy" with a "Close / Esc" button in the top right. Inside the modal, there is a "Create New Policy" header with "New" and "Reset" buttons. The form is organized into several sections:

- Select Device:** A dropdown menu showing "[device 1]".
- Domain Name:** A text input field containing "docmail.sciencelogic.com".
- Name Server IP Address:** A text input field containing "192.168.10.21".
- Record Type:** A dropdown menu showing "A - Address Record".
- Timeout:** A dropdown menu showing "[10 sec.]".
- Result Match:** A text input field containing "192.168.10.201".
- Alert if Found:** A dropdown menu showing "[No]".
- State:** A dropdown menu showing "[Enabled]".

A "Save" button is located at the bottom right of the form area.

3. In the **Domain Name Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining a Monitoring Policy for Domain Name](#).
4. To save your changes to the policy, select the **[Save]** button.

Example Policy for Domain Name

This screenshot shows the same "Create New Domain Name Policy" modal window, but with the following example values entered:

- Select Device:** "[device 1]"
- Domain Name:** "docmail.sciencelogic.com"
- Name Server IP Address:** "192.168.10.21"
- Record Type:** "A - Address Record"
- Timeout:** "[10 sec.]"
- Result Match:** "192.168.10.201"
- Alert if Found:** "[No]"
- State:** "[Enabled]"


The "Save" button is visible at the bottom right of the form.

- In this policy, we associated the device "device 1" with our policy.
- On the name server 192.168.10.21, we searched for the domain "docmail.sciencelogic.com". Specifically we searched the "A" record for the domain.
- We expect the "A" record to include the IP address "192.168.10.201" (this is the IP address of the device "device 1").
- If the "A" record doesn't exist or doesn't include the specified IP address, SL1 will generate an event.

Executing the Domain-Name Monitoring Policy

After creating or editing a domain-name monitoring policy, you can manually execute the policy and view detailed logs of each step during the execution. To do so:

NOTE: After you define a domain-name monitoring policy and enable the policy, SL1 will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.


1. In the **Domain Name Monitoring** (Registry > Monitors > Domain Name) page, find the policy you want to run manually.
2. Select the lightning bolt icon () to manually execute the policy.
3. While the policy is executing, SL1 opens a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is helpful for diagnosing possible problems with a policy.

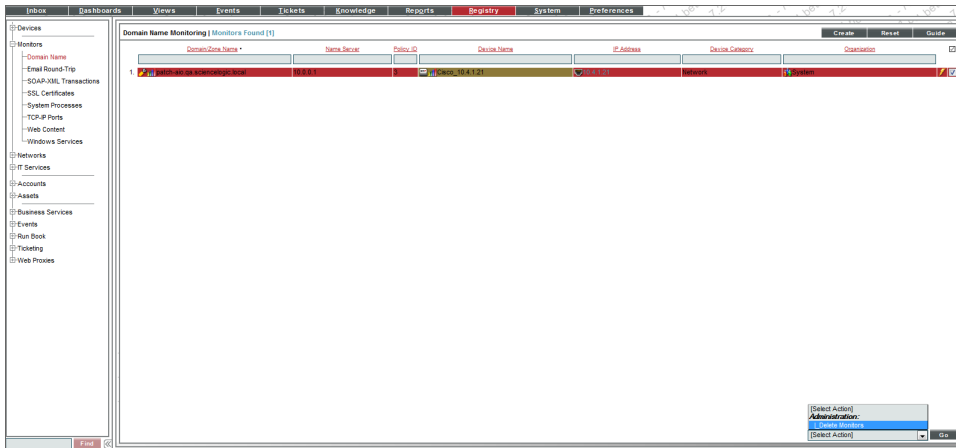
Viewing Reports for a Domain-Name Monitoring Policy

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for domain-name monitoring.

Deleting a Domain-Name Policy

You can delete a domain-name policy from the **Domain Name Monitoring** page. Deleting a domain-name monitoring policy will remove all data that was previously collected by the policy. You can delete individual, multiple, or all existing domain-name monitoring policies. To delete a domain-name monitoring policy:

1. Go to the **Domain Name Monitoring** page (Registry > Monitors > Domain Name).
2. In the **Domain Name Monitoring** page, select the checkbox(es) for each domain name policy you want to delete. Click the checkmark icon () to select all of the domain-name monitoring policies.
3. In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.



4. Select the **[Go]** button to delete the selected domain-name monitoring policies.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.



Chapter

18

Monitoring Email Round-Trips

Overview

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:

<i>Monitoring Email</i>	367
<i>Viewing the Email Round-Trip Monitoring Policies</i>	369
<i>Filtering the List of Email Round-Trip Monitoring Policies</i>	369
<i>Defining an Email Round-Trip Monitoring Policy</i>	370
<i>Editing an Email Round-Trip Monitoring Policy</i>	375
<i>Example Email Round-Trip Monitoring Policy</i>	376
<i>How the ScienceLogic Platform Collects and Calculates Round-Trip Time</i>	376
<i>Viewing Reports on an Email Round-Trip Monitoring Policy</i>	377
<i>Deleting an Email Round-Trip Monitoring Policy</i>	377
<i>Events for Email Round-Trip Policies</i>	378

Monitoring Email

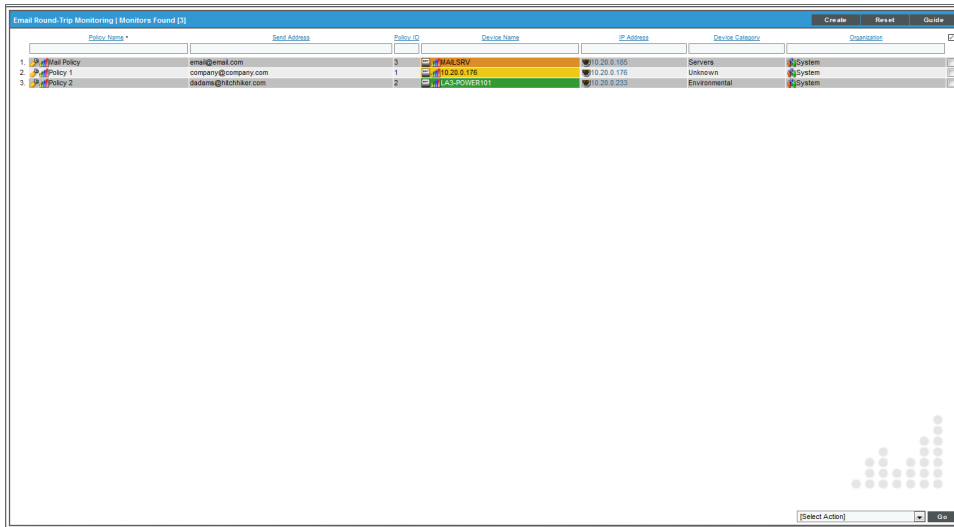
An Email Round-Trip policy monitors the total amount of time it takes to:

- Send an Email message from SL1 to an external Email server.
- Receive a response from the external Email server.

In the policy editor, you specify which mailbox SL1 should send messages to. For each Email policy, SL1 will collect data and create trend reports about availability and round-trip time.

Viewing the Email Round-Trip Monitoring Policies

You can view a list of Email round-trip monitoring policies from the **Email Round-Trip Monitoring** page. The **Email Round-Trip Monitoring** page displays the following about each Email policy:



The screenshot shows a web interface titled "Email Round-Trip Monitoring [Monitors Found: 3]". It contains a table with the following columns: Policy Name, Send Address, Policy ID, Device Name, IP Address, Device Category, and Organization. There are three rows of data:

Policy Name	Send Address	Policy ID	Device Name	IP Address	Device Category	Organization
Mail Policy	email@email.com	0	MAIL-SRV	10.20.0.100	Servers	System
Policy 1	comsary@comsary.com	1	10.20.0.100	10.20.0.100	Unknown	System
Policy 2	adams@hchikar.com	2	LA3-POWER01	10.20.0.253	Environmental	System

- **Email Round-Trip Policy Name.** Name of the policy.
- **Send Address.** Address to which the policy sends test messages.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of Email Round-Trip Monitoring Policies

You can filter the list on the **Email Round-Trip Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **Email Round-Trip Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Email Round-Trip Monitoring** page searches for policies 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:

- **Policy Name.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching name.
- **Send Address.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching send address.
- **Policy ID.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching policy ID.
- **Device Name.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Class.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device class.
- **Organization.** You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching organization.

Defining an Email Round-Trip Monitoring Policy

NOTE: As soon as you save an Email Round-Trip policy, SL1 will begin sending Email messages to the external Email server. ScienceLogic recommends that you define system settings and configure the external Email system **before** saving the Email Round-Trip policy.

Required System Settings in the ScienceLogic Platform

Before you can define a monitoring policy for round-trip Email, you must define the following system settings for SL1:

1. Go to the **Email Settings** page (System > Settings > Email).

The screenshot displays the 'Email Settings' configuration page. It features a header with 'Email Settings' and buttons for 'Refresh' and 'Guide'. The main content area contains several input fields with the following values: 'Authorized Email Domains' is 'your-domain-goes-here.com'; 'System From Email Address' is 'root@your-domain-goes-here.com'; 'Email Formal Name' is 'EM7 Event Notifier'; 'Email Gateway' is '192.168.0.1'; 'Email Gateway Alt' is '192.168.0.2'; and 'Escalation Notify Subject' is 'TICKET ESCALATED: #%I | %M | %T | %F'. A 'Save' button is located at the bottom center of the form.

2. In the **Email Settings** page, you must define the value of the following fields to use Email round-trip monitoring policies:
 - **Authorized Email Domains.** The fully qualified domain name of the Database Server or the All-In-One Appliance.
 - A DNS MX record must already exist or be created for each domain specified in this field. Each All-In-One Appliance and each Database Server includes a built-in Email server. When creating the required DNS MX record, you can specify the fully-qualified name of the Database Server or the fully-qualified name of the All-In-One Appliance as the name of the Email server.
 - **System From Email Address.** Full Email address from which SL1 will sent all outbound Email. Specify a mailbox and an Email domain from the list specified in the **Authorized Email Domains** field. For example, if company.com is one of the authorized Email domains, you could specify "mailbox@company.com". SL1 would then check this mailbox for Email messages associated with Email round-trip policies.
 - **Email Formal Name.** Name that will appear in "from" field in Email messages sent from SL1.

- **Email Gateway.** IP address or fully-qualified name of SL1's SMTP Relay server. To use the relay server that is built-in to SL1, enter the IP address or fully-qualified name of the Database Server of the All-In-One Appliance.

If SL1 cannot use its built-in SMTP relay server to route Email messages directly to their destination server (for example, due to firewall rules or DNS limitations), SL1 can use another relay server. You can specify the IP address or fully-qualified name of the relay server in this field. Make sure you have configured your network to allow the SL1 appliance to access this SMTP Relay server.

- **Email Gateway Alt.** IP address or fully-qualified name of the secondary SMTP Relay server. If the SMTP Relay server specified in the previous field fails or is unavailable, SL1 will use the secondary SMTP Relay server. Make sure you have configured your network to allow the SL1 appliance to access this SMTP Relay server.

3. Select the **[Save]** button to save the settings.

Required Configuration on the External Email Client

NOTE: As soon as you save the Email Round-Trip policy, SL1 will begin sending Email messages to the external Email server. ScienceLogic recommends that you define system settings and configure the external Email system **before** saving the Email Round-Trip policy.

For an Email round-trip policy to work correctly, the external Email system must automatically send a reply message to SL1. To make this happen, you must define an auto-forwarding policy or rule on the external Email system that causes the external Email system to send a reply Email message back to SL1.

- You must define an auto-forwarding policy on the external Email system.
- The auto-forwarding policy should look for Email with a "from" address defined in the **Address Masquerade** field of the Email policy.
- If necessary, the auto-forwarding policy can also search for text in the message body. The text will be that defined in the **Message Body** field of the Email policy.
- The auto-forwarding policy should send a return message from the same Email address as that specified in the **Send To Address** field of the Email policy.
- The auto-forwarding policy should **include the subject from the original message and the body from the original message** (from SL1) in the reply Email. This is easiest to achieve by forwarding the original Email message to SL1.
- The auto-forwarding policy should send the Email to the following address:

notify@domain-name-of-SL1

Where "domain-name-of-SL1" is one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the **Authorized Email Domains** field in the **Email Settings** page.

Defining the Policy

There are two places in SL1 from which you can define a monitoring policy for round-trip Email:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon (🔧) for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - From the **[Create]** menu in the upper right, select **Create Email Round-Trip Policy**.

Or:

2. From the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip):
 - In the **Email Round-Trip Monitoring** page select the **[Create]** button.
3. The **Email Round-Trip Policy** modal page appears.

The screenshot shows a modal window titled "Create New Email Round-Trip Policy" with a red header bar. Below the header is a status bar indicating "Editing Policy [1] | Policy Successfully Saved" and buttons for "New" and "Reset". The main area is split into two columns. The left column contains several form fields: "Policy Name" (silos_email_rt), "Validation Type" (Email Round Trip), "Send To Address" (mantone@sciencelogic.com), "Address Masquerade" (empty), "Timeout" (2 minutes), and "State" (Enabled). A "Save" button is at the bottom of this column. The right column is titled "Message Body" and contains a text area with the text "testing email round trip".



4. In the **Email Round-Trip Policy** modal page, supply a value in each of the following fields:
 - **Select Device**. Select a device from this drop-down list to align with this policy. By default, the current device is selected in this field.

NOTE: Before you can define an Email round-trip policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the device to which SL1 will send test messages, but you aren't required to do so. Alternately, you might want to create a virtual device to associate with a Email round-trip policy. Although SL1 will use only the **Send To Address** to execute the policy, the reports that result from the Email round-trip policy will be aligned with the device you specify in the **Select Device** field.


- **Policy Name.** Name of the Email round-trip policy. Can be any combination of letters and numbers.
 - **Validation Type.** Can select only *Email Round Trip*.
 - **Send To Address.** Email address for the external Email server. Must be a valid Email address. This mailbox must be configured to auto-respond to messages from the Email round-trip policy.
 - **Address Masquerade.** Email address to use as the "From" address. Must be a valid Email address. You should choose an address that allows the external Email client to easily identify the incoming Email as one from the Email round-trip policy.
 - **Timeout.** Number of seconds SL1 should wait for a response Email message. If SL1 does not receive a response message after the specified number of seconds, SL1 generates an event.
 - **State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Admin Processes) for the **Data Collection: E-Mail round-Trip** process.
 - *Disabled.* SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.
 - **Message Body.** Body of the Email message to be sent. In some cases, the auto-responder on the external Email server may search this message body. Therefore, you should choose a message body that allows the external Email client to easily identify the incoming Email as one from the Email round-trip policy.
5. Select the **[Save]** button to save the new policy. SL1 will immediately begin sending Email messages to the **Send To Address**.

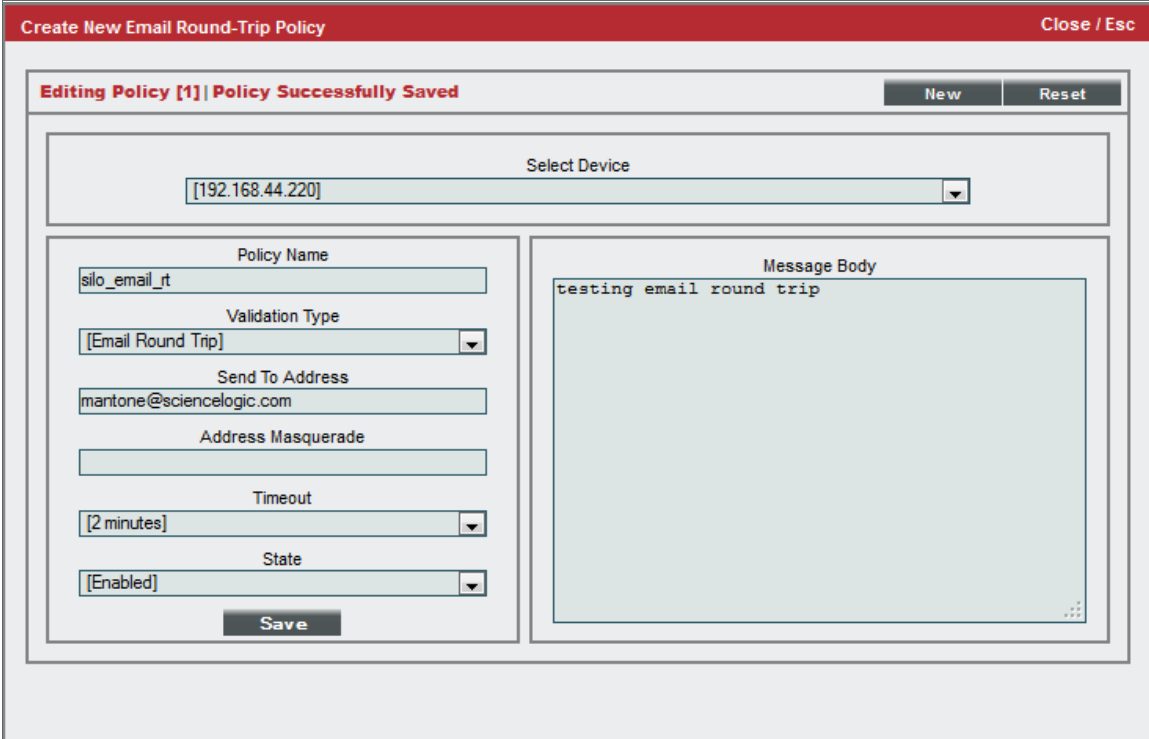
Editing an Email Round-Trip Monitoring Policy

There are two places in SL1 from which you can edit a monitoring policy for a round-trip Email:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ().

Or

2. From the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip):
 - In the **Email Round-Trip Monitoring** page, find the policy you want to edit and select its wrench icon ().
3. The **Email Round-Trip Policy** modal page appears.



Create New Email Round-Trip Policy Close / Esc

Editing Policy [1] | Policy Successfully Saved New Reset

Select Device
[192.168.44.220]

Policy Name
silo_email_rt

Validation Type
[Email Round Trip]

Send To Address
mantone@sciencelogic.com

Address Masquerade

Timeout
[2 minutes]

State
[Enabled]

Save

Message Body
testing email round trip

4. In the **Email Round-Trip Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining an Email Round-Trip Monitoring Policy](#).
5. Select the **[Save]** button to save your changes to the policy.

Example Email Round-Trip Monitoring Policy

The screenshot shows a web-based configuration interface for an email round-trip policy. The window title is "Create New Email Round-Trip Policy" with a "Close / Esc" button in the top right. The main content area has a red header bar that says "Editing Policy [1] Policy Successfully Saved" and contains "New" and "Reset" buttons. Below this is a "Select Device" dropdown menu with the value "[192.168.44.220]". The main configuration area is split into two columns. The left column contains several fields: "Policy Name" (silo_email_rt), "Validation Type" (Email Round Trip), "Send To Address" (mantone@sciencelogic.com), "Address Masquerade" (empty), "Timeout" (2 minutes), and "State" (Enabled). A "Save" button is at the bottom of this column. The right column contains a "Message Body" text area with the text "testing email round trip".

- In this example, we associated the policy with the device "192.168.44.220".
- The policy sent an Email message to "mantone@sciencelogic.com". The message contained the body "testing Email round trip".
- The mailbox for mantone@sciencelogic.com included a rule to automatically forward the message back to the original sender.

How the ScienceLogic Platform Collects and Calculates Round-Trip Time

After an Email Round-Trip Monitoring Policy has been configured, SL1 will send one Email every five minutes to the **Send To Address** defined in the policy. SL1 keeps a record of every sent Email. The same process also checks to see if a response has been received from previously sent Emails.

The response Email that SL1 receives must contain the body of the Email that was sent by SL1, which contains a unique ID number. SL1 compares the unique ID in the response Email to the record of Emails that SL1 sent. By matching the response to the original Email using the unique ID, SL1 can handle cases where the response Emails are received out of order.

After SL1 has matched the response Email to the corresponding sent Email, SL1 calculates the round-trip time. To calculate the round-trip time, SL1 subtracts the time the original Email was sent from the time the response was received. The time the response was received is determined by the timestamp in the "Received" header of the response Email.

NOTE: The smallest unit of time recorded in the "Received" header of a response Email is seconds; therefore, Email round-trip times are accurate only to the nearest second. If the response Email is received in the same second the original Email was sent, SL1 will record a round-trip time of zero seconds.

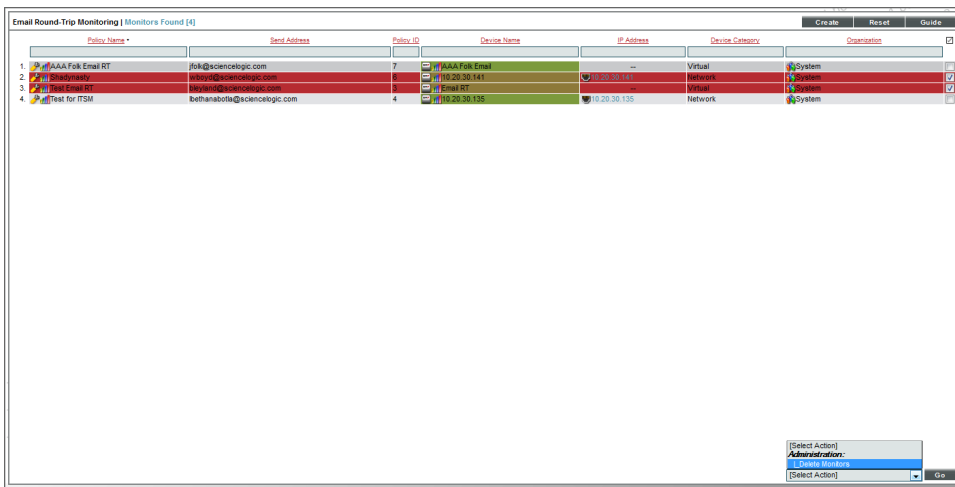
Viewing Reports on an Email Round-Trip Monitoring Policy

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for Email round-trip monitoring.

Deleting an Email Round-Trip Monitoring Policy

You can delete one or more Email round-trip policies. When you delete a Email round-trip policy, SL1 no longer uses the policy to collect data from the aligned device. SL1 also deletes the reports associated with the policy. To delete an Email round-trip monitoring policy:

1. Go to the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip).
2. In the **Email Round-Trip Monitoring** page, select the checkbox(es) for each Email round-trip monitoring policy you want to delete. Click the checkmark icon (☑) to select all of the Email round-trip monitoring policies.



3. In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.
4. Select the **[Go]** button to delete the selected Email round-trip monitoring policies.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Events for Email Round-Trip Policies

If the Email Round-Trip policy encounters problems, SL1 will trigger events. You can view these events in the **Event Console**.



An Email Round-Trip policy can generate one or more of the following events:

Event Message	Severity	Description	Cause	Clears Event(s)
Mail arrived late - round trip time: %V (%V is replaced with the value returned by SL1)	Notice	External Email system sent an email back to SL1, but not within the Timeout period for the policy.	A delay occurred at some point in the path from the external Email system to SL1.	N/A
Mail did not arrive within threshold time	Major	External Email system did not send an Email back to SL1.	A block occurred at some point in the path from the external Email system to SL1.	N/A
Email Round Trip Outage Ended	Healthy	Round-trip Email policy is working again as expected.	Previous problem was solved.	Mail arrived late - round trip time: %V Mail did not arrive within threshold time
Mail returned to sender - reason: %V %V is replaced with the value returned by SL1)	Major	SL1 was unable to successfully send an Email to the external Email system.	There is a problem with the destination mailbox, or rules on the destination server prevent mail from being delivered from SL1.	N/A

Monitoring SOAP and XML Transactions

Overview

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:

<i>Monitoring SOAP or XML Transactions</i>	380
<i>Viewing the SOAP/XML Transaction Monitoring Policies</i>	381
<i>Filtering the List of SOAP/XSL Transaction Policies</i>	382
<i>Defining a SOAP/XML Transaction Policy</i>	382
<i>Editing a SOAP/XML Transaction Policy</i>	385
<i>Executing a SOAP/XML Transaction Policy</i>	387
<i>Example SOAP/XML Transaction Policy</i>	387
<i>Viewing Reports on a SOAP/XML Transaction Policy</i>	388
<i>Viewing Raw Data from a SOAP/XML Policy</i>	388
<i>Deleting a SOAP/XML Policy</i>	388

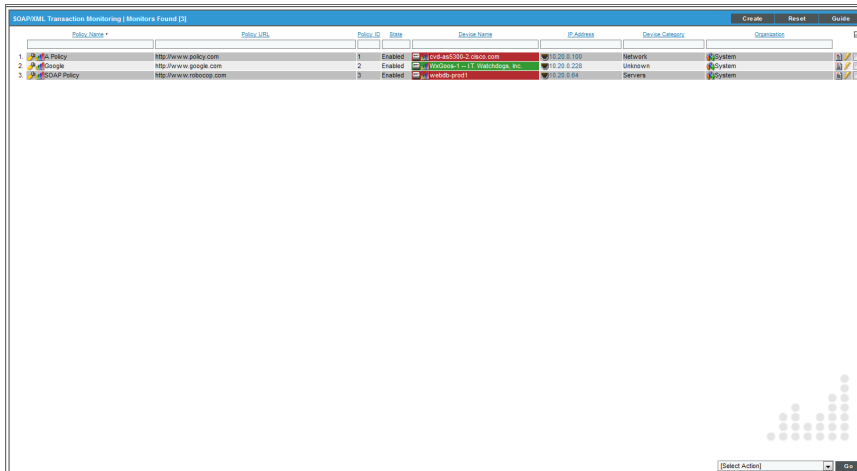
Monitoring SOAP or XML Transactions

A SOAP/XML transaction policy can monitor any server-to-server transaction that uses HTTP and can post files or forms (most commonly SOAP or XML but also Email or RSS feeds). SL1 sends a request and some data and then examines the result of the transaction and compares it to a specified expression match.

For each SOAP/XML policy, SL1 will collect data and create trend reports about availability, page size, download speed, lookup time, connection time, and transaction time.

Viewing the SOAP/XML Transaction Monitoring Policies

You can view a list of SOAP/XML transaction monitoring policies from the **SOAP/XML Transaction Monitoring** page. The **SOAP/XML Transaction Monitoring** page displays the following information on each policy:



The screenshot shows a web application window titled "SOAP/XML Transaction Monitoring (Monitors Found [2])". It contains a table with the following columns: Policy Name, Policy URL, Policy ID, State, Device Name, IP Address, Device Category, and Organization. There are three rows of data:

Policy Name	Policy URL	Policy ID	State	Device Name	IP Address	Device Category	Organization
1 Policy	http://www.policy.com	1	Enabled	ip-10-20-0-100	10.20.0.100	Network	System
2 Google	http://www.google.com	2	Enabled	ip-10-20-0-228	10.20.0.228	Unknown	System
3 SOAP Policy	http://www.ibmsoap.com	3	Enabled	ip-10-20-0-104	10.20.0.104	Server	System

- **SOAP/XML Policy Name**. Name of the policy.
- **Policy URL**. URL to which the policy sends test transactions.
- **Policy ID**. Unique, numeric ID, assigned to the policy automatically by SL1.
- **Device Name**. Name of the device associated with the policy.
- **IP Address**. IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category**. Device category of the device associated with the policy.
- **Organization**. Organization for the device associated with the policy.

Filtering the List of SOAP/XSL Transaction Policies

You can filter the list of policies on the **SOAP/XML Transaction Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **SOAP/XML Transaction Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **SOAP/XML Transaction Monitoring** page searches for policies 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:

- **Policy Name.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies that have a matching name.
- **Policy URL.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies that act on a matching URL.
- **Policy ID.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies that have a matching policy ID.
- **Device Name.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Category.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies aligned with a device with a matching device category.
- **Organization.** You can enter text to match, including special characters, and the **SOAP/XML Transaction Monitoring** page will display only policies that have a matching organization.

Defining a SOAP/XML Transaction Policy

There are two places in SL1 from which you can define a monitoring policy for SOAP/XML transactions:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - From the **[Create]** menu in the upper right, select **Create SOAP/XML Transaction Policy**.

Or:

2. From the **SOAP/XML Transaction Monitoring** page (Registry > Monitors > SOAP/XML Transactions):
 - In the **SOAP/XML Transaction Monitoring** page, select the **[Create]** button.
3. The **SOAP/XML Transaction Policy** modal page appears.

4. In the **SOAP/XML Transaction Policy** modal page, supply a value in each of the following fields:
 - **Select Device**. Select a device from this drop-down list to align with this policy. By default, the current device is selected in this field.

NOTE: Before you can define a SOAP/XML policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the device where the SOAP server or XML datastore resides, but you aren't required to do so. Alternately, you might want to create a virtual device to associate with a SOAP/XML transaction policy. Although SL1 will not use the device name to determine where to send the policy data, the reports that result from the policy will be aligned with the device you specify in the **Select Device** field.

- **Policy Name**. Name of the new policy. Can be any combination of letters and numbers.
- **State**. Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:

- *Enabled*. SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Processes) for the **Data Collection: Web Transaction Verifier** process.
- *Disabled*. SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.
- **Port**. Port on web-server to which SL1 will send queries. This is usually port 80 (the HTTP port), or port 443 (the HTTPS port).
- **Timeout**. After the specified number of seconds, SL1 should stop trying to connect to the server. If the timeout period elapses before SL1 can connect to the server, an event is generated.
- **Proxy Server:Port**. For companies or organizations that use proxy servers, enter the URL and port for the proxy server in this field. Use the format:

URL:port_number.

- **Proxy Account:Password**. For companies or organizations that use proxy servers, enter the username and password for the proxy server in this field. Use the format:

username:password.

- **Post File Name**. Some server-to-server transactions require data to be uploaded or sent as a Post File. For example, such a file may contain an XML or RSS feed. To send a Post File, specify a name, such as "myrss.xml" in this field. Supply the deliverable data in the **Post Data Content** field.
- **Uniform Resource Locator (URL)**. URL or URI of the server to send the transaction to.
- **Post String**. If the URL is very long or requires data that cannot be transferred with a standard "GET" request (that is, data that cannot be included in the URL), you can enter a POST string in this field. The format is:

var1=val1&var2=val2&var3=val3

If you are going to include more than one variable/value pair, separate each pair with an ampersand (&).

For example, suppose you want to send values for the following fields:

Birthyear

Value

You could enter the following in the **Post String** field:

Birthyear=1980%Value=OK



NOTE: If you want to include non-alphanumeric characters in the **Post String** field, make sure you encode the characters using appropriate URL encoding.

- **Content Encoding**. Specifies the encoding method used for the request. Choices are:
 - *text/xml*
 - *application/x-www-form-urlencoded*
 - *multipart/form-data*
 - *application/soap+xml*
 - *text/xml; charset=utf-8*
- **Request Method**. Specifies whether the request will be sent as an HTTP POST or an HTTP GET request.
- **Post Data / Content**. Data to send to the remote server, such as the body of a SOAP request. If you entered a value in the **Post File Name** field, enter the deliverable data in this field.
- **Auth Account:Password**. For websites that pop-up a dialog box asking for user name and password, use this field. Enter the username and password in this field. Use the format username:password.
- **SSL Mode**. Specifies whether SL1 should use SSL when communicating with the httpd service.
- **Expression Check #1**. Regular expression to search for. Can be any alphanumeric value, up to 128 characters in length.
- **Expression Check #2**. Another regular expression to search for. Can be any alphanumeric value, up to 128 characters in length.
- **Custom Header Elements**. Allows you to include a custom header with your transaction. Enter the header in this field.
- **Compatibility**. Specifies the type of application SL1 will be communicating with on the server. Choices are:
 - *Default*. Standard HTTP/HTTPS.
 - *SOAP*. SOAP-based requests.
 - *Cisco AXL*. Cisco AXL interface.

5. Select the **[Save]** button to save the new policy.

Editing a SOAP/XML Transaction Policy

There are two places in SL1 from which you can edit a monitoring policy for SOAP/XML transactions:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ().

Or:


2. From the **SOAP/XML Transaction Monitoring** page (Registry > Monitors > SOAP-XML Transactions):
 - In the **SOAP/XML Transaction Monitoring** page, find the policy you want to edit and select its wrench icon (🔧).
3. The **SOAP/XML Transaction Policy** modal page appears.

4. In the **SOAP/XML Transaction Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining a Policy for Monitoring SOAP/XML Transactions](#).
5. Select the **[Save]** button to save your changes to the policy.

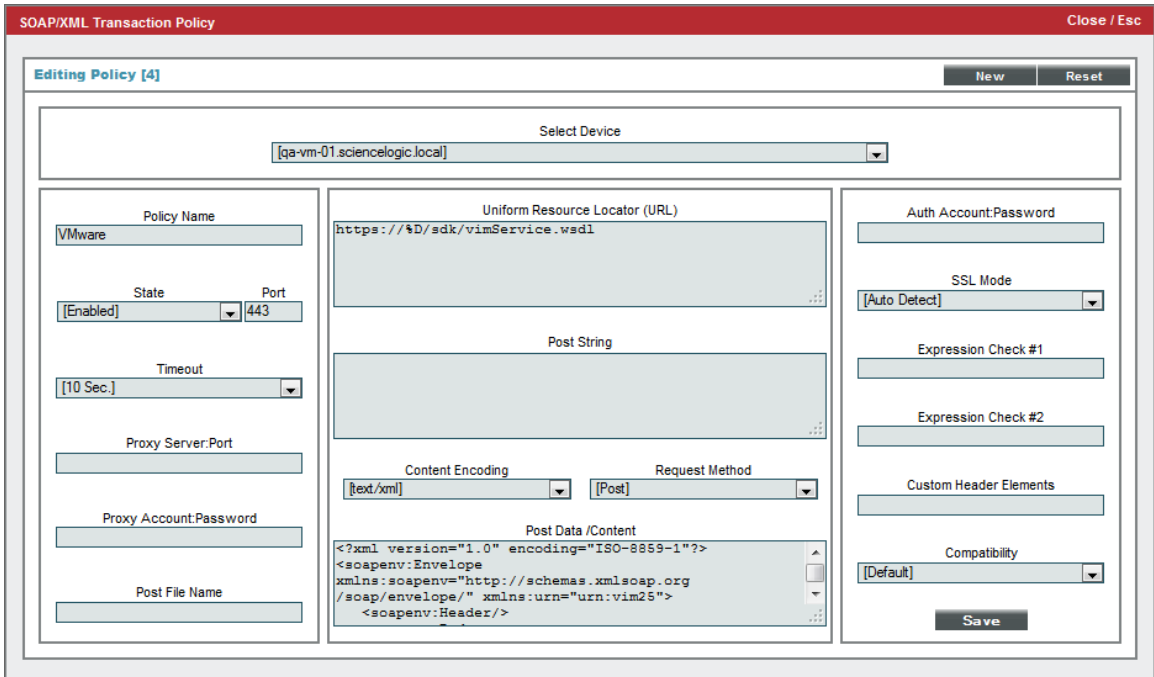
Executing a SOAP/XML Transaction Policy

After creating or editing a SOAP/XML transaction policy, you can manually execute the policy and view detailed logs of each step during the execution. To do so:

NOTE: After you define a SOAP/XML transaction monitoring policy and enable the policy, SL1 will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.

1. In the **SOAP/XML Transaction Monitoring** page, find the policy you want to run manually.
2. Select the lightning bolt icon () to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Example SOAP/XML Transaction Policy



The screenshot shows a web-based configuration interface for a SOAP/XML Transaction Policy. The interface is titled "Editing Policy [4]" and includes a "Close / Esc" button in the top right corner. The main configuration area is divided into several sections:

