ScienceLogic

Monitoring Device Infrastructure Health

SL1 version 12.1.0

Table of Contents

Introduction 8
What is a Device? 9
What is a Dynamic Application? 9
What is the SL1 Agent? 10
Overview of Data Collection 11
What is Collection? 11
What are Monitoring Policies? 12
What are Collection Processes? 13
What Vital Metrics Can SL1 Collect? 14
Metric Descriptions 14
Supported Data Collection Methods for Monitoring Windows 16
Supported Data Collection Methods for Monitoring Linux 16
Viewing Details in the Device Reports Panel 18
What is the Device Reports Panel? 18
Device Dashboards in the Device Summary Page 21
The Default Device Summary Page 23
Read-Only Information 24
Vitals 25
Tickets and Events 27
Elements 27
Monitors 28
System Component Utilization 29
Hourly Interface Usage 29
Shortcut Keys for Device Reports Panel 30
Monitoring Device Availability and Latency 32
Availability 32
Configuring Availability Monitoring on a Device 33
Defining Availability Thresholds 35
Configuring Availability for Component Devices 36
Critical Ping 38
Latency 40
Configuring Latency Monitoring on a Device 40
Defining Latency Thresholds 41
Viewing Reports on Device Availability and Device Latency 42
Viewing Configuration & Journal Data 43
Viewing Device Configuration Data 43
Generating a Device Configuration Report 44
Viewing Device Configuration Data in the Classic SL1 User Interface 44
Selecting Device Configuration Data to View in the Classic SL1 User Interface 45
Generating a Device Configuration Report in the Classic SL1 User Interface 46
Viewing Historical Device Configuration Data in the Classic SL1 User Interface 46
Editing the Configuration Dynamic Application 47
Viewing Device Journal Data 48
Viewing Device Journal Data in the Classic SL1 User Interface 48
Searching & Filtering the List of Data 49
Special Characters 51
Selecting Data to View 54
Generating a Report of the Device Journal Data 55
Editing the Journal Dynamic Application 56
Viewing Performance Graphs 57

Features of the Performance Tab 58
Viewing System Vitals for a Device 60
Viewing Availability Reports for a Device 62
Viewing Latency Reports for a Device 65
Viewing a Report on CPU Usage for a Device 67
Changing the Dynamic Application Precedence Settings for CPU and Memory Utilization 69
Viewing a Report on Physical Memory Usage for a Device 71
Viewing a Report on Virtual Memory Usage for a Device 74
Viewing a Report on File System Usage for a Device 76
Viewing Performance Report Graphs on Network Interfaces 80
Default Performance Graph Reports for Network Interfaces 81
Network Utilization Report 82
Network Bandwidth Usage Report 83
Network Bandwidth Usage Report (Stacked) 84
Network Error Report 85
Network Error Report (Percent) 87
CBQoS Reports for Network Interfaces 88
Class Map Overview 90
Match Statements Overview 91
Policing Overview 92
Queueing Overview 93
Set Overview 94
Traffic Shaping Overview 96
WRED Overview 98
Viewing Reports about DNS Servers and DNS Records for a Device 100
Viewing Reports on an Email Round-Trip Monitoring Policy 102
Viewing Reports on a SOAP or XML Transaction Policy 104
Viewing Availability Reports for a Single System Process on a Device 110
Viewing Port Availability Reports for a Single Device 113
Viewing Reports for a Web Content Policy 114
Viewing Availability Reports for a Single Windows Service on a Device 121
Monitoring Networks 124
IPv4 Networks 125
Viewing the List of IPv4 Networks 126
Filtering the List of Networks 128
Browsing a Network 130
Viewing Used and Unused IP Addresses in a Network 131
Viewing Devices Aligned with a Network 131
Viewing Interfaces Aligned with a Network 131
Viewing a Map of a Network 132
Generating a Report for a Network 132
Defining a New Network 133
Merging One or More Networks 134
Synchronizing One or More Networks 135
Editing a Network's Properties 136
Performing Dynamic Discovery for a Network 136
Creating a Ticket About a Network 137
Deleting One or More IPv4 Networks 138
Monitoring Network Interfaces 139
Discovering Interfaces 139
Viewing a List of All Interfaces Discovered by SL1 140
Viewing Interfaces for a Single Device 143

Viewing Interfaces for a Single Device in the Classic User Interface 145
Global Settings that Affect Interfaces 148
Behavior Settings 149
Interface Threshold Defaults 150
Quality of Service Threshold Defaults 158
Defining Interface Monitoring Policies and Thresholds 162
Defining a Detailed Monitoring Policy for a Single Interface 163
Defining Thresholds for a Single Interface 169
Defining Monitoring Settings for Multiple Interfaces 173
Class-Based Quality of Service (CBQoS) 178
Viewing the List of Discovered CBQoS Objects 178
Filtering the List of Quality of Service (QoS) Objects 180
Editing Thresholds for a Quality of Service (QoS) Object 181
Concurrent Network Interface Collection 184
Enabling Concurrent Network Interface Collection for All Interfaces 185
Configuring Concurrent Network Interface Collection for a Collector Group 185
Additional Configuration for Concurrent Network Interface Collection 186
Enabling PDU Packing 186
Increasing the Maximum Number of PDUs in a Single SNMP Request 186
Troubleshooting Concurrent Network Interface Collection 187
Viewing Performance Graphs and Reports About Interfaces 187
Generating a Report for a Single Network Interface 187
Generating a Report for Multiple Network Interfaces 189
Hardware and Software 191
Viewing the List of All Discovered Hardware Components 192
Filtering the List of Hardware Components 194
Generating a Report for Multiple Hardware Components on Multiple Devices 195
Hiding a File System 195
Changing Thresholds for One or More File Systems 196
Viewing the List of All Discovered Software Titles 197
Filtering the List of Software Titles 198
Viewing a List of Software Titles for a Single Device 199
Viewing a List of Software Titles for a Single Device in the Classic SL1 User Interface 200
Filtering the List of Software 202
Generating a Report on All Software on All Devices 202
Generating an Exclusion Report for a Single Software Title 204
Viewing Device Logs 206
Viewing Device Logs and Messages 206
Viewing Device Logs and Messages in the Classic SL1 User Interface 208
Viewing Events Associated with a Log Entry 210
Creating an Event Policy from a Log Entry 211
Redirecting Log Data from One Device to Another 212
Viewing Logs for All Devices 214
Monitoring SSL Certificates 215
System Settings that Affect SSL Certificates in SL1 216
Viewing the List of SSL Certificates 217
Filtering the List of SSL Certificates 219
Monitoring Domain Servers and DNS Records 220
Viewing the List of Domain Name Monitoring Policies 221
Filtering the List of Domain Name Monitoring Policies 222
Defining a Monitoring Policy for a Domain Name 223
Example Policy for Domain Name 225

Defining a Monitoring Policy for a Domain Name in the Classic SL1 User Interface 225
Editing a Monitoring Policy for a Domain Name 226
Editing a Monitoring Policy for a Domain Name in the Classic SL1 User Interface 226
Executing the Domain Name Monitoring Policy 227
Executing the Domain Name Monitoring Policy in the Classic SL1 User Interface 227
Deleting a Domain Name Policy 227
Deleting a Domain Name Policy in the Classic SL1 User Interface 228
Viewing Reports for a Domain Name Monitoring Policy 228
Monitoring Email Round-Trips 229
Required Settings and Configuration 230
Required System Settings in SL1 230
Required Configuration on the External Email Client 231
How SL1 Collects and Calculates Round-Trip Time 232
Viewing the Email Round-Trip Monitoring Policies 232
Filtering the List of Email Round-Trip Monitoring Policies 233
Defining an Email Round-Trip Monitoring Policy 234
Example Email Round-Trip Monitoring Policy 236
Defining an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface 237
Events for Email Round-Trip Policies 237
Editing an Email Round-Trip Monitoring Policy 238
Editing an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface 238
Deleting an Email Round-Trip Monitoring Policy 239
Deleting an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface 239
Viewing Reports on an Email Round-Trip Monitoring Policy 240
Monitoring Ports 241
What is a Port? 242
Port Security 242
Port Availability 242
System Settings that Affect Port Availability Monitoring 243
Viewing the List of TCP/IP Port Monitoring Policies 244
Filtering the List of TCP/IP Port Monitoring Policies 245
Defining a Port Monitoring Policy 245
Example Policy for TCP/IP Port Availability 247
Defining a Port Monitoring Policy in the Classic SL1 User Interface 248
Editing a Port Monitoring Policy 248
Editing a Port Monitoring Policy in the Classic SL1 User Interface 248
Executing a Port Monitoring Policy 249
Executing a Port Monitoring Policy in the Classic SL1 User Interface 250
Deleting a Port Monitoring Policy 250
Deleting a Port Monitoring Policy in the Classic SL1 User Interface 250
Viewing a List of All TCP/IP Ports 251
Defining a New TCP/IP Port 252
Editing the Properties of a Port 253
Deleting a Port Definition 253
Viewing a List of All Open Ports on All Devices 254
Filtering the List of Network IP Ports 255
Viewing a List of All Open Ports on a Single Device 257
Viewing a List of All Open Ports on a Single Device in the Classic SL1 User Interface 258
Viewing Port Availability Reports for a Single Device 259
Monitoring SOAP and XML Transactions 260
Viewing the SOAP/XML Transaction Monitoring Policies 261
Filtering the List of SOAP/XSL Transaction Policies 261