- Select Device:** A dropdown menu showing "qa-vm-01.sciencelogic.local".
- Policy Name:** A text input field containing "VMware".
- State:** A dropdown menu set to "Enabled".
- Port:** A text input field containing "443".
- Timeout:** A dropdown menu set to "[10 Sec.]".
- Proxy Server:Port:** An empty text input field.
- Proxy Account:Password:** An empty text input field.
- Post File Name:** An empty text input field.
- Uniform Resource Locator (URL):** A text area containing "https://%D/sdk/vimService.wsdl".
- Post String:** An empty text area.
- Content Encoding:** A dropdown menu set to "[text/xml]".
- Request Method:** A dropdown menu set to "[Post]".
- Post Data /Content:** A text area containing the following XML content:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org
/soap/envelope/" xmlns:urn="urn:vim25">
<soapenv:Header/>
```
- Auth Account:Password:** An empty text input field.
- SSL Mode:** A dropdown menu set to "[Auto Detect]".
- Expression Check #1:** An empty text input field.
- Expression Check #2:** An empty text input field.
- Custom Header Elements:** An empty text input field.
- Compatibility:** A dropdown menu set to "[Default]".

A "Save" button is located at the bottom right of the configuration area.

- In this example, the policy monitors SOAP transaction to a VMware ESX server at "https://%D/sdk/vimService.wsdl". VMware ESX servers accept SOAP requests.
- The policy uses cURL to send a SOAP request to the ESX server.

- The SOAP request includes a SOAP API "RetrieveServiceContent". This API ensures the SL1 can communicate with the VMware server and returns information about the services available on the VMware server.


Viewing Reports on a SOAP/XML Transaction Policy

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for monitoring port availability.

Viewing Raw Data from a SOAP/XML Policy

You can view the raw data sent from SL1 to the external URL and the raw data returned to SL1. This feature can be helpful when troubleshooting a policy.


To view raw data from a SOAP/XML policy:

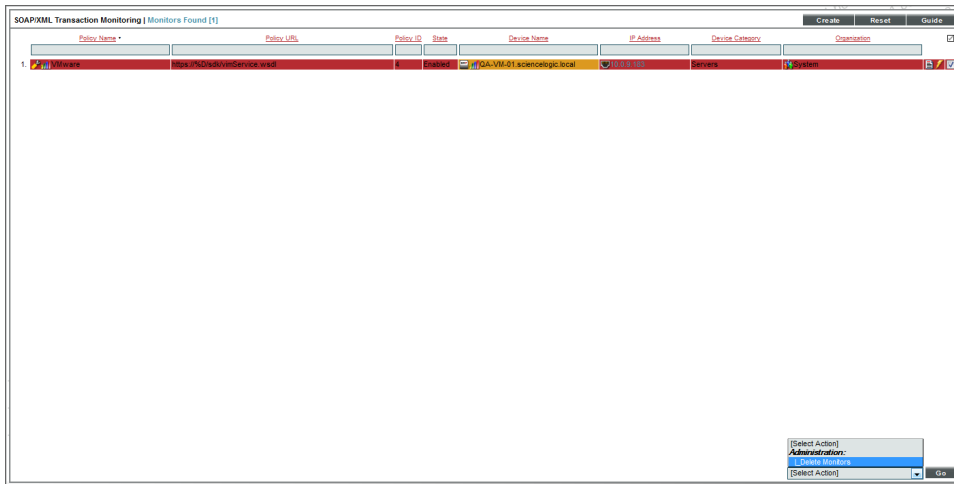
1. In the **SOAP/XML Transaction Monitoring** page, find the policy you want to view raw data for.
2. Select the page icon () to the far left in the table.
3. The **Results Page Dump** modal page appears. This page displays the raw data sent to the external URL and the raw data returned to SL1.

Deleting a SOAP/XML Policy

You can delete individual, multiple, or all existing SOAP/XML policies. When you delete a SOAP/XML Transaction Monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

To delete a SOAP/XML policy:

1. Go to the **SOAP/XML Transaction Monitoring** page (Registry > Monitors > SOAP-XML Transactions).
2. In the **SOAP/XML Transaction Monitoring** page, select the checkbox(es) for each SOAP/XML policy you want to delete. Click the checkmark icon () to select all of the SOAP/XML policies.
3. In the **Select Action** menu in the bottom right of the page, select *Delete Monitors*.



4. Select the **[Go]** button to delete the selected SOAP/XML monitoring policies.
5. The policy is deleted from SL1 . The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.



Chapter

20

Monitoring Web Content

Overview

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:

<i>Monitoring Web Content</i>	390
<i>Viewing the Web Content Monitoring Policies</i>	391
<i>Filtering the List of Web Content Monitoring Policies</i>	392
<i>Defining a Web Content Policy</i>	393
<i>Executing the Web Content Monitoring Policy</i>	398
<i>Editing a Web Content Policy</i>	398
<i>Viewing Reports on a Web Content Policy</i>	400
<i>Viewing ASCII Page Content</i>	400
<i>Viewing the Monitored Website</i>	401
<i>Deleting a Web Content Monitoring Policy</i>	402

Monitoring Web Content

SL1 allows users to create policies that monitor a website for specific content. This is helpful:

- To determine if a website is up and running.
- To determine if the connection between a webserver and a database is up and running.
- To monitor system tools that can be accessed through a browser.
- To monitor content on a website.

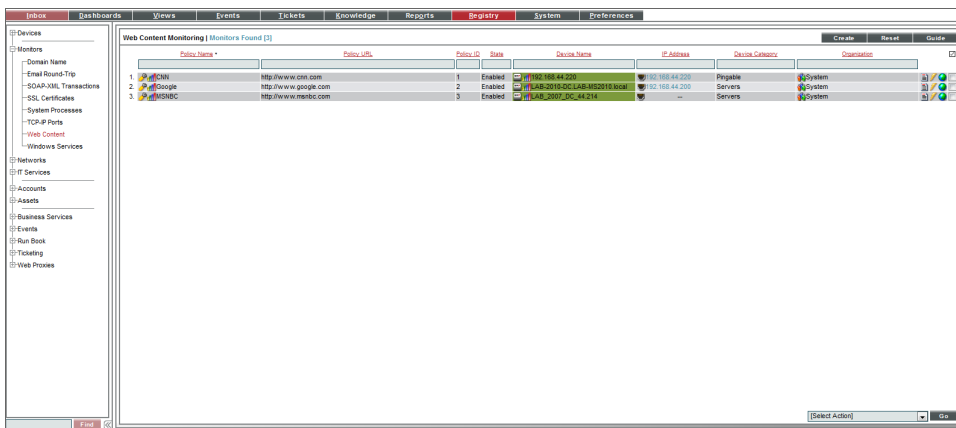
If SL1 cannot match the expression in the content policy with the text on the website, SL1 generates an event.

SL1 uses cURL to send and receive data from the website.

NOTE: Web content monitoring policies cannot monitor web sites larger than 1 MB.

Viewing the Web Content Monitoring Policies

You can view a list of web content monitoring policies from the **Web Content Monitoring** page (Registry > Monitors > Web Content). The **Web Content Monitoring** page displays the following information for each web content monitoring page:



- **Web Content Policy Name.** Name of the policy.
- **Policy URL.** The URL that SL1 will monitor for specified content.
- **Policy ID.** Unique, numeric ID, assigned to the policy automatically by SL1.
- **State.** Whether SL1 will monitor the external website. This column will either show "Enabled" (SL1 will monitor the external website) or "Disabled" (SL1 will not monitor the external website).
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of Web Content Monitoring Policies

You can filter the list of policies on the **Web Content Monitoring** page by one or more parameters. Only policies that meet all the filter criteria will be displayed in the **Web Content Monitoring** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Web Content Monitoring** page searches for policies 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:

- **Policy Name.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies with a matching name.
- **Policy URL.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies that monitor URLs that match the text.
- **Policy ID.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies that have a matching policy ID.
- **State.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies that have a matching state (enabled or disabled).
- **Device Name.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Category.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies aligned with a device with a matching device category.
- **Organization.** You can enter text to match, including special characters, and the **Web Content Monitoring** page will display only policies that have a matching organization.

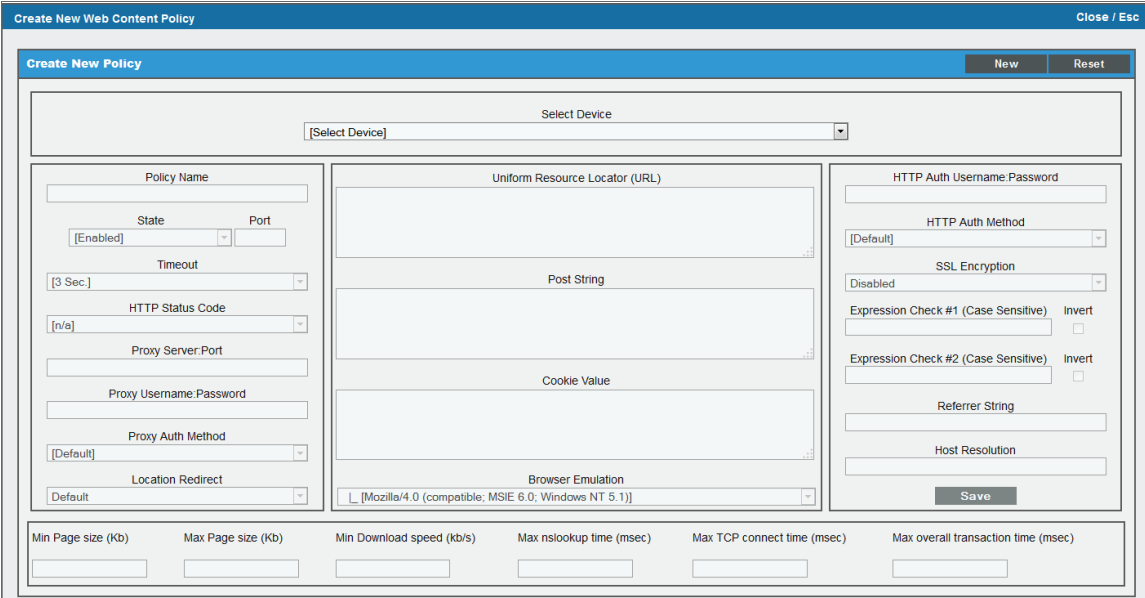
Defining a Web Content Policy

There are two places in SL1 from which you can define a policy for monitoring web content:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select the wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - From the **[Create]** menu in the upper right, select **Create Web Content Policy**.

Or:

2. From the **Web Content Monitoring** page (Registry > Monitors > Web Content):
 - In the **Web Content Monitoring** page, select the **[Create]** button.
3. The **Web Content Policy** modal page appears.



4. In the **Web Content Policy** modal page, supply a value in the following fields:
 - **Select Device**. From this drop-down list, select a device to align with this policy. By default, the current device is selected in this field.

NOTE: Before you can define a content policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the web server you will be monitoring with the policy, but you aren't required to do so. The requests to the web server will be sent from an appliance, but you must still associate the policy with a device.

- **Policy Name.** Name of the new policy. Can be any combination of letters and numbers.
- **State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Processes) for the **Data Collection: Web Content Verifier** process.
 - *Disabled.* SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.
- **Port.** Port on web-server to which SL1 will send queries. This is usually port 80 (the HTTP port), or port 443 (the HTTPS port).
- **Timeout.** After specified number of seconds, SL1 should stop trying to connect to the server. If the timeout period elapses before SL1 can connect to the server, an event is generated.
- **HTTP Status Code.** Specify the HTTP status code you expect to receive in the response. If any other status code is returned, SL1 will generate an event.
- **Proxy Server:Port.** For companies or organizations that use proxy servers, enter the URL and port for the proxy server in this field. Use the format:
URL:port_number.
- **Proxy Username:Password.** For companies or organizations that use proxy servers, enter the username and password for the proxy server in this field. Use the format "user name:password".
- **Proxy Auth Method.** For companies or organizations that use proxy servers, specify the type of authentication:
 - *Default.* By default, no authentication parameters are sent. Use this option for proxy servers that do not require authentication. However, if you supply a value in another field that requires authentication, e.g. **Proxy Username:Password**, the *Any* authentication parameter will be used.
 - *Basic.* Most widely compatible authentication across platforms. Sends a Base64-encoded string that contains a user name and password for the client. Base64 is not a form of encryption and should be considered the same as sending the user name and password in clear text.

- *Digest*. Password is transmitted as encrypted text, but the user name and content of the message are not encrypted. Digest authentication is a challenge-response scheme that is intended to replace Basic authentication. The server sends a string of random data called a **nonce** to the client as a challenge. The client responds with a hash that includes the user name, password, and nonce, among additional information.
 - *GSS-Negotiate*. Authenticates using Kerberos and the GSS-API. Kerberos authentication is faster than NTLM and allows the use of mutual authentication and delegation of credentials to remote machines.
 - *NTLM*. NT LAN Manager (NTLM) authentication is a challenge-response scheme that is a more secure variation of Digest authentication. NTLM uses Windows credentials to transform the challenge data instead of the unencoded user name and password. NTLM authentication requires multiple exchanges between the client and server. The server and any intervening proxies must support persistent connections to successfully complete the authentication
 - *Any*. Accept any type of authentication.
 - *Any except Basic (Any Safe)*. Accept any type of authentication except Basic.
- **Location Redirect**. Specifies how you want the policy to behave when it encounters an HTTP redirect in a target website. Choices are:
 - *Default*. If you selected 301, 302, or 303 in the **HTTP Status Code** field, the web content policy will not follow redirection by default. The default behavior for all other web content policies is to follow redirection and search for the regular expression on the website to which SL1 has been redirected.
 - *Always Follow*. When you select this option, web content policies follow redirection and search for the regular expression on the website to which SL1 has been redirected.
 - *Never Follow*. When you select this option, web content policies never follow redirection. This option allows the web content policy to search for a 301, 302, or 303 HTTP status code.
- **Uniform Resource Locator (URL)**. URL or IP address where the website is located. If the website requires login and the login is forms based (user enters username and password in the index page), include the username and password in the URL.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that this policy is aligned to.
 - You can include the variable **%N** in this field. SL1 will replace the variable with the name of the device that this policy is aligned to.
 - You can include the variable **%H** in this field. SL1 will replace the variable with the hostname of the device that this policy is aligned to. If the device was not discovered by hostname, SL1 will replace this variable with the IP address of the device.
- **Post String**. If the URL is very long or requires data that cannot be transferred with a standard "GET" request (that is, data that cannot be included in the URL), you can enter a POST string in this field. The data will be sent with the cURL equivalent of an HTTP POST command. Data should be formatted as follows:

variable=value

If you are going to include more than one variable/value pair, separate each pair with an ampersand (&).

For example, suppose you want to send values for the following fields:

Birthyear

Value

You could enter the following in the **Post String** field:

Birthyear=1980&Value=OK

NOTE: If you want to include non-alphanumeric characters in the **Post String** field, make sure you encode the characters using appropriate URL encoding.

- **Cookie Value.** For pages that require a cookie value to be set, enter the cookie value in this field.
- **Browser Emulation.** Specifies how to format the query. Select the agent that is compatible with the webserver.
- **HTTP Auth Username:Password.** For websites that pop-up a dialog box asking for username and password, use this field. Enter the username and password in this field. Use the format "username:password".
- **HTTP Auth Method.** For websites that require authentication, use one of the selected methods:
 - *Default.* By default, no authentication parameters are sent. Use this option for websites that do not require authentication. However, if you supply a value in another field that requires authentication, e.g. **HTTP Auth Username:Password**, the Any authentication parameter will be used.
 - *Basic.* Most widely compatible authentication across platforms. Sends a Base64-encoded string that contains a user name and password for the client. Base64 is not a form of encryption and should be considered the same as sending the user name and password in clear text.
 - *Digest.* Password is transmitted as encrypted text, but the user name and content of the message are not encrypted. Digest authentication is a challenge-response scheme that is intended to replace Basic authentication. The server sends a string of random data called a **nonce** to the client as a challenge. The client responds with a hash that includes the user name, password, and nonce, among additional information.
 - *GSS-Negotiate.* Authenticates using Kerberos and the GSS-API. Kerberos authentication is faster than NTLM and allows the use of mutual authentication and delegation of credentials to remote machines.
 - *NTLM.* NT LAN Manager (NTLM) authentication is a challenge-response scheme that is a more secure variation of Digest authentication. NTLM uses Windows credentials to transform the challenge data instead of the unencoded user name and password. NTLM authentication requires multiple exchanges between the client and server. The server and any intervening proxies must support persistent connections to successfully complete the authentication

- *Any*. Accept any type of authentication.
 - *Any except Basic (Any Safe)*. Accept any type of authentication except *Basic*.
- **SSL Encryption**. Specifies whether SL1 should use SSL when communicating with the website. If login for the website is forms-based, enable this option.
- **Expression Check #1**. Text to search for:
 - If you select the **Invert** checkbox, SL1 will trigger an event if the text is found.
 - If you do not select the **Invert** checkbox, SL1 will trigger an event if the text is not found.
- **Expression Check #2**. Another text string to search for:
 - If you select the **Invert** checkbox, SL1 will trigger an event if the text is found.
 - If you do not select the **Invert** checkbox, SL1 will trigger an event if the text is not found.
- **Referrer String**. URL of the website. Some load-balanced configurations will not allow a request for a specific IP address. If you entered a specific IP address in the URL field, you can spoof a URL in this field.
- **Host Resolution**. Host name of the website. Some load-balanced configurations will not allow a request for a specific IP address. If you entered a specific IP address in the URL field, you can spoof a fully-qualified host name in this field.
 - You can include the variable **%N** in this field. SL1 will replace the variable with hostname of the device that this policy is aligned to. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
- **Min Page size (Kb)**. Page size means the size of the page, in Kb, specified in the URL of the policy. If the returned page is not at least the size specified in this field, SL1 generates an event. This threshold triggers the event "Page size below minimum threshold."
- **Max Page size (Kb)**. Page size means the size of the page, in Kb, specified in the URL of the policy. If the returned page is larger than the size specified in this field, SL1 generates an event. This threshold triggers the event "Page size above maximum threshold."
- **Min Download speed (kb/s)**. Download speed is the speed, measured in Kb/s, at which data was downloaded from the server (specified in the policy) to SL1. If the download speed is not at least the speed specified in this field, SL1 generates an event. This threshold triggers the event "Download speed below threshold."
- **Max nslookup time (msec)**. NSlookup speed is the speed at which your DNS system was able to resolve the name of the server specified in the policy. If the lookup time exceeds the value in this field, SL1 generates an event. This threshold triggers the event "DNS hostname resolution time above threshold."
- **Max TCP connect time (msec)**. TCP connect time is the time it takes for SL1 to establish communication with the external server. In other words, the time it takes from the beginning of the HTTP request to the TCP/IP connection. If the connection time exceeds the value in this field, SL1 generates an event. This threshold triggers the event "TCP connection time above threshold."


- **Max Overall transaction time (msec)**. Overall transaction time is the total time it takes to make a connection to the external server, send the HTTP request, wait for the server to parse the request, receive the requested data from the server, and close the connection. If the overall transaction time exceeds the value in this field, SL1 generates an event. This threshold triggers the event "Total transaction time above threshold."

5. Select the **[Save]** button to save the new policy.

Executing the Web Content Monitoring Policy



After creating or editing a web content monitoring policy, you can manually execute the policy and view detailed logs of each step during the execution. To do so:

NOTE: After you define a web content monitoring policy and enable the policy, SL1 will automatically execute the policy every five minutes. However, you can use the steps in this section to execute the policy immediately and see debug information about the execution of the policy.


1. In the **Web Content Monitoring** page (Registry > Monitors > Web Content), find the policy you want to run manually.
2. Select the lightning bolt icon () to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal page called **Session Logs**. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Editing a Web Content Policy

There are two places in SL1 from which you can edit a policy to monitor web content:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select its wrench icon ().

Or:

2. From the **Web Content Monitoring** page (Registry > Monitors > Web Content):
 - In the **Web Content Monitoring** page, find the policy you want to edit and select its wrench icon ().

3. The **Web Content Policy** modal page appears:

The screenshot shows the 'Web Content Policy' modal window with the title 'Editing Policy [1]'. At the top, there's a 'Select Device' dropdown menu with 'web content virtual device' selected. Below this, the form is organized into several sections. On the left, there's a 'Policy Name' field with 'MSNBC' entered, and a 'State' dropdown set to 'Enabled'. Other fields include 'Port', 'Timeout' (3 Sec), 'HTTP Status Code' (n/a), 'Proxy Server Port', 'Proxy Username Password', 'Proxy Auth Method' (Default), and 'Location Redirect' (Default). The middle section contains 'Uniform Resource Locator (URL)' with 'http://www.msnbc.com/' and 'Post String'. Below that is 'Cookie Value' and 'Browser Emulation' set to 'Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)'. The right section has 'HTTP Auth Username Password', 'HTTP Auth Method' (Default), 'SSL Encryption' (Disabled), 'Expression Check #1 (Case Sensitive)' with 'Prosecutor' entered and 'Invert' checked, 'Expression Check #2 (Case Sensitive)', 'Referrer String', and 'Host Resolution'. A 'Save' button is at the bottom right of this section. At the very bottom, there are six performance metrics: 'Min Page size (Kb)', 'Max Page size (Kb)', 'Min Download speed (kb/s)', 'Max nslookup time (msec)', 'Max TCP connect time (msec)', and 'Max overall transaction time (msec)', each with an empty input field.

4. In the **Web Content Policy** modal page, you can change the values in one or more of the fields described in the section on [Defining a Web Content Policy](#).

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

Example Web Content Policy

This screenshot is identical to the one above, showing the 'Web Content Policy' modal window with the 'Editing Policy [1]' form. The 'Expression Check #1' field contains the value 'Prosecutor', and the 'Save' button is highlighted in a darker shade, indicating it is the focus of the example.

- This policy is aligned with the device "Web Content Virtual Device".
- This policy will search for the expression "Prosecutor", entered in the **Expression Check #1** field, in `www.msnbc.com` ("`http://www.msnbc.com/`").

Viewing Reports on a Web Content Policy

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for monitoring port availability.



Viewing ASCII Page Content

From the **Web Content Monitoring** page, you can view the ASCII content (from the web page) that was retrieved by the web content monitoring policy. The ASCII content is returned only when the policy is manually executed.



The **Content Page Dump** page displays:

- The regular expression(s) used in the web-content monitoring policy. SL1 searches the web content for these text strings.
- The text (from the website) that was searched.

There are two ways to access the **Content Page Dump** page:

1. From the **Device Manager** page (Devices > Device Manager):
 - In the **Device Manager** page, find the device that you want to associate with the monitoring policy. Select wrench icon () for the device.
 - In the **Device Administration** panel, select the **[Monitors]** tab.
 - In the **Monitoring Policies** page, find the policy you want to edit and select the page icon ()

Or:

2. From the **Web Content Monitoring** page (Registry > Monitors > Web Content):
 - Select the lightning bolt icon () to manually execute the policy.
 - In the **Web Content Monitoring** page, find the policy you want to edit and select its page icon ()

3. The **Content Page Dump** page appears.



```
Content Page Dump | Policy [MSNBC] | Last Refresh: 2012-04-09 14:30:00 [Close] [Reset] [Guide]
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: http://www.msnbc.msn.com/
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Mon, 09 Apr 2012 18:30:38 GMT
Transfer-Encoding: chunked

HTTP/1.1 200 OK
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Cache-Control: max-age=28
Expires: Mon, 09 Apr 2012 18:31:07 GMT
Date: Mon, 09 Apr 2012 18:30:39 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Connection: Transfer-Encoding

<html><head><title>msnbc.com - Breaking news, science and tech news, world news, US news, local news- msnbc.com</title><link
rel="stylesheet" type="text/css" href="http://assets.msnbc.msn.com/rendering/msnbc/wb/assets/wb_html40.css" /><link rel="stylesheet"
type="text/css" href="http://assets.msnbc.msn.com/rendering/msnbc/wb/assets/wb_front_cover_core.css" /><script type="text/javascript"
src="http://ajax.aspnetcdn.com/ajax/jquery/jquery-1.5.2.min.js"></script><script type="text/javascript" src="/js/std.js"></script>
<script type="text/javascript" src="/id/28644474/agency"></script><script type="text/javascript">gEnabled=false;</script><meta
http-equiv="content-type" content="text/html; charset=UTF-8"><meta name="description" content="Msnbc.com is a leader in breaking news,
video and original journalism. Stay current with daily news updates in health, entertainment, business, science, technology and sports
videos"><meta name="robots" content="nooodp, noydir"><meta name="Search.Document" content="front"><meta name="Search.Updated"
content="Mon, 09 Apr 2012 18:28:07 GMT"><meta name="Search.Section" content="Cover"><link rel="alternate" type="application/rss+xml"
title="MSNBC - Top Stories" href="http://rss.msnbc.msn.com/id/3032091/device/rss/rss.xml">
<link rel="alternate" type="application/rss+xml" title="MSNBC - Most Viewed" href="http://rss.msnbc.msn.com/id/3058960/displaymode
/1026/eventType/1/rss/rss.xml"><!-- empty tracking cdata 29473223 --><script type="text/javascript">

function DateTime(){
var ma=["Jan","Feb","March","April","May","June","July","Aug","Sept","Oct","Nov","Dec"];
var wa=["Sun","Mon","Tues","Wed","Thurs","Fri","Sat"];
var za=["ET","CT","MT","PT","AKT","HT","HT"];

this.D2S=function(d,f){
var r="as of ";
return r+"<span class=\"time\">"+GetT(d)+"</span> <span class=\"date\">"+GetD(d)+"</span>";
};