Defining a SOAP/XML Transaction Monitoring Policy 262
Example SOAP/XML Transaction Monitoring Policy 267
Defining a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface 267
Editing a SOAP/XML Transaction Monitoring Policy 268
Editing a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface 268
Executing a SOAP/XML Transaction Monitoring Policy 269
Executing a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface 269
Deleting a SOAP/XML Transaction Monitoring Policy 269
Deleting a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface 270
Viewing Reports on a SOAP/XML Transaction Policy 271
Viewing Raw Data from a SOAP/XML Policy 271
Monitoring System Processes 272
What is a Process? 273
Viewing the List of System Processes on All Devices 273
Filtering the List of System Processes 275
Viewing a List of System Processes on a Single Device 276
Viewing a List of System Processes on a Single Device in the Classic SL1 User Interface 277
Viewing the System Process Monitoring Policies 279
Filtering the List of System Process Monitoring Policies 280
Defining a System Process Monitoring Policy 281
Example Policy for a System Process 284
Defining a Monitoring Policy for a System Process in the Classic SL1 User Interface 285
Editing a System Process Monitoring Policy 285
Editing a Monitoring Policy for a System Process in the Classic SL1 User Interface 286
Executing a System Process Monitoring Policy 286
Executing a System Process Monitoring Policy in the Classic SL1 User Interface 287
Deleting a System Process Monitoring Policy 287
Deleting a System Process Monitoring Policy in the Classic SL1 User Interface 287
Generating a Report on Multiple System Processes 288
Generating an Exclusion Report for a Single System Process 290
Viewing Reports for a System Process Policy 291
Monitoring Web Content 292
Viewing the Web Content Monitoring Policies 293
Filtering the List of Web Content Monitoring Policies 294
Defining a Web Content Policy 295
Example Web Content Policy 300
Defining a Web Content Policy in the Classic SL1 User Interface 300
Editing a Web Content Policy 301
Editing a Web Content Policy in the Classic SL1 User Interface 301
Executing the Web Content Monitoring Policy 302
Executing the Web Content Monitoring Policy in the Classic SL1 User Interface 302
Deleting a Web Content Monitoring Policy 302
Deleting a Web Content Monitoring Policy in the Classic SL1 User Interface 303
Viewing Reports on a Web Content Policy 303
Viewing ASCII Page Content 304
Viewing the Monitored Website 305
Monitoring Windows Services 306
Windows Services Monitoring Policies 307
Viewing the List of Windows Service Monitoring Policies 308
Filtering the List of Windows Service Monitoring Policies 309
Prerequisites and Configuration for Windows Service Monitoring Policies 310
Optional Settings in SL1 310

Required Configuration 311
Defining a Monitoring Policy for Windows Services 311
Defining a Monitoring Policy for Windows Services in the Classic SL1 User Interface 314
Example Policy for Windows Service 315
Editing a Windows Service Monitoring Policy 315
Editing a Windows Service Monitoring Policy in the Classic SL1 User Interface 316
Executing a Windows Service Monitoring Policy 316
Executing a Windows Service Monitoring Policy in the Classic SL1 User Interface 317
Deleting a Windows Service Monitoring Policy 317
Deleting a Windows Service Monitoring Policy in the Classic SL1 User Interface 317
Viewing a List of All Windows Services 318
Filtering the List of Windows Services 320
Viewing a List of Windows Services on a Single Device 321
Viewing a List of Windows Services on a Single Device in the Classic SL1 User Interface 322
Generating and Viewing Reports about Windows Services 324
Generating a Report on Multiple Windows Services 325
Generating an Exclusion Report for a Single Windows Service 326
Viewing Reports about Windows Services 327
Grouping Dynamic Application Data Using Collection Labels 328
What are Collection Labels and Collection Groups? 329
Viewing the List of Collection Labels 329
Filtering the List of Collection Labels 330
Special Characters 331
Creating a Collection Group 335
Creating a Collection Label 335
What is Normalization? 336
What are Duplicates and How Does SL1 Manage Them? 338
What is Precedence? 339
Aligning a Presentation Object with a Collection Label 339
Viewing and Managing the List of Presentation Objects Aligned with a Collection Label 341
Viewing and Editing Duplicate Presentation Objects by Collection Label 345
Viewing and Managing the List of Devices Aligned with a Collection Label 347
Editing Duplicate Presentation Objects by Device 349
Editing Duplicate Presentation Objects for a Single Device 351
Editing a Collection Label 352
Deleting a Collection Label 353
Viewing Reports About Collection Labels on a Single Device 353
Viewing Dashboards About Collection Labels 354