var TZM=function(t){
return parseInt((t-621355968000000000)/10000);
};
```

4. In the **Content Page Dump** page, you can view the content that is searched and the regular expressions that SL1 searched for.

5. If the Web Content policy has not yet completed, this page will display the message:

"Web content verification data may take up to 5 minutes to appear. Try again later."

Viewing the Monitored Website

In some cases, you might want to view the website being monitored, directly from the user interface. To do this:

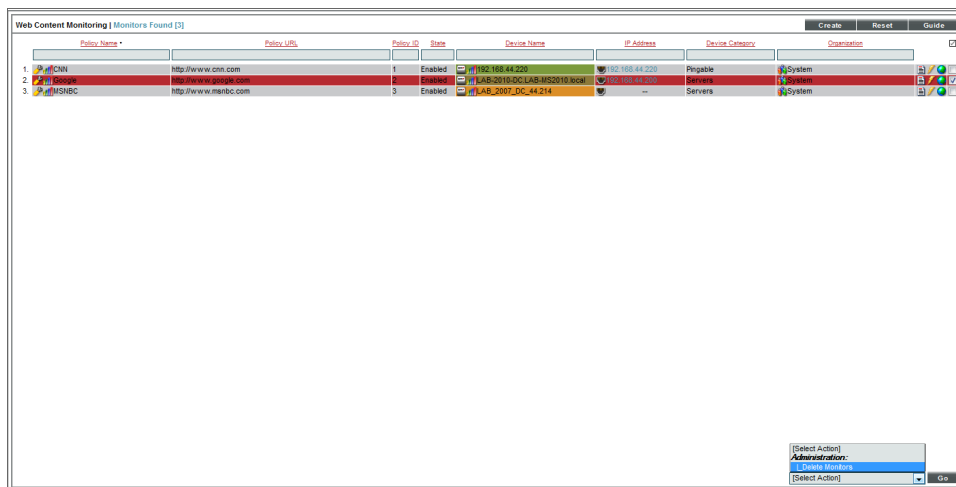
1. Go to the **Web Content Monitoring** page (Registry > Monitors > Web Content).
2. Find the policy for which you want to view the website. Select its globe icon (🌐).
3. SL1 will spawn a new browser page and display the monitored website.

Deleting a Web Content Monitoring Policy

You can delete a web content monitoring policy from the **Web Content Monitoring** page. You can delete individual, multiple, or all existing web content monitoring policies. When you delete a web content monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

To delete a web content monitoring policy:

1. Go to the **Web Content Monitoring** page (Registry > Monitors > Web Content).
2. In the **Web Content Monitoring** page, select the checkbox(es) for each web content monitoring policy you want to delete. Click the checkmark icon (☑) to select all of the web content monitoring policies.
3. In the **Select Action** menu in the bottom right of the page, select *Delete Monitors*.





4. Select the **[Go]** button to delete the web content monitoring policy.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Managing a Single Device with the Device Administration Panel

Overview

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:

<i>What is the Device Administration Panel?</i>	404
<i>Actions Menu</i>	407
<i>Device Properties</i>	410
<i>Viewing Read-Only Information About the Device</i>	411
<i>Editing Device Settings</i>	412
<i>Adding an IP Address to a Device</i>	418
<i>Removing an IP Address from a Device</i>	420
<i>Managing Device IP Addresses</i>	421
<i>Clearing the Device Cache</i>	423
<i>Aligning a Secondary Credential</i>	425
<i>Adding the Device to a Device Group</i>	427
<i>Creating a Ticket About the Device</i>	429
<i>Adding a Note to a Device</i>	431

Aligning Custom Attributes with a Device	434
Associating a Product SKU with the Device	438
Merging Devices	439
Performing Administrative Tasks for One or More Devices	444
Shortcut Keys for Device Administration panel	445

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.

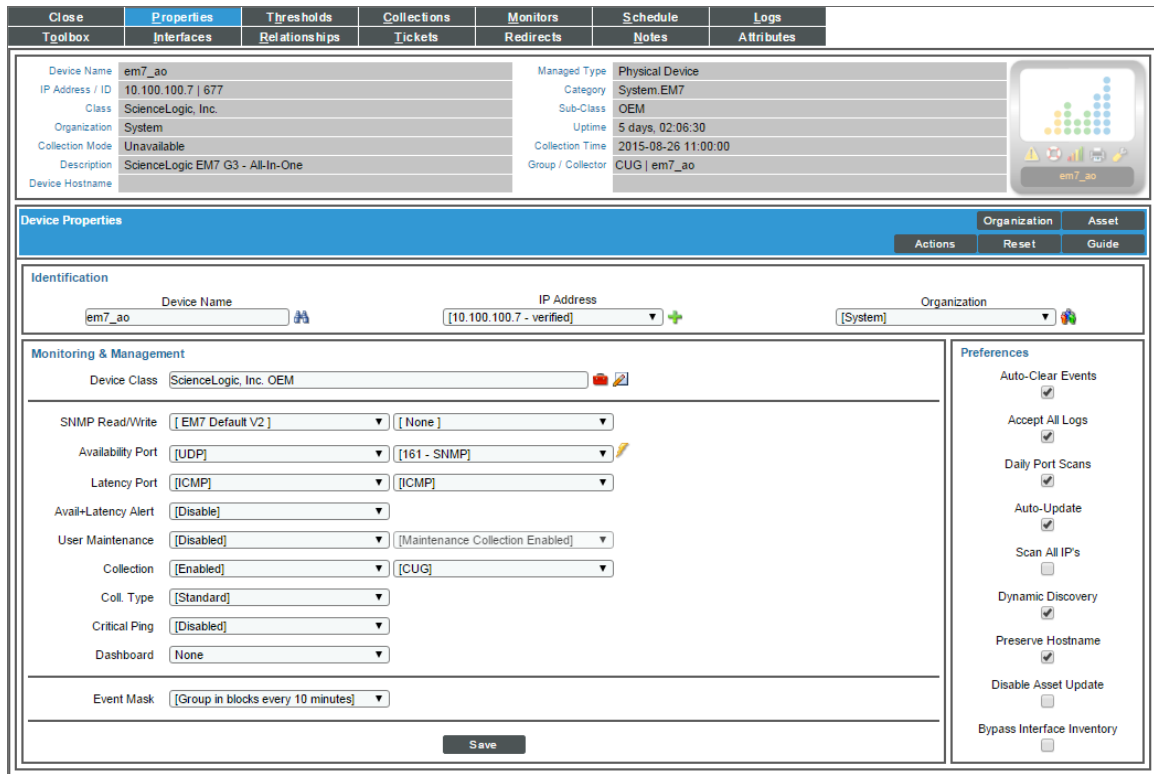
To access the **Device Administration** panel for a device:

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

Device Name	Device Hostname	IP Address	Device Category	Device Class / Subclass	DID	Organization	Current State	Collection Status	Collection Size	SNMP Subclass	SNMP Status
10.100.100.40	--	10.100.100.40	Private	Priv / ICHP	274	System	Healthy	CFG	User-Disabled	--	...
10.100.100.46	--	10.100.100.46	Private	FreeBSD / ICHP	294	Jinto	Healthy	CFG	User-Disabled	--	...
10.107.11.106	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2778	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	3193	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108.9222	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	2228	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108.9706	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	1951	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.107	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2485	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.107	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2391	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.107.4269	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	2648	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.107.5699	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	1952	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.107.3959	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	1431	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2080	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2602	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108.8562	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	3058	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108.8562	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	2102	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.108.7940	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	1591	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.109.1031	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	955	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.237	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2632	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.11.237.7699	--	--	Network App FS Networks, Inc.	BIG-IP LTM Pool Mem	1423	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2333	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2170	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2136	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2714	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2981	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	1979	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2429	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2281	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2641	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2662	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2371	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	274	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2879	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	3053	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2165	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	3008	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2268	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2790	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2642	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2206	System	Healthy	CFG	Active	SNMP Public V2	V2
10.107.12.125	--	--	Network App FS Networks, Inc.	BIG-IP LTM Node	2385	System	Healthy	CFG	Active	SNMP Public V2	V2

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:

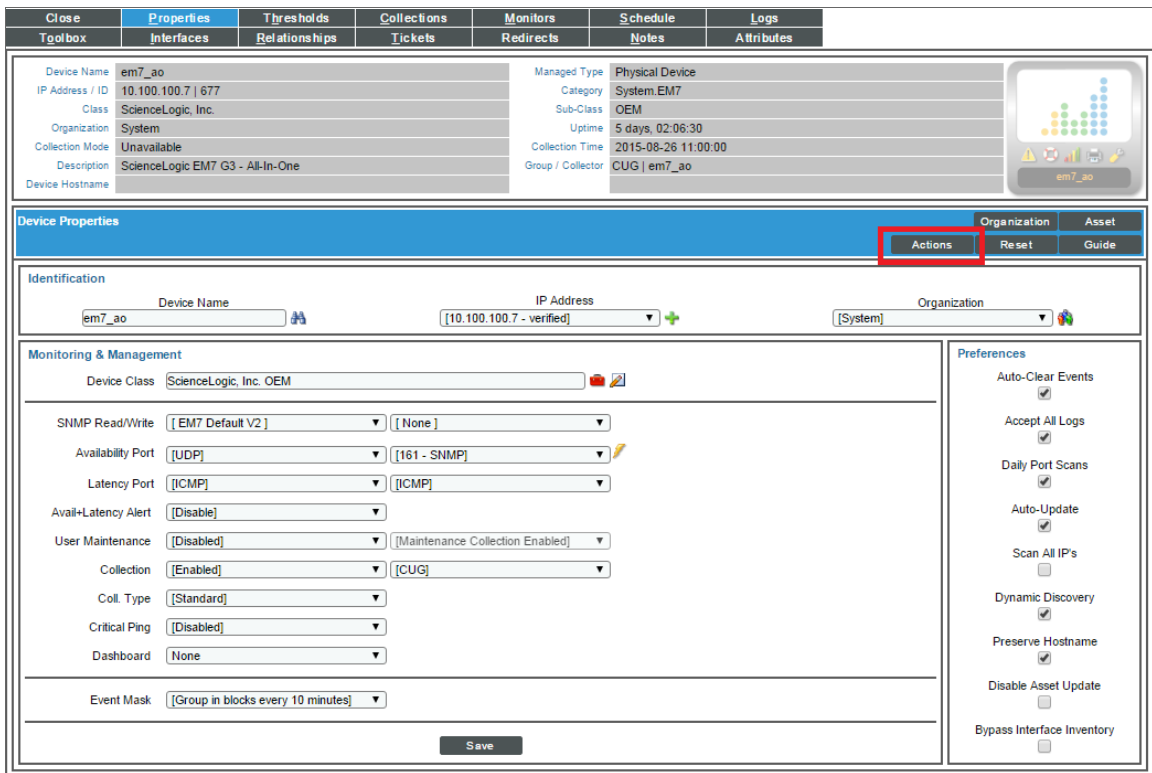


Tab	Description
Properties	In the Device Properties page, you can edit parameters that affect how SL1 "sees" the device and monitors the device. For details on the Device Properties page, see the section in this chapter called Device Properties .
Thresholds	The Device Thresholds page allows you to define usage and performance thresholds and data retention thresholds for a device. When these thresholds are exceeded, SL1 will generate an event for the device. For details on device thresholds, see the chapter on Thresholds and Data Retention .
Collections	<p>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. For details on credentials and Dynamic Applications, see the manual on Credentials and Discovery.</p> <p>You can specify a credential for use with the Dynamic Application for the specific device only.</p> <p>You can enable or disable one or more report policies for the specific device only.</p> <p>You can enable or disable monitoring of one or more objects for the specific device only.</p>

Tab	Description
Monitors	<p>The Monitoring Policies page allows you to define monitoring policies for a device.</p> <p>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.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>NOTE: All these monitoring policies can generate events. SL1 uses the data collected by these policies to create performance reports and graphs.</p> </div>
Schedule	In the Maintenance Schedule page you can view, edit, and schedule downtimes for the device. For details on scheduling maintenance for a device, see the chapter on Maintenance .
Logs	The Device Logs & Messages page displays all the messages SL1 has collected from the device and from SL1 about the device. For details on device logs, see the chapter on Device Logs .
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. For details on the Device Toolbox, see the chapter on Device Toolbox .
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. For details on interfaces and bandwidth, see the chapter on Network Interfaces .
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. For details on device relations, see the chapter on Defining Device 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. For details on creating tickets, see the manual Ticketing .
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. For details on virtual devices, see the chapter on Virtual Devices .
Notes	The Notes & Attachments page displays a list of all comments and attachments associated with the device properties. When you select the <i>Notepad Editor</i> option in the Device Properties page, the notes appear in this page. For details, see the section on Adding a Note to a Device .
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. For details, see the section on Aligning Custom Attributes with 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 chapter 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 chapter 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 chapter 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.

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs		
Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes		
Device Name	em7_ao	Managed Type	Physical Device					
IP Address / ID	10.100.100.7 677	Category	System EM7					
Class	ScienceLogic, Inc.	Sub-Class	OEM					
Organization	System	Uptime	5 days, 02:06:30					
Collection Mode	Unavailable	Collection Time	2015-08-26 11:00:00					
Description	ScienceLogic EM7 G3 - All-In-One	Group / Collector	CUG em7_ao					
Device Hostname								
Device Properties								
						Organization	Asset	
						Actions	Reset	Guide
Identification								
Device Name		IP Address		Organization				
em7_ao		[10.100.100.7 - verified]		[System]				
Monitoring & Management								
Device Class: ScienceLogic, Inc. OEM								
SNMP Read/Write: [EM7 Default V2] [None]								
Availability Port: [UDP] [161 - SNMP]								
Latency Port: [ICMP] [ICMP]								
Avail+Latency Alert: [Disable]								
User Maintenance: [Disabled] [Maintenance Collection Enabled]								
Collection: [Enabled] [CUG]								
Coll. Type: [Standard]								
Critical Ping: [Disabled]								
Dashboard: [None]								
Event Mask: [Group in blocks every 10 minutes]								
Save								
Preferences								
Auto-Clear Events <input checked="" type="checkbox"/>								
Accept All Logs <input checked="" type="checkbox"/>								
Daily Port Scans <input checked="" type="checkbox"/>								
Auto-Update <input checked="" type="checkbox"/>								
Scan All IP's <input type="checkbox"/>								
Dynamic Discovery <input checked="" type="checkbox"/>								
Preserve Hostname <input checked="" type="checkbox"/>								
Disable Asset Update <input type="checkbox"/>								
Bypass Interface Inventory <input type="checkbox"/>								

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 chapter 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 chapter 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 chapter [Customizing the 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 chapter on [Performance Graphs](#).
- **Create a Report About the Device.** This is described in the chapter on [Performance Graphs](#).

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:

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Topbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes
Device Name	em7_ao	Managed Type	Physical Device	Category	System EM7	
IP Address / ID	10.100.100.7 677	Sub-Class	OEM	Uptime	5 days, 02:06:30	
Class	ScienceLogic, Inc.	Collection Time	2015-08-26 11:00:00	Group / Collector	CUG em7_ao	
Organization	System					
Collection Mode	Unavailable					
Description	ScienceLogic EM7 G3 - All-In-One					
Device Hostname						

Device Properties		Organization	Asset
		Actions	Reset
		Reset	Guide
Identification			
Device Name	em7_ao	IP Address	[10.100.100.7 - verified]
Organization	[System]		
Monitoring & Management			
Device Class	ScienceLogic, Inc. OEM		
SNMP Read/Write	[EM7 Default V2]		[None]
Availability Port	[UDP]		[161 - SNMP]
Latency Port	[ICMP]		[ICMP]
Avail-Latency Alert	[Disable]		
User Maintenance	[Disabled]		[Maintenance Collection Enabled]
Collection	[Enabled]		[CUG]
Coil Type	[Standard]		
Critical Ping	[Disabled]		
Dashboard	None		
Event Mask	[Group in blocks every 10 minutes]		
Save			
Preferences			
Auto-Clear Events	<input checked="" type="checkbox"/>		
Accept All Logs	<input checked="" type="checkbox"/>		
Daily Port Scans	<input checked="" type="checkbox"/>		
Auto-Update	<input checked="" type="checkbox"/>		
Scan All IPs	<input type="checkbox"/>		
Dynamic Discovery	<input checked="" type="checkbox"/>		
Preserve Hostname	<input checked="" type="checkbox"/>		
Disable Asset Update	<input type="checkbox"/>		
Bypass Interface Inventory	<input type="checkbox"/>		

- **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 chapter [Monitoring Device Availability and Device Latency](#).

- **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](#) chapter.

"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).

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.

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

The screenshot shows the 'Device Properties' page for a device named 'em7_ao'. The 'IP Address' field is set to '10.100.100.7 - verified' and has a plus sign icon next to it. The 'Organization' is set to '[System]'. The 'Monitoring & Management' section includes settings for SNMP Read/Write, Availability Port, Latency Port, User Maintenance, Collection, Coll. Type, Critical Ping, and Dashboard. The 'Preferences' section on the right includes options like Auto-Clear Events, Accept All Logs, Daily Port Scans, Auto-Update, Scan All IP's, Dynamic Discovery, Preserve Hostname, Disable Asset Update, and Bypass Interface Inventory.

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

The 'Add an IP Address' modal page displays two input fields: 'IP Address' with the value '10.10.204.20' and 'Subnet Mask' with the value '255.255.255.0'. Below the input fields is a dark grey button labeled 'Add'.

- 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

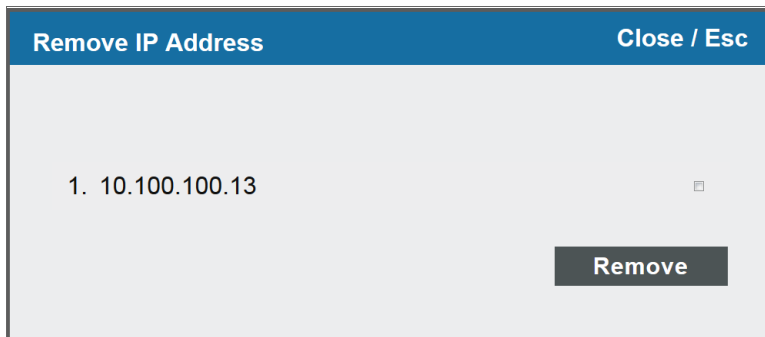
If you have added an IP address to a device using the steps in the section on [Associating an Additional IP Address with the Device](#), you can also delete that IP address.

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 IP Addresses

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.

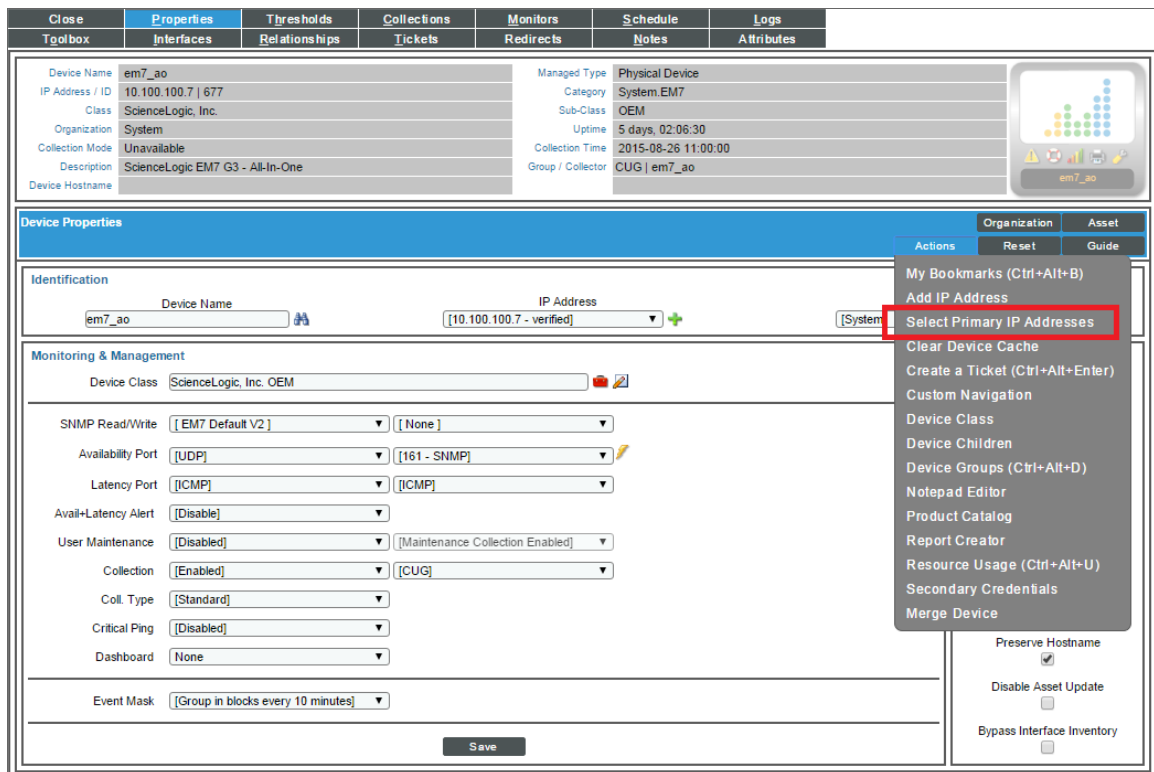
- Although SL1 will not allow duplicate IP addresses within a single Collector Group, SL1 does allow duplicate IP addresses if each device is aligned with a different Collector Group.

- 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.

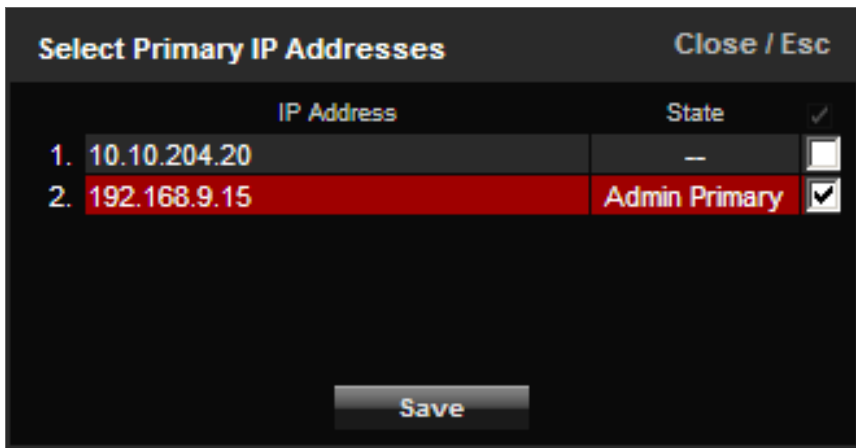
NOTE: For All-In-One Appliances, the function provided by a Message Collector is built in to the All-In-One Appliance. All-In-One systems contain only one built-in Collector Group.

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 ()

Device Manager (Devices Found [1293])													Actions	Report	Reset	Guide
Device Name	Device Hostname	IP Address	Device Gateway	Device Class / Sub-class	DIG	Organization	Current State	Collection Status	Collection State	SNMP Credentials	SNMP Status					
1	10.100.100.40	10.100.100.40	Pingable	Ping / ICMP	274	System	Healthy	CUG	User-Disabled	--	--					
2	10.100.100.46	10.100.100.46	Pingable	FreeBSS / ICMP	294	Johns	Healthy	CUG	User-Disabled	--	--					
3	10.7.11.189	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2779	System	Healthy	CUG	Active	SNMP Public V2	V2					
4	10.7.11.186	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3193	System	Healthy	CUG	Active	SNMP Public V2	V2					
5	10.7.11.188	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2226	System	Notice	CUG	Active	SNMP Public V2	V2					
6	10.7.11.189.5951	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1430	System	Healthy	CUG	Active	SNMP Public V2	V2					
7	10.7.11.186.8222	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1204	System	Healthy	CUG	Active	SNMP Public V2	V2					
8	10.7.11.186.7706	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1951	System	Healthy	CUG	Active	SNMP Public V2	V2					
9	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2					
10	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2					
11	10.7.11.187	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2					
12	10.7.11.187.4289	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1952	System	Healthy	CUG	Active	SNMP Public V2	V2					
13	10.7.11.187.5996	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1206	System	Healthy	CUG	Active	SNMP Public V2	V2					
14	10.7.11.187.5690	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1431	System	Healthy	CUG	Active	SNMP Public V2	V2					
15	10.7.11.189	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2080	System	Healthy	CUG	Active	SNMP Public V2	V2					
16	10.7.11.189	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2					
17	10.7.11.189	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3658	System	Notice	CUG	Active	SNMP Public V2	V2					
18	10.7.11.189.6992	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	2102	System	Healthy	CUG	Active	SNMP Public V2	V2					
19	10.7.11.189.7340	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1391	System	Healthy	CUG	Active	SNMP Public V2	V2					
20	10.7.11.189.7881	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	855	System	Healthy	CUG	Active	SNMP Public V2	V2					
21	10.7.11.237	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2					
22	10.7.11.237.7659	--	--	Network App F5 Networks, Inc. BIG-IP LTM Pool Mem	1423	System	Healthy	CUG	Active	SNMP Public V2	V2					
23	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2933	System	Notice	CUG	Active	SNMP Public V2	V2					
24	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2					
25	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2					
26	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2					
27	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2651	System	Healthy	CUG	Active	SNMP Public V2	V2					
28	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2					
29	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2					
30	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2					
31	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2					
32	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2952	System	Healthy	CUG	Active	SNMP Public V2	V2					
33	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2					
34	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2					
35	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2679	System	Notice	CUG	Active	SNMP Public V2	V2					
36	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2					
37	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2					
38	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2					
39	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2369	System	Healthy	CUG	Active	SNMP Public V2	V2					
40	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2					
41	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2					
42	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2					
43	10.7.12.125	--	--	Network App F5 Networks, Inc. BIG-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2					

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

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name em7_ao IP Address / ID 10.100.100.7 677 Class ScienceLogic, Inc. Organization System Collection Mode Unavailable Description ScienceLogic EM7 G3 - All-In-One Device Hostname	Managed Type Physical Device Category System EM7 Sub-Class OEM Uptime 5 days, 02:06:30 Collection Time 2015-08-26 11:00:00 Group / Collector CUG / em7_ao
--	--

Device Properties		Organization	Asset
Identification Device Name em7_ao IP Address [10.100.100.7 - verified]		[System]	
Monitoring & Management Device Class ScienceLogic, Inc. OEM SNMP Read/Write [EM7 Default V2] [None] Availability Port [UDP] [161 - SNMP] Latency Port [ICMP] [ICMP] Avail+Latency Alert [Disable] User Maintenance [Disabled] [Maintenance Collection Enabled] Collection [Enabled] [CUG] Coll. Type [Standard] Critical Ping [Disabled] Dashboard [None] Event Mask [Group in blocks every 10 minutes]			

Actions

- My Bookmarks (Ctrl+Alt+B)
- Add IP Address
- Select Primary IP Addresses
- Clear Device Cache**
- Create a Ticket (Ctrl+Alt+Enter)
- Custom Navigation
- Device Class
- Device Children
- Device Groups (Ctrl+Alt+D)
- Notepad Editor
- Product Catalog
- Report Creator
- Resource Usage (Ctrl+Alt+U)
- Secondary Credentials
- Merge Device

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


Aligning a Secondary Credential

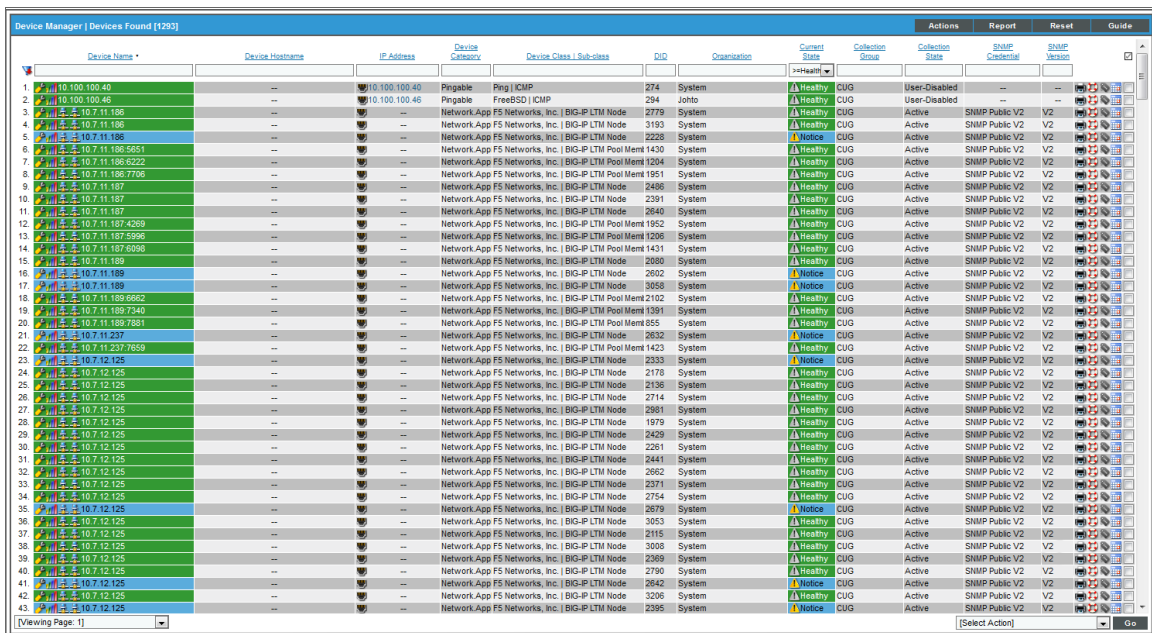
During initial discovery of a device, SL1 uses a specified SNMP credential. If you specified that SL1 should discover non-SNMP devices, SL1 will use ICMP and nmap to gather information about a device. After SL1 finds devices, discovery can use a second list of specified credentials to access database 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.

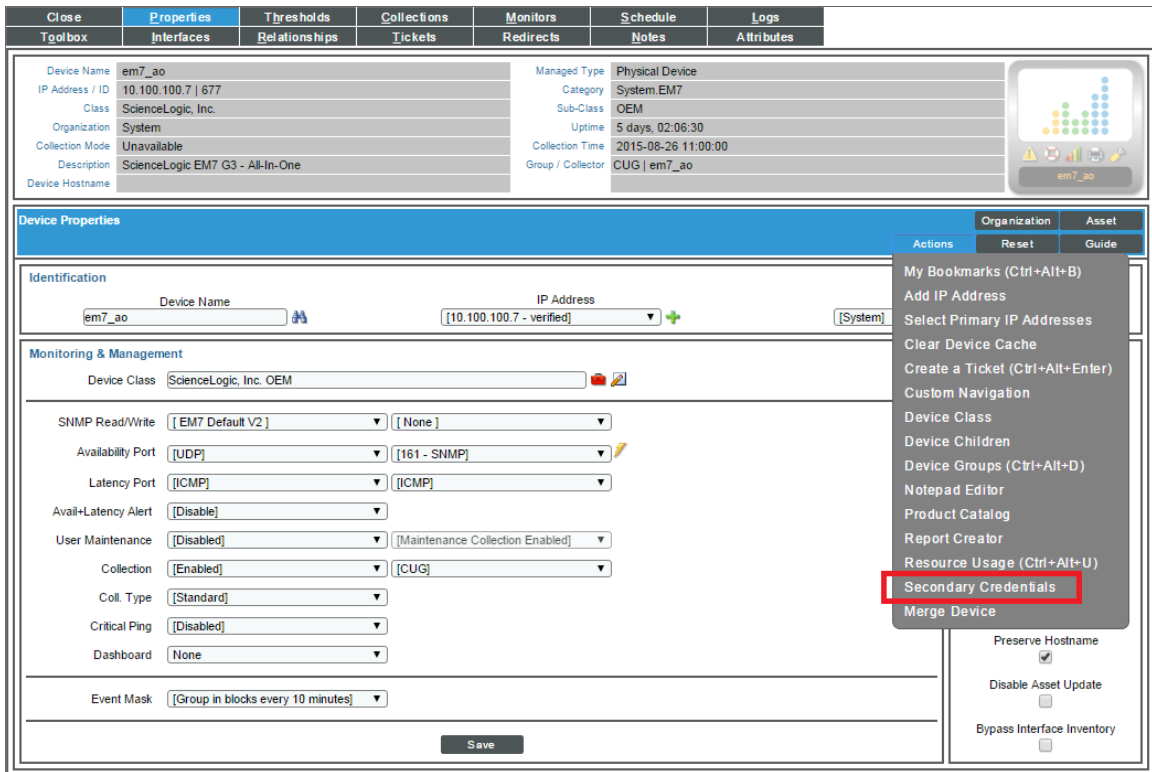
To associate one or more additional credentials with a device:

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.

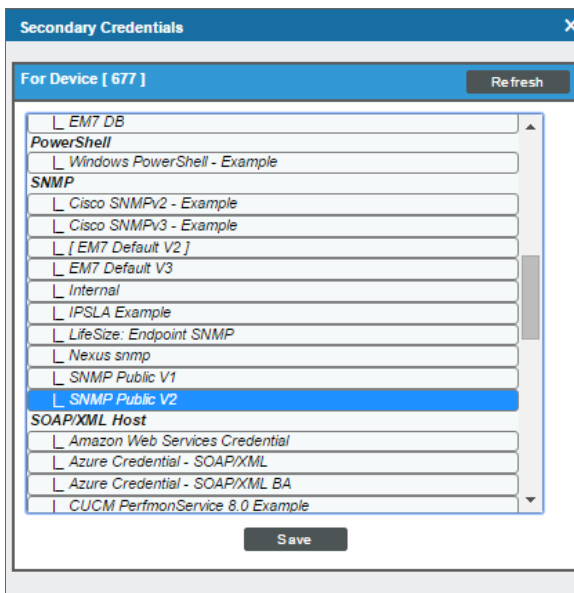


Device Name	Device Hostname	IP Address	Device Class	Device Subclass	OID	Organisation	Current State	Collection Scope	Subscription State	SNMP Credential	SNMP Version	Actions	Report	Reset	Guide
10.100.100.40	--	10.100.100.40	Pingable	Ping/ICMP	274	System	Healthy	CUG	User-Disabled	--	--	[Wrench]	[Report]	[Reset]	[Guide]
10.100.100.46	--	10.100.100.46	Pingable	FreeBSD/ICMP	284	Johto	Healthy	CUG	User-Disabled	--	--	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.186	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2778	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.188	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2228	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.186.5651	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1430	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.186.8222	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1204	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.186.7186	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1951	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2486	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2391	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2640	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187.4268	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1952	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187.9266	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1206	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.187.5098	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1431	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2080	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2602	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	3656	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189.6662	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	2102	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189.7340	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	1391	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.189.7881	--	--	Network App F5 Networks, Inc.	Big-IP LTM Pool Mem1	855	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.11.237	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2632	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2333	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2178	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2136	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2714	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2981	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	1979	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2429	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2261	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2441	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2692	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2371	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2754	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2678	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	3053	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2115	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	3008	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2368	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2790	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2642	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	3206	System	Healthy	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]
10.7.12.125	--	--	Network App F5 Networks, Inc.	Big-IP LTM Node	2395	System	Notice	CUG	Active	SNMP Public V2	V2	[Wrench]	[Report]	[Reset]	[Guide]

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



- 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**.

The screenshot shows the 'Device Properties' page for a device named 'em7_ao'. The page is divided into several sections: Identification, Monitoring & Management, and a right-hand sidebar with an 'Actions' menu. The 'Actions' menu is open, and 'Device Groups (Ctrl+Alt+D)' is highlighted with a red box. Other options in the menu include 'My Bookmarks (Ctrl+Alt+B)', 'Add IP Address', 'Select Primary IP Addresses', 'Clear Device Cache', 'Create a Ticket (Ctrl+Alt+Enter)', 'Custom Navigation', 'Device Class', 'Device Children', 'Notepad Editor', 'Product Catalog', 'Report Creator', 'Resource Usage (Ctrl+Alt+U)', 'Secondary Credentials', and 'Merge Device'. Below the menu, there are checkboxes for 'Preserve Hostname' (checked), 'Disable Asset Update' (unchecked), and 'Bypass Interface Inventory' (unchecked). A 'Save' button is located at the bottom of the main form area.

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name: em7_ao
IP Address / ID: 10.100.100.7 | 677
Class: ScienceLogic, Inc.
Organization: System
Collection Mode: Unavailable
Description: ScienceLogic EM7 G3 - All-In-One
Device Hostname: em7_ao

Managed Type: Physical Device
Category: System EM7
Sub-Class: OEM
Uptime: 5 days, 02:06:30
Collection Time: 2015-08-26 11:00:00
Group / Collector: CUG | em7_ao

Device Properties

Identification

Device Name: em7_ao | IP Address: [10.100.100.7 - verified] | [System]

Monitoring & Management

Device Class: ScienceLogic, Inc. OEM

SNMP Read/Write: [EM7 Default V2] | [None]

Availability Port: [UDP] | [161 - SNMP]

Latency Port: [ICMP] | [ICMP]

Avail-Latency Alert: [Disable]

User Maintenance: [Disable] | [(Maintenance Collection Enabled)]

Collection: [Enabled] | [CUG]

Coll. Type: [Standard]

Critical Ping: [Disable]

Dashboard: None

Event Mask: [Group in blocks every 10 minutes]

Save

Organization: Asset

Actions: Reset, Guide

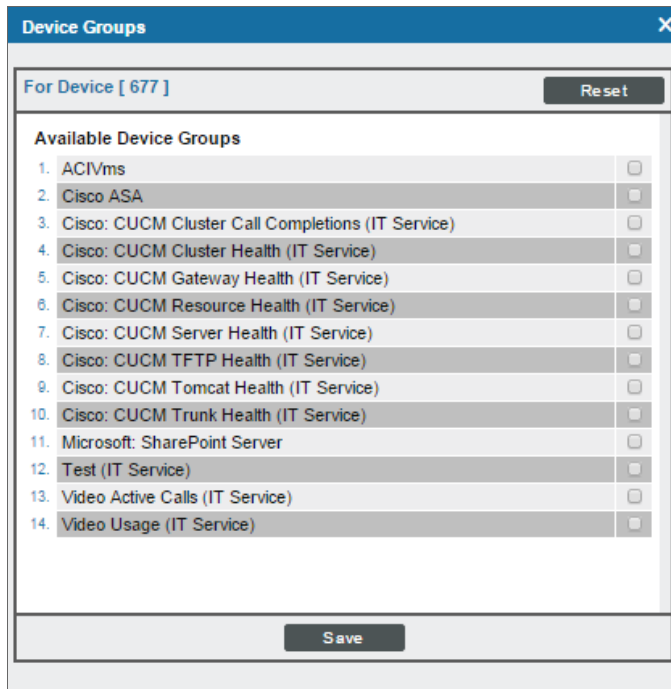
- My Bookmarks (Ctrl+Alt+B)
- Add IP Address
- Select Primary IP Addresses
- Clear Device Cache
- Create a Ticket (Ctrl+Alt+Enter)
- Custom Navigation
- Device Class
- Device Children
- Device Groups (Ctrl+Alt+D)**
- Notepad Editor
- Product Catalog
- Report Creator
- Resource Usage (Ctrl+Alt+U)
- Secondary Credentials
- Merge Device

Preserve Hostname:

Disable Asset Update:

Bypass Interface Inventory:

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

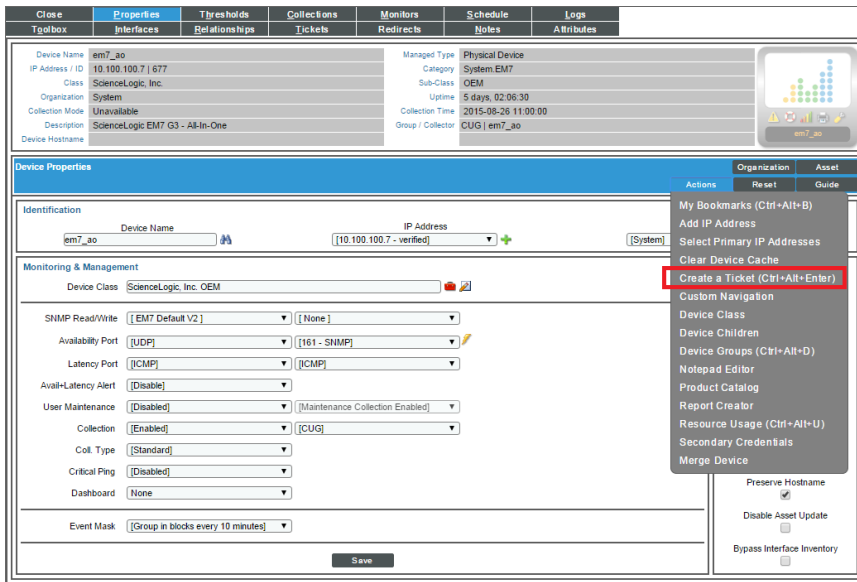
Creating a Ticket About the Device

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*.

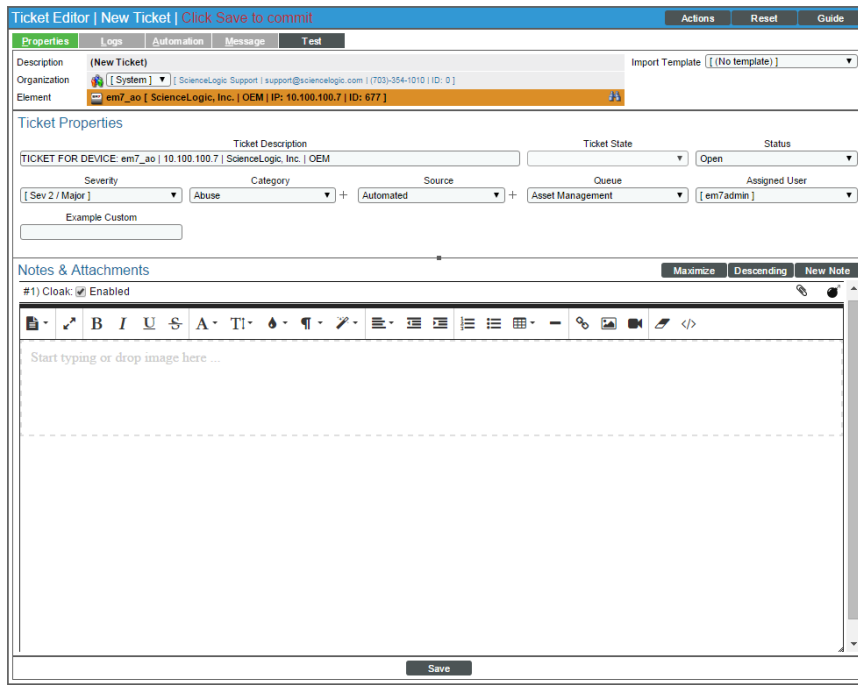
To create a ticket for a device:

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**.



The screenshot displays the 'Device Properties' page for a device named 'em7_ao'. The page is divided into several sections: Identification, Monitoring & Management, and Actions. The Identification section includes fields for Device Name, IP Address, and Organization. The Monitoring & Management section contains various configuration options such as Device Class, SNMP Read/Write, Availability Port, Latency Port, Avail-Latency Alert, User Maintenance, Collection, Col. Type, Critical Ping, Dashboard, and Event Mask. The Actions menu is open on the right side, showing options like My Bookmarks, Add IP Address, Select Primary IP Addresses, Clear Device Cache, and Create a Ticket (Ctrl+Alt+Enter), which is highlighted in red. Other options in the menu include Custom Navigation, Device Class, Device Children, Device Groups, Notepad Editor, Product Catalog, Report Creator, Resource Usage, Secondary Credentials, and Merge Device. There are also checkboxes for Preserve Hostname, Disable Asset Update, and Bypass Interface Inventory.

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.



The screenshot shows the 'Ticket Editor' interface. At the top, there's a header with 'Ticket Editor | New Ticket | click Save to commit' and buttons for 'Actions', 'Reset', and 'Guide'. Below the header are tabs for 'Properties', 'Logs', 'Automation', 'Message', and 'Test'. The 'Properties' tab is active, showing fields for 'Description' (populated with '(New Ticket)'), 'Organization' (populated with 'ScienceLogic, Inc. | OEM | IP: 10.100.100.7 | ID: 677'), and 'Element' (populated with 'em7_ao | ScienceLogic, Inc. | OEM | IP: 10.100.100.7 | ID: 677'). Below these are 'Ticket Properties' with fields for 'Ticket Description', 'Ticket State', 'Status', 'Severity', 'Category', 'Source', 'Queue', and 'Assigned User'. At the bottom is a 'Notes & Attachments' section with a rich text editor and a 'Save' button.

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

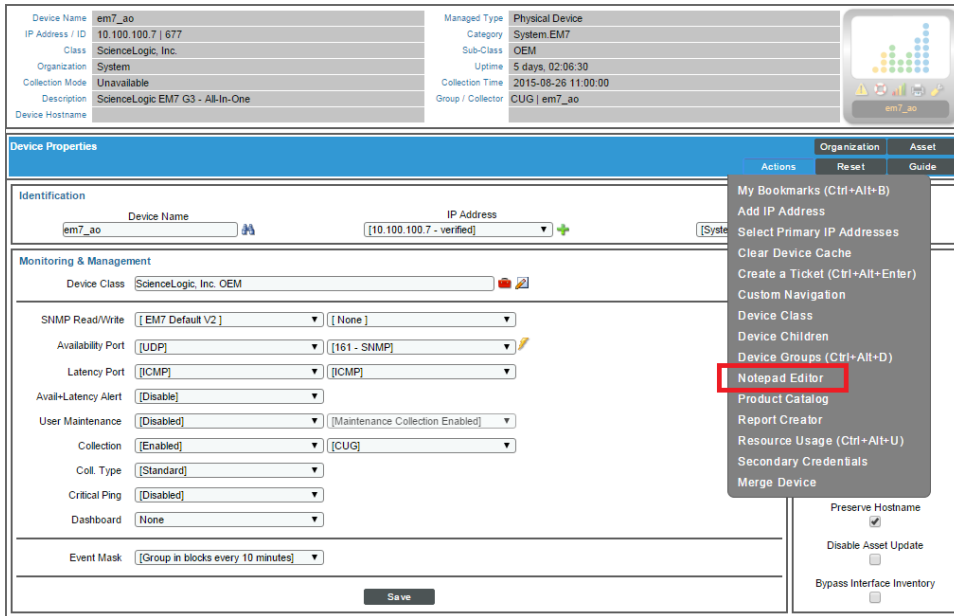
Adding a Note to a Device

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.

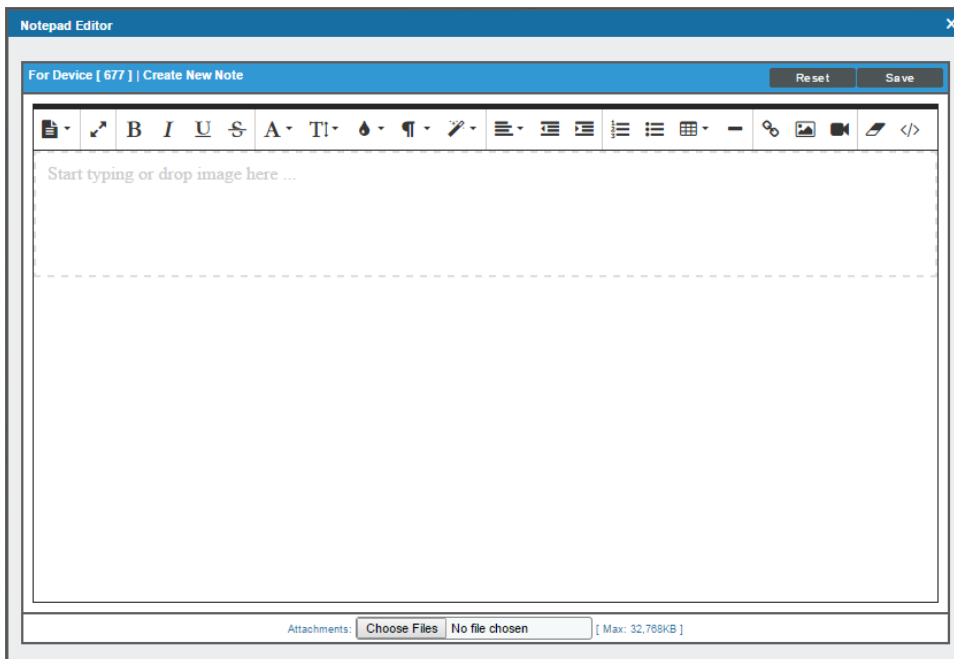
To add a note to a device:

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.

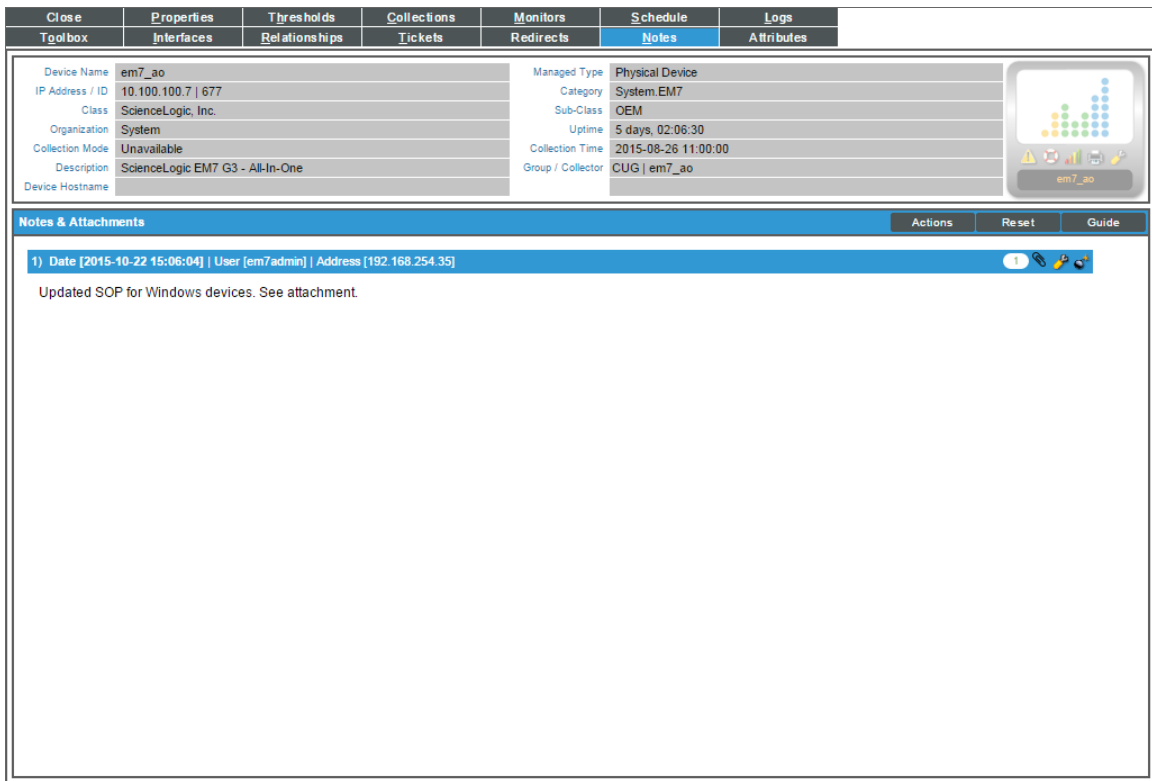
3. In the **Device Properties** page, click the **[Actions]** menu and select **Notepad Editor**.






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.




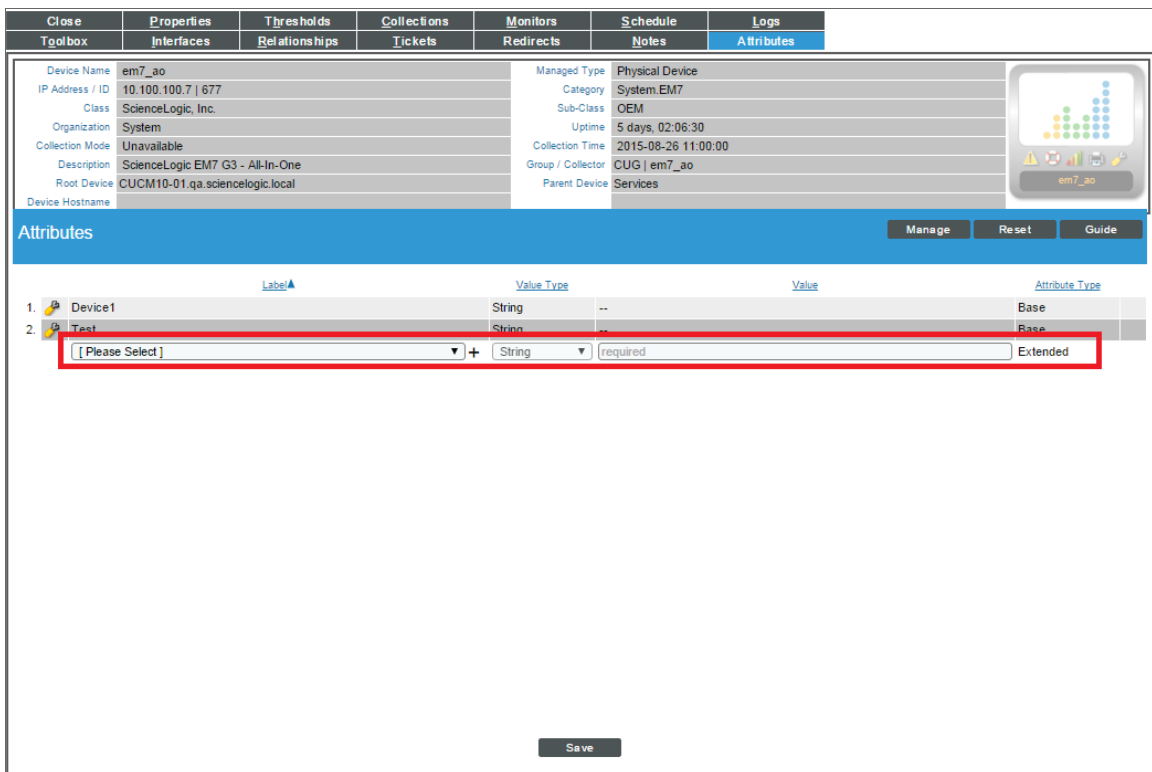
7. The **Notes & Attachments** page displays all the notes about the device that were created with the **Notepad Editor** modal page. In the **Notes & Attachments** page, each entry includes the username, date and time, and text of the comment. You can perform the following on each note entry:
 - **To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

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

Label	Value Type	Value	Attribute Type
1. Device1	String	--	Base
2. Test	String		Base
required	String	required	Extended

- 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, SL 1 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, SL 1 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.

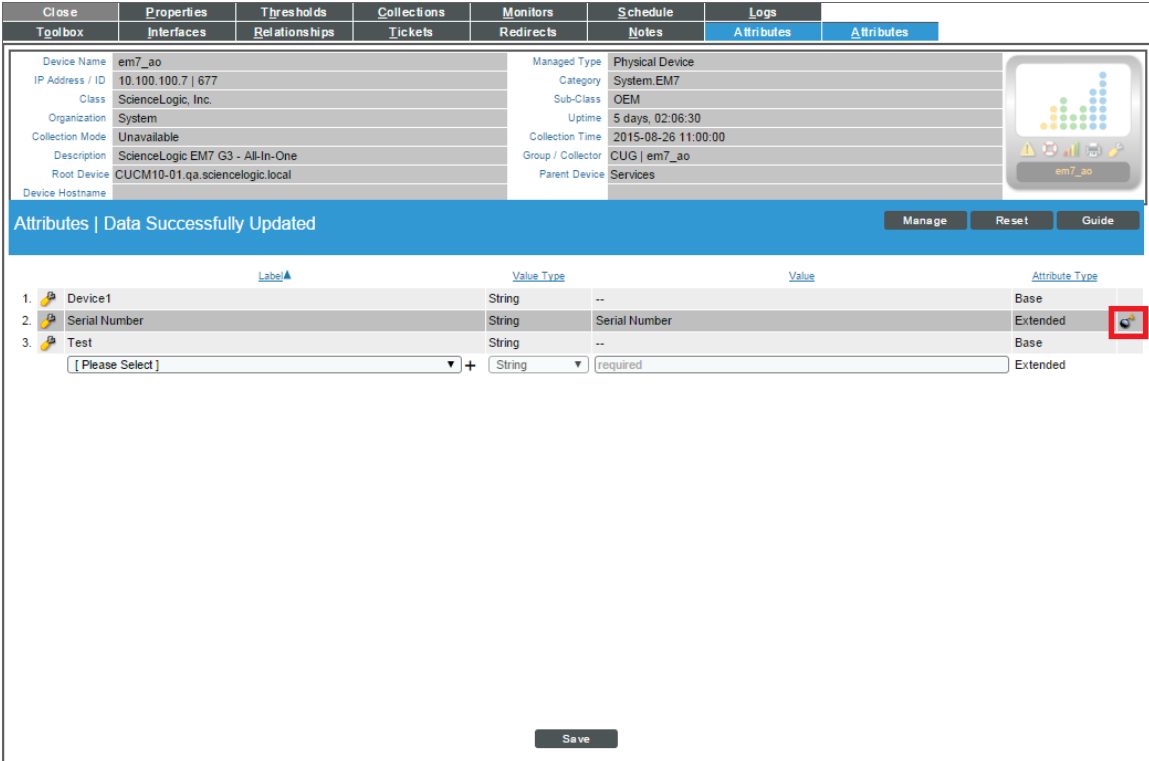
Deleting an Extended Custom Attribute from a Device

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). For more information, see the chapter on [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 (.



The screenshot shows the 'Attributes' page for device 'em7_ao'. The page has a blue header with 'Attributes | Data Successfully Updated' and buttons for 'Manage', 'Reset', and 'Guide'. Below the header is a table of attributes:

	Label	Value Type	Value	Attribute Type
1.	Device1	String	--	Base
2.	Serial Number	String	Serial Number	Extended
3.	Test	String	--	Base
	[Please Select]	String	required	Extended

The 'Test' attribute row is highlighted, and its bomb icon is circled in red. A 'Save' button is located at the bottom center of the page.

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

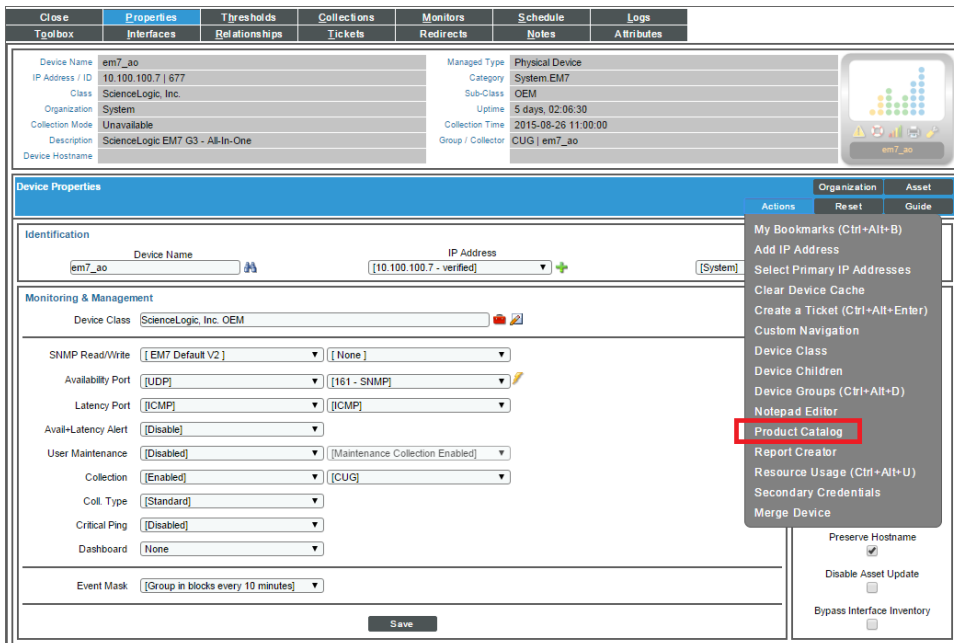
A product SKU describes a billable product or service and can be used later to create a billing policy. For details on creating and editing product SKUs, see the **Product Catalog** page (Registry > Business Services > Product Catalog). For information on billing policies, see the **Bandwidth Billing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

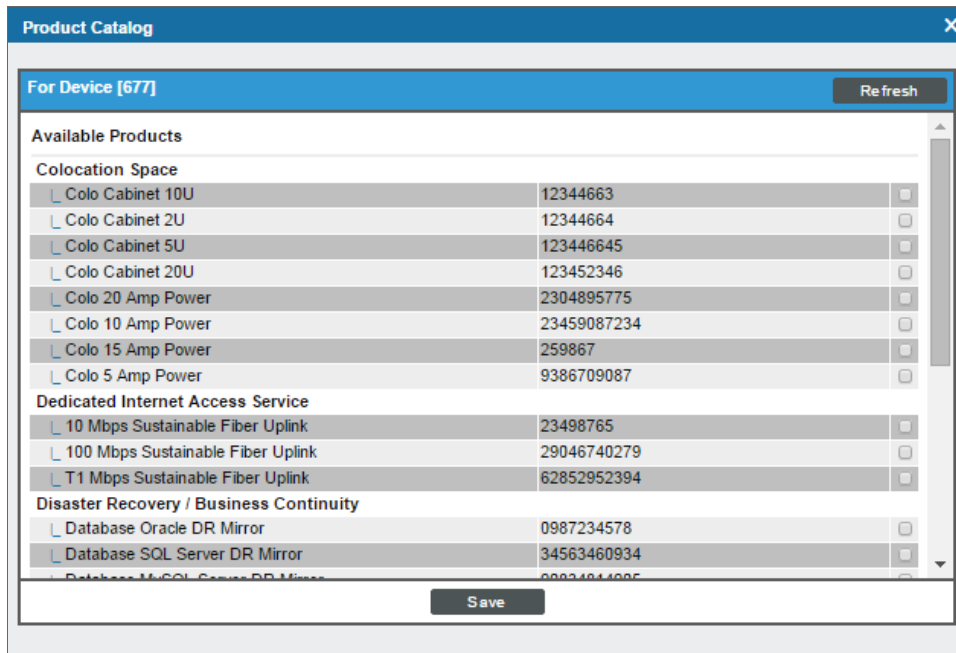
For details on product SKUs and bandwidth billing policies, see the manual **Business Services**.

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.

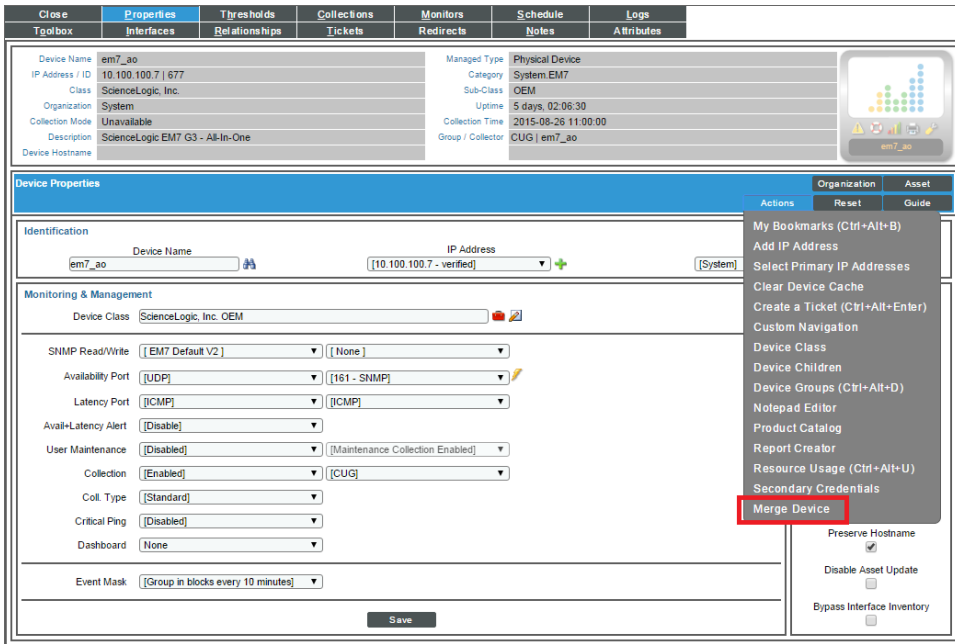
NOTE: If you have a large number of devices you want to merge, it might be more efficient to use the Bulk Merge feature, which is described in the [Performing a Bulk Device Merge](#) section.

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.

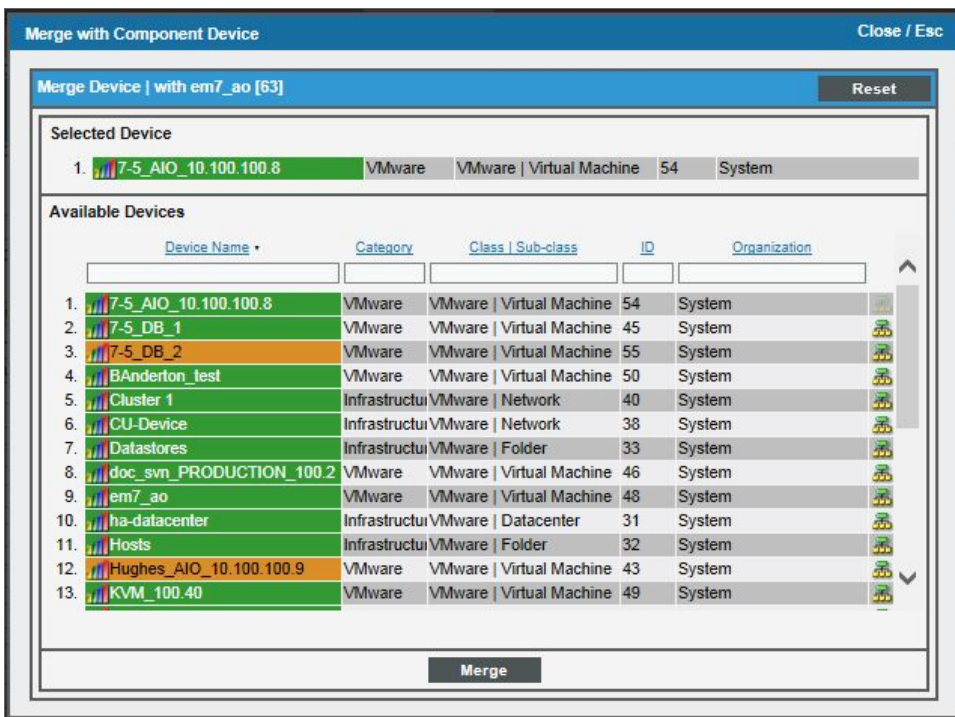
To merge individual devices:

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.

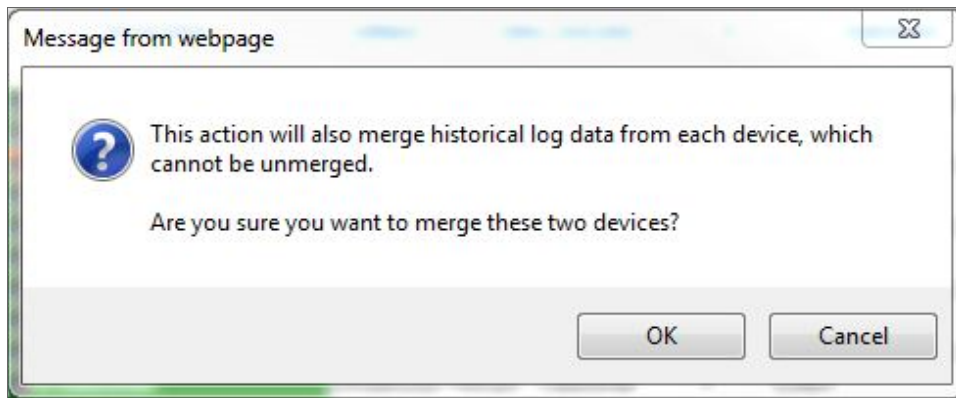
- On the **Device Properties** page, click the **[Actions]** menu and then select *Merge Device*.



- 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.

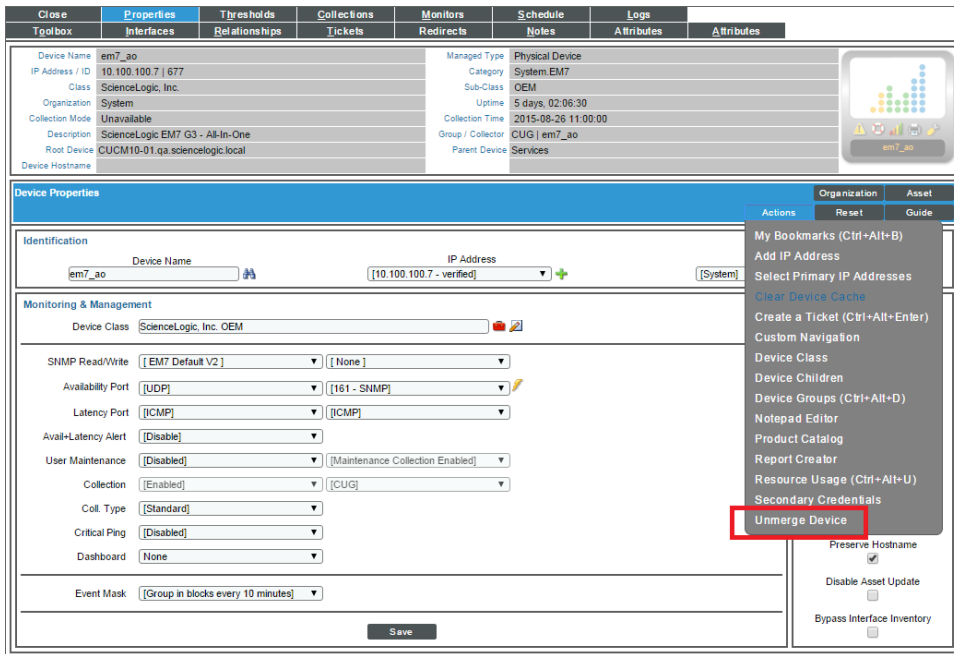
NOTE: If you have a large number of devices you want to unmerge, it might be more efficient to use the Bulk Unmerge feature, which is described in the [Performing a Bulk Device Unmerge](#) section.

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.

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



- 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 Collections page	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>

Managing Device Classes and Device Categories

Overview

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:

<i>Device Classes</i>	448
<i>Agent-Only Device Classes</i>	449
<i>Viewing the List of Device Classes</i>	450
<i>Filtering the List of Device Classes</i>	452
<i>Creating Device Classes</i>	453
<i>Creating a New Device Class of Type "SNMP-Enabled"</i>	454
<i>Editing an SNMP-Enabled Device Class</i>	457
<i>Creating a New Device Class for a Device with Device Class "Generic SNMP"</i>	457
<i>Creating a New Device Class for Devices That Do Not Support SNMP</i>	461
<i>Editing a Device Class That is Not SNMP-Enabled</i>	467
<i>Creating a Device Class of Type "Component"</i>	468
<i>Editing a Device Class of Type "Component"</i>	470
<i>Legacy Device Classes of Type "ICMP"</i>	470

<i>Managing Device Classes</i>	471
<i>Manually Changing the Device Class for a Device</i>	471
<i>Changing the Icon for a Device Class</i>	473
<i>Deleting One or More Device Classes</i>	473
<i>Aligning One or More Device Classes with a Device Dashboard</i>	474
<i>Device Categories</i>	474
<i>Viewing the List of Device Categories</i>	475
<i>"Pingable" Device Category</i>	476
<i>Creating a New Device Category</i>	476
<i>Editing a Device Category</i>	477
<i>Deleting a Device Category</i>	478
<i>Aligning One or More Device Categories with a Device Dashboard</i>	479

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

The ScienceLogic platform 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.

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

Device Class	Description	Device Category	Device Class Tier	Class ID	Collection Type	Process Collection	Device Dashboard	PowerPack	Device Icon	Discovery Identifier	Subs
10xlarge	AWS EC2 Instance Cloud Compute		No Tier	791	Component	n/a	--	Yes	ec2-10xl.png	AwsEc2Instance	--
2Wire	OEM	Unknown	No Tier	4140	Physical	n/a	--	Yes	_generic_unknown.png	1.3.6.1.4.1.4839	--
2xlarge	AWS EC2 Instance Cloud Compute		No Tier	781	Component	n/a	--	Yes	ec2-2xl.png	AwsEc2Instance	--
3Com	11Mbps Wlan Wireless		No Tier	668	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.20.2	--
3Com	2000 Termin Network Terminals		No Tier	634	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.3	--
3Com	210 Termin Network Terminals		No Tier	636	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.5	--
3Com	2100 Termin Network Terminals		No Tier	637	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.6	--
3Com	2500 Termin Network Terminals		No Tier	632	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.1	--
3Com	2600 Termin Network Terminals		No Tier	633	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.2	--
3Com	3000 Termin Network Terminals		No Tier	638	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.7	--
3Com	3100 Termin Network Terminals		No Tier	639	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.8	--
3Com	3com Corp. Network Switches		No Tier	692	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.16.2.2.3.1	--

- 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.

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:

The screenshot shows the 'Device Class Editor' interface. The top section contains several configuration panels: 'Device Type' (set to 'SNMP Enabled'), 'Device Class' (empty), 'Description' (empty), 'Correlation Method' (set to '[n/a]'), 'Agent Identifier 1' and 'Agent Identifier 2' (empty), 'Root Device' (checkbox), 'Discovery Identifier (SysObjectID)' (empty), 'Device Class Tier' (set to '1'), 'Discovery Qualifier (SNMP OID)' (empty), 'Device Icon' (set to '[generic_unknown.png]'), 'Collection Type' (set to '[Physical Device (Enabled)]'), 'Process Collection' (set to '[n/a]'), 'Service Collection' (set to '[n/a]'), 'Device Category' (set to '[Servers Search]'), 'System Uptime OID' (set to '[sysUptime (1.3.6.1.2.1.13.6)]'), 'Device Dashboard' (set to '[None]'), and 'L3 Topology' (checkbox). A 'Save' button is at the bottom right of the configuration area.

Below the configuration area is the 'Device Class Register' table, which lists existing device classes. The table has columns for Device Class, Description, Device Category, Device Class Tier, Class ID, Collection Type, Process Collection, Device Dashboard, ProcessPack, Device Icon, Discovery Identifier, and Subs.

Device Class	Description	Device Category	Device Class Tier	Class ID	Collection Type	Process Collection	Device Dashboard	ProcessPack	Device Icon	Discovery Identifier	Subs
10xlarge	AWS EC2 // Cloud Compute	No Tier	791	Component	n/a	--	Yes	ec2-10x.png	AwsEc2Instance	--	--
2Wire	OEM	Unknown	No Tier	4140	Physical	n/a	Yes	generic_unknown.png	1.3.6.1.4.1.4839	--	--
2xlarge	AWS EC2 // Cloud Compute	No Tier	781	Component	n/a	--	Yes	ec2-2x.png	AwsEc2Instance	--	--
3Com	11Mbps Wirt Wireless	No Tier	698	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.20.2	--	--
3Com	2000 Termin Network Terminals	No Tier	634	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.3	--	--
3Com	210 Termin Network Terminals	No Tier	635	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.5	--	--
3Com	2100 Termin Network Terminals	No Tier	637	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.6	--	--
3Com	2500 Termin Network Terminals	No Tier	632	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.1	--	--
3Com	2600 Termin Network Terminals	No Tier	633	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.2	--	--
3Com	3000 Termin Network Terminals	No Tier	638	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.7	--	--
3Com	3100 Termin Network Terminals	No Tier	639	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.1.8	--	--
3Com	3com Corp. Network Switches	No Tier	692	Physical	n/a	--	Yes	3com.png	1.3.6.1.4.1.43.1.16.2.2.3.1	--	--

- **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.

Device Manager Devices Found (176)												Actions		Report	Reset	Guide
Device Name	IP Address	Device Category	Device Class Sub-class	OID	Organization	Current State	Collection Group	Collection Status	SNMP Credential	SNMP Version						
server-651	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
ShorelineSwitch	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
Simulcast-01 on ScienceLogic local	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	pbm05	2.0						
SNAP652146	10.20.0.249	Storage NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
SNS-PRIX-MDC1-Texas	10.20.0.247	Network Switches	Juniper Networks M71 Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
SOM2353DX	10.20.0.188	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
Suma-1	10.20.0.92	Network Switches	Enterprise Networks Summit480c Version 7.1.1	191	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
sunprod1	10.20.0.27	Servers	NET-SNMP Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
Suvan_MonmouthJuncUSA	10.20.0.210	Telephony	Quantum Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
SW275SR4C1_NewDA	10.20.0.1	Network Switches	Cisco Systems Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
Swach2	10.20.0.16	Network Switches	Brocade ChampionAL Switch	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
Tandberg	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
tgernskic-fw0.ra1.hostedsolutions.com	10.20.0.157	Network Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
TOSHIBA-e-STUDIO451c	10.20.0.86	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
ttccomm	10.20.0.229	Unknown	terix OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
ts2 local	10.20.0.71	Network Switches	Cisco Systems TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
ts3 local	10.20.0.72	Network Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
TULLPT15-ACCOUNTING	10.20.0.160	Unknown	HP OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
upst1.tvm.az	10.20.0.77	Environmental UPS	APC SmartUPS 2200	86	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
UT1000	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
vxtarget	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
webdb-prod1	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
WILLIAMS-CORE-R01	10.20.0.82	Network Router	Cisco Systems 4766	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
WY5005-IT_Watchdogs, Inc.	10.20.0.228	Unknown	Generic SNMP	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						
wyosony134	10.20.0.23	Servers	Red River Networks	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0						

- In the **Device Administration** panel, select the **[Toolbox]** tab.

Close	Properties	Thresholds	Collections	Monitors	Tickets	Redirects	Notes
Schedule	Logs	Toolbox	Interfaces	Relationships			

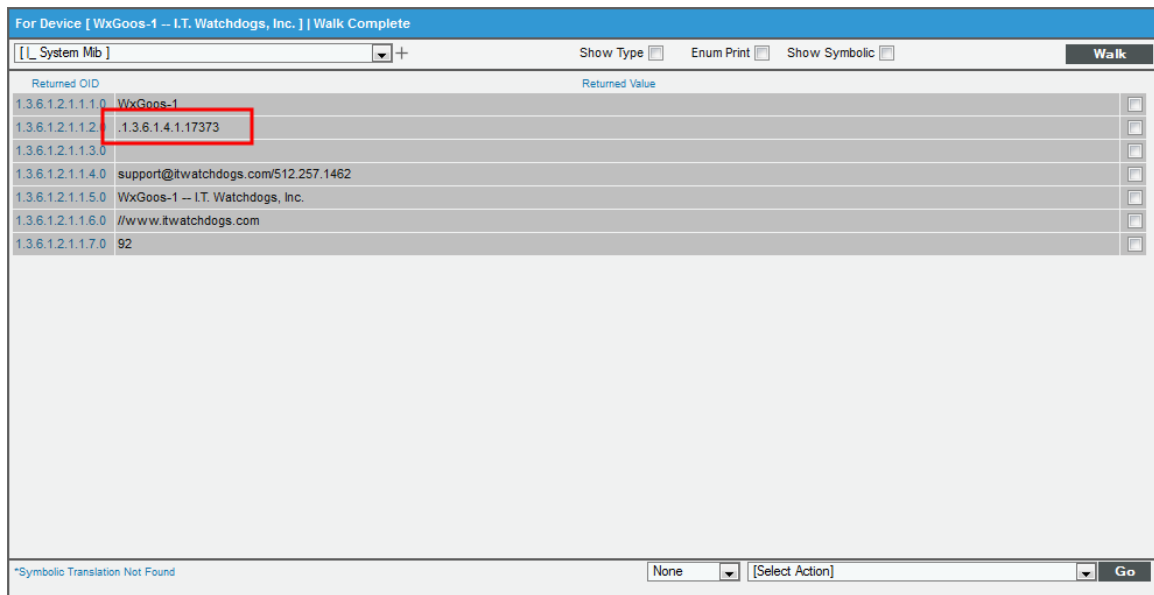
Device Name	WxGoos-1 -- I.T. Watchdogs, Inc.	Managed Type	Physical Device
IP Address / ID	10.20.0.228 78	Category	Unknown
Class	Generic	Sub-Class	SNMP
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2014-10-22 11:35:00
Description	WxGoos-1	Group / Collector	CUG1 MOSS_ISO_CU
Device Hostname			

Device Toolbox									Actions	Reset	Guide
SSH	SNMP Walker	Port Scan	Deep Port Scan	Traceroute	Ping Tool	Forward DIG	Reverse DIG	ARIN Whois			
ARP Lookup	ARP Ping	SNMP Dump	Web Policy								


Toolbox Sessions Logs Session Logs Found [0]					
Device	IP Address	Tool	Run Date	Run User	Session ID

- In the **Device Toolbox** page, select the icon for SNMP Walker.




- 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.



- 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.
- 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.
- To assign the new device class to a device, follow the instructions in the section [Manually Changing the Device Class for a Device](#).

- 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 re-discover. Select its wrench icon () . In the **Device Properties** page for the device, select the binoculars icon () .

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes
Device Name	10.20.0.175	Managed Type	Physical Device									
IP Address / ID	10.20.0.175 62	Category	Unknown									
Class	Generic	Sub-Class	SNMP									
Organization	System	Uptime	0 days, 00:00:00									
Collection Mode	Active	Collection Time	2014-06-12 17:20:00									
Description		Group / Collector	CUG2 em7_cu2									
Device Hostname												

Device Properties		Organization	Asset
		Actions	Reset Guide
Identification			
Device Name	10.20.0.175 	IP Address	[10.20.0.175 - verified] +
		Organization	[System] 
Monitoring & Management		Preferences	
Device Class	Generic SNMP 	Auto-Clear Events	<input checked="" type="checkbox"/>
SNMP Read/Write	[Cisco SNMPv2 - Example] [None]	Accept All Logs	<input checked="" type="checkbox"/>
Availability Port	[UDP] [161 - SNMP]	Daily Port Scans	<input checked="" type="checkbox"/>
Latency Port	[ICMP] [ICMP]	Auto-Update	<input checked="" type="checkbox"/>
Avail+Latency Alert	[Disable]	Scan All IPs	<input type="checkbox"/>
User Maintenance	[Disabled] [Maintenance Collection Enabled]	Dynamic Discovery	<input checked="" type="checkbox"/>
Collection	[Enabled] [CUG2]	Preserve Hostname	<input checked="" type="checkbox"/>
Coll. Type	[Standard]	Disable Asset Update	<input type="checkbox"/>
Critical Ping	[Disabled]		
Dashboard	[None]		
Event Mask	[Group in blocks every 10 minutes]		
Save			

- 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.

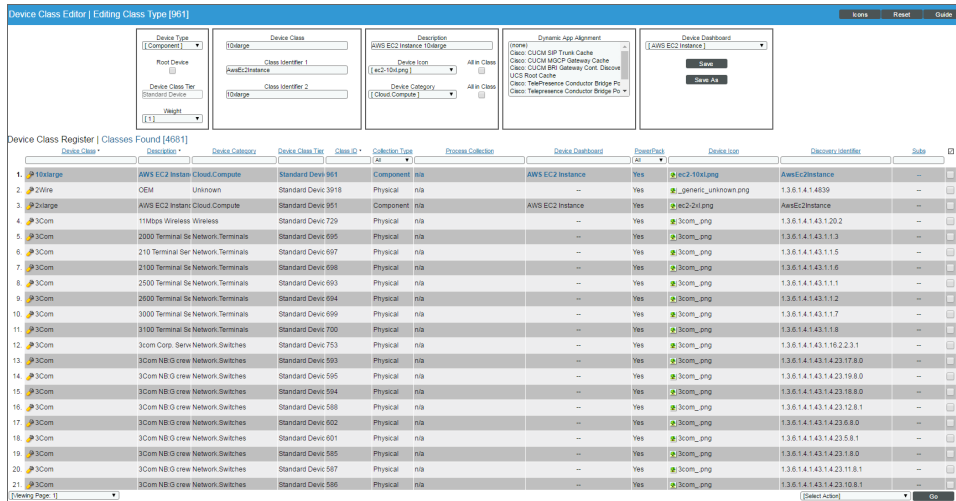
NOTE: For information on XPATH syntax, see http://www.w3schools.com/xpath/xpath_syntax.asp

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", extrainfo="(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`

- 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 **Weight** 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 your 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 your 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 your 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.

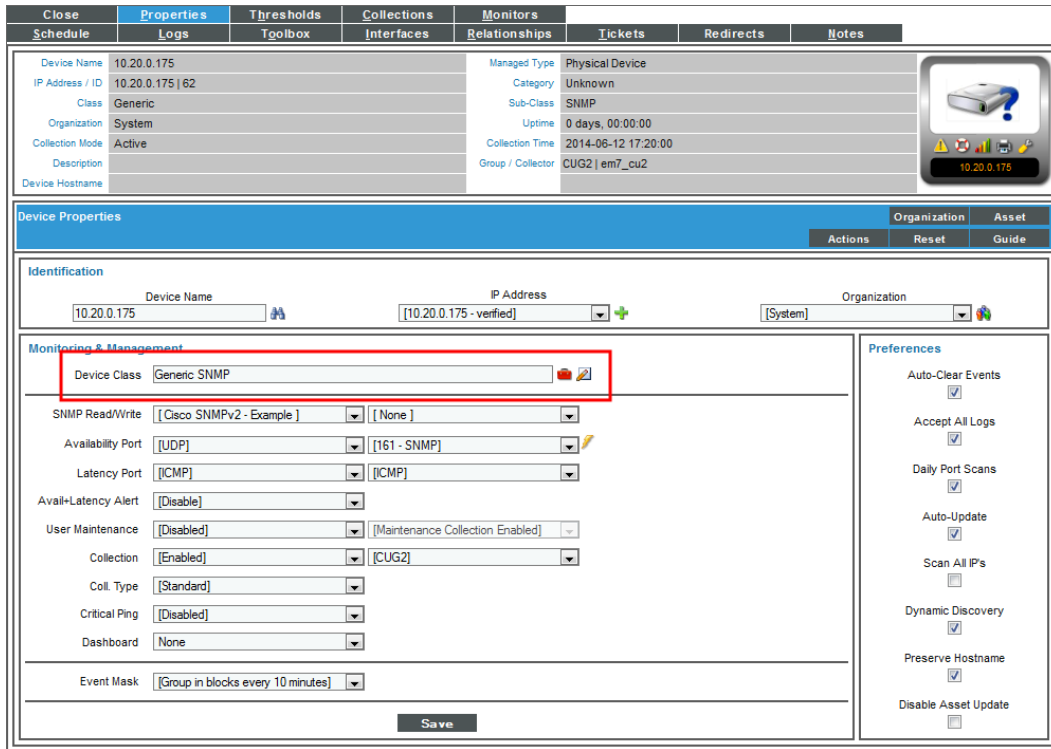
In the **Device Properties** page, you can assign a different device class to the device.

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 ().

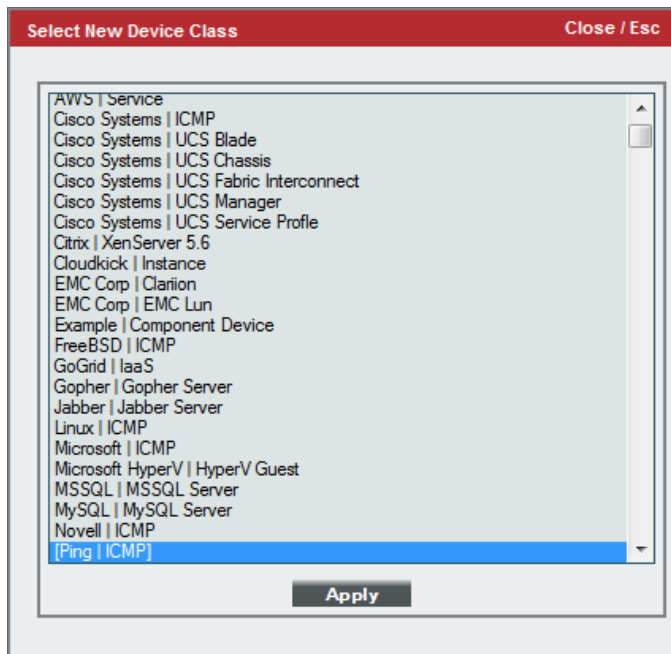
Device Manager Devices Found (176)										Actions		Report	Reset	Guide	
Device Name	IP Address	Device Category	Device Class / Subclass	OID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version					
151	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
152	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
153	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	cbamba V2	2.0					
154	10.20.0.249	Storage NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
155	10.20.0.247	Network Switches	Juniper Networks JMI Router	152	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
156	10.20.0.188	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
157	10.20.0.92	Network Switches	Extreme Networks Summit45a) Version 7.1.1	101	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
158	10.20.0.27	Servers	NET-SNMP Solaris	169	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
159	10.20.0.210	Telephony	Quintum Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
160	10.20.0.1	Network Switches	Cisco Systems Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
161	10.20.0.16	Network Switches	Brocade Channel-AL Switch	184	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
162	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
163	10.20.0.187	Network Firewall	Cisco Systems ASA 5520	148	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
164	10.20.0.98	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
165	10.20.0.209	Unknown	Xerox OEM	81	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
166	10.20.0.71	Network Switches	Cisco Systems TS 5520	68	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
167	10.20.0.72	Network Switches	Cisco Systems TS SEC	87	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
168	10.20.0.168	Unknown	HP OEM	168	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
169	10.20.0.205	Unknown	Yenno OEM	85	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
170	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
171	10.20.0.227	Telephony	Vina Technologies Multiplexor	138	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
172	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	97	System	Critical	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
173	10.20.0.82	Network Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
174	10.20.0.228	Unknown	Generic SNMP	78	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					
175	10.20.0.23	Servers	XenServer Xen Host	116	System	Healthy	CUG1	Active	Cisco SNMPV2 - Exa V2	2.0					

- In the **Device Properties** page, find the *Device Class* field. Select the toolbox icon ().





The screenshot shows the 'Device Properties' page for a device with IP 10.20.0.175. The 'Device Class' field is set to 'Generic SNMP' and is highlighted with a red box. A red box also highlights the toolbox icon (a red square with a white 'X') next to the field. The page includes tabs for Identification, Monitoring & Management, and Preferences. The 'Monitoring & Management' section contains various configuration options for SNMP, availability, and collection. The 'Preferences' section on the right has several checkboxes for event handling and updates.

- In the **Select New Device Class** modal page, select a device class.





The screenshot shows the 'Select New Device Class' modal window. It features a list of device classes with a scroll bar on the right. The class '[Ping | ICMP]' is highlighted in blue at the bottom of the list. An 'Apply' button is located at the bottom center of the modal. The window title is 'Select New Device Class' and it includes a 'Close / Esc' button in the top right corner.

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.

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.

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.

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).

ID	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.	EMT 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. 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.

Categories		TRIAL LICENSE 30 DAYS REMAINING				Reset	Guide
	Category Name	Category Key Words	Dashboards	Reports	Widgets		
1.	SolenoLogic		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.

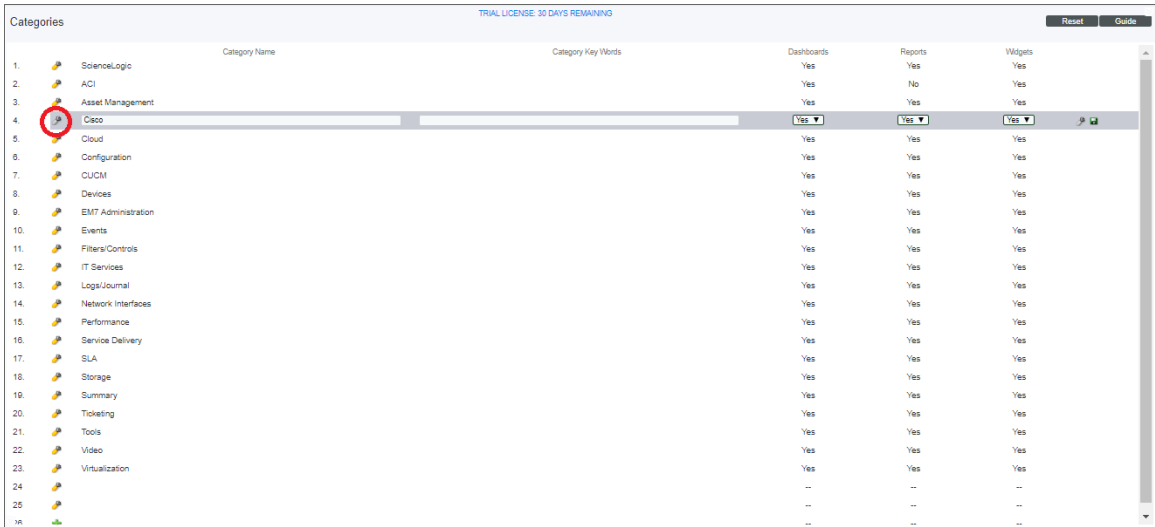
- **Map Icon.** Select an icon to be associated with this device category. You can select from a list of all possible icons for device categories. The selected icon will be used to represent members of the device category in the network maps in Views and maps.
 - **Device Dashboard.** Select a device 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).

- 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 ().



	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.	EMT 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.			--	--	--
25.			--	--	--
26.			--	--	--


- 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.
- 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:

- Go to the **Categories** page (System > Customize > Categories).
- In the **Categories** page, find the device category you want to delete. Select its bomb icon ().
- 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.

Monitoring Device Availability and Device Latency

Overview

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:

<i>Availability</i>	480
<i>Configuring Availability Monitoring on a Device</i>	481
<i>Defining Availability Thresholds</i>	483
<i>Configuring Availability for Component Devices</i>	483
<i>Latency</i>	486
<i>Configuring Latency Monitoring on a Device</i>	486
<i>Defining Latency Thresholds</i>	488
<i>Viewing Reports on Device Availability and Device Latency</i>	488

Availability

Availability means a device's ability to accept connections and data from the network. 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.

By default, the method SL1 uses to monitor availability of the device is determined by the first method of discovery:

- If the agent is installed and creates a device record before the device is discovered as an SNMP or pingable device, availability is measured based on whether the agent is reporting data to SL1.
- If the device is discovered as an SNMP or pingable device before the agent is installed, availability is measured based on the method used to discover the device (SNMP, ICMP, or TCP).

If a device or interface becomes unavailable multiple times in a specified time frame, SL1 can generate an "availability flapping" event. By default, SL1 generates an event if a device becomes unavailable three times in an hour, or if an interface becomes unavailable three times in twenty-four hours.

To generate availability reports, SL1 must be configured to collect availability and latency data from devices. The following section describes how to configure SL1 to collect this data.

NOTE: Unlike for hardware-based devices, SL1 does not use an ICMP, TCP, or UDP to monitor availability for component devices. 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.

Configuring Availability Monitoring on a Device

SL1 uses ports to monitor a device's availability. You specify which ports to use for device availability in the **Device Properties** page.

NOTE: Unlike for hardware-based devices, SL1 does not use use an ICMP, TCP, or UDP to monitor availability for component devices. 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.

To configure availability monitoring for a device:

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

- In the **Device Manager** page, find the device for which you want to configure availability monitoring. Select its wrench icon (🔧). The **Device Properties** page is displayed:

Close	Properties	Thresholds	Collections	Monitors	Tickets	Redirects	Notes
Schedule	Logs	Toolbox	Interfaces	Relationships			

Device Name	192.168.54.17	Managed Type	Physical Device
IP Address / ID	192.168.54.17 185	Category	Servers
Class	Cisco Systems	Sub-Class	UCS Manager
Organization	System	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2014-05-15 20:12:00
Description		Group / Collector	CUG1 em7_cu1
Device Hostname			

Device Properties Organization: [System] Asset: [192.168.54.17]

Actions: [Reset] [Guide]

Identification

Device Name: [192.168.54.17] IP Address: [192.168.54.17 - verified] Organization: [System]

Monitoring & Management

Device Class: Cisco Systems UCS Manager

SNMP Read/Write: [None] [None]

Availability Port: [UDP] [161 - snmp]

Latency Port: [ICMP] [ICMP]

Avail+Latency Alert: [Disable]

User Maintenance: [Disable] [Maintenance Collection Enabled]

Collection: [Enabled] [CUG1]

Coll. Type: [Standard]

Critical Ping: [Disable]

Dashboard: [None]

Event Mask: [Group in blocks every 10 minutes]

Save

Preferences

Auto-Clear Events

Accept All Logs

Daily Port Scans

Auto-Update

Scan All IPs

Dynamic Discovery

Preserve Hostname

Disable Asset Update

- In the **Device Properties** page, edit the following fields:
 - Availability Port** . Specifies the protocol (first drop-down menu) and specific port (second drop-down menu) SL1 should monitor to determine if the device is available. The list of ports will contain the ports discovered by SL1 . The data collected from this port will be used in device availability 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 availability.

NOTE: Component Devices use a Dynamic Application collection object to measure availability.

- **Avail + Latency Alert.** Specifies how SL1 should respond when the device fails an availability check, a latency check, or 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 (indicated by the device failing both the availability check and the latency check). 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 only the event "Device Failed Availability Check: UDP - SNMP". The event "Network Latency Exceeded Threshold: No Response" is suppressed under the availability event.

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

Defining Availability Thresholds

SL1 allows you to define global Availability Thresholds that apply to all devices and device-specific Availability Thresholds that apply to only a selected device. When a device fails to meet the availability threshold (that is, is not available as specified in the threshold), SL1 generates an event about the device.

For details on defining availability thresholds, see the chapter on [Thresholds and Data Retention](#).

NOTE: Unlike for hardware-based devices, SL1 does not use ICMP, TCP, or UDP to monitor availability for component devices. 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 section on [monitoring availability of component devices](#).


Configuring Availability for Component Devices

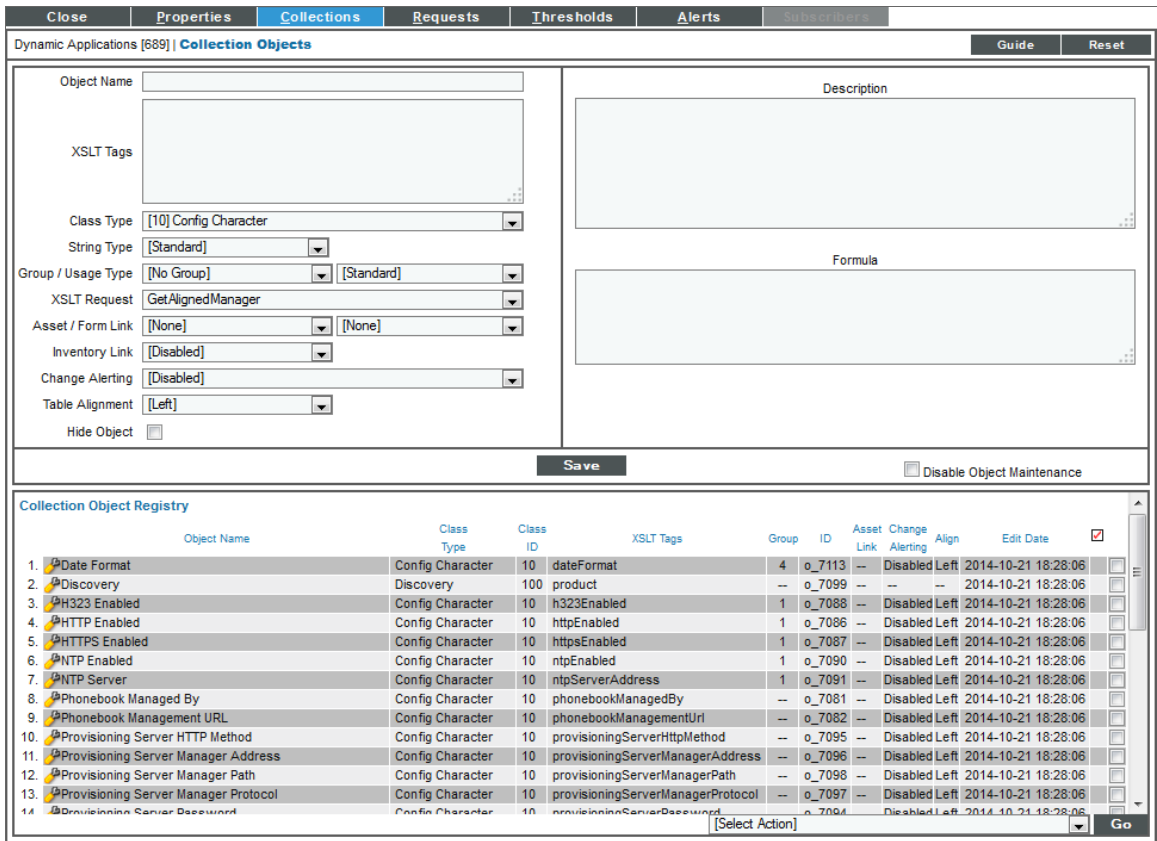
Dynamic Applications that create component devices have the **Component Mapping** checkbox selected in the **Dynamic Applications Properties Editor** page and also include the **Component Identifiers** field.















In the **Component Identifiers** field, you map the value of a collection object to the *Device Name* identifier and *Unique Identifier* identifier, so SL1 can create one or more component devices.


In the **Component Identifiers** field, you can also map a collection object to the *Availability* identifier. For hardware-based devices, SL1 monitors an ICMP, TCP, or UDP port to determine availability. Because component devices might not include ICMP, TCP, or UDP ports, you must use a Component Identifier to determine availability.

To configure SL1 to monitor availability for a component device:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. Find the Dynamic Application that creates and monitors the component devices you are interested in. Select its wrench icon ().
3. In the **Dynamic Applications Properties Editor** page, examine the **Component Mapping** checkbox. If the checkbox is selected, this is the correct Dynamic Application to edit.
4. Select the **[Collections]** tab.



Object Name	Class Type	Class ID	XSLT Tags	Group	ID	Asset Link	Change Alerting	Align	Edit Date	
1. Date Format	Config Character	10	dateFormat	4	o_7113	--	Disabled	Left	2014-10-21 18:28:06	
2. Discovery	Discovery	100	product	--	o_7099	--	--	--	2014-10-21 18:28:06	
3. H323 Enabled	Config Character	10	h323Enabled	1	o_7088	--	Disabled	Left	2014-10-21 18:28:06	
4. HTTP Enabled	Config Character	10	httpEnabled	1	o_7086	--	Disabled	Left	2014-10-21 18:28:06	
5. HTTPS Enabled	Config Character	10	httpsEnabled	1	o_7087	--	Disabled	Left	2014-10-21 18:28:06	
6. NTP Enabled	Config Character	10	ntpEnabled	1	o_7090	--	Disabled	Left	2014-10-21 18:28:06	
7. NTP Server	Config Character	10	ntpServerAddress	1	o_7091	--	Disabled	Left	2014-10-21 18:28:06	
8. Phonebook Managed By	Config Character	10	phonebookManagedBy	--	o_7081	--	Disabled	Left	2014-10-21 18:28:06	
9. Phonebook Management URL	Config Character	10	phonebookManagementUrl	--	o_7082	--	Disabled	Left	2014-10-21 18:28:06	
10. Provisioning Server HTTP Method	Config Character	10	provisioningServerHttpMethod	--	o_7095	--	Disabled	Left	2014-10-21 18:28:06	
11. Provisioning Server Manager Address	Config Character	10	provisioningServerManagerAddress	--	o_7096	--	Disabled	Left	2014-10-21 18:28:06	
12. Provisioning Server Manager Path	Config Character	10	provisioningServerManagerPath	--	o_7098	--	Disabled	Left	2014-10-21 18:28:06	
13. Provisioning Server Manager Protocol	Config Character	10	provisioningServerManagerProtocol	--	o_7097	--	Disabled	Left	2014-10-21 18:28:06	
14. Provisioning Server Password	Config Character	10	provisioningServerPassword	--	o_7094	--	Disabled	Left	2014-10-21 18:28:06	

5. In the list of Collection Objects in the **Collection Object Registry** pane, determine which collection object will always be available if the component device is available. Click on the wrench icon () for that collection object.

6. In the **Component Identifiers** field, select:

- **Availability**. Object that specifies whether a component device is available. If SL1 can collect a value for a component device using the aligned collection object and the value is not 0 (zero) or "false", SL1 considers the component device as "available". If SL1 cannot collect a value for a component device using the aligned collection object or SL1 collects a value that is 0 (zero) or "false", SL1 considers the component device as "unavailable".
 - If the collection objects aligned with the *Device Name* and *Unique Identifier* component identifiers return lists of values, SL1 will create multiple component devices. Each component device will be associated with an index, i.e. a location in the list of values. If all the component devices in the list should be considered available, the collection object aligned with the *Availability* component identifier should return a list of values with a value at each index associated with a component device. A component device is unavailable when the list of values returned by the collection object aligned with the *Availability* component identifier does not include a value at the index or returns a value of 0 (zero) or false at the index for the component device. For more information about Dynamic Application indexing, see the **Dynamic Application Development** manual.
 - If you align a collection object with this component identifier, SL1 will create a system availability graph for each component device in the **Device Performance** page.
 - If you align a collection object with this component identifier and SL1 cannot collect a value for a component device using the aligned collection object SL1 will supply the Value "Unavailable" in the **Collection State** column in the **Device Components** page.

7. Select the **[Save]** button to save your changes.

8. SL1 will now monitor availability and graph availability statistics for the component devices aligned with the Dynamic Application.

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.

Latency

Latency means the amount of time it takes SL1 to communicate with a device. Specifically, latency refers to the amount of time between when SL1 initiates communication with a device and when the device responds and allows communication. Latency is expressed in milliseconds (ms).

SL1 uses ports to monitor a device's latency. You specify which ports to use for device latency on the **[Settings]** tab of the **Device Investigator** page.

Configuring Latency Monitoring on a Device

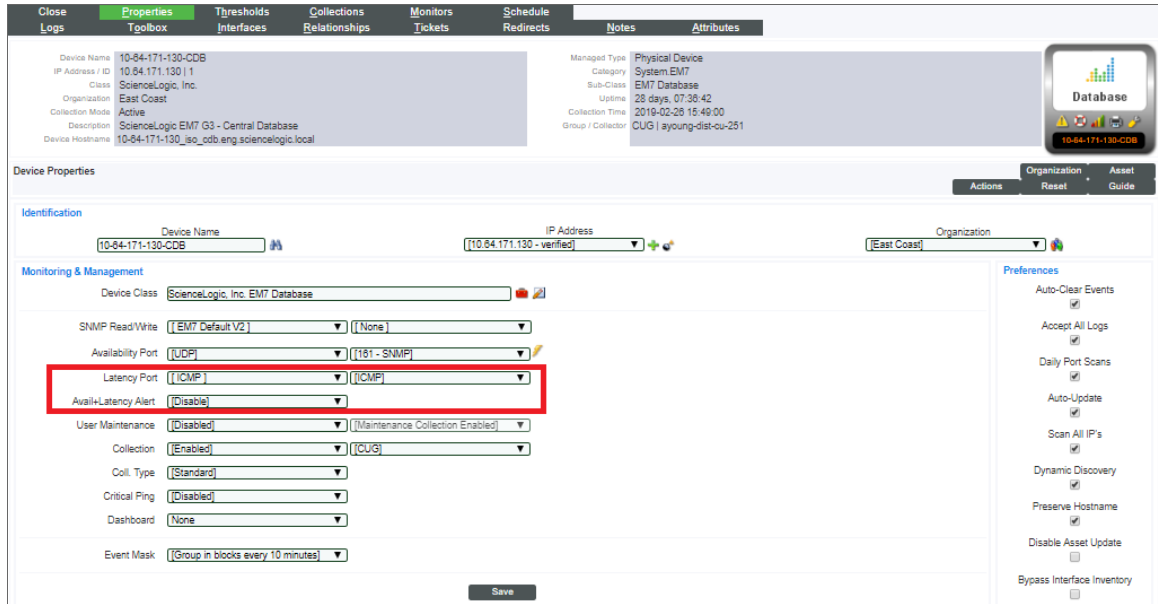
SL1 uses ports to monitor a device's latency. You specify which ports to use for device latency in the **Device Properties** page.

To configure latency monitoring for a device:

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

Device Name	IP Address	Device Category	Device Class Sub-class	CID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version
server-851	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
Shoreline-Switch	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
SimpleGDR.ca.ScienceLogic.local	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	pbim0s V2	
SNAP562146	10.20.0.249	Storage.NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
SNS-PRIX-MDC1-Texas	10.20.0.247	Network.Switches	Juniper Networks M71 Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
SOM2353DX	10.20.0.188	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
Somni-1	10.20.0.92	Network.Switches	Enterprise Networks Summit4800 Version 7.1.1	181	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
sunprod1	10.20.0.217	Servers	NET-SNMP Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2	
Suvan_MonmouthJunctUSA	10.20.0.210	Telephony	Quantum Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
SW275DR4C1_NewDA	10.20.0.1	Network.Switches	Cisco Systems Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
Switch	10.20.0.16	Network.Switches	Brocade Chassis-AL Switch	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
Tandberg	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
tgertskic-fw0.ral.hostedsolutions.com	10.20.0.157	Network.Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
TOSHIBA-e-STUDIO451c	10.20.0.88	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
Tecnum	10.20.0.229	Unknown	Kenix OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
ts3.local	10.20.0.71	Network.Switches	Cisco Systems TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
ts3.local	10.20.0.72	Network.Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
TULLPT15-ACCOUNTING	10.20.0.168	Unknown	HPI OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
upst1.tvm.az	10.20.0.77	Environmental.UPS	APC SmartUPS 2200	86	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	
US100	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
vxTarget	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
webdb-prod1	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	
WILLIAMS-CORE-R01	10.20.0.82	Network.Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
Wixom201-IT.Watchdogs, Inc.	10.20.0.228	Unknown	Generic SNMP	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
wixomssn124	10.20.0.23	Servers	XenServer Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	

2. In the **Device Manager** page, find the device for which you want to configure latency monitoring. Select its wrench icon (🔧).
3. The **Device Properties** page appears.



4. In the **Device Properties** page, edit the following fields:
 - **Latency Port**. Specifies the protocol (first drop-down menu) and specific port (second drop-down menu) SL1 should monitor to determine latency for the device. The list of ports will contain all the ports discovered by SL1. The data collected from this port 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, a latency check, or 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 only the event "Device Failed Availability Check: UDP - SNMP". The event "Network Latency Exceeded Threshold: No Response" is suppressed under the availability event.

Defining Latency Thresholds

SL1 allows you to define global Latency Thresholds that apply to all devices and device-specific Latency Thresholds that apply only to a specific device. When a device fails to meet the latency threshold (that is, takes longer than the specified time-span to respond), SL1 generates an event about the device. For example, if the latency threshold is "100 ms", when a device does not respond to a poll within 100 ms, SL1 will generate an event about that device.

To disable the latency threshold for a single device, set the threshold to 0% (zero percent). When you disable a threshold, SL1 does not generate an event for the threshold.

For details on defining latency thresholds, see the chapter on [Thresholds and Data Retention](#).

Viewing Reports on Device Availability and Device Latency

See the chapter [Viewing Performance Graphs](#) to view information and examples of reports for device availability and device latency.



Chapter

24

Device Toolbox

Overview

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?	489
Accessing the Device Toolbox page	489
Viewing the Session Logs	492


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 ()

Device Manager Devices Found [176]										Actions	Report	Reset	Guide	
Device Name	IP Address	Device Category	Device Class / Subclass	CPU	Organization	Current State	Collection Group	Collection Rate	SNMP Credentials	SNMP Version				
151	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
152	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
153	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	c8sm0s - V2					
154	10.20.0.249	Storage.NAS	Quantum Corp - Snap Division Snap Server	156	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
155	10.20.0.247	Network.Switches	Juniper Networks NFX Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
156	10.20.0.199	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
157	10.20.0.92	Network.Switches	Extreme Networks Summ484i Version 7.1.1	101	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
158	10.20.0.27	Servers	NET-SNMP Solars	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2					
159	10.20.0.210	Telephony	DuPont Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
160	10.20.0.1	Network.Switches	Cisco Systems Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
161	10.20.0.15	Network.Switches	Brocade Channel-AL Switch	104	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
162	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
163	10.20.0.157	Network.Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
164	10.20.0.86	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
165	10.20.0.229	Unknown	Xerox OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
166	10.20.0.71	Network.Switches	Cisco Systems TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
167	10.20.0.72	Network.Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
168	10.20.0.166	Unknown	HP OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
169	10.20.0.77	Environmental	URS APC SmartUPS 2200	66	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2					
170	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
171	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
172	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
173	10.20.0.92	Network.Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2					
174	10.20.0.228	Unknown	Generic SNMP	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					
175	10.20.0.23	Servers	XenServer Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2					

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

Close	Properties	Thresholds	Collections	Monitors	Tickets	Redirects	Notes
Schedule	Logs	Toolbox	Interfaces	Relationships			
Device Name: WxGoos-1 - IT, Watchdogs, Inc. IP Address / ID: 10.20.0.228 78 Class: Generic Organization: System Collection Mode: Active Description: WxGoos-1 Device Hostname:		Managed Type: Physical Device Category: Unknown Sub-Class: SNMP Uptime: 0 days, 00:00:00 Collection Time: 2014-10-22 11:35:00 Group / Collector: CUG1 MOSS_ISO_CU					
Device Toolbox							
SSH	SNMP Walker	Port Scan	Deep Port Scan	Traceroute	Ping Tool	Forward DIG	Reverse DIG
ARP Lookup	ARP Ping	SNMP Dump	Web Policy				ARIN Whois
Toolbox Sessions Logs Session Logs Found [0]							
Device	IP Address	Tool	Run Date	Run User	Session ID		

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).





Device	IP Address	Tool	Run Date	Run User	Session ID
1. WxGoos-1 -- IT, Watchdogs, Inc.	10.20.0.228	SNMP Walker	2014-10-22 11:37:07	mantone	1

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

25

Device Maintenance

Overview

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:

<i>What is Scheduled Maintenance?</i>	495
<i>What is User Maintenance?</i>	496
<i>The Maintenance Minimum Severity Setting</i>	497
<i>Enabling and Disabling User Maintenance for a Single Device</i>	497
<i>Enabling and Disabling User Maintenance for a One or More Devices</i>	499
<i>Scheduling Maintenance for a Single Device</i>	500
<i>Scheduling Maintenance for One or More Devices</i>	504
<i>Enabling or Disabling Scheduled Maintenance for One or More Devices</i>	505
<i>Deleting Scheduled Maintenance for One or More Devices</i>	506

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).

Device Name	IP Address	Device Category	Device Class / Subclass	CPU	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version	Actions
Server-01	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
ShorelineSwitch	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
SimpleSet.qa.ScienceLogic.local	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	cbSmS V2		[Icons]
SNAP562146	10.20.0.249	Storage.NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
SNS-PRN-MDC1-Texas	10.20.0.247	Network.Switches	Juniper Networks M71 Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
SUR2333DX	10.20.0.193	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Summit-1	10.20.0.92	Network.Switches	Extreme Networks Summit46s Version 7.1.1	101	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
sunprod1	10.20.0.217	Servers	NET-SNMP Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Sween_MonmouthJunctUSA	10.20.0.210	Telephony	Quantum Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
SW2750RAC1-NewGA	10.20.0.1	Network.Switches	Cisco Systems Catalyst 3750-Slack	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
svs03	10.20.0.15	Network.Switches	Brocade Chameleon Switch	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Tandberg	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Tigerakko-fw0.ra1.hostedsoolutions.com	10.20.0.157	Network.Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
TOSHIBA-e-STUDD451c	10.20.0.86	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Tecsum	10.20.0.229	Unknown	Kenex OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
ts2.local	10.20.0.71	Network.Switches	Cisco Systems TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
ts3.local	10.20.0.72	Network.Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
TULLPT15-ACCOUNTING	10.20.0.168	Unknown	HP OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
UPL11.twin.ae	10.20.0.77	Environmental[UPC]	SmartUPS 2200	86	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
V11000	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
vixTarget	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
wrdb06-prod	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
WLAN5-CORE-R01	10.20.0.82	Network.Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
Wdcdog1.mt.Watchdogs, Inc.	10.20.0.229	Unknown	Generic SNMP	79	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]
wxmonsrv134	10.20.0.23	Servers	XenServer Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2		[Icons]

- 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:

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name	em7_ao	Managed Type	Physical Device
IP Address / ID	10.100.100.7 677	Category	System EM7
Class	ScienceLogic, Inc.	Sub-Class	OEM
Organization	System	Uptime	5 days, 02:06:30
Collection Mode	Unavailable	Collection Time	2015-08-26 11:00:00
Description	ScienceLogic EM7 G3 - All-In-One	Group / Collector	CUG em7_ao
Device Hostname			

Device Properties		Organization	Asset
		Actions	Reset
			Guide

Identification		
Device Name	em7_ao	IP Address
		[10.100.100.7 - verified]
Organization	[System]	

Monitoring & Management		Preferences
Device Class	ScienceLogic, Inc. OEM	Auto-Clear Events
SNMP Read/Write	[EM7 Default V2] [None]	<input checked="" type="checkbox"/>
Availability Port	[UDP] [161 - SNMP]	Accept All Logs
Latency Port	[ICMP] [ICMP]	<input checked="" type="checkbox"/>
Avail+Latency Alert	[Disable]	Daily Port Scans
User Maintenance	[Disabled] [Maintenance Collection Enabled]	<input checked="" type="checkbox"/>
Collection	[Enabled] [CUG]	Auto-Update
Coll. Type	[Standard]	<input checked="" type="checkbox"/>
Critical Ping	[Disabled]	Scan All IP's
Dashboard	None	<input type="checkbox"/>
Event Mask	[Group in blocks every 10 minutes]	Dynamic Discovery
		<input checked="" type="checkbox"/>
		Preserve Hostname
		<input checked="" type="checkbox"/>
		Disable Asset Update
		<input type="checkbox"/>
		Bypass Interface Inventory
		<input type="checkbox"/>

Save

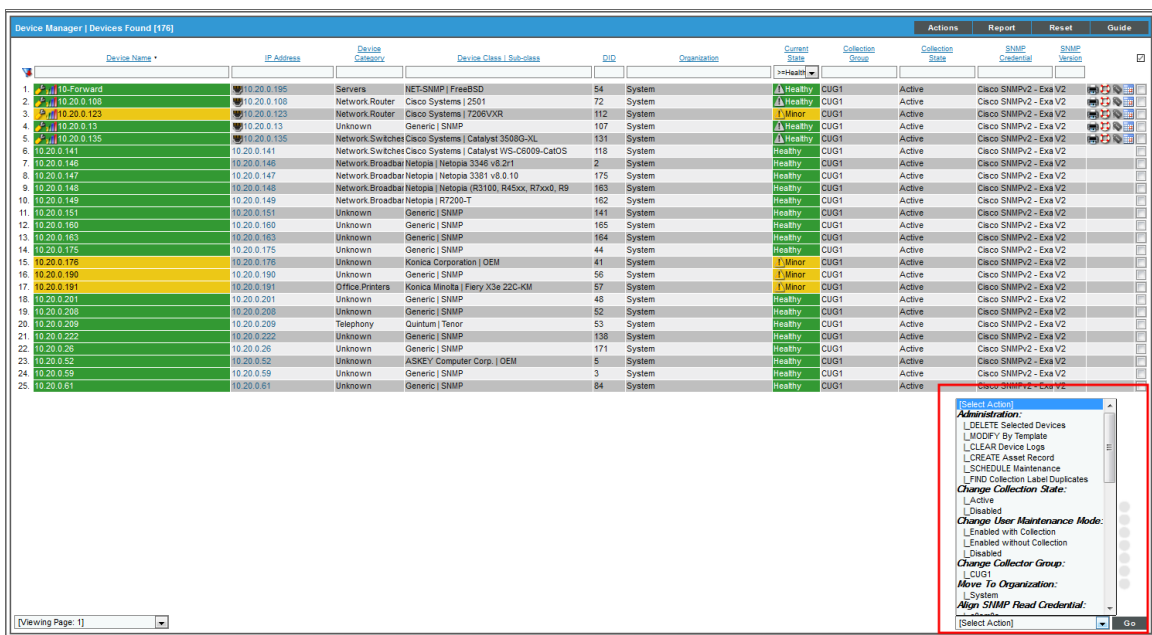
- In the **Device Properties** page, edit the following fields:
 - User Maintenance.** Specifies whether the device is in user maintenance mode. During maintenance mode, for the selected devices SL1 will generate only events with a severity less than the system-wide **Maintenance Minimum Severity** setting. 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.
- Select the **[Save]** button.

Enabling and Disabling User Maintenance for a 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:

The screenshot shows the 'Schedule Manager' interface. At the top, there are tabs for 'Close', 'Properties', 'Thresholds', 'Collections', 'Monitors', 'Schedule', 'Logs', 'Toolbox', 'Interfaces', 'Relationships', 'Tickets', 'Redirects', 'Notes', and 'Attributes'. The 'Schedule' tab is active, displaying details for a device with IP 10.2.9.54. Below this, there is a table titled 'Schedule Manager | Schedules Found [2]' with columns: Schedule Summary, Schedule Description, Event ID, sch id, Context, Timezone, Start Time, Duration, Recurrence Interval, End Date, Last Run, Owner, Organization, Visibility, and Enabled. Two rows of data are shown: 'Monthly maintenance' and 'One-time maintenance'.

Schedule Summary	Schedule Description	Event ID	sch id	Context	Timezone	Start Time	Duration	Recurrence Interval	End Date	Last Run	Owner	Organization	Visibility	Enabled
1. Monthly maintenance	Monthly test maintenance	151	80	Devices	America/New_	2017-01-17 03:00:00	80 min	Every 1 Month	2017-12-17 03:00:00	--	banderton	System	Private	Yes
2. One-time maintenance	One-time test maintenance	152	61	Devices	America/New_	2017-01-20 00:00:00	300 min	--	--	--	banderton	System	Private	Yes

- **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".

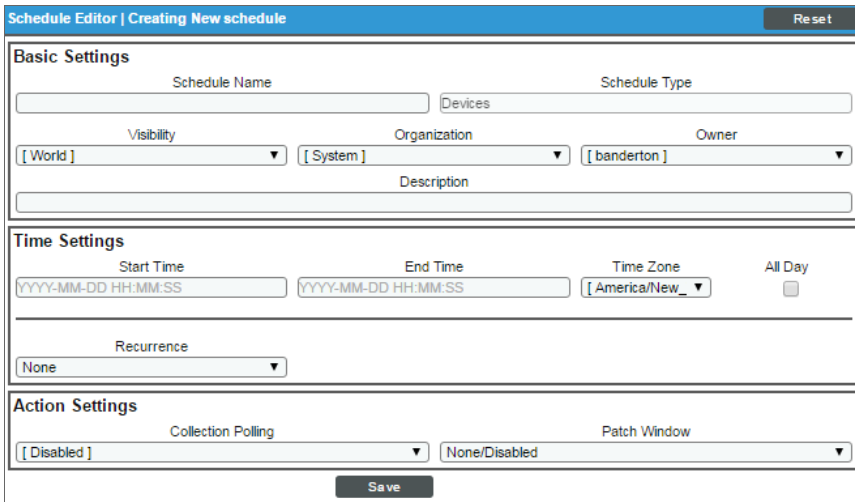
To edit a scheduled or recurring device maintenance window, click its wrench icon () and update the settings as needed on the **Schedule Editor** modal page. (For more information, see the section [Defining a Scheduled or Recurring Device Maintenance Window for a Single Device](#).)

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:



The screenshot shows the 'Schedule Editor | Creating New schedule' modal page. It is divided into three main sections: Basic Settings, Time Settings, and Action Settings. At the top right is a 'Reset' button, and at the bottom center is a 'Save' button.

- Basic Settings:** Includes fields for 'Schedule Name' (empty), 'Schedule Type' (set to 'Devices'), 'Visibility' (set to '[World]'), 'Organization' (set to '[System]'), 'Owner' (set to '[banderton]'), and a 'Description' field (empty).
- Time Settings:** Includes 'Start Time' (format: YYYY-MM-DD HH:MM:SS), 'End Time' (format: YYYY-MM-DD HH:MM:SS), 'Time Zone' (set to '[America/New_]'), and an 'All Day' checkbox (unchecked). Below these is a 'Recurrence' dropdown menu set to 'None'.
- Action Settings:** Includes 'Collection Polling' (set to '[Disabled]') and 'Patch Window' (set to 'None/Disabled').

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):

The screenshot shows the 'Device Manager' page with a table of 25 devices. The table columns include Device Name, IP Address, Device Category, Device Class | Sub-class, CID, Organisation, Current State, Collection Group, Collection State, SNMP Credential, and SNMP Version. The 'Select Action' dropdown menu is open, showing options such as Administration (DELETE, MODIFY, CLEAR, CREATE, SCHEDULE, FIND), Change Collection State, Change User Maintenance Mode, Change Collector Group, Move To Organization, and Align SNMP Read Credential.

Device Name	IP Address	Device Category	Device Class Sub-class	CID	Organisation	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version
10.20.0.195	10.20.0.195	Servers	NET-SNMP FreeBSD	84	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.109	10.20.0.109	Network Router	Cisco Systems 2901	72	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.123	10.20.0.123	Network Router	Cisco Systems 7206VXR	112	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.13	10.20.0.13	Unknown	Generic SNMP	107	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.135	10.20.0.135	Network Switches	Cisco Systems Catalyst 3508G-XL	131	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.141	10.20.0.141	Network Switches	Cisco Systems Catalyst WS-C6509-CatOS	118	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.146	10.20.0.146	Network Broadbar	Netopia Netopia 3346 v8.2r1	2	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.147	10.20.0.147	Network Broadbar	Netopia Netopia 3381 v8.0.10	175	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.148	10.20.0.148	Network Broadbar	Netopia Netopia (R3100, R450x, R7x00, R9	183	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.149	10.20.0.149	Network Broadbar	Netopia R7200-T	162	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.151	10.20.0.151	Unknown	Generic SNMP	141	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.160	10.20.0.160	Unknown	Generic SNMP	165	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.163	10.20.0.163	Unknown	Generic SNMP	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.175	10.20.0.175	Unknown	Generic SNMP	44	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.176	10.20.0.176	Unknown	Konica Corporation OEM	41	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.190	10.20.0.190	Unknown	Generic SNMP	56	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.191	10.20.0.191	Office Printers	Konica Minolta Fiery X3e 22C-KM	57	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.201	10.20.0.201	Unknown	Generic SNMP	48	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.209	10.20.0.209	Unknown	Generic SNMP	52	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.209	10.20.0.209	Telephony	Quintum Tenor	53	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.222	10.20.0.222	Unknown	Generic SNMP	138	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.26	10.20.0.26	Unknown	Generic SNMP	171	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.52	10.20.0.52	Unknown	ASKEY Computer Corp. OEM	5	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.59	10.20.0.59	Unknown	Generic SNMP	3	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	
10.20.0.61	10.20.0.61	Unknown	Generic SNMP	84	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	

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).

The screenshot shows the 'Schedule Manager' interface. At the top, there are tabs for 'Close', 'Properties', 'Thresholds', 'Collections', 'Monitors', 'Schedule', 'Logs', 'Toolbox', 'Interfaces', 'Relationships', 'Tickets', 'Redirects', 'Notes', and 'Attributes'. The 'Schedule' tab is active. Below the tabs, there are fields for 'Device Name', 'IP Address / ID', 'Class', 'Organization', 'Collection Mode', and 'Description'. To the right, there are fields for 'Managed Type', 'Category', 'Sub-Class', 'Uptime', 'Collection Time', and 'Group / Collector'. A 'Ping Device' button is visible on the right side. Below these fields, there is a table titled 'Schedule Manager | Schedules Found [2]'. The table has columns for 'Schedule Summary', 'Schedule Description', 'Event ID', 'sch. id', 'Context', 'Timezone', 'Start Time', 'Duration', 'Recurrence Interval', 'End Date', 'Last Run', 'Owner', 'Organization', 'Visibility', and 'Enabled'. Two rows are listed: '1. Monthly maintain Monthly test maintenar' and '2. One-time maintain One-time test mainten'. At the bottom right, a red box highlights a dropdown menu with the text '[Select Action]' and a 'Go' button. The dropdown menu is open, showing three options: '_DELETE Schedules', '_ENABLE Schedules', and '_DISABLE Schedules'.

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).

The screenshot shows the 'Schedule Manager' interface. At the top, there are tabs for 'Close', 'Properties', 'Thresholds', 'Collections', 'Monitors', 'Schedule', 'Logs', 'Toolbox', 'Interfaces', 'Relationships', 'Tickets', 'Redirects', 'Notes', and 'Attributes'. The 'Schedule' tab is active. Below the tabs, there are several sections: 'Device Name', 'IP Address / ID', 'Class', 'Organization', 'Collection Mode', 'Description', 'Device Hostname', 'Managed Type', 'Physical Device', 'Category', 'Sub-Class', 'Uptime', 'Collection Time', and 'Group / Collector'. A 'Ping Device' button is visible on the right. Below these sections, there is a 'Schedule Manager | Schedules Found [2]' header with 'Create' and 'Reset' buttons. A table lists the schedules:

	Schedule Summary	Schedule Description	Event ID	sch. id	Context	Timezone	Start Time	Duration	Recurrence Interval	End Date	Last Run	Owner	Organization	Visibility	Enabled
1.	Monthly maintain	Monthly test mainten	151	80	Devices	America/New_	2017-01-17 03:00:00	80 min	Every 1 Month	2017-12-17 03:00:00	--	banderton	System	Private	Yes
2.	One-time maintain	One-time test mainte	152	81	Devices	America/New_	2017-01-20 00:00:00	300 min	--	--	--	banderton	System	Private	Yes

At the bottom right, a dropdown menu is open, showing options: '[Select Action]', '[Select Action]', 'Administration:', 'DELETE Schedules', 'ENABLE Schedules', and 'DISABLE Schedules'. A 'Go' button is next to the dropdown. A red box highlights the dropdown menu and the 'Go' button.

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.



Managing Dynamic Applications

Overview

This chapter will describe how to manage Dynamic Applications. This chapter will describe:

- [Viewing the List of Installed Dynamic Applications](#)
- [Viewing the Dynamic Applications Associated With a Device](#)
- [Viewing the Status of a Dynamic Application](#)
- [Maintenance of Collection State](#)
- [Status of Objects for Deviation Alerting](#)
- [Manually Associating a Dynamic Application with a Device](#)
- [Manually Associating a Credential with a Dynamic Application](#)
- [Performing Other Administrative Tasks for an Aligned Dynamic Application](#)
- [Setting Thresholds for Dynamic Applications](#)
- [How Dynamic Applications work with Discovery](#)

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 ().

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.

Dynamic Application Name	Poll Rate	Type	State	Version	ID	Subscribers	PowerPack	Environment	Collects	Alerts	Events	Thresh	Edited By	Last Edit
1. Not Test ICDA	1 min.	Snippet Configuration	Enabled	1	1502	--	ScienceLogic: ICDA Harc	SYSTEM	1	--	--	--	em7admin	2018-07-20 09:27:05
2. 2-level DCM app cache producer	15 min.	Snippet Configuration	Enabled	0.1	1517	--	2-level DCM app test	SYSTEM	1	--	--	--	em7admin	2018-07-20 09:26:21
3. 2-level DCM app config	1 min.	Snippet Configuration	Enabled	0.1	1520	--	2-level DCM app test	SYSTEM	1	1	1	--	em7admin	2018-07-20 09:26:21
4. 2-level DCM app level1 discovery	1 min.	Snippet Configuration	Enabled	0.1	1518	--	2-level DCM app test	SYSTEM	2	--	--	--	em7admin	2018-07-20 09:26:21
5. 2-level DCM app level2 discovery	1 min.	Snippet Configuration	Enabled	0.1	1519	--	2-level DCM app test	SYSTEM	2	--	--	--	em7admin	2018-07-20 09:26:21
6. Alteon: Configuration	120 min.	SNMP Configuration	Enabled	1.2	1174	--	Alteon Base Pack	n/a	30	5	5	--	em7admin	2018-07-19 23:27:21
7. Alteon: Load Trending	15 min.	SNMP Performance	Enabled	1.1	1173	--	Alteon Base Pack	n/a	6	--	--	--	em7admin	2018-07-19 23:27:21
8. Alteon: Performance	15 min.	SNMP Performance	Enabled	2.7	1175	--	Alteon Base Pack	n/a	6	--	--	--	em7admin	2018-07-19 23:27:22
9. APC: Environmental T/H	5 min.	SNMP Performance	Enabled	6.1	713	--	APC Base Pack	n/a	3	2	2	1	em7admin	2018-07-19 23:24:41
10. APC: Asset Tracking	1440 min.	SNMP Configuration	Enabled	1.1	707	--	APC Base Pack	n/a	11	--	--	--	em7admin	2018-07-19 23:24:41
11. APC: Battery Performance	15 min.	SNMP Performance	Enabled	1.1	708	--	APC Base Pack	n/a	7	--	--	--	em7admin	2018-07-19 23:24:41
12. APC: Battery Status	15 min.	SNMP Configuration	Enabled	1.2	709	--	APC Base Pack	n/a	9	12	12	2	em7admin	2018-07-19 23:24:41
13. APC: Configuration	360 min.	SNMP Configuration	Enabled	1.1	710	--	APC Base Pack	n/a	20	4	4	--	em7admin	2018-07-19 23:24:41
14. APC: Environmental Asset	1440 min.	SNMP Configuration	Enabled	6.1	714	--	APC Base Pack	n/a	12	--	--	--	em7admin	2018-07-19 23:24:41
15. APC: PDU Performance	15 min.	SNMP Performance	Enabled	1.3	712	--	APC Base Pack	n/a	3	--	--	--	em7admin	2018-07-19 23:24:41
16. APC: SmartUPS Power Output	5 min.	SNMP Performance	Enabled	6.1	715	--	APC Base Pack	n/a	2	--	--	--	em7admin	2018-07-19 23:24:42
17. APC: UPS Testing	1440 min.	SNMP Configuration	Enabled	1.2	711	--	APC Base Pack	n/a	6	9	9	--	em7admin	2018-07-19 23:24:41
18. Aruba: Asset	1440 min.	SNMP Configuration	Enabled	2.8	1434	--	Aruba Base Pack	n/a	18	--	--	--	em7admin	2018-07-19 23:28:45
19. Aruba: Voice Counters	5 min.	SNMP Performance	Enabled	2.8	1435	--	Aruba Base Pack	n/a	15	--	--	--	em7admin	2018-07-19 23:28:45






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 ***Database Dynamic 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 ***Database Dynamic 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 ICDA's can also collect configuration data about interfaces, such as physical address, operational status, and IP addresses. For details on creating ICDA's, 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 ICDA's, 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 ***IT Services Manual***.
 - *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***.
 - *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***.

- *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***.
- *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. SL 1 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 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:

"!?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 contain 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*i*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!^s*i*i*o\$". Matches all text that does not contain the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" 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", "1 n", 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:


Close	Properties	Thresholds	Collections	Monitors	Schedule			
Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes	
Device Name: 10.2.117.3 IP Address / ID: 10.2.117.3 135 Class: Pure Storage Organization: Knights_Pure Collection Mode: Active Description: Device Hostname:		Managed Type: Physical Device Category: Storage Array Sub-Class: FlashArray Storage System Uptime: 0 days, 00:00:00 Collection Time: 2018-07-20 14:07:00 Group / Collector: CUG-Knights-OL7 10-64-171-139-CU-Knights						
Dynamic Application™ Collections Expand Actions Reset Guide								
Dynamic Application		ID	Poll Frequency	Type	Credential	Collector		
+ Pure Storage: Array Capacity Stats		1552	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Array Stats		1543	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Kr		
- Pure Storage: Temperature Stats		1553	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Kr		
Presentation Object -								
+ [Temperature [°C]		1		p_6298	yes	yes	--	0
+ [Temperature [°F]		1		p_6299	yes	yes	--	0
Misc Collection Object -								
+ [Discovery Object]					o_17691	no	yes	--
+ [Temperature (Labels)]					o_17690	yes	yes	--
+ Pure Storage: Array Discovery		1542	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Controller Config		1554	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Drive Config		1550	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Hardware Config		1551	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Hosts & Groups Config		1558	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Message Log Config		1555	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Protection Groups Config		1556	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Volume Discovery		1544	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
+ Pure Storage: Volume Snapshots Config		1548	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Kr		
[Select Action] Go								
Save								


- **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 the ScienceLogic Platform 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 two days 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:

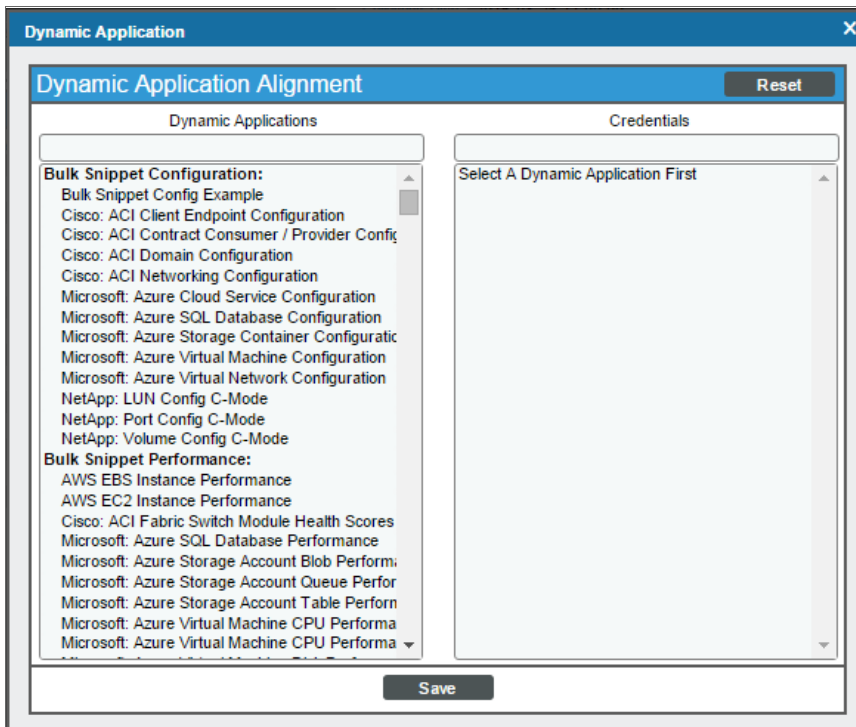
All objects ready for deviation alerting.

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.

- 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.
- 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.

The screenshot shows the 'Dynamic Application Collections' page in the Pure Storage management interface. The top section displays device information for '10.2.117.3', including its IP address, class (Pure Storage), organization (Knights_Pure), and collection mode (Active). Below this is a table of dynamic applications. The table has columns for 'Dynamic Application', 'ID', 'End Frequency', 'Trnd', 'Credential', and 'Collector'. A dropdown menu is open over the 'Credential' column, showing a list of credentials to select from. The 'Save' button is located at the bottom of the table.

Dynamic Application	ID	End Frequency	Trnd	Credential	Collector
Pure Storage: Array Capacity Stats	1552	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Array Stats	1543	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Temperature Stats	1553	5 mins	Snippet Performance	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Array Discovery	1542	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Controller Config	1554	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Drive Config	1550	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Hardware Config	1551	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Hosts & Groups Config	1558	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Message Log Config	1555	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Protection Groups Config	1556	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Volume Discovery	1544	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights
Pure Storage: Volume Snapshots Config	1548	15 mins	Snippet Configuration	Knights - Pure Storage	10-64-171-139-CU-Knights

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*.

- 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:

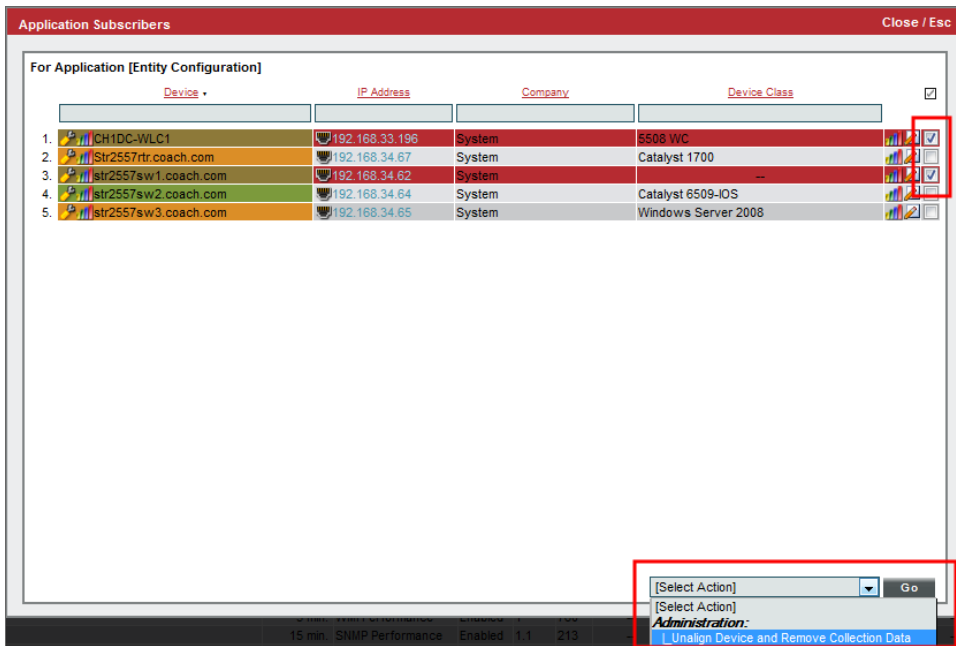
1. In the **Dynamic Application Collections** page, select the checkbox () of the Dynamic Application for which you want to remove data. To remove data for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the **Select Action** drop-down list, select one of the 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:

Device Thresholds [Actions] [Reset] [Guide]

Operating System Thresholds

System Latency: 100 ms [Default: 100 ms]

System Availability: 99 % [Default: 99 %]

[Save]

Data Retention Thresholds

Device Logs Max: 50000 records [Default: 50000 records]

Device Logs Age: 90 days [Default: 90 days]

Bandwidth Data: 365 days [Default: 365 days]

Daily Rollup Bandwidth Data: 365 days [Default: 365 days]

Frequent Rollup Bandwidth Data: 365 days [Default: 365 days]

Hourly Rollup Bandwidth Data: 365 days [Default: 365 days]

Raw Performance Data: 14 days [Default: 14 days]

Daily Rollup Performance Data: 720 days [Default: 720 days]

Frequent Rollup Performance Data: 60 days [Default: 60 days]

Hourly Rollup Performance Data: 365 days [Default: 365 days]

Journal Data: 60 days [Default: 60 days]

Configuration Data: 30 records [Default: 30 records]

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 the ScienceLogic Platform 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.

The screenshot shows the 'Dynamic Applications Manager' interface with a table of 19 applications. The table columns include Dynamic Application Name, Poll Rate, Type, State, Version, ID, Subscribers, PowerPack, Environment, Collects, Alerts, Events, Thresh, Edited By, and Last Edit. A dropdown menu is open over the table, showing 'Select Action' options: Administration (DELETE Application, CLEAR Application, DISCOVER Applications), Change Type (VALIDATE & REPAIR Applications), and Change Type (CHANGE to Bulk Snippet Configuration, CHANGE to Bulk Snippet Performance, CHANGE to Database Configuration, CHANGE to Database Performance, CHANGE to Internal Collection Inventory, CHANGE to Internal Collection Performance, CHANGE to IT Service, CHANGE to PowerShell Config, CHANGE to Snippet Configuration, CHANGE to Snippet Journal, CHANGE to Snippet Performance, CHANGE to SNMP Configuration). The 'DISCOVER Applications' option is highlighted.



Dynamic Application Name	Poll Rate	Type	State	Version	ID	Subscribers	PowerPack	Environment	Collects	Alerts	Events	Thresh	Edited By	Last Edit
1. Not Test ICDA	1 min	Snippet Configuration	Enabled	1	1502	--	ScienceLogic: ICDA Harc	SYSTEM	1	--	--	--	em7admin	2018-07-20 09:27:05
2. 2-level DCM app cache producer	15 min	Snippet Configuration	Enabled	0.1	1517	--	2-level DCM app test	SYSTEM	1	--	--	--	em7admin	2018-07-20 09:26:21
3. 2-level DCM app config	1 min	Snippet Configuration	Enabled	0.1	1520	--	2-level DCM app test	SYSTEM	1	1	1	--	em7admin	2018-07-20 09:26:21
4. 2-level DCM app level1 discovery	1 min	Snippet Configuration	Enabled	0.1	1518	--	2-level DCM app test	SYSTEM	2	--	--	--	em7admin	2018-07-20 09:26:21
5. 2-level DCM app level2 discovery	1 min	Snippet Configuration	Enabled	0.1	1519	--	2-level DCM app test	SYSTEM	2	--	--	--	em7admin	2018-07-20 09:26:21
6. Alteon: Configuration	120 min	SNMP Configuration	Enabled	1.2	1174	--	Alteon Base Pack	n/a	30	5	5	--	em7admin	2018-07-19 23:27:21
7. Alteon: Load Trending	15 min	SNMP Performance	Enabled	1.1	1173	--	Alteon Base Pack	n/a	6	--	--	--	em7admin	2018-07-19 23:27:21
8. Alteon: Performance	15 min	SNMP Performance	Enabled	2.7	1175	--	Alteon Base Pack	n/a	6	--	--	--	em7admin	2018-07-19 23:27:22
9. APC: Environmental T/H	5 min	SNMP Performance	Enabled	6.1	713	--	APC Base Pack	n/a	3	2	2	1	em7admin	2018-07-19 23:24:41
10. APC: Asset Tracking	1440 min	SNMP Configuration	Enabled	1.1	707	--	APC Base Pack	n/a	11	--	--	--	em7admin	2018-07-19 23:24:41
11. APC: Battery Performance	15 min	SNMP Performance	Enabled	1.1	708	--	APC Base Pack	n/a	7	--	--	--		
12. APC: Battery Status	15 min	SNMP Configuration	Enabled	1.2	709	--	APC Base Pack	n/a	9	12	12	--		
13. APC: Configuration	360 min	SNMP Configuration	Enabled	1.1	710	--	APC Base Pack	n/a	20	14	14	--		
14. APC: Environmental Asset	1440 min	SNMP Configuration	Enabled	6.1	714	--	APC Base Pack	n/a	12	--	--	--		
15. APC: PDU Performance	15 min	SNMP Performance	Enabled	1.3	712	--	APC Base Pack	n/a	3	--	--	--		
16. APC: SmartUPS Power Output	5 min	SNMP Performance	Enabled	6.1	715	--	APC Base Pack	n/a	2	--	--	--		
17. APC: UPS Testing	1440 min	SNMP Configuration	Enabled	1.2	711	--	APC Base Pack	n/a	6	9	9	--		
18. Aruba: Asset	1440 min	SNMP Configuration	Enabled	2.8	1434	--	Aruba Base Pack	n/a	18	--	--	--		
19. Aruba: Voice Counters	5 min	SNMP Performance	Enabled	2.8	1435	--	Aruba Base Pack	n/a	15	--	--	--		

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.

Grouping Dynamic Application Data Using Collection Labels

Overview

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:

<i>What are Collection Labels and Collection Groups?</i>	535
<i>Viewing the List of Collection Labels</i>	535
<i>Creating a Collection Group</i>	540
<i>Creating a Collection Label</i>	541
<i>What are Duplicates and How Does the ScienceLogic Platform Manage Them?</i>	544
<i>What is Precedence?</i>	545
<i>Aligning a Presentation Object with a Collection Label</i>	545
<i>Viewing and Managing the List of Presentation Objects Aligned with a Collection Label</i>	547
<i>Viewing and Editing Duplicate Presentation Objects by Collection Label</i>	551
<i>Viewing and Managing the List of Devices Aligned with a Collection Label</i>	553
<i>Editing Duplicate Presentation Objects by Device</i>	555
<i>Editing Duplicate Presentation Objects for a Single Device</i>	557
<i>Editing a Collection Label</i>	558

Deleting a Collection Label 559

Viewing Reports About Collection Labels on a Single Device 559

Viewing Dashboards About Collection Labels 560

What are Collection Labels and Collection Groups?

Collection Labels and Collection Groups allow you to group and view data from multiple performance Dynamic Applications in a single dashboard widget.

For example:

- Suppose you monitor phone systems from multiple vendors.
- Suppose you want to create a dashboard that displays the ten phone systems that drop the most calls.
- You could create a Collection Group called "Dropped Calls".
- You could create two Collection Labels: "Average Dropped Calls", and "Raw Dropped Calls".
- For each vendor, you could edit the appropriate performance Dynamic Application and align a collected value with "Average Dropped Calls" and align another collected value with "Raw Dropped Calls".
- You could then create a dashboard that displays the ten phone systems with the highest values for "Raw Dropped Calls" and also displays the ten phone systems with the highest values for "Average Dropped Calls".

Viewing the List of Collection Labels

The **Collection Labels** page (System > Manage > Collection Labels) displays a list of all the existing Collection Labels. By Default, SL1 includes the following Collection Groups:

- **Vitals.** Includes the Collection Labels "CPU", "Memory", and "Swap".
- **Video Performance.** Includes Collection Labels for common performance metrics associated with video endpoint devices.

The **Collection Labels** page displays the following about each existing Collection Label:

Collection Labels Collection Labels Found [17]							Reset	Guide
Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates		
1. In Use	In Use	Video Performance	No	2	--	--		
2. Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--		
3. Max Jitter	Max Jitter	Video Performance	No	2	--	--		
4. Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--		
5. Rx Audio Pkts Lost	Receive Audio Packets Lost	Video Performance	No	2	--	--		
6. Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--		
7. Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--		
8. Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--		
9. Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--		
10. Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--		
11. Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--		
12. Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--		
13. Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--		
14. Usage	Usage	Video Performance	No	2	--	--		
15. CPU		Vitals	No	37	9	--		
16. Memory		Vitals	No	17	--	--		
17. Swap		Vitals	No	6	--	--		

- **Label Name.** Name of the Collection Label.
- **Label Description.** Description of the Collection Label. This field is optional.
- **Group Name.** Collection Group that contains this Collection Label.
- **Frequent Data.** Specifies whether *frequently rolled up data* is calculated for the Collection Label.
- **Aligned Presentations.** Presentation Objects aligned with this Collection Label.
- **Aligned Devices.** Devices that currently populate the Collection Label.
- **Duplicates.** Number of devices for which two or more Presentation Objects are aligned with the same Collection Label.

Filtering the List of Collection Labels

You can filter the list of Collection Labels on the **Collection Labels** page by one or more parameters. Only Collection Labels that meet all the filter criteria will be displayed in the **Collection Labels** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **Collection Labels** page searches for Collection Labels 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:

- **Label Name.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching label name.
- **Label Description.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching label description.
- **Group Name.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching group name.
- **Frequent Data.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that have a matching value in the **Frequent Data** field.
- **Aligned Presentations.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching number of presentations.
- **Aligned Devices.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching number of aligned devices.
- **Duplicates.** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Collection Labels** page will display only Collection Labels that are associated with a matching number of duplicates.

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 contain the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!O\$". Matches only text that does not end with "O".
- "!^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!*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!^s*i!*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 "sXiXo" 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".

Creating a Collection Group

You cannot create a Collection Group separately from creating a Collection Label. When you [create a Collection Label](#), you can specify a new Collection Group or specify an existing Collection Group. If you specify a new Collection Group, SL1 saves the new Collection Group when it saves the new Collection Label.


Creating a Collection Label

You can create a new Collection Label from the **Collection Labels** page (System > Manage > Collection Labels). To do so:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).
2. Select the green plus-sign in the lower left of the page.

	Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates
1	In Use	In Use	Video Performance	No	2	--	--
2	Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--
3	Max Jitter	Max Jitter	Video Performance	No	2	--	--
4	Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--
5	Rx Audio Pkts Lost	Receive Audio Packets Lost	Video Performance	No	2	--	--
6	Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--
7	Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--
8	Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--
9	Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--
10	Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--
11	Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--
12	Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--
13	Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--
14	Usage	Usage	Video Performance	No	2	--	--
15	CPU		Vitals	No	37	9	--
16	Memory		Vitals	No	17	--	--
17	Swap		Vitals	No	6	--	--
			Vitals	Yes	--	--	--

3. Enter values in the following columns:

- **Label Name**. Name of the Collection Label. This field is required.
- **Label Description**. Description of the Collection Label. This field is optional.
- **Group Name**. Collection Group to align with the Collection Label. You can select from a list of existing Collection Groups or enter the name of a new Collection Group. This field is required.
- **Frequent Data**. Specifies whether *frequently rolled up data* is calculated for the Collection Label. If the Collection Label will include data that is collected every five minutes or more frequently, and you require that dashboard data be updated every 15 minutes or 20 minutes, select Yes in this field. This data is available immediately for use in a collection label.
- **Save icon** (). Select this icon to save your new Collection Label.

4. The new Collection Label appears in the page.


What is Normalization?

Normalization and roll-up are the processes by which SL1 manages collected performance data for display and storage.

- **Raw data** is the data exactly as it was collected from a device or application.
- **Normalized** and **rolled up** data is data for which SL1 has performed calculations, usually averaging raw data over a period of time.

Dynamic Applications can collect raw performance data from a device at the following intervals:

- 1 minute
- 2 minutes
- 3 minutes
- 5 minutes
- 10 minutes
- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 6 hours
- 12 hours
- 24 hours

For performance Dynamic Applications, you specify this interval in the **Poll Frequency** field, in the **Properties Editor** page (System > Manage > Dynamic Applications > Create or )

SL1 **rolls up** data so that reports with a larger timespan do not become difficult to view and to save storage space on the ScienceLogic database. When SL1 rolls up data, SL1 groups data into larger sets and calculates the average value for the larger set.

There are two types of roll up:

- **Hourly.** Way to group and average data that is collected at intervals of less than or equal to 60 minutes. SL1 rolls up data and calculates an average hourly value for each metric. Hourly samples include samples from the top of the hour to the end of the hour. For example, for an hourly rollup of data collected at 1-minute intervals between 1 am and 2 am, the first data point would be the one collected at 01:00:00 and ending at 01:59:00.
- **Daily.** Way to group and average all data. SL1 rolls up data and calculates an average daily value for each metric. Daily samples include samples from the beginning of the day until the end of the day. For example, for a daily roll-up of data collected at 1-minute intervals, the first data point is collected at 00:00:00 and the last data point is collected at 23:59:00.

SL1 rolls up raw performance data as follows:

Frequency of Raw Collection	Roll-up
Every 1 minute	60 minutes, 24 hours
Every 2 minutes	60 minutes, 24 hours
Every 3 minutes	60 minutes, 24 hours

Frequency of Raw Collection	Roll-up
Every 5 minutes	60 minutes, 24 hours
Every 10 minutes	60 minutes, 24 hours
Every 15 minutes	60 minutes, 24 hours
Every 30 minutes	60 minutes, 24 hours
Every 60	60 minutes, 24 hours
Every 120 minutes or longer	24 hours

Before SL1 normalizes data, EM7 **transforms** the data. To transform data, SL1 :

- For bandwidth data and data from Dynamic Applications of type "Performance", SL1 derives rates from counter metrics.
- The rate from counter metrics are expressed in units-per-polling_interval. For example, rates for 5-minute collections are expressed as units-per-5-minutes.
- For data from Dynamic Applications of type "Performance", SL1 evaluates presentation formulas. Counter metrics are first transformed into rates before evaluation.

NOTE: During the data transform steps, SL1 does not directly roll up the raw data in the database tables.

When SL1 rolls up data, SL1 must **normalize** that data. To normalize data, SL1 :

- groups and orders the data
- determines the sample size
- calculates count
- determines the maximum value
- determines the minimum value
- calculates the mean value
- calculates the average value
- calculates the sum
- determines the standard deviation

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 sample size, maximum values, minimum values, or average values.

Example

For example, suppose that **every five minutes**, SL1 collects data about file system usage on the device named **my_device**. When SL1 normalizes and rolls up the collected data for file system usage for **my_device**, SL1 will:

1. Apply any necessary data transforms (mentioned above).
2. Repeat the following step for both hourly normalization and daily normalization:
3. If this is the first data point for an hourly normalization or a daily normalization, insert summary statistics for that one data point:
 - Sample size = 1
 - Average = value of new data point
 - Max = value of new data point
 - Min = value of new data point
 - Sum = value of new data point
 - Standard Deviation = 0
3. For all subsequent data points for an hourly normalization or a daily normalization, SL1 will update the summary statistics for the already existing data points in the data set (either hourly data set or daily data set).
4. If there are no gaps in collection, the summary statistics for hourly normalization will represent 12 data points, and the summary statistics for daily normalization will represent 288 data points.

What are Duplicates and How Does the ScienceLogic Platform Manage Them?

Multiple presentation objects can be aligned with a single Collection Label. For example, suppose that a Dynamic Application includes a presentation object for "memory used", and another Dynamic Application includes a presentation object for "memory usage". Suppose that both of these presentation objects are aligned with the Collection Label named "Memory".

Suppose that one of the devices monitored by SL1 subscribes to both of those Dynamic Applications (for example, a Dynamic Application that monitors OEM hardware and a Dynamic Application that monitors the operating system). For that device, SL1 will collect values for both presentation objects that are aligned with the Collection Label named "Memory".

When this situation arises, SL1 uses precedence and some internal rules to assign a single presentation object to the Collection Label for that device. However, you can manually assign a different presentation object to the Collection Label after discovery.

If a device has a duplicate, SL1 uses the following rules to determine which presentation object to use for that Collection Label for that device:

- If a manually defined Collection Label-presentation object pair exists, use that pair.
- If SL1 cannot find a manually defined Collection Label-presentation object pair, use the pair with the lowest **precedence** value.
- If SL1 finds more than one Collection Label-presentation object pair with the same precedence value, SL1 will create a pair using the presentation object with the lowest presentation ID.

What is Precedence?

SL1 performs discovery (during initial discovery and during nightly updates) and aligns Dynamic Applications with devices. During discovery, SL1 will also align Collection Labels with devices. For devices with **duplicates**, SL1 evaluates **precedence** to automatically align a single presentation object with each Collection Label. For devices with duplicates, SL1 assigns the Collection Label-presentation object pair with the lowest precedence value.

SL1 evaluates precedence:

- During nightly update discovery.



NOTE: If you have manually defined a Collection Label-presentation object pair for one or more devices, nightly update discovery will not change the Collection Label-presentation object pair.

- When a Dynamic Application is manually aligned with a device in the **Dynamic Application Collections** page
- When devices are manually merged.

Aligning a Presentation Object with a Collection Label

You can align one or more presentation objects with a collection label. This allows SL1 to compare and display reports on data from multiple performance Dynamic Applications.

To align a presentation object with a collection label:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. Find the performance Dynamic Application that contains the presentation object you are interested in. Select the wrench icon () for that Dynamic Application.
3. In the Dynamic Application panel, select the **Presentations** tab.
4. In the **Presentation Objects** page, go to the **Presentation Object Registry** pane and find the presentation object you want to align with a Collection Label. Select the wrench icon () for that presentation object.

Close Properties Collections **Presentations** Requests Thresholds Alerts Subscribers

Dynamic Applications [656] | Presentation Objects Guide Reset

Report Name:

Active State:

Data Unit:

Abbreviation / Suffix:

Show as Percent: Precedence:

Label Group: Label:

Formula Editor

(o_6443)

7	8	9	6435: Transmit Audio Rate	()	CE
4	5	6	6436: Transmit Video Rate Used	()	
1	2	3	6437: Transmit Video Rate	()	
0	Add			-	+

Guide Text

Save Save As

Presentation Object Registry

	Report Name	State	Abbreviation Suffix	Group	Label	Precedence	Show as Percent	ID	Date Edit
1	Receive Audio Jitter	Enabled	ms	--	--	--	No	pres_2283	2014-06-25 12:06:29
2	Receive Audio Packet Loss	Enabled	pkts	--	--	--	No	pres_2284	2014-06-25 12:06:29
3	Receive Audio Rate	Enabled	kbps	--	--	--	No	pres_2285	2014-06-25 12:06:29
4	Receive Packet Loss Percent	Enabled	--	--	--	--	No	pres_2292	2014-06-25 12:06:29
5	Receive Video Frame Rate	Enabled	frps	--	--	--	No	pres_2286	2014-06-25 12:06:29
6	Receive Video Jitter	Enabled	ms	--	--	--	No	pres_2287	2014-06-25 12:06:29
7	Receive Video Packet Loss	Enabled	pkts	--	--	--	No	pres_2288	2014-06-25 12:06:29
8	Receive Video Rate	Enabled	kbps	--	--	--	No	pres_2289	2014-06-25 12:06:29
9	Receive Video Rate Used	Enabled	kbps	--	--	--	No	pres_2290	2014-06-25 12:06:29
10	Transmit Audio Jitter	Enabled	ms	--	--	--	No	pres_2282	2014-06-25 12:06:29
11	Transmit Audio Packet Loss	Enabled	pkts	--	--	--	No	pres_2280	2014-06-25 12:06:29
12	Transmit Audio Rate	Enabled	kbps	--	--	--	No	pres_2275	2014-06-25 12:06:29
13	Transmit Packet Loss Percent	Enabled	--	--	--	--	No	pres_2291	2014-06-25 12:06:29
14	Transmit Video Frame Rate	Enabled	frps	--	--	--	No	pres_2278	2014-06-25 12:06:29

Copyright © 2003 - 2014 ScienceLogic, Inc. All rights reserved. 7.5.1.alpha - build 30630

5. The top pane is populated with values from the selected presentation object. Select values for the following fields:
 - **Precedence**. Set the global precedence for this Collection Label-presentation object pair. For more information, see the section on [Precedence](#).
 - **Label Group**. Select from a list of existing Collection Groups or click on the plus-sign icon (+) and enter the value for a new Collection Group. The current presentation object will be a member of the specified Collection Group.
 - **Label**. Select from a list of existing Collection Labels or click on the plus-sign icon (+) and enter the value for a new Collection Label. The current presentation object will be aligned with the specified Collection Label.


6. When you generate reports on the selected Collection Label, this presentation object will be included in the report.

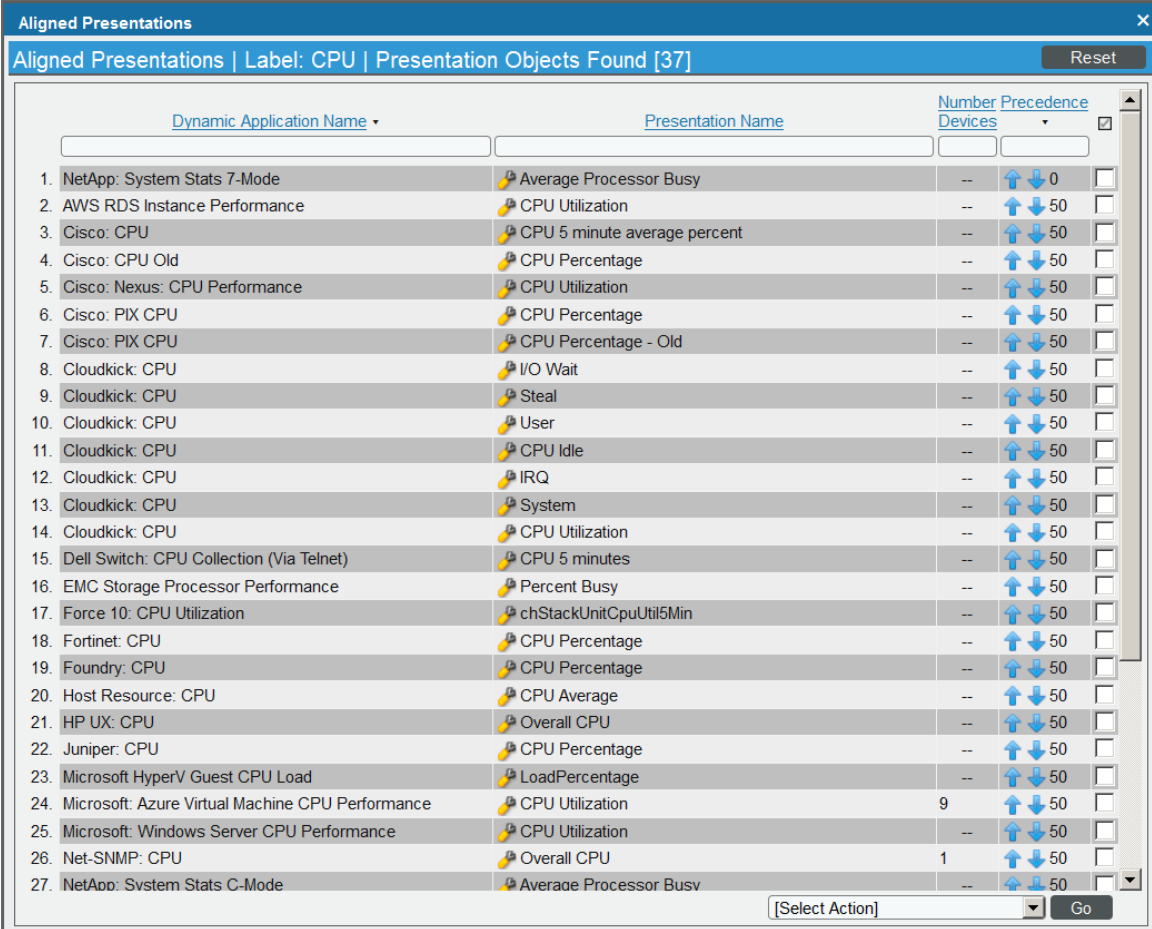
Viewing and Managing the List of Presentation Objects Aligned with a Collection Label

From the **Collection Labels** page, you can view information about each Collection Label. For each Collection Label, you can view a list of presentation objects aligned with that Collection Label. To view this information:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).

Collection Labels Collection Labels Found [17]							Reset	Guide
Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates		
1. In Use	In Use	Video Performance	No	2	--	--		
2. Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--		
3. Max Jitter	Max Jitter	Video Performance	No	2	--	--		
4. Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--		
5. Rx Audio Pkts Lost	Receive Aduio Packets Lost	Video Performance	No	2	--	--		
6. Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--		
7. Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--		
8. Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--		
9. Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--		
10. Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--		
11. Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--		
12. Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--		
13. Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--		
14. Usage	Usage	Video Performance	No	2	--	--		
15. CPU		Vitals	No	37	9	--		
16. Memory		Vitals	No	17	--	--		
17. Swap		Vitals	No	6	--	--		
					--	--		

- Find the Collection Label you are interested in. In the **Aligned Presentations** column, select the pencil icon (). The **Aligned Presentations** modal page appears:

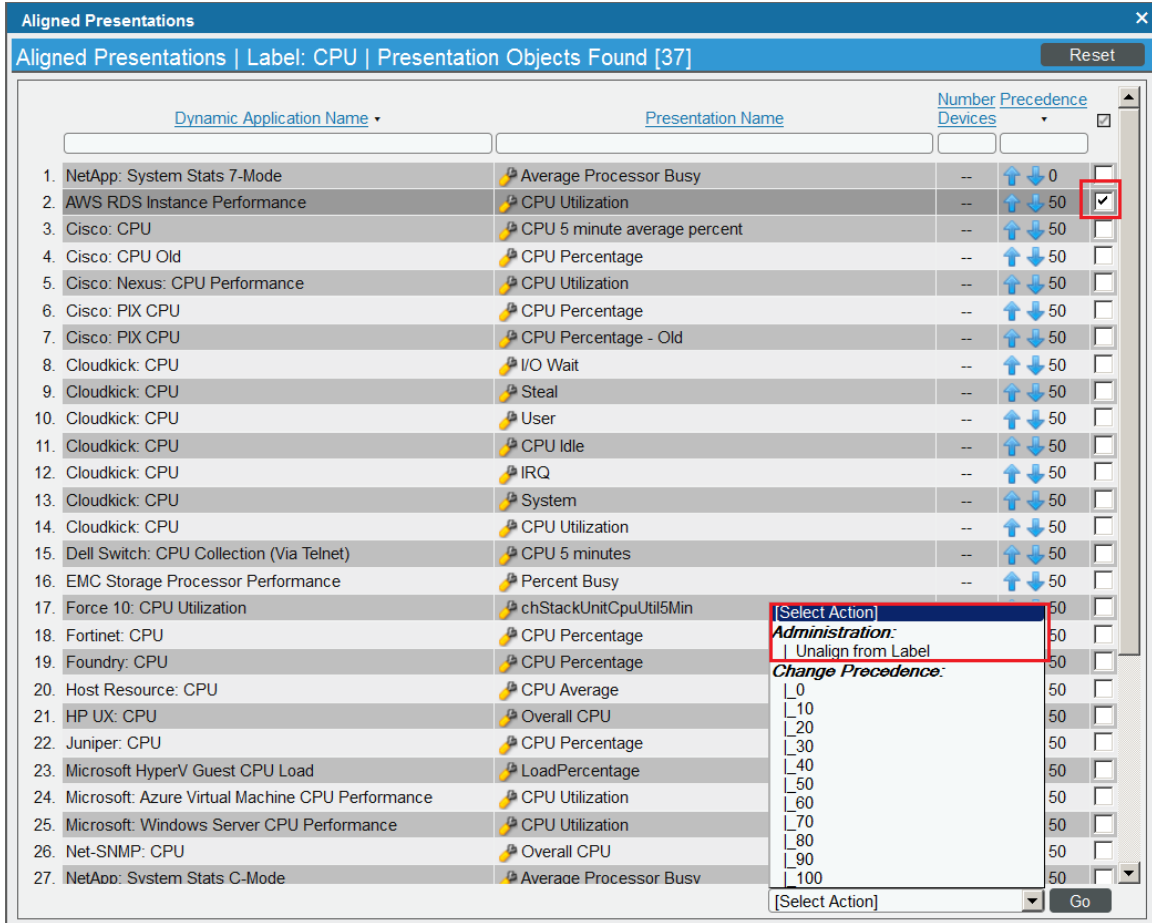


Dynamic Application Name	Presentation Name	Number Devices	Precedence
1. NetApp: System Stats 7-Mode	Average Processor Busy	--	0
2. AWS RDS Instance Performance	CPU Utilization	--	50
3. Cisco: CPU	CPU 5 minute average percent	--	50
4. Cisco: CPU Old	CPU Percentage	--	50
5. Cisco: Nexus: CPU Performance	CPU Utilization	--	50
6. Cisco: PIX CPU	CPU Percentage	--	50
7. Cisco: PIX CPU	CPU Percentage - Old	--	50
8. Cloudkick: CPU	I/O Wait	--	50
9. Cloudkick: CPU	Steal	--	50
10. Cloudkick: CPU	User	--	50
11. Cloudkick: CPU	CPU Idle	--	50
12. Cloudkick: CPU	IRQ	--	50
13. Cloudkick: CPU	System	--	50
14. Cloudkick: CPU	CPU Utilization	--	50
15. Dell Switch: CPU Collection (Via Telnet)	CPU 5 minutes	--	50
16. EMC Storage Processor Performance	Percent Busy	--	50
17. Force 10: CPU Utilization	chStackUnitCpuUtil5Min	--	50
18. Fortinet: CPU	CPU Percentage	--	50
19. Foundry: CPU	CPU Percentage	--	50
20. Host Resource: CPU	CPU Average	--	50
21. HP UX: CPU	Overall CPU	--	50
22. Juniper: CPU	CPU Percentage	--	50
23. Microsoft HyperV Guest CPU Load	LoadPercentage	--	50
24. Microsoft: Azure Virtual Machine CPU Performance	CPU Utilization	9	50
25. Microsoft: Windows Server CPU Performance	CPU Utilization	--	50
26. Net-SNMP: CPU	Overall CPU	1	50
27. NetApp: System Stats C-Mode	Average Processor Busv	--	50

- In the **Aligned Presentations** modal page, you can view information about the presentation objects aligned with the current Collection Label and perform actions to manage those presentation objects. You can also [unalign a presentation object](#) from a Collection Label and [change the precedence](#) for one or more Collection Label-presentation object pairs.

To globally unalign a presentation object from a Collection Label:

1. In the **Aligned Presentations** modal page, find the presentation object that you want to unalign from the Collection Label and select its checkbox.



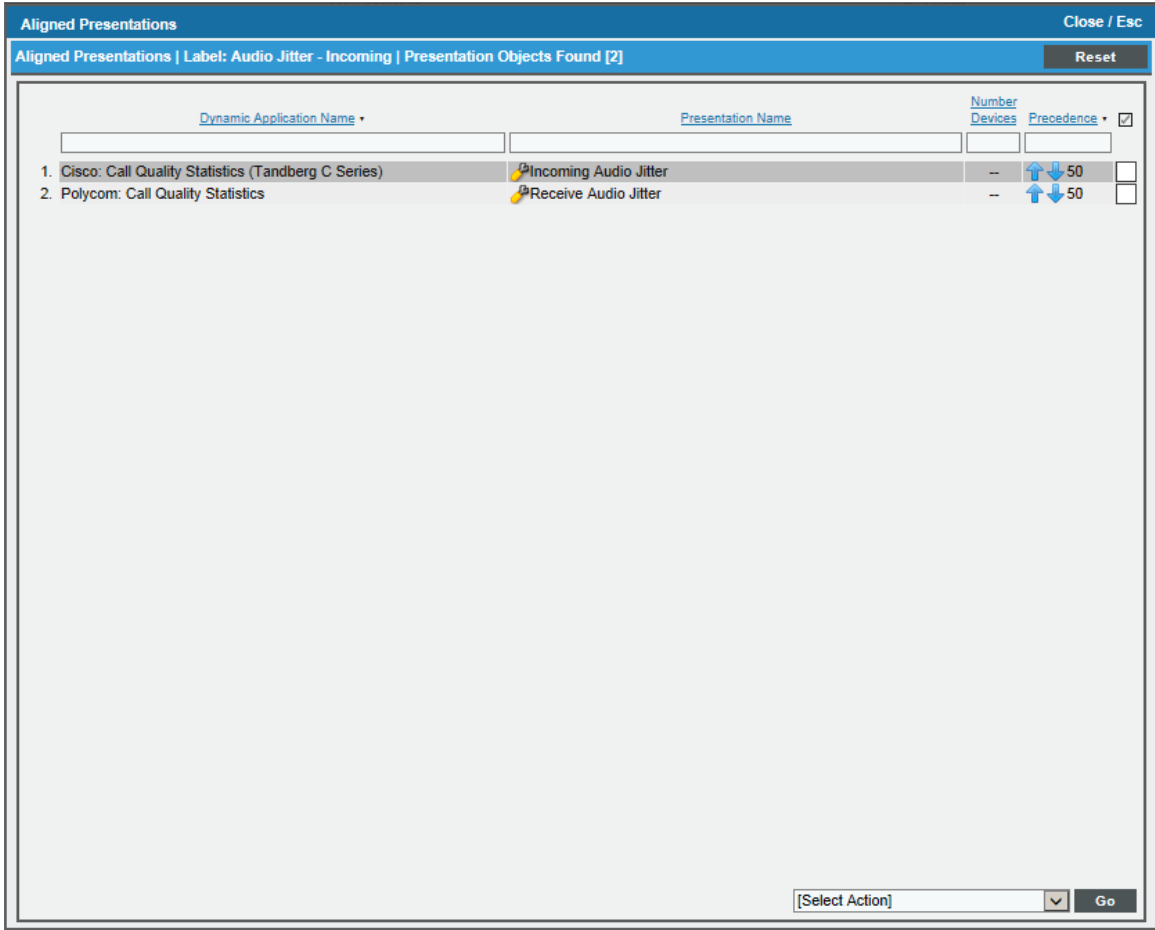
2. From the **Select Action** field in the lower right, select *Unalign from Label*. Select the Go button.
3. The selected presentation object will no longer be associated with the Collection Label.

For each Collection Label-presentation object pair, you can define precedence. For example, suppose that both the "Cisco: CPU" Dynamic Application and the "Host Resource: CPU" include a presentation object that is aligned with the **CPU** Collection Label. You can define precedence to specify priority for each presentation object associated with a Collection Label.

Collection Group / Collection Label	Presentation Object	Dynamic Application
Vitals / CPU	CPU Average	Host Resource: CPU
Vitals / CPI	CPU 5 minutes average percent	Cisco: CPU

To set the precedence for the Collection Label (in our example, "CPU"):

1. The **Aligned Presentations** modal page displays all the presentation objects associated with the selected Collection Label. By default, each presentation object has a precedence of 50.



2. In the **Aligned Presentations** modal page, you can edit precedence in two ways:
 - In the **Precedence** column, use the up arrow and down arrow to change the value for a single presentation object. Repeat for each presentation object for which you want to edit precedence.
 - Select the checkbox of one or more presentation objects. In the **Select Action** field, select **Change Precedence** and a value. Select the **[Go]** button. Each selected presentation object will be assigned the new (and identical) precedence value.
3. Repeat steps 2–4 for each Presentation Object for which you want to edit the precedence value.


NOTE: The precedence values you define in the **Aligned Presentations** modal page override the precedence value you set per presentation object in the **Presentation Objects** page.

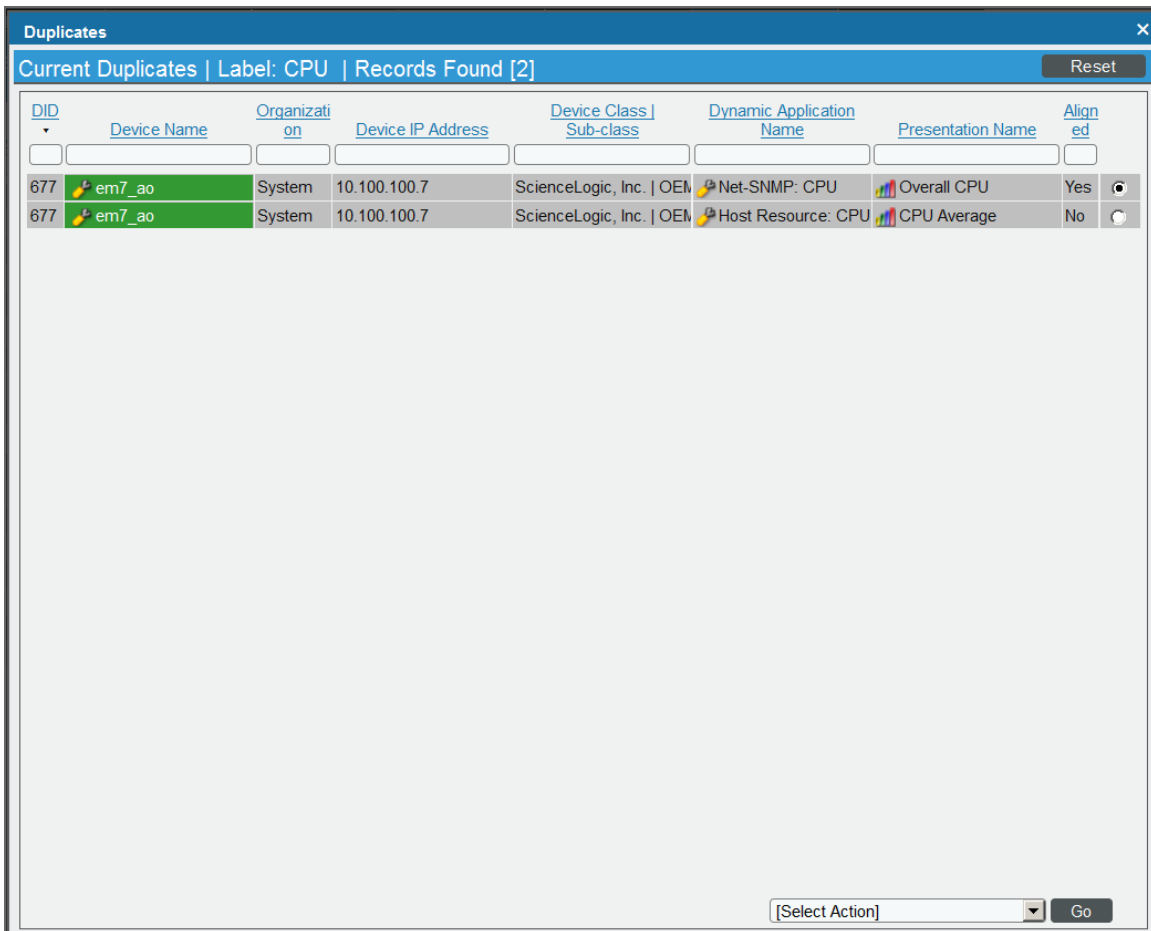
Viewing and Editing Duplicate Presentation Objects by Collection Label

You can view a list of devices where duplicates occur, view how SL1 assigned the Collection Label-presentation object pair, and edit the Collection Label-presentation object pair for one or more devices. When you manually define a Collection Label-presentation object pair for a device, SL1 will not edit or change that pair.

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).

Collection Labels Collection Labels Found [17]							Reset	Guide
Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates		
1. In Use	In Use	Video Performance	No	2	--	--		
2. Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--		
3. Max Jitter	Max Jitter	Video Performance	No	2	--	--		
4. Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--		
5. Rx Audio Pkts Lost	Receive Aduio Packets Lost	Video Performance	No	2	--	--		
6. Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--		
7. Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--		
8. Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--		
9. Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--		
10. Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--		
11. Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--		
12. Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--		
13. Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--		
14. Usage	Usage	Video Performance	No	2	--	--		
15. CPU		Vitals	No	37	10	1		
16. Memory		Vitals	No	17	1	--		
17. Swap		Vitals	No	6	1	--		
				--	--	--		

- Find the Collection Label you are interested in. In the **Duplicates** column, select the pencil icon (). The **Duplicates** modal page appears.



DID	Device Name	Organization	Device IP Address	Device Class Sub-class	Dynamic Application Name	Presentation Name	Aligned
677	em7_ao	System	10.100.100.7	ScienceLogic, Inc. OEM	Net-SNMP: CPU	Overall CPU	Yes <input checked="" type="radio"/>
677	em7_ao	System	10.100.100.7	ScienceLogic, Inc. OEM	Host Resource: CPU	CPU Average	No <input type="radio"/>

- In the **Duplicates** modal page, you can view a list of devices for which there are multiple possible Collection Label-presentation object pairs. You can view which pair is currently assigned to the device.
- To change the pair for a device, click on the pair's radio button.
- Repeat step #4 for each device on which you want to edit the duplicate.
- In the **Select Action** field (in the lower right), select *Align Presentation for Device*. Select the **[Go]** button.
- Each edited device will now use the selected Collection Label-presentation object pair.

Viewing and Managing the List of Devices Aligned with a Collection Label

From the **Collection Labels** page, you can view information about each Collection Label. For each Collection Label, you can view a list of devices from which SL1 is collecting values. To view this information:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).

Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates
1 In Use	In Use	Video Performance	No	2	--	--
2 Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--
3 Max Jitter	Max Jitter	Video Performance	No	2	--	--
4 Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--
5 Rx Audio Pkts Lost	Receive Audio Packets Lost	Video Performance	No	2	--	--
6 Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--
7 Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--
8 Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--
9 Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--
10 Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--
11 Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--
12 Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--
13 Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--
14 Usage	Usage	Video Performance	No	2	--	--
15 CPU		Vitals	No	37	10	--
16 Memory		Vitals	No	17	1	--
17 Swap		Vitals	No	6	1	--

2. Find the Collection Label you are interested in. In the **Aligned Devices** column, select the pencil icon ().

Device Name	Organization	Device IP Address	Device Class Sub-class	Dynamic App Name	Aligned Presentation
1 2008r2-2	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
2 Azure-Team-DC1	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
3 Azure-Team-DC2	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
4 azureteam-vm2	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
5 em7_ao	System	10.100.100.7	ScienceLogic, Inc. OEM	Net-SNMP: CPU	Overall CPU
6 vm-2008r1-tmp	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
7 vm-temp-006	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
8 vm-temp-201	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
9 vm-tmp-1	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
10 vm-tmp-100	Azure	--	Microsoft Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization

3. In the **Aligned Devices** modal page, you can view information about the devices that are aligned with the current Collection Label and perform actions to manage those devices.

For devices that include duplicates, you can reset the presentation object for one or more devices. When you manually define a Collection Label-presentation object pair for a device, SL1 will not edit or change that pair.

1. In the **Aligned Devices** modal page, select the checkbox for one or more devices for which you want to change the Collection Label-presentation object pair.

Device Name	Organization	Device IP Address	Device Class Sub-class	Dynamic App Name	Aligned Presentation	
10.20.0.123	System	10.20.0.123	Cisco Systems 7206VXR	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
10.20.0.13	System	10.20.0.13	Generic SNMP	Host Resource: CPU	CPU Average	<input checked="" type="checkbox"/>
10.20.0.135	System	10.20.0.135	Cisco Systems Catalyst 3508C	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
10.20.0.141	System	10.20.0.141	Cisco Systems Catalyst WS-C	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
10.20.0.176	System	10.20.0.176	Konica Corporation OEM	Host Resource: CPU	CPU Average	<input type="checkbox"/>
10.20.0.190	System	10.20.0.190	Generic SNMP	Host Resource: CPU	CPU Average	<input type="checkbox"/>
10.20.0.191	System	10.20.0.191	Konica Minolta Fiery X3e 22C	Host Resource: CPU	CPU Average	<input type="checkbox"/>
22437158.lou01.hosting.c	System	10.20.0.250	F5 Networks, Inc. BIG-IP 1600	Net-SNMP: CPU	Overall CPU	<input type="checkbox"/>
7301-DS3	System	10.20.0.45	Cisco Systems 7301	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
asst-bq-01.vicnet.org	System	10.20.0.63	Cisco Systems 2691	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
ATL-2924-S.AC.gnax.net	System	10.20.0.68	Cisco Systems Catalyst 2924X	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
aus-rt-1	System	10.20.0.254	Juniper Networks J6350 Route	Juniper: CPU	CPU Percentage	<input type="checkbox"/>
bbaudr1	System	10.20.0.18	Cisco Systems 2811	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
bbhstvt01	System	10.20.0.30	Nokia IP 710	Host Resource: CPU	CPU Average	<input type="checkbox"/>
BLADE1	System	10.20.0.6	Microsoft Windows Server 200	Host Resource: CPU	CPU Average	<input type="checkbox"/>
Boise-DMZ	System	10.20.0.67	Cisco Systems Catalyst 2912X	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
BOTTORFF	System	10.20.0.189	Microsoft Windows XP	Host Resource: CPU	CPU Average	<input type="checkbox"/>
cat4000	System	10.20.0.137	Cisco Systems Catalyst 4003	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
cat5500-2	System	10.20.0.140	Cisco Systems Catalyst 5500	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
Cisco_10.20.0.107.yourdo	System	10.20.0.107	Cisco Systems 1841	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
Cisco_10.20.0.125	System	10.20.0.125	Cisco Systems 7206VXR	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
Cisco_10.20.0.142	System	10.20.0.142	Cisco Systems Catalyst 6509-I	Cisco: CPU	CPU 5 minute average per	<input type="checkbox"/>
Cly-McO	System	10.20.0.198	NET-SNMP Linux sat softronic	Net-SNMP: CPU	Overall CPU	<input type="checkbox"/>
cosas3.land.net	System	10.20.0.224	UCD-SNMP Linux	Net-SNMP: CPU	Overall CPU	<input type="checkbox"/>
CTM1	System	10.20.0.48	Cisco TelePresence Cisco Tel	Host Resource: CPU	CPU Average	<input type="checkbox"/>

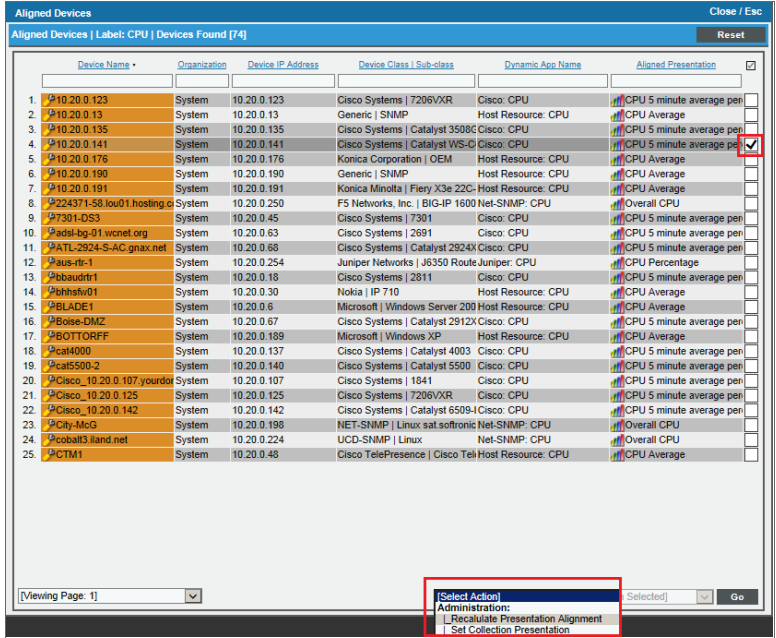
Viewing Page: 1 | Set Collection Presenta | Host Resource: CPU: CPU | Go

2. In the menus in the lower right, select **Set Collection Presentation** and then select the presentation object. Select the **[Go]** button.

For devices that include duplicates, you can clear all current settings, including manual settings. SL1 will then automatically evaluate the precedence for each possible presentation object and assign the Collection Label-presentation object pair with the lowest precedence.

To clear the current Collection Label-presentation object pair for one or more devices:

1. In the **Aligned Devices** modal page, select the checkbox for one or more devices for which you want to clear the aligned presentation object.



2. In the menus in the lower right, select **Recalculate Presentation Alignment**. Select the **[Go]** button.
3. SL1 will evaluate the precedence of each possible presentation object and assign the presentation object with the lowest precedence.

Editing Duplicate Presentation Objects by Device

You can view a list of devices where duplicates occur, view how SL1 assigned the Collection Label-presentation object pair, and edit the Collection Label-presentation object pair for one or more selected devices. When you manually define a Collection Label-presentation object pair for a device, SL1 will not edit or change that pair:

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

- Select the checkbox for each device you are interested in.

Device Manager (Devices Found [36])												
Device Name	Device Hostname	IP Address	Device Category	Device Class Sub-class	IID	Organization	Current State	Collection Group	Collection State	SNMP Credentials	SNMP Access	Actions
<input type="checkbox"/>	10.100.100.40	--	Pingable	Ping ICMP	274	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.48	--	Pingable	FreeBSD ICMP	294	System	Notice	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-3_AIO_10.100.100.10	--	Servers.VMw.VMware	Virtual Machine	348	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_AIO_10.100.100.8	--	Servers.VMw.VMware	Virtual Machine	353	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_AIO_100.11	--	Servers.VMw.VMware	Virtual Machine	349	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Cluster_1	--	Virtual.Infrastr.VMware	Network	341	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_CU-Device	--	Virtual.Infrastr.VMware	Network	339	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Datastores	--	Virtual.Infrastr.VMware	Folder	334	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_800_vmr_PRODUCTION_100.2	--	Servers.VMw.VMware	Virtual Machine	348	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	em7_73001_latest	192.168.33.51	System.EM7	ScienceLogic, Inc. EM7 Data Collector	289	System	Healthy	CUG	Active	EM7 Default V2	V2	[Actions]
<input type="checkbox"/>	em7_73002_latest	192.168.33.52	System.EM7	ScienceLogic, Inc. EM7 Data Collector	288	System	Healthy	CUG	Active	EM7 Default V2	V2	[Actions]
<input type="checkbox"/>	em7_73003_latest	192.168.33.50	System.EM7	ScienceLogic, Inc. EM7 Database	287	System	Minor	CUG	Active	EM7 Default V2	V2	[Actions]
<input type="checkbox"/>	10.100.100.7-5_GW_CU_100.15	--	Servers.VMw.VMware	Virtual Machine	358	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_GW_CU_100.13	--	Servers.VMw.VMware	Virtual Machine	354	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_ha-datascenter	--	Virtual.Infrastr.VMware	Datacenter	332	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Hosts	--	Virtual.Infrastr.VMware	Folder	333	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Hughes_AIO_10.100.100.9	--	Servers.VMw.VMware	Virtual Machine	344	System	Major	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_KVM_100.40	--	Servers.VMw.VMware	Virtual Machine	350	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Networks	--	Virtual.Infrastr.VMware	Folder	335	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_OS_ISOs	--	Virtual.Infrastr.VMware	Datastore	337	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_qa_pm	--	Virtual.Infrastr.VMware	Network	340	System	Major	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_SUSE_10_100.35	--	Servers.VMw.VMware	Virtual Machine	345	System	Major	CUG	Unavailable	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_SUSE_10_100.36	--	Servers.VMw.VMware	Virtual Machine	351	System	Major	CUG	Unavailable	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_SUSE_11_100.30	--	Servers.VMw.VMware	Virtual Machine	343	System	Major	CUG	Unavailable	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_SUSE_11_NS	--	Servers.VMw.VMware	Virtual Machine	352	System	Major	CUG	Unavailable	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_TestVM1	--	Virtual	KVM Virtual Machine	331	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_TRAIN-VM-01.sciencelogic.io	--	Servers.VMw.VMware	Host Server	336	System	Major	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_TRAIN-VM-01_0401	--	Virtual.Infrastr.VMware	Datastore	335	System	Major	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_UCSPF_10.100.100.21 (2)	--	Servers.VMw.VMware	Virtual Machine	355	System	Major	CUG	Unavailable	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_VM_Network	--	Virtual.Infrastr.VMware	Network	342	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_WN-2012-21.DDCS.LOCAL	10.100.100.21	Servers	Microsoft Windows Server 2012 R2	326	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_WN-2012-22.DDCS.LOCAL	10.100.100.22	Servers	Microsoft Windows Server 2012 R2	327	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_WN-2012-23.DDCS.LOCAL	10.100.100.23	Servers	Microsoft Windows Server 2012 R2	329	System	Major	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Wn2012_100.21	--	Servers.VMw.VMware	Virtual Machine	347	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Wn2012_100.22	--	Servers.VMw.VMware	Virtual Machine	350	System	Healthy	CUG	Active	--	--	[Actions]
<input type="checkbox"/>	10.100.100.7-5_Wn2012_100.23	--	Servers.VMw.VMware	Virtual Machine	357	System	Healthy	CUG	Active	--	--	[Actions]

- If you want to view a list of duplicates for all possible devices, select the red check-box (☒) in the top row of the page. This selects all devices.
- In the **Select Action** field (lower right), select **FIND Collection Label Duplicates**. Select the **[Go]** button.

Current Duplicates							Close / Esc
Current Duplicates Label: [Vitals: CPU] Records Found [2]							Reset
IID	Device Name	Organization	Device IP Address	Device Class Sub-class	Dynamic Application Name	Presentation Name	Align ed
28	CTM1	System	10.20.0.48	Cisco TelePresence Cisco	Net-SNMP: CPU	Overall CPU	No
28	CTM1	System	10.20.0.48	Cisco TelePresence Cisco	Host Resource: CPU	CPU Average	Yes

5. The **Current Duplicates** page is displayed. For each device, you can edit the presentation object that is aligned with a Collection Label.
 - To select a Collection Label, use the drop-down list in the upper left.
 - To change the aligned presentation object for one or more devices:
 - Click on the radio button for the desired presentation object for the device.
 - For each additional device you want to edit, click on the radio button for the desired presentation object.
 - In the **Select Action** menu (lower right), select *Align Presentation for Device*. Select the **[Go]** button.

Editing Duplicate Presentation Objects for a Single Device

You can edit the Collection Label-presentation object pair for a single device. If a single device includes duplicate Collection Label-presentation object pairs, you can specify which one SL1 should use for that device.

To edit the Collection Label-presentation object pairs for a single device:

1. Go to the **Device Manager** page (Devices > Device Manager).
2. Find the device you want to edit. Select its wrench icon (🔧).
3. Select the **[Collections]** tab. In the **Dynamic Application Collections** page, click on the plus signs (+) to expand each Dynamic Application.

The screenshot shows the 'Dynamic Application Collections' page for device CTM1. The page is divided into several sections:

- Device Information:** Includes fields for Device Name (CTM1), IP Address (10.20.0.48), Class (Cisco TelePresence), Organization (System), Collection Mode (Active), and Description (*Hardware:7835H, 1 Intel(R) Xeon(TM) CPU 3.40GHz, 2048 MB Memory).
- Dynamic Application™ Collections:** A table with columns for ID, Poll Frequency, Type, and Credential. It lists various collection objects such as Net-SNMP: CPU, Idle CPU Time, IO Wait CPU Time, Nice CPU Time, Overall CPU, System CPU Time, and User CPU Time. The 'Overall CPU' object has a red box around its 'Label' column, which contains 'CPU'.
- Misc Collection Object:** A section below the main table listing other collection objects like Net-SNMP: Physical Memory, Net-SNMP: Swap, and Host Resource: CPU Config.

At the bottom of the page, there is a '[Select Action]' dropdown menu and a 'Go' button.



- You will notice that some presentation objects include the chart icon in the **Label** column. These presentation objects are duplicates that are not currently aligned with a Collection Label. If you want to align one of these presentation objects with the Collection Label (instead of the current alignment), click on the chart icon.
- You will be prompted before SL1 aligns the presentation object with the Collection Label. After approving, you will notice that a new presentation object now displays a chart icon in its **Label** column. This is because this presentation object is no longer associated with a Collection Label.

Editing a Collection Label

You can edit a Collection Label from the **Collection Labels** page (System > Manage > Collection Labels). To do so:

- Go to the **Collection Labels** page (System > Manage > Collection Labels).

Collection Labels Collection Labels Found [17]							Reset	Guide
Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates		
1. In Use	In Use	Video Performance	No	2	--	--		
2. Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--		
3. Max Jitter	Max Jitter	Video Performance	No	2	--	--		
4. Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--		
5. Rx Audio Pkts Lost	Receive Audio Packets Lost	Video Performance	No	2	--	--		
6. Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--		
7. Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--		
8. Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--		
9. Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--		
10. Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--		
11. Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--		
12. Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--		
13. Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--		
14. Usage	Usage	Video Performance	No	2	--	--		
15. CPU		Vitals	No	37	9	--		
16. Memory		Vitals	No	17	--	--		
17. Swap		Vitals	No	6	--	--		

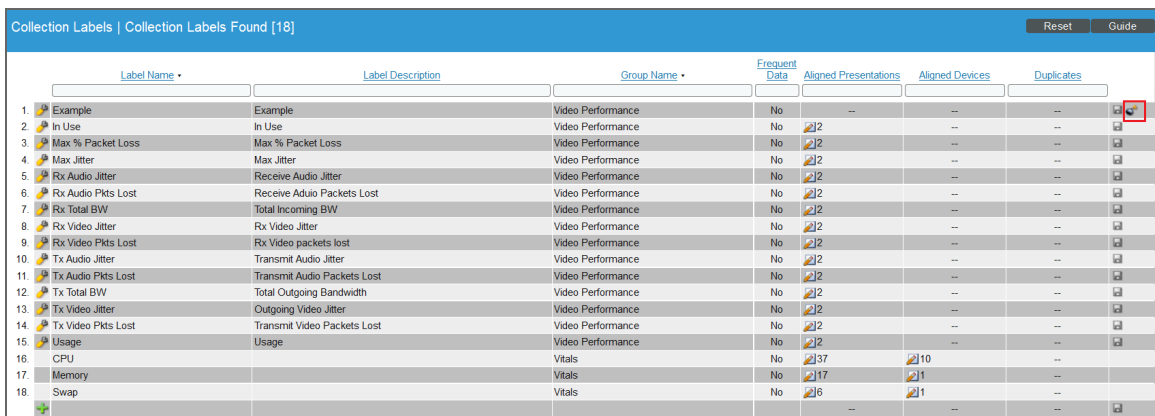
- Find the Collection Label you want to edit. Select its wrench icon ().
- You can edit one or more of the following:
 - Label Name.** Name of the Collection Label. This field is required.
 - Label Description.** Description of the Collection Label. This field is optional.
 - Group Name.** Collection Group to align with the Collection Label. You can select from a list of existing Collection Groups or enter the name of a new Collection Group. This field is required.
 - Frequent Data.** Specifies whether **frequently rolled up data** is calculated for the Collection Label. If the Collection Label will include data that is collected every five minutes or more frequently, and you require that dashboard data be updated every 15 minutes or 20 minutes, select Yes in this field. This data is available immediately for use in a collection label.
 - Save icon** (). Select this icon to save your changes.
















Deleting a Collection Label


You can delete a Collection Label from the **Collection Labels** page (System > Manage > Collection Labels) only if the Collection Label has no **Aligned Presentations**. To delete a Collection Label:

NOTE: You can delete a Collection Label only if no presentation objects are aligned with that label.

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).



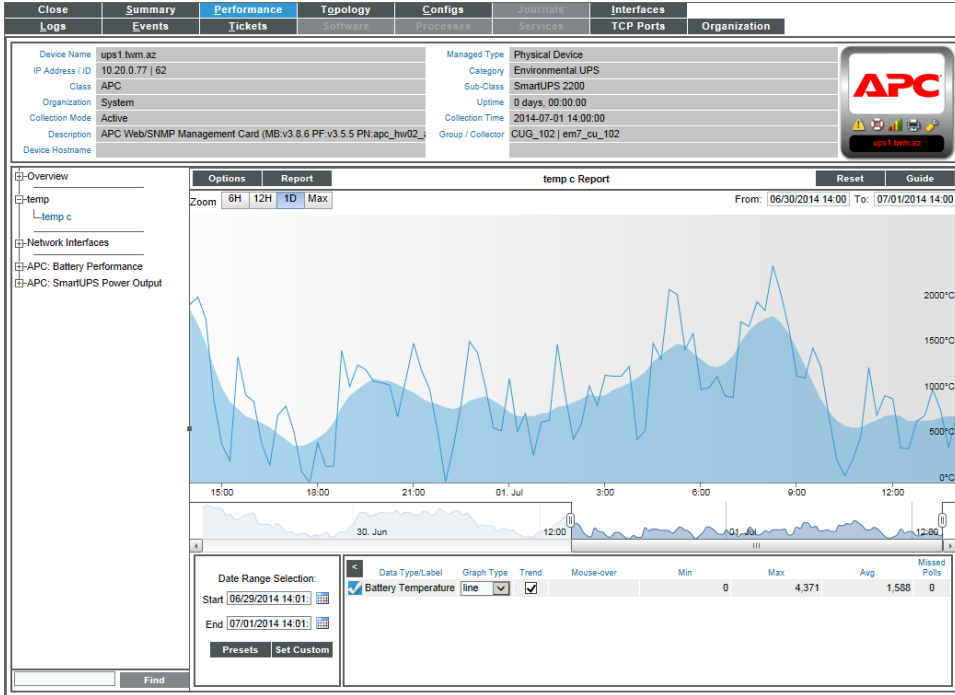
	Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates	
1	Example	Example	Video Performance	No	--	--	--	
2	In Use	In Use	Video Performance	No	2	--	--	
3	Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--	
4	Max Jitter	Max Jitter	Video Performance	No	2	--	--	
5	Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--	
6	Rx Audio Pkts Lost	Receive Audio Packets Lost	Video Performance	No	2	--	--	
7	Rx Total BW	Total Incoming BW	Video Performance	No	2	--	--	
8	Rx Video Jitter	Rx Video Jitter	Video Performance	No	2	--	--	
9	Rx Video Pkts Lost	Rx Video packets lost	Video Performance	No	2	--	--	
10	Tx Audio Jitter	Transmit Audio Jitter	Video Performance	No	2	--	--	
11	Tx Audio Pkts Lost	Transmit Audio Packets Lost	Video Performance	No	2	--	--	
12	Tx Total BW	Total Outgoing Bandwidth	Video Performance	No	2	--	--	
13	Tx Video Jitter	Outgoing Video Jitter	Video Performance	No	2	--	--	
14	Tx Video Pkts Lost	Transmit Video Packets Lost	Video Performance	No	2	--	--	
15	Usage	Usage	Video Performance	No	2	--	--	
16	CPU		Vitals	No	37	10	--	
17	Memory		Vitals	No	17	1	--	
18	Swap		Vitals	No	6	1	--	

2. Find the Collection Label you want to delete.
3. Select its bomb icon ().
4. The Collection Label will be deleted from SL1.

Viewing Reports About Collection Labels on a Single Device

For each device in SL1, the **Device Performance** page displays time-series graphs about the data collected from that device.

If a device subscribes to a Dynamic Application that includes Collection Labels, SL1 will display the Collection Group in the left pane of the **Device Performance** page. You can expand the Collection Group and select a Collection Label.



The graph for a Collection Label displays collected values on the Y-axis and time on the X-axis.

Viewing Dashboards About Collection Labels

You can use the following dashboard widgets to include data associated with Collection Labels in a dashboard:

- Multi-Series Performance Widget
- Leaderboard / Top-N Widget
- Gauge / Meter

For details on each widget, see the **Dashboards** manual.

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	562
Device Thresholds	566

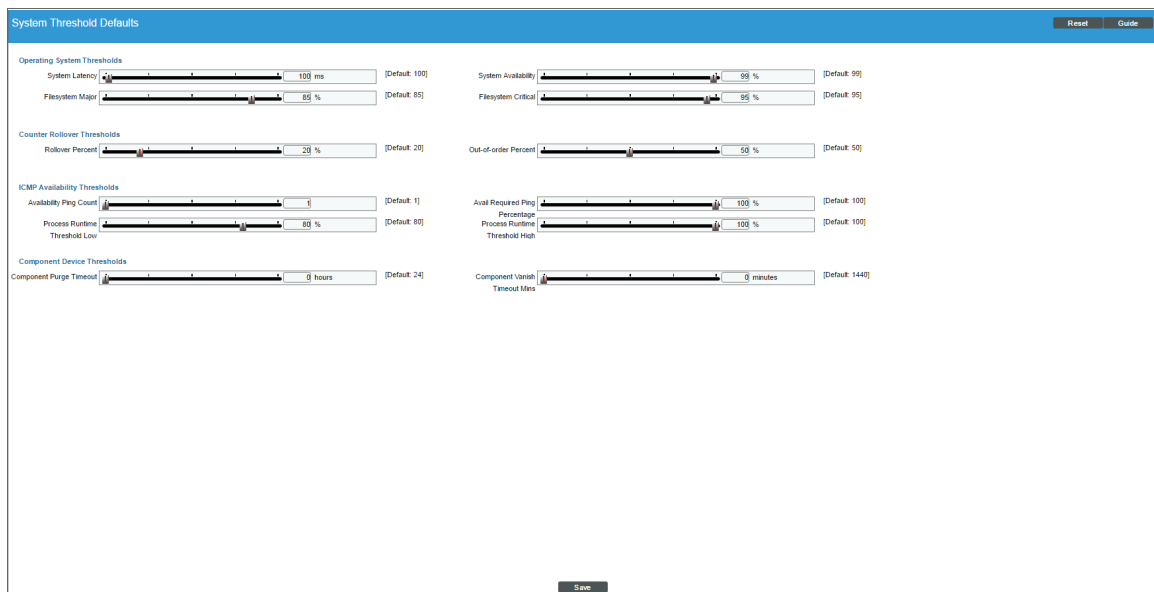
Global Settings for Thresholds

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 Device Latency* in the **Device Management** manual.

- **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):
$$2^{32} - \text{Last Collected Value} + \text{Current Collected Value}$$
- 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 ()

Device Manager Devices Found (176)											Actions		Report	Reset	Guide
Device Name	IP Address	Device Category	Device Class Subclass	OID	Organization	Current State	Collection Group	Collection Status	SNMP Credentials	SNMP Version					
server-851	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
StorageSwitch	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
SimpleSRV.ca.ScienceLogic.local	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	pbAmS	V2					
SNAP662146	10.20.0.249	Storage NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
SNS-PRX-IDC1-Texas	10.20.0.247	Network Switches	Juniper Networks M71 Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
SOM2353DX	10.20.0.188	Servers	Microsoft Windows CE Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
Suma-1	10.20.0.92	Network Switches	Enterprise Networks Summit400 Version 7.1.1	191	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
sunprod1	10.20.0.27	Servers	NET-SNMP Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
Suvan_MonmouthJunctUSA	10.20.0.210	Telephony	Quantum Tenor A800	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
SW275DR4C1_NewDA	10.20.0.1	Network Switches	Cisco Systems Catalyst 3750-Stack	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
swach	10.20.0.15	Network Switches	Brocade ChannelAL Switch	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
tsandberg	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
tgperiskic-fw0.ra1.hostedsolutions.com	10.20.0.157	Network Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
TOSHIBA-e-STUDIO451c	10.20.0.86	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
ttccomm	10.20.0.229	Unknown	Xerox OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
ts2.local	10.20.0.71	Network Switches	Cisco Systems TS SEC	65	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
ts3.local	10.20.0.72	Network Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
TULLPT15-ACCOUNTING	10.20.0.168	Unknown	HPI OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
upst1vmz	10.20.0.77	Environmental UPS	APC SmartUPS 2200	66	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
ut1000	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
vxTarget	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
webdb-prod1	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
WILLIAMS-CORE-R01	10.20.0.82	Network Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
WIX0095-IT_Watchdogs, Inc.	10.20.0.228	Unknown	Generic DMPP	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					
wxomax134	10.20.0.23	Servers	XenServer Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2					

- In the **Device Administration** panel, click the **[Thresholds]** tab.

Close	Properties	Thresholds	Collections	Monitors	Schedule			
Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes	
Device Name	WIN-RA4KHSMQG59	Managed Type	Physical Device					
IP Address / ID	10.2.9.18 1471	Category	Servers					
Class	Microsoft	Sub-Class	Windows Server 2012 R2					
Organization	SAC_Sanity_Group_Test	Uptime	0 days, 15:32:09					
Collection Mode	Active	Collection Time	2017-08-25 13:40:00					
Description	Hardware: Intel® Family 6 Model 63 Stepping 2 AT/AT COMPATIBLE -	Group / Collector	CUG-Core2-COS5-mysql56 10-64-170-43_cu_core2_mysql56					
Device Hostname								

Device Thresholds Actions Reset Guide

Dynamic App Thresholds | Host Resource: Configuration

Raw Data Retention 7 records [Default: 7]

Save

Dynamic App Thresholds | Host Resource: CPU

CPU Utilization High 90 % [Default: 90]

Raw Data Retention 7 days [Default: 7]

Hourly Rollup Retention 120 days [Default: 120]

Daily Rollup Retention 730 days [Default: 730]

Save

Dynamic App Thresholds | Host Resource: Memory

Swap Memory Utilization High 60 % [Default: 60]

Physical Memory Utilization High 80 % [Default: 80]

Raw Data Retention 7 days [Default: 7]

Hourly Rollup Retention 120 days [Default: 120]

Daily Rollup Retention 730 days [Default: 730]

Save


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 SL 1 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 chapter on [monitoring availability of component devices](#).

- **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):

$$\text{maximum value (either } 2^{32}\text{)} - \text{Last Collected Value} + \text{Current Collected Value}$$

- 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:

$$\text{current value} / \text{last collected value}$$

- 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:

$$\text{last collected value} - \text{current collected value}$$

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 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.

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:

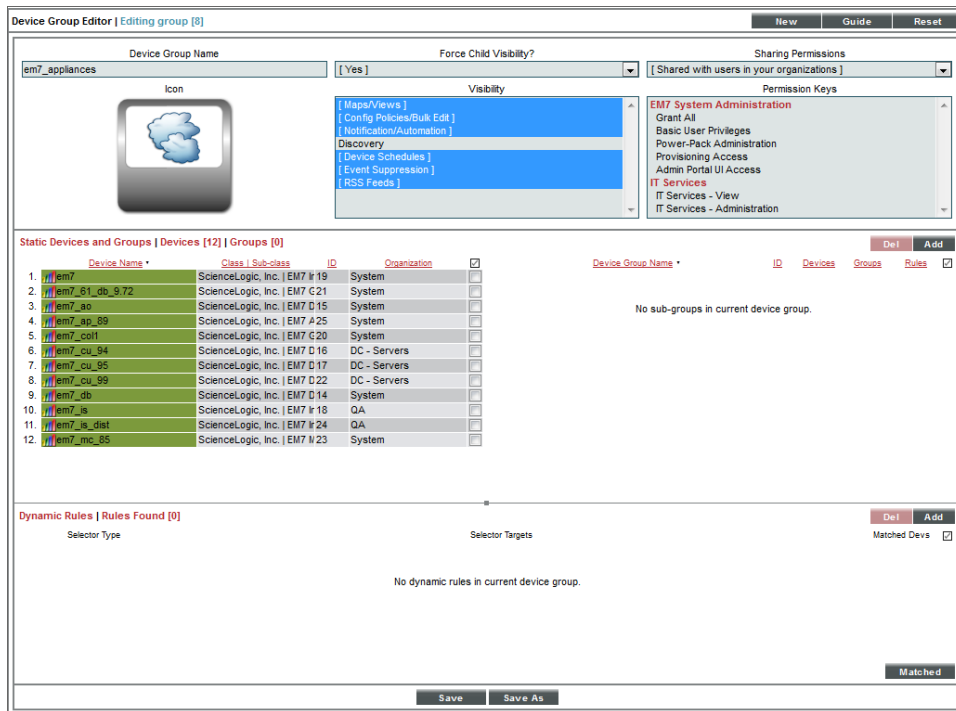
- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

What is a Device Group?	578
What is a Device Template?	580

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.
- In Devices > 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.

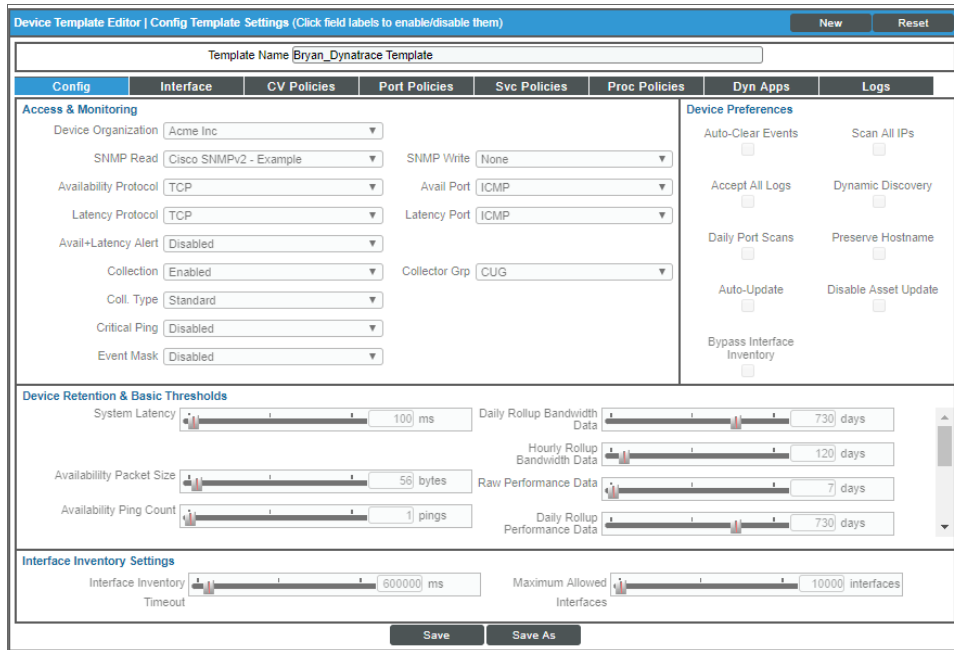
You can add devices to a device group either explicitly or dynamically.

- 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

30

Virtual Devices

Overview

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?	583
Defining a Virtual Device	584
Directing Data to a Virtual Device	585
Redirecting Log Data to a Virtual Device	586
Aligning a Dynamic Application with a Virtual Device	588

What is a Virtual Device?

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

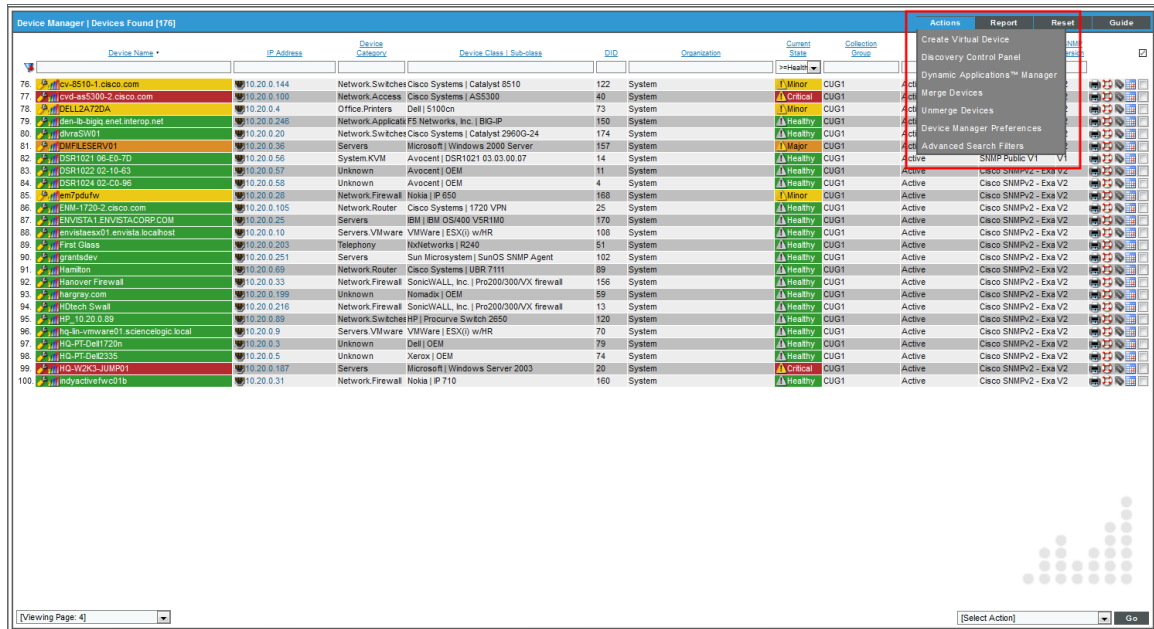
- Monitor a device or application that doesn't support TCP/IP, SNMP, or both. The device's data can be pushed to SL1 via another method (for example, email) and stored in a virtual device.
- Monitor multiple SNMP agents on a single device. In such a case, one of the SNMP agents (for example, a hardware 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

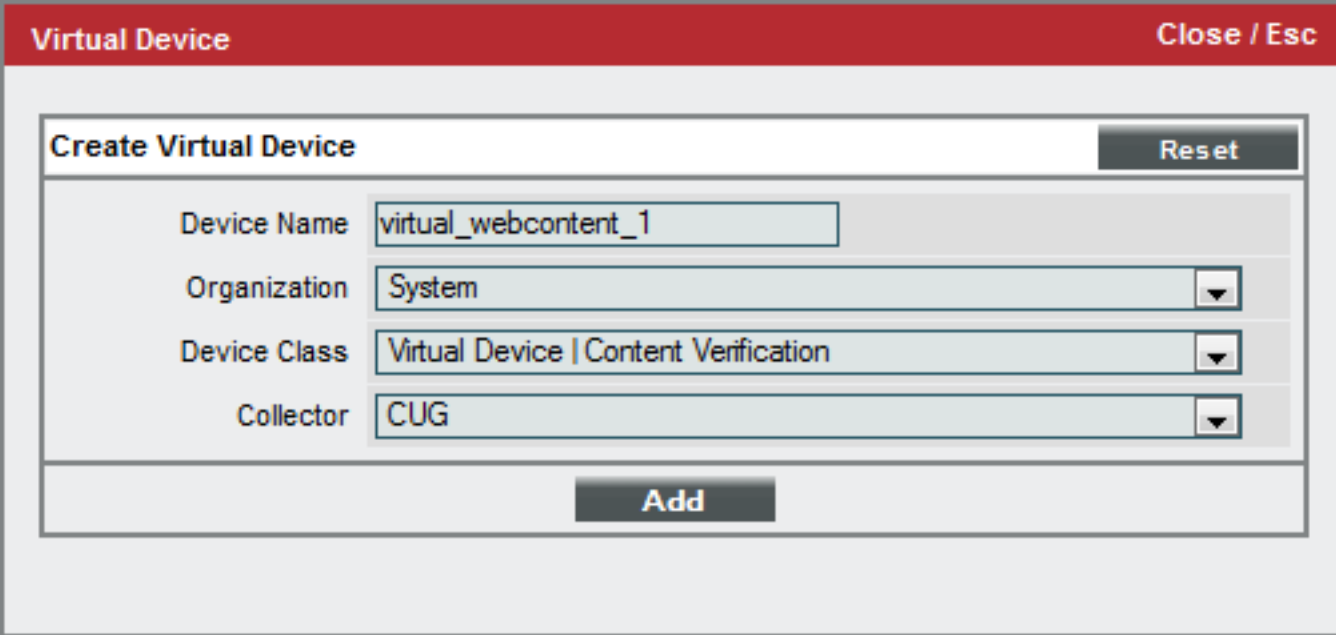
To create a virtual device, you must complete the following tasks:

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



- From the **[Actions]** menu, select *Create Virtual Device*.

4. The **Create Virtual Device** modal page appears.





The screenshot shows a modal window titled "Virtual Device" with a red header bar containing "Close / Esc". Inside the modal, there is a sub-header "Create Virtual Device" and a "Reset" button. The form contains four fields: "Device Name" with the value "virtual_webcontent_1", "Organization" with the value "System", "Device Class" with the value "Virtual Device | Content Verification", and "Collector" with the value "CUG". Each field is a text input or a dropdown menu. At the bottom of the form is an "Add" button.

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:

- Go to the **Device Manager** page (Devices > Device Manager).
- In the **Device Manager** page, find the virtual device to which you want to redirect data. Select its wrench icon [].

Device Manager Devices Found [176]										Actions		Report	Reset	Guide
Device Name	IP Address	Device Category	Device Class Subclass	OID	Organization	Current State	Collection Group	Collection State	SNMP Credential	SNMP Version				
151	10.20.0.177	Office Printers	Lexmark International Print Server	42	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
152	10.20.0.214	Unknown	Shoreline Teleworks OEM	15	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
153	10.20.0.7	Servers	Microsoft Windows Server 2008 R2	77	System	Minor	CUG1	Active	cbasm5 V2	2				
154	10.20.0.249	Storage.NAS	Quantum Corp - Snap Division Snap Server	158	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
155	10.20.0.247	Network.Switches	Juniper Networks M71 Router	152	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
156	10.20.0.183	Servers	Microsoft Windows CC Version 3.0 (Multiple	27	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
157	10.20.0.92	Network.Switches	Extreme Networks Summit46s Version 7.1.1	101	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
158	10.20.0.27	Servers	NET-SNMP Solaris	169	System	Major	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
159	10.20.0.210	Telephony	Quantum Tenor AB00	18	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
160	10.20.0.1	Network.Switches	Cisco Systems Catalyst 3750-Slack	78	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
161	10.20.0.15	Network.Switches	Brocade Chameleon Switch	164	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
162	10.20.0.217	Unknown	Tandberg ASA OEM	12	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
163	10.20.0.157	Network.Firewall	Cisco Systems ASA 5520	146	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
164	10.20.0.86	Unknown	Tec Corporation OEM	124	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
165	10.20.0.229	Unknown	Xerox OEM	81	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
166	10.20.0.71	Network.Switches	Cisco Systems TS SEC	68	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
167	10.20.0.72	Network.Switches	Cisco Systems TS SEC	67	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
168	10.20.0.168	Unknown	HP OEM	166	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
169	10.20.0.77	Environmental.UPLCI	SmartUPS 2200	86	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
170	10.20.0.166	Unknown	General Instrument OEM	55	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
171	10.20.0.227	Telephony	Vina Technologies Multiplexor	136	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
172	10.20.0.64	Servers	Empire Technologies Default Enterprise Agent	87	System	Critical	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
173	10.20.0.82	Network.Router	Cisco Systems 1750	83	System	Minor	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
174	10.20.0.228	Unknown	Genesys SNMP	76	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				
175	10.20.0.23	Servers	XenServer Xen Host	176	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2				

3. In the **Device Administration** panel, select the **[Redirects]** tab.

The screenshot displays the SL1 Device Administration interface. At the top, there is a navigation bar with tabs: Close, Properties, Thresholds, Collections, Monitors, Tickets, **Redirects** (highlighted with a red box), and Notes. Below this, the main content area is divided into several sections:

- Device Information:** A table showing details for device 'virtual_webcontent_1'.

Device Name	virtual_webcontent_1	Managed Type	Virtual Device
ID	12	Category	Virtual
Class	Virtual Device	Sub-Class	Content Verification
Organization	System	Uptime	0 days, 00:00:00
		Group / Collector	CUG em7_ao
- Redirect Policy Editor:** A form with three input fields: 'Source Device' (a dropdown menu with '[Select Device]'), 'Expression Match' (a text field containing '[URL http://www.cnn.com/TECH?hpt=Sbin]'), and 'Active State' (a dropdown menu with '[Enabled]'). A 'Save' button is located below these fields. To the right of the form are buttons for 'Actions', 'Reset', and 'Guide'.
- Redirect Policy Registry:** A large empty area with a red message in the center: 'There are no redirect policies aligned with this device.'

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.

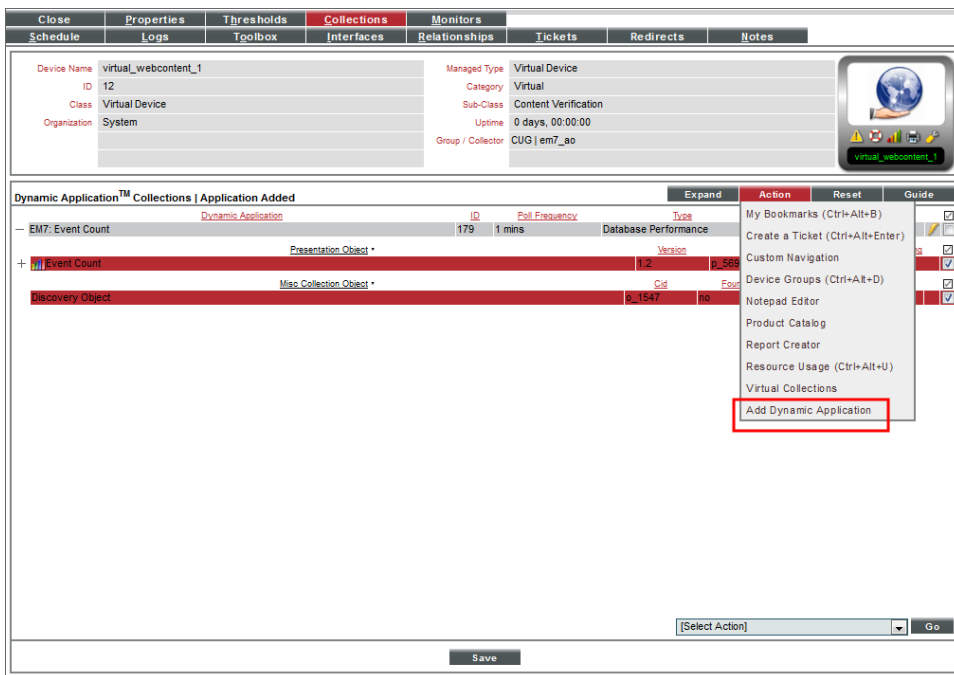
Aligning a Dynamic Application with a Virtual Device

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.

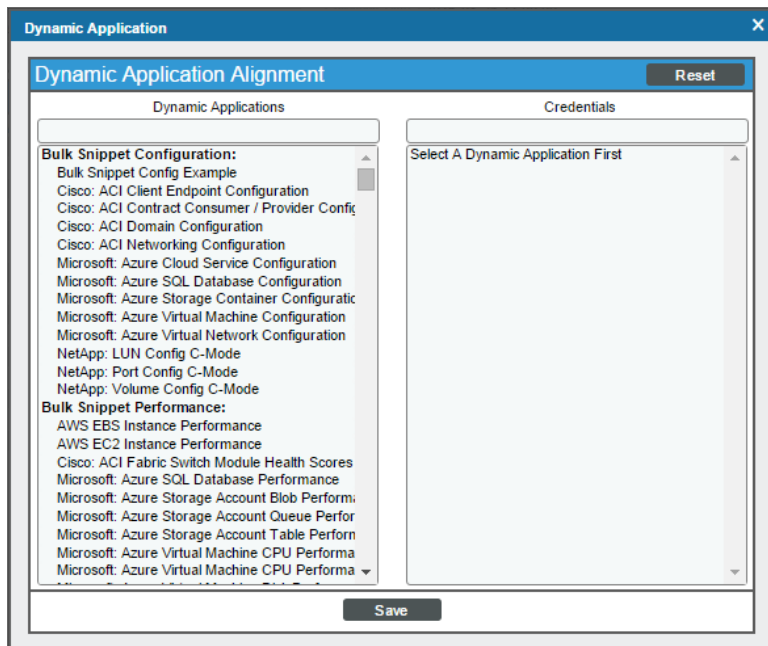
NOTE: You cannot align SNMP Dynamic Applications with a virtual device. You can align all other types of Dynamic Applications with a virtual device.

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.

Customizing the User Interface for a Device

Overview

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:

<i>Custom Navigation</i>	590
<i>Editing a Custom Navigation tab</i>	593

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).

- In the **Device Manager** page, find the device for which you want to create a custom tab. Select its wrench icon (🔧).

Device Name	IP Address	Device Category	Device Class Sub-class	DID	Organization	Guest State	Collection Group	Collection State	SNMP Credential	SNMP Version
lisa11wm1az	10.0.0.101	Network Switches	Cisco Systems Catalyst 3750-Stack	104	System	Healthy	CUG1	Active	Cisco SNMPv2 - Exa V2	2.0

- In any page in the **Device Administration** panel, select the **[Actions]** menu and choose *Custom Navigation*.

Device Administration Panel - Actions Menu

- My Bookmarks (Ctrl+Alt+B)
- Add IP Address
- Select Primary IP Addresses
- Clear Device Cache
- Create a Ticket (Ctrl+Alt+Enter)
- Custom Navigation**
- Device Class
- Device Children
- Device Groups (Ctrl+Alt+D)
- Notepad Editor
- Product Catalog
- Report Creator
- Resource Usage (Ctrl+Alt+U)
- Secondary Credentials
- Merge Device

Device Properties: Device Name: 10.0.0.101, IP Address: [10.0.0.101 - verified], Organization: Intel, Category: Network Switches, Sub-Class: Catalyst 2948G-GE-TX, Uptime: 393 days, 22:26:38, Collection Time: 2014-06-16 15:45:00, Group / Collector: CUG1 | em7_cu1

Monitoring & Management: Device Class: Cisco Systems Catalyst 2948G-GE-TX, SNMP Read/Write: [Cisco SNMPv2 - Example], Availability Port: [UDP], Latency Port: [ICMP], User Maintenance: [Disabled], Collection: [Enabled], Coll. Type: [Standard], Critical Ping: [Disabled], Dashboard: None, Event Mask: [Group in blocks every 10 minutes]

Save

4. The **Custom Navigation** modal page appears.

The screenshot shows a modal window titled "Custom Navigation" with a "Close / Esc" button in the top right corner. The main content area is titled "For Device [35]" and contains a "Refresh" button in the top right. Below the title bar, there are three input fields: "Title (Shown on Tab)", "Limit Access" (a dropdown menu currently showing "Administrators"), and "External URL / URI Link". A "Save" button is located below these fields. At the bottom of the modal, there is a table with four columns: "Title (Shown on Tab)", "Access", "User Edit", and "Date Edit".

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**.

The screenshot displays the configuration page for a Cisco Catalyst switch. The top navigation bar includes tabs for Close, Properties, Thresholds, Collections, Monitors, Schedule, Logs, Toolbox, Interfaces, Relationships, Tickets, Redirects, and Notes. The main content area is divided into sections: Identification, Monitoring & Management, and a bottom section with a Save button. The Identification section shows fields for Device Name (10.0.0.101), IP Address (10.0.0.101 - verified), and Organization (Intel). The Monitoring & Management section includes various configuration options like SNMP Read/Write, Availability Port, Latency Port, User Maintenance, Collection, Coll. Type, Critical Ping, Dashboard, and Event Mask. On the right side, there is an Actions menu with options such as My Bookmarks, Add IP Address, Select Primary IP Addresses, Clear Device Cache, Create a Ticket, Custom Navigation (highlighted with a red box), Device Class, Device Children, Device Groups, Notepad Editor, Product Catalog, Report Creator, Resource Usage, Secondary Credentials, Merge Device, Dynamic Discovery, Preserve Hostname, and Disable Asset Update.

4. The **Custom Navigation** modal page appears:

Title (Shown on Tab)	Access	User Edit	Date Edit
1. Navigation Examp	Access	em7admin	2013-07-02 13:58:17

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

32

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.



If a component device is merged with a physical device:

- The device can be vanished only if SL1 cannot retrieve information about a component device and the availability check for the physical device has determined that the device is unavailable.
- The **Component Vanish Timeout** and **Component Purge Timeout** settings for that device are compared to the time since the availability check for the physical device determined that the device is unavailable.

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	596
Viewing the List of Vanished Devices	598
Filtering the List of Devices	600
Using the Advanced Filters	601
Manually Purge Selected Devices	603
Set One or More Devices to Never Purge	604

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.

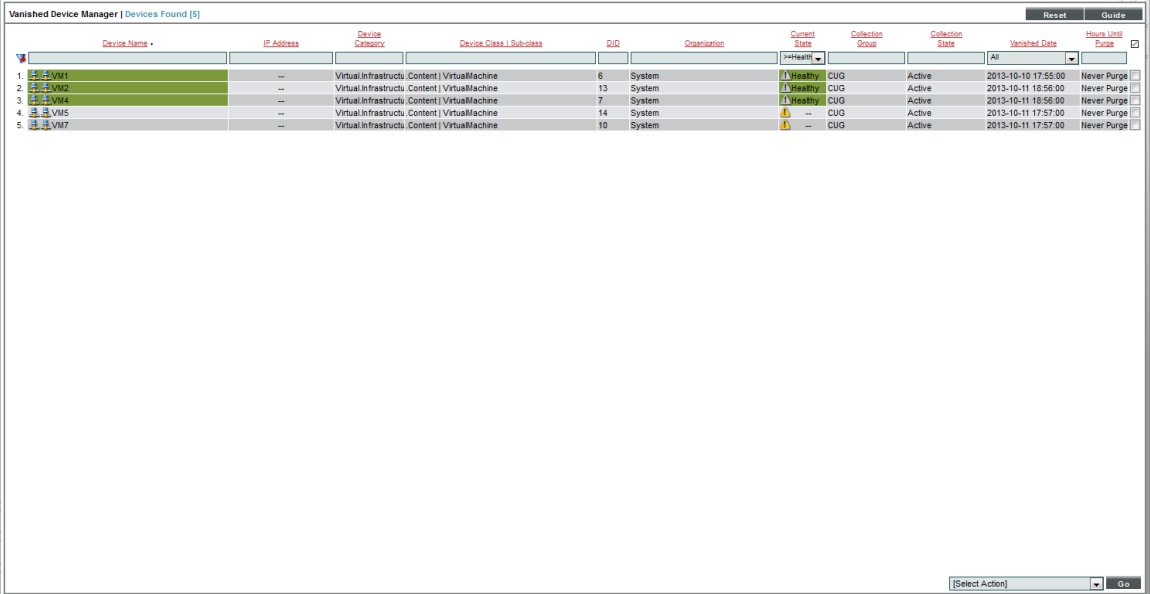
SL1 uses the following logic to determine the threshold value for a given component device when determining whether the component should be vanished or purged:

- 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:



Device Name	IP Address	Device Category	Device Class / Sub-class	DID	Organization	Current State	Collection Group	Collection State	Vanished Date	Hours Until Purge
1. VM1	--	Virtual Infrastructu	Content VirtualMachine	6	System	Healthy	CUG	Active	2013-10-10 17:55:00	Never Purge
2. VM2	--	Virtual Infrastructu	Content VirtualMachine	13	System	Healthy	CUG	Active	2013-10-11 18:56:00	Never Purge
3. VM3	--	Virtual Infrastructu	Content VirtualMachine	7	System	Healthy	CUG	Active	2013-10-11 18:56:00	Never Purge
4. VM5	--	Virtual Infrastructu	Content VirtualMachine	14	System	Warning	CUG	Active	2013-10-11 17:57:00	Never Purge
5. VM7	--	Virtual Infrastructu	Content VirtualMachine	10	System	Critical	CUG	Active	2013-10-11 17:57:00	Never Purge

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 Purge Selected Devices

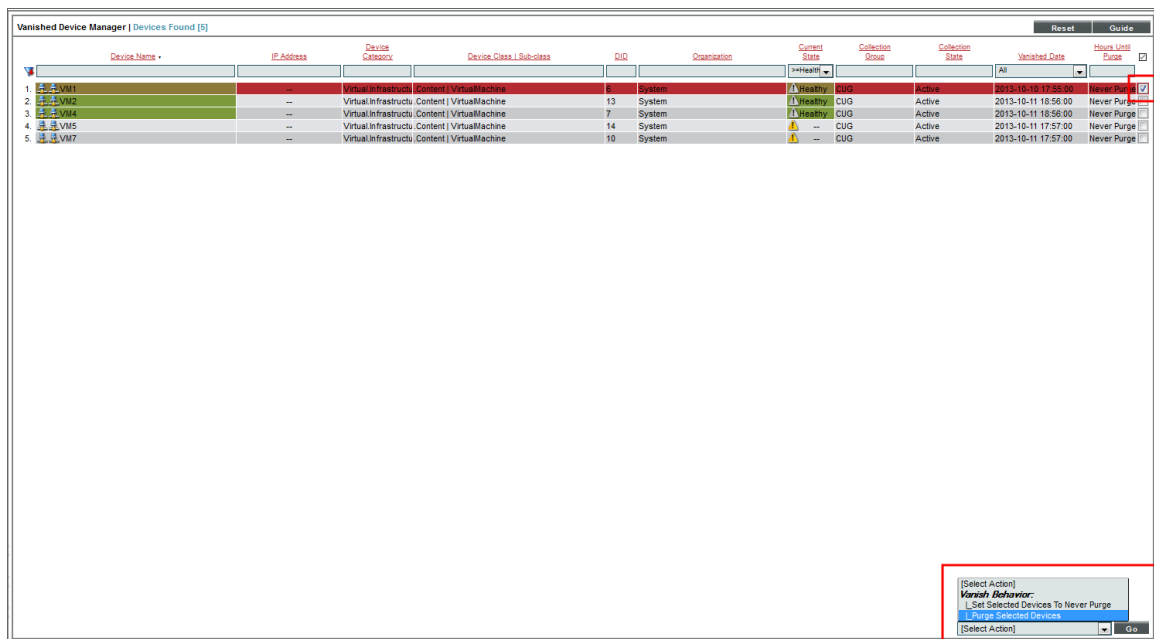
You can manually purge one or more devices in the **Vanished Device Manager** page.

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.

Set 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.

The screenshot shows the 'Vanished Device Manager' interface with a table of 5 devices. The table has columns for Device Name, IP Address, Device Category, Device Class | Sub-class, GUID, Organization, Current State, Collection Group, Collection State, Vanished Date, and a 'Never Purge' checkbox. The first device, VM1, has its 'Never Purge' checkbox checked. A red box highlights the 'Select Action' dropdown menu at the bottom right, which is open and shows the option 'Set Selected Devices to Never Purge' selected. Another red box highlights the 'Go' button at the bottom right of the dropdown menu.

Device Name	IP Address	Device Category	Device Class Sub-class	GUID	Organization	Current State	Collection Group	Collection State	Vanished Date	Never Purge
VM1	...	Virtual Infrastructure	Content VirtualMachine	8	System	Healthy	CUG	Active	2013-10-16 17:55:00	<input checked="" type="checkbox"/>
VM2	...	Virtual Infrastructure	Content VirtualMachine	13	System	Healthy	CUG	Active	2013-10-11 18:56:00	<input type="checkbox"/>
VM3	...	Virtual Infrastructure	Content VirtualMachine	7	System	Healthy	CUG	Active	2013-10-11 18:56:00	<input type="checkbox"/>
VM5	...	Virtual Infrastructure	Content VirtualMachine	14	System	Warning	CUG	Active	2013-10-11 17:57:00	<input type="checkbox"/>
VM7	...	Virtual Infrastructure	Content VirtualMachine	10	System	Warning	CUG	Active	2013-10-11 17:57:00	<input type="checkbox"/>

2. In the **Select Action** drop-down list, select *Set Selected Devices to Never Purge*.
3. Select the **[Go]** button.


Chapter

33

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, 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.

This chapter includes the following topics:

<i>Viewing the List of Device Dashboards</i>	606
<i>Creating a Device Dashboard</i>	608
<i>Aligning Device Dashboards</i>	609
<i>Editing a Device Dashboard</i>	613
<i>Deleting a Device Dashboard</i>	613
<i>Copying a Device Dashboard</i>	614
<i>Defining the Global Default for Device Dashboards</i>	614

<i>Unaligning a Device Dashboard</i>	616
<i>Moving Alignment for Device Dashboards</i>	617

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:

<i>Viewing the List of Device Dashboards</i>	606
<i>Creating a Device Dashboard</i>	608
<i>Aligning Device Dashboards</i>	609
<i>Editing a Device Dashboard</i>	613
<i>Deleting a Device Dashboard</i>	613
<i>Copying a Device Dashboard</i>	614
<i>Defining the Global Default for Device Dashboards</i>	614
<i>Unaligning a Device Dashboard</i>	616
<i>Moving Alignment for Device Dashboards</i>	617

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:

Device Dashboard Name	ID	Global Default	Categories	Classes	Devices	Dynamic Apps	Edited By	Last Edited
1. AWS Account	90	No	0	1	0	1	em7admin	2017-04-13 08:42:33
2. AWS Auto Scale Group	95	No	0	1	0	1	em7admin	2017-04-13 08:42:36
3. AWS EBS Instance	92	No	0	1	0	1	em7admin	2017-04-13 08:42:34
4. AWS EC2 Instance	91	No	0	11	0	1	em7admin	2017-04-13 08:42:34
5. AWS ELB Instance	95	No	0	1	0	1	em7admin	2017-04-13 08:42:36
6. AWS OpsWorks Stack	98	No	0	1	0	1	em7admin	2017-04-13 08:42:38
7. AWS RDS Instance	89	No	0	2	0	1	em7admin	2017-04-13 08:42:33
8. AWS Redshift Cluster	93	No	0	1	0	1	em7admin	2017-04-13 08:42:35
9. AWS Redshift Node	94	No	0	1	0	1	em7admin	2017-04-05 10:41:24
10. AWS SNS Topic	88	No	0	1	0	1	em7admin	2017-04-13 08:42:33
11. AWS SQS Instance	97	No	0	1	0	1	em7admin	2017-04-13 08:42:36
12. Cisco TelePresence Conductor	125	No	0	1	0	0	em7admin	2017-04-10 01:30:57
13. Cisco TelePresence MCU	125	No	0	1	0	0	em7admin	2017-04-10 01:30:57
14. Cisco TelePresence Server	127	No	0	1	0	0	em7admin	2017-04-10 01:30:57
15. Cisco ACI APIC	72	No	0	1	0	0	em7admin	2017-04-05 10:06:15
16. Cisco ACI Application	75	No	0	1	0	0	em7admin	2017-04-05 10:06:21
17. Cisco ACI Endpoint Group	76	No	0	1	0	0	em7admin	2017-04-05 10:06:21
18. Cisco ACI Leaf Switch	73	No	1	0	0	0	em7admin	2017-04-05 10:06:16
19. Cisco ACI Pod	71	No	0	1	0	0	em7admin	2017-04-05 10:06:15
20. Cisco ACI Root	77	No	0	1	0	0	em7admin	2017-04-05 10:06:25
21. Cisco ACI Spine Switch	74	No	1	0	0	0	em7admin	2017-04-05 10:06:20
22. Cisco ACI Tenant	78	No	0	1	0	0	em7admin	2017-04-05 10:06:25
23. Cisco CCE Admin and Data Server	109	No	0	1	0	0	em7admin	2017-04-05 19:05:03
24. Cisco CCE Call Router	107	No	0	1	0	0	em7admin	2017-04-05 19:05:00
25. Cisco CCE Campaign	113	No	0	1	0	0	em7admin	2017-04-05 19:05:05

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.

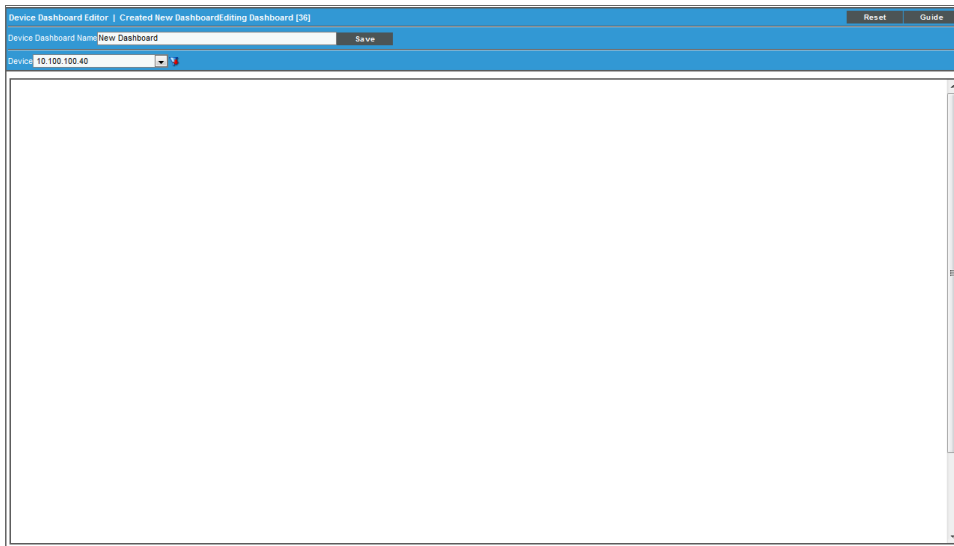
- **Device Dashboard Name.** Name of the device dashboard.
- **ID.** Unique ID that SL1 automatically assigned to each device dashboard.
- **Global Default.** Specifies whether the device dashboard is the default device dashboard for all devices.
- **Categories.** Specifies the number of device categories 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:

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Toglobox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes

Device Name	em7_ao	Managed Type	Physical Device
IP Address / ID	10.64.68.17 677	Category	System:EM7
Class	ScienceLogic, Inc.	Sub-Class	OEM
Organization	System	Uptime	6 days, 00:08:53
Collection Mode	Active	Collection Time	2015-11-05 12:40:00
Description	ScienceLogic EM7 G3 - All-In-One	Group / Collector	CUG em7_ao
Root Device	CUCM10-01.qa.sciencelogic.local	Parent Device	Services
Device Hostname			

Device Properties		Organization	Asset
		Actions	Reset
			Guide

Identification					
Device Name	em7_ao	IP Address	[10.64.68.17 - verified]	Organization	[System]

Monitoring & Management		Preferences	
Device Class	ScienceLogic, Inc. OEM	Auto-Clear Events	<input checked="" type="checkbox"/>
SNMP Read/Write	[EM7 Default V2] [None]	Accept All Logs	<input checked="" type="checkbox"/>
Availability Port	[UDPI] [161 - SNMP]	Daily Port Scans	<input checked="" type="checkbox"/>
Latency Port	[ICMP] [ICMP]	Auto-Update	<input checked="" type="checkbox"/>
Avail+Latency Alert	[Disable]	Scan All IP's	<input type="checkbox"/>
User Maintenance	[Disable] [Maintenance Collection Enabled]	Dynamic Discovery	<input checked="" type="checkbox"/>
Collection	[Enabled] [CUG]	Preserve Hostname	<input checked="" type="checkbox"/>
Coll. Type	[Standard]	Disable Asset Update	<input type="checkbox"/>
Critical Ping	[Disable]	Bypass Interface Inventory	<input type="checkbox"/>
Dashboard	None		
Event Mask	[Group in blocks every 10 minutes]		

- **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

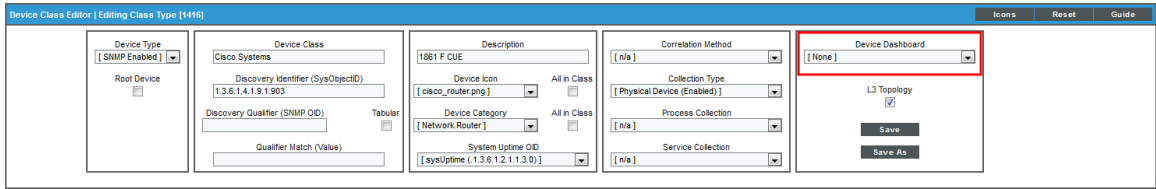
You can manually align a device dashboard with a device class. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the Device Class will appear as the default view in the **Device Summary** page.

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.

- 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.



- 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.

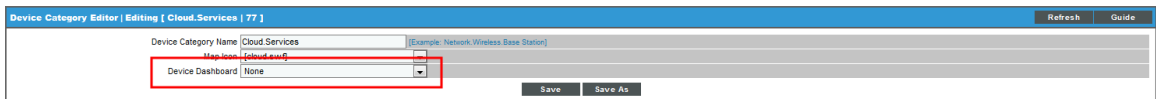
Aligning a Device Dashboard with a Device Category

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:

- Go to the **Device Category Editor** page (System > Customize > Device Categories).
- In the **Register** pane, find the device category you want to align with a device dashboard. Click the wrench icon (🔧) for that device category.
- 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.

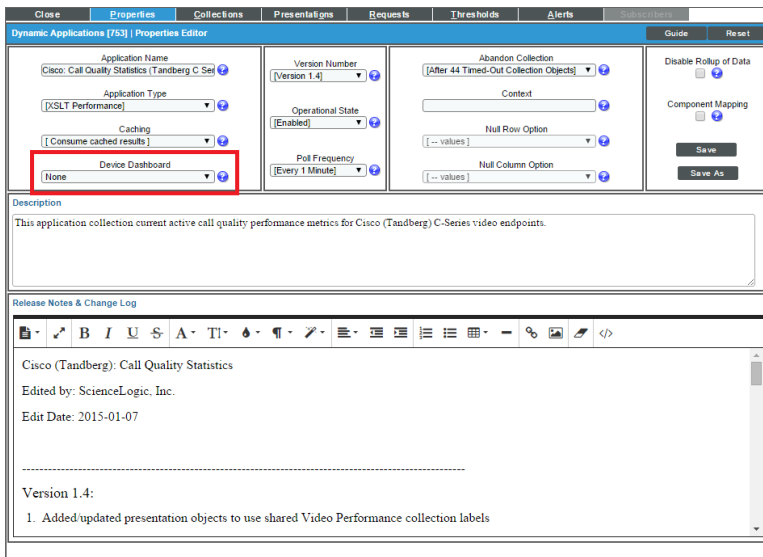
Aligning a Device Dashboard with a Dynamic Application

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.




The screenshot shows the 'Dynamic Applications Properties Editor' for 'Cisco: Call Quality Statistics (Tandberg C-Series)'. The 'Device Dashboard' dropdown is highlighted with a red box and set to 'None'. Other fields include 'Version Number' (1.4), 'Operational State' (Enabled), 'Poll Frequency' (Every 1 Minute), 'Abandon Collection' (After 44 Timed-Out Collection Objects), 'Context', 'Null Row Option', 'Null Column Option', 'Disable Rollup of Data', and 'Component Mapping'. The description field contains: 'This application collection current active call quality performance metrics for Cisco (Tandberg) C-Series video endpoints.' The release notes section shows: 'Version 1.4: 1. Added updated presentation objects to use shared Video Performance collection labels'.

- 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

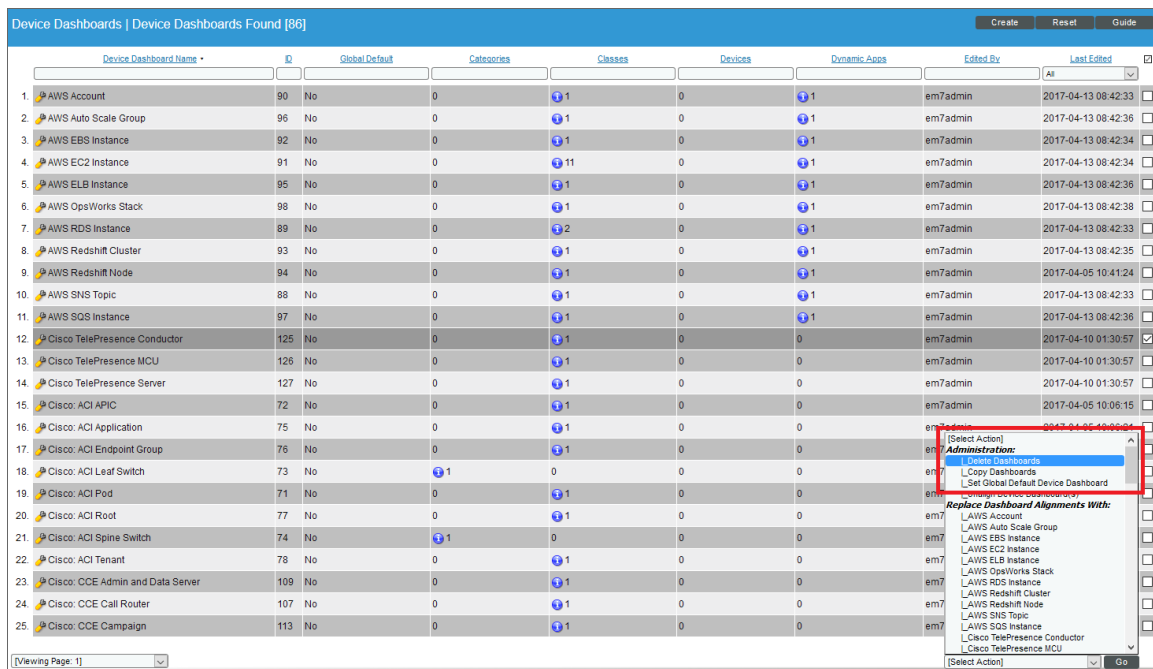
To edit a device dashboard:

- Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
- In the **Device Dashboards** page, find the device dashboard you want to edit. Click its wrench icon ()
- The **Device Dashboard Editor** page appears. Edit one or more fields and/or the dashboard widgets.
- SL1 automatically saves your changes.

Deleting a Device Dashboard

To delete one or more device dashboards:

- Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
- In the **Device Dashboards** page, select the checkbox for each dashboard you want to delete.
- In the **Select Action** drop-down list, select *Delete Dashboards*.



The screenshot shows a table titled "Device Dashboards | Device Dashboards Found [86]". The table has columns for ID, Global Default, Categories, Classes, Devices, Dynamic Apps, Edited By, and Last Edited. A red box highlights the "Select Action" dropdown menu for the row with ID 17, "Cisco: ACI Endpoint Group". The menu options include "Administration", "Copy Dashboards", "Set Global Default Device Dashboard", and "Replace Dashboard Alignments With:". The "Replace Dashboard Alignments With:" option is expanded, showing a list of dashboard names such as "L_AWS Account", "L_AWS Auto Scale Group", "L_AWS EBS Instance", etc.

ID	Global Default	Categories	Classes	Devices	Dynamic Apps	Edited By	Last Edited
1. AWS Account	90	No	0	1	0	em7admin	2017-04-13 08:42:33
2. AWS Auto Scale Group	96	No	0	1	0	em7admin	2017-04-13 08:42:36
3. AWS EBS Instance	92	No	0	1	0	em7admin	2017-04-13 08:42:34
4. AWS EC2 Instance	91	No	0	11	0	em7admin	2017-04-13 08:42:34
5. AWS ELB Instance	95	No	0	1	0	em7admin	2017-04-13 08:42:38
6. AWS OpsWorks Stack	98	No	0	1	0	em7admin	2017-04-13 08:42:38
7. AWS RDS Instance	89	No	0	2	0	em7admin	2017-04-13 08:42:33
8. AWS Redshift Cluster	93	No	0	1	0	em7admin	2017-04-13 08:42:35
9. AWS Redshift Node	94	No	0	1	0	em7admin	2017-04-05 10:41:24
10. AWS SNS Topic	88	No	0	1	0	em7admin	2017-04-13 08:42:33
11. AWS SQS Instance	97	No	0	1	0	em7admin	2017-04-13 08:42:38
12. Cisco TelePresence Conductor	125	No	0	1	0	em7admin	2017-04-10 01:30:57
13. Cisco TelePresence MCU	126	No	0	1	0	em7admin	2017-04-10 01:30:57
14. Cisco TelePresence Server	127	No	0	1	0	em7admin	2017-04-10 01:30:57
15. Cisco: ACI APIC	72	No	0	1	0	em7admin	2017-04-05 10:06:15
16. Cisco: ACI Application	75	No	0	1	0	em7admin	2017-04-05 10:06:04
17. Cisco: ACI Endpoint Group	76	No	0	1	0	em7admin	2017-04-05 10:06:04
18. Cisco: ACI Leaf Switch	73	No	1	0	0	em7admin	2017-04-05 10:06:04
19. Cisco: ACI Pod	71	No	0	1	0	em7admin	2017-04-05 10:06:04
20. Cisco: ACI Root	77	No	0	1	0	em7admin	2017-04-05 10:06:04
21. Cisco: ACI Spine Switch	74	No	1	0	0	em7admin	2017-04-05 10:06:04
22. Cisco: ACI Tenant	78	No	0	1	0	em7admin	2017-04-05 10:06:04
23. Cisco: CCE Admin and Data Server	109	No	0	1	0	em7admin	2017-04-05 10:06:04
24. Cisco: CCE Call Router	107	No	0	1	0	em7admin	2017-04-05 10:06:04
25. Cisco: CCE Campaign	113	No	0	1	0	em7admin	2017-04-05 10:06:04

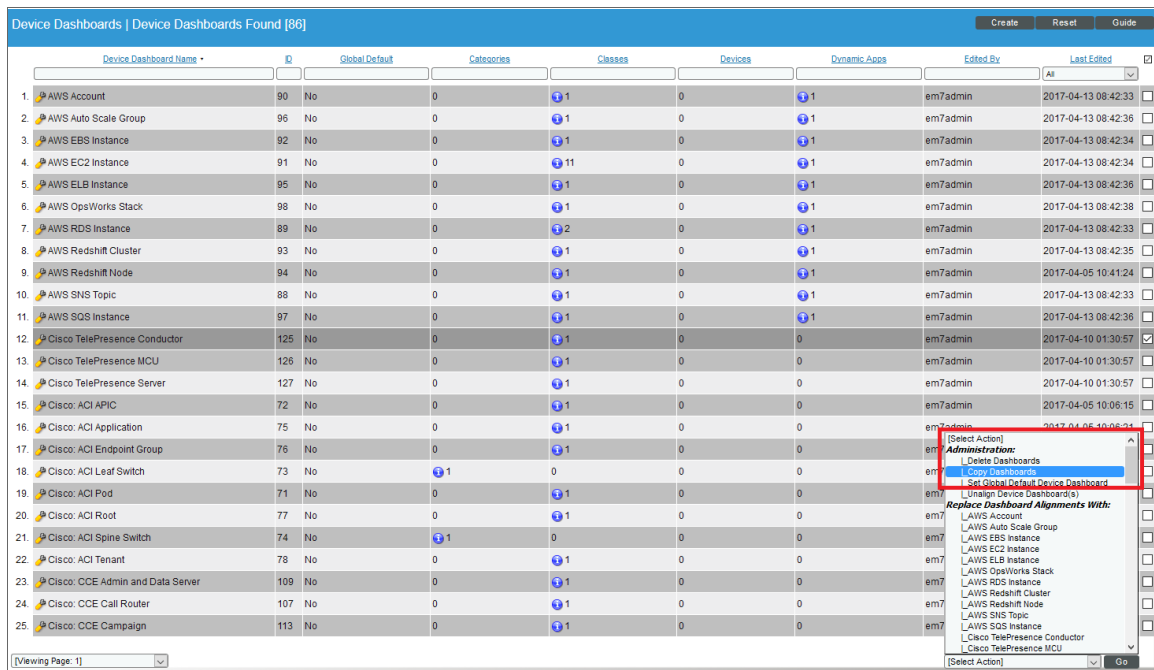
- Click the **[Go]** button. The selected device dashboard(s) will no longer appear in this page or be accessible in the **Device Summary** page.

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:

- Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
- In the **Device Dashboards** page, select the checkbox for each dashboard you want to copy.
- In the **Select Action** drop-down list, select **Copy Dashboards**.



- 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.

- In the **Select Action** drop-down list, select *Set Global Default Device Dashboard*.

Device Dashboard Name	ID	Global Default	Categories	Classes	Devices	Dynamic Apps	Edited By	Last Edited
1. AWS Account	90	No	0	1	0	1	em7admin	2017-04-13 08:42:33
2. AWS Auto Scale Group	96	No	0	1	0	1	em7admin	2017-04-13 08:42:36
3. AWS EBS Instance	92	No	0	1	0	1	em7admin	2017-04-13 08:42:34
4. AWS EC2 Instance	91	No	0	11	0	1	em7admin	2017-04-13 08:42:34
5. AWS ELB Instance	95	No	0	1	0	1	em7admin	2017-04-13 08:42:36
6. AWS OpsWorks Stack	98	No	0	1	0	1	em7admin	2017-04-13 08:42:38
7. AWS RDS Instance	89	No	0	2	0	1	em7admin	2017-04-13 08:42:33
8. AWS Redshift Cluster	93	No	0	1	0	1	em7admin	2017-04-13 08:42:36
9. AWS Redshift Node	94	No	0	1	0	1	em7admin	2017-04-05 10:41:24
10. AWS SNS Topic	88	No	0	1	0	1	em7admin	2017-04-13 08:42:33
11. AWS SQS Instance	97	No	0	1	0	1	em7admin	2017-04-13 08:42:36
12. Cisco TelePresence Conductor	125	No	0	1	0	0	em7admin	2017-04-10 01:30:57
13. Cisco TelePresence MCU	126	No	0	1	0	0	em7admin	2017-04-10 01:30:57
14. Cisco TelePresence Server	127	No	0	1	0	0	em7admin	2017-04-10 01:30:57
15. Cisco ACI APIC	72	No	0	1	0	0	em7admin	2017-04-05 10:06:15
16. Cisco ACI Application	75	No	0	1	0	0	em7admin	2017-04-05 10:06:21
17. Cisco ACI Endpoint Group	76	No	0	1	0	0	em7admin	2017-04-05 10:06:21
18. Cisco ACI Leaf Switch	73	No	1	0	0	0	em7admin	2017-04-05 10:06:21
19. Cisco ACI Pod	71	No	0	1	0	0	em7admin	2017-04-05 10:06:21
20. Cisco ACI Root	77	No	0	1	0	0	em7admin	2017-04-05 10:06:21
21. Cisco ACI Spine Switch	74	No	1	0	0	0	em7admin	2017-04-05 10:06:21
22. Cisco ACI Tenant	78	No	0	1	0	0	em7admin	2017-04-05 10:06:21
23. Cisco COE Admin and Data Server	109	No	0	1	0	0	em7admin	2017-04-05 10:06:21
24. Cisco COE Call Router	107	No	0	1	0	0	em7admin	2017-04-05 10:06:21
25. Cisco COE Campaign	113	No	0	1	0	0	em7admin	2017-04-05 10:06:21

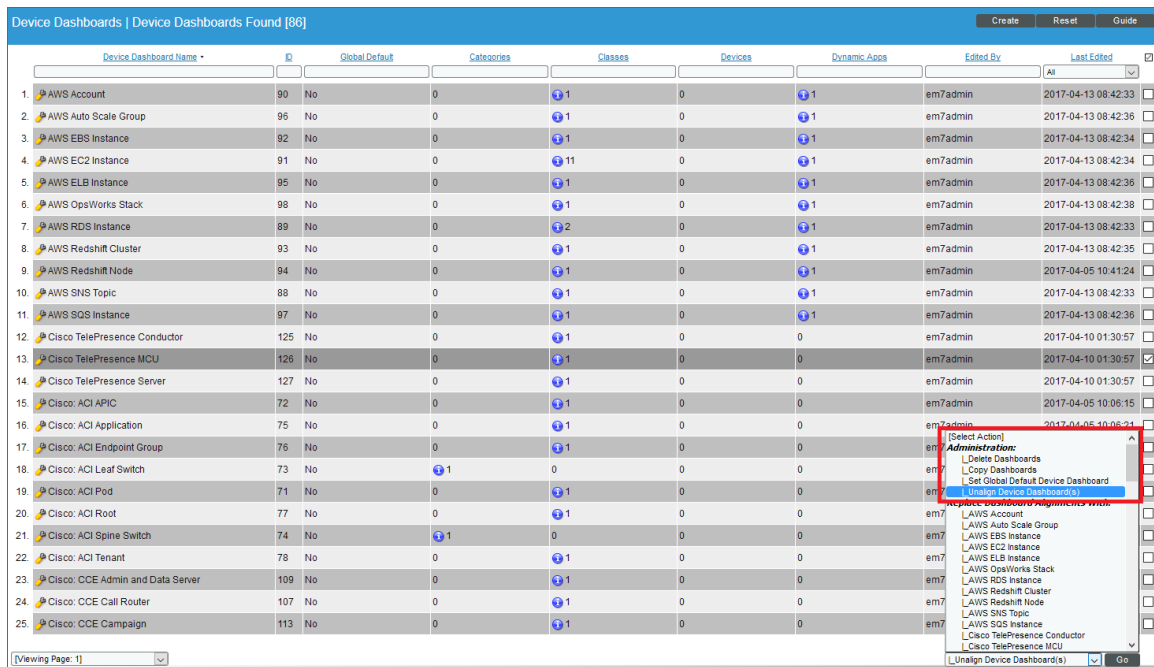
- Click the **[Go]** button. In the **Global Default** field for the selected device dashboard the value "Yes" will appear.

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:

- Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
- In the **Device Dashboards** page, select the checkbox for the dashboard you want to remove from the **Device Summary** page.

- In the **Select Action** drop-down list, select *Unalign Device Dashboard(s)*.



- Click the **[Go]** button.
- 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:

- Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
- In the **Device Dashboards** page, select the checkbox for the dashboard that you want to "steal" alignments.

- 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.

The screenshot shows the 'Device Dashboards' page with a table of 25 device dashboards. The table columns are: Device Dashboard Name, ID, Global Default, Categories, Classes, Devices, Dynamic Apps, Edited By, and Last Edited. The 'Cisco: ACI APIC' dashboard (ID 72) is selected, and its context menu is open. The menu options include: [Select Action], Administration, Delete Dashboards, Copy Dashboards, Set Global Default Device Dashboard, Unalign Device Dashboards, and Replace Dashboard Alignments With. The 'Replace Dashboard Alignments With' option is highlighted, and a list of device dashboards is shown below it, including AWS Auto Scale Group, AWS EBS Instance, AWS EC2 Instance, AWS ELB Instance, AWS OpsWorks Stack, AWS RDS Instance, AWS Redshift Cluster, AWS Redshift Node, AWS SNS Topic, AWS SQS Instance, Cisco TelePresence Conductor, Cisco TelePresence MCU, Cisco TelePresence Server, Cisco: ACI Application, Cisco: ACI Endpoint Group, Cisco: ACI Leaf Switch, Cisco: ACI Pod, Cisco: ACI Root, Cisco: ACI Spine Switch, Cisco: ACI Tenant, Cisco: CCE Admin and Data Server, Cisco: CCE Call Router, and Cisco: CCE Campaign. The 'Unalign Device Dashboards' option is also visible at the bottom of the menu.

Device Dashboard Name	ID	Global Default	Categories	Classes	Devices	Dynamic Apps	Edited By	Last Edited
AWS Account	90	No	0	1	0	1	em7admin	2017-04-13 08:42:33
AWS Auto Scale Group	96	No	0	1	0	1	em7admin	2017-04-13 08:42:36
AWS EBS Instance	92	No	0	1	0	1	em7admin	2017-04-13 08:42:34
AWS EC2 Instance	91	No	0	11	0	1	em7admin	2017-04-13 08:42:34
AWS ELB Instance	95	No	0	1	0	1	em7admin	2017-04-13 08:42:36
AWS OpsWorks Stack	98	No	0	1	0	1	em7admin	2017-04-13 08:42:38
AWS RDS Instance	89	No	0	2	0	1	em7admin	2017-04-13 08:42:33
AWS Redshift Cluster	93	No	0	1	0	1	em7admin	2017-04-13 08:42:35
AWS Redshift Node	94	No	0	1	0	1	em7admin	2017-04-05 10:41:24
AWS SNS Topic	88	No	0	1	0	1	em7admin	2017-04-13 08:42:33
AWS SQS Instance	97	No	0	1	0	1	em7admin	2017-04-13 08:42:36
Cisco TelePresence Conductor	125	No	0	1	0	0	em7admin	2017-04-10 01:30:57
Cisco TelePresence MCU	126	No	0	1	0	0	em7admin	2017-04-10 01:30:57
Cisco TelePresence Server	127	No	0	1	0	0	em7admin	2017-04-10 01:30:57
Cisco: ACI APIC	72	No	0	1	0	0	em7admin	2017-04-05 10:06:16
Cisco: ACI Application	75	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Endpoint Group	76	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Leaf Switch	73	No	1	0	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Pod	71	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Root	77	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Spine Switch	74	No	1	0	0	0	em7admin	2017-04-05 10:06:21
Cisco: ACI Tenant	78	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: CCE Admin and Data Server	109	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: CCE Call Router	107	No	0	1	0	0	em7admin	2017-04-05 10:06:21
Cisco: CCE Campaign	113	No	0	1	0	0	em7admin	2017-04-05 10:06:21

- Click the **[Go]** button.
- 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.

Using Custom Attributes

Overview



Custom Attributes are name-value pairs. You can use custom attributes to add custom descriptive fields to assets, devices, interfaces, themes, and vendors. In the 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.

This chapter will describe how you can create and use custom attributes for devices.

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

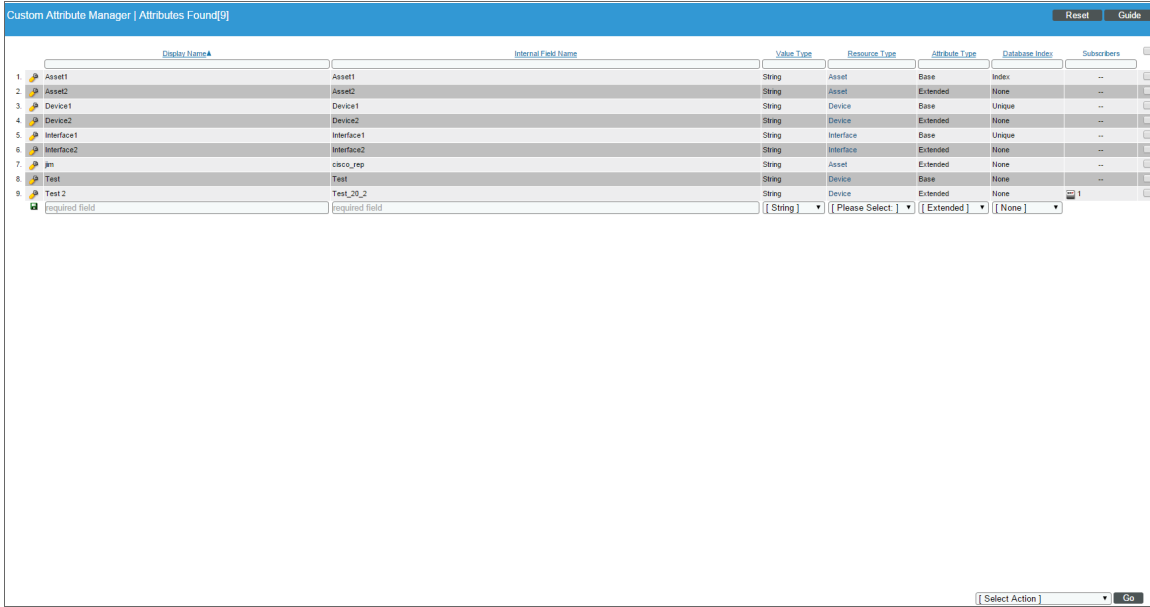
- To view a pop-out list of menu options, click the menu icon (.
- To view a page containing all of the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

Viewing the List of Custom Attributes	620
Creating Custom Attributes	624
Custom Attributes in the ScienceLogic API	626
Using a Dynamic Application to Create and/or Populate Custom Attributes	626

Viewing the List of Custom Attributes

The **Custom Attribute Manager** page (System > Manage > Custom Attributes) displays a list of all the existing custom attributes created through the user interface.



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.** 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.** 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.** 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.** 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.

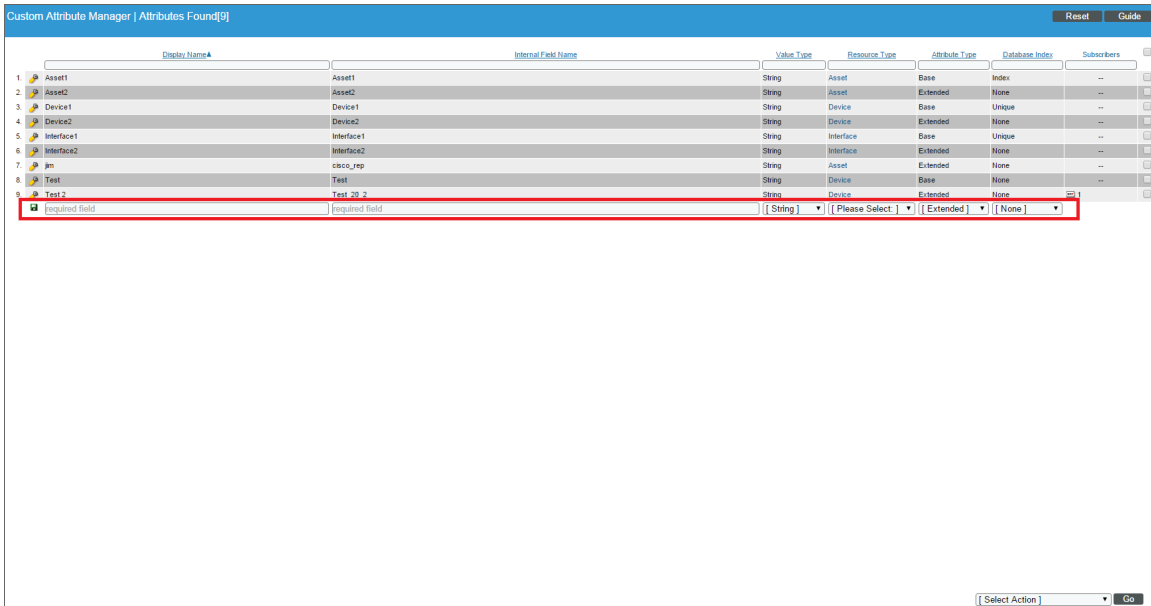
Creating Custom Attributes


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 chapter [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.

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 a Dynamic 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:

The screenshot shows the configuration interface for a collection object. Key fields include:

- Object Name:** dyn_val
- XML Tags:** <tags><tag><shape>
- Class Type:** [10 Config Character]
- String Type:** [Standard]
- Custom Attribute:** Dynamic Value
- dyn_key:** dyn_key
- Group / Usage Type:** [Group 1] [Standard]
- Asset / Form Link:** [None] [None]
- Inventory Link:** [Disabled]
- Change Alerting:** [Disabled]
- Table Alignment:** [Left]
- Hide Object:**

At the bottom, there is a **Save** button and a **Disable Object Maintenance** checkbox.

- **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*.

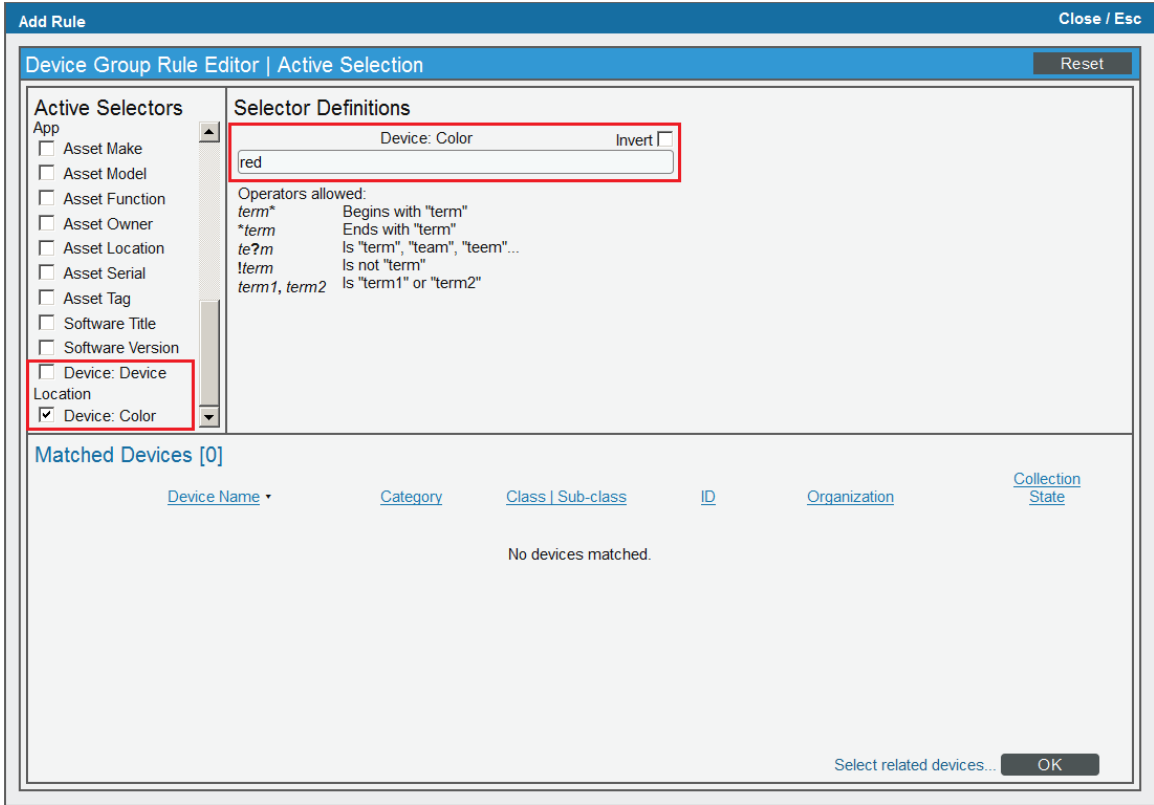
Using Custom Attributes to Define Device Groups

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.



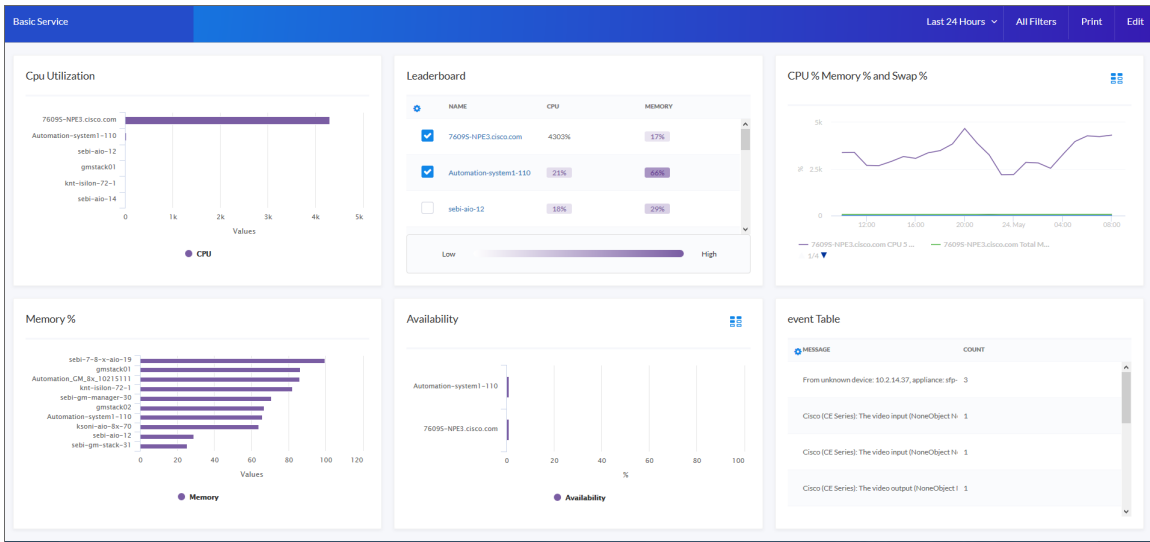
In the example above, we selected the custom attribute *Device:Color* and specified the value *red*. Our device group will include only devices that have the value *red* assigned to the *Device:Color* custom attribute.

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 'New Widget Configuration' dialog box shows the configuration for a 'Custom Table' widget. The 'Entity Type' is set to 'Device'. The 'Layout Editor' pane shows a table with columns for Device Name, IP Address, Current State, Organizational Group, Cell, Sub-Class, Avail, Latency, CPU, Mem, Swap, Data Time, Last Poll, Date Added, Color, and Device Location. The 'Color' and 'Device Location' columns are highlighted with red boxes, indicating they are custom attributes.

ID	Device Name	IP Address	Current State	Organizational Group	Cell	Sub-Class	Avail	Latency	CPU	Mem	Swap	Data Time	Last Poll	Date Added	Color	Device Location
1	em7_db	10.0.9.147	Healthy	System	CUG116	ScienceLo	--	--	--	--	--	2015-05-08 09:00	2015-04-07	--	--	--
2	em7_js	10.0.9.227	Healthy	System	CUG116	ScienceLo	--	--	--	--	--	2015-05-08 12:44	2015-04-07	--	--	--
3	em7	10.0.9.145	Healthy	System	CUG116	ScienceLo	--	--	--	--	--	2015-05-08 09:00	2015-04-07	--	--	--
4	em7_io	10.0.9.146	Healthy	System	CUG116	ScienceLo	--	--	--	--	--	2015-05-08 09:00	2015-04-07	--	--	--
5	MiuxkeDB	10.0.9.144	Healthy	System	CUG116	ScienceLo	--	--	--	--	--	2015-05-08 09:00	2015-04-07	--	--	--

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 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010