Chapter 1

Introduction

Overview

This manual describes the data that SL1 collects from monitored devices, how to configure monitoring policies to collect that data, and how SL1 displays the data in the user interface.

> **NOTE:** For information about how SL1 discovers devices, or how to configure and manage those devices in SL1 after they have been discovered, see the manual ***Device Management***.

For more information about infrastructure monitoring, watch the video at https://sciencelogic.com/product/resources/infrastructure-monitoring-in-the-digital-first-world.

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

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

This chapter covers the following topics:

What is a Device? 9
What is a Dynamic Application? 9
What is the SL1 Agent? 10

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.

For more information about managing devices in SL1, see the ***Device Management*** manual.

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 the SL1 Agent?

The ***SL1 agent*** is a program that you can install on a device monitored by SL1. There is a Windows agent and a Linux agent. The agent collects data from the device and pushes that data back to SL1.

Similar to a Data Collector or Message Collector, the agent collects data about infrastructure and applications.

You can configure an agent to communicate with either the Message Collector or the Compute Cluster.

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

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 covers the following topics:

What is Collection? *11*
What Vital Metrics Can SL1 Collect? *14*

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.

SL1 uses the following methods for collection:

- Dynamic Applications use collection processes to collect data.
- Monitoring Policies for devices also trigger collection. These polices 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

> **NOTE:** For more information about how SL1 manages devices and collects data, see the ***Device Management*** manual.

What are 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 or email). Periodically, SL1 sends a request and some data, and then examines the result of the transaction and compares it to a specified expression match.
- ***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 the 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 from the **[Monitors]** tab of the **Device Investigator**, the **Device Administration** panel, or the pages in the Registry > Monitors section.

What are Collection Processes?

Unlike discovery, collection tasks run at scheduled intervals throughout the day. Collection tasks collect the types of data described below. The interval specified is the default interval and can be modified.

- Device availability and device latency (based on the port through which SL1 communicates), every five minutes.
- CDP relationships between devices, every two hours.
- LLDP relationships between devices, every two hours.
- Critical device availability (if enabled, based on ping to specified port), every 5 seconds, 30 seconds, 60 seconds or 120 seconds (defined by user).
- Critical port availability (if enabled, based on ping to specified port), every 5 seconds, 30 seconds, 60 seconds or 120 seconds (defined by user).
- DNS availability based on DNS-monitoring policies, every five minutes.

- Data specified in Dynamic Applications. Collection tasks retrieve data from each aligned device, at the frequency specified in the Dynamic Application.
- Email round-trip statistics based on Email-monitoring policies, every five minutes.
- File system information, every five minutes.
- File system inventory, every two hours.
- Bandwidth usage on managed interfaces, every minute, 5 minutes, 10 minutes, 15 minutes, 30 minutes, 60 minutes, or 120 minutes (defined by user).
- Layer-3 relationships between devices, every two hours.
- List of all discovered system processes on all discovered devices, every two hours.
- Availability of system processes based on process-monitoring policies, every five minutes.
- List of all discovered Windows services on all discovered devices, every two hours.
- Availability of Windows services based on service-monitoring policies, every five minutes.
- SNMP details for each discovered device, every five minutes.
- Availability of ports based on port-monitoring policies, every five minutes.
- Layer-2 relationships between devices, every hour.
- Virtual machine relationships between devices, every hour.
- Availability of web content based on web content-monitoring policies, every five minutes.
- Web-transaction statistics based on a SOAP/XML-monitoring policy, every five minutes.
- If the SL1 agent is installed, SL1 collects a list of all processes running on a device, every five minutes.

For details on collection processes, go to the **[Processes]** tab of the **Device Investigator** or the **Process Manager** page (System > Settings > Admin Processes) and look for processes with names that start with "*Data Collection*".

What Vital Metrics Can SL1 Collect?

The following sections describe the system vitals that can be collected with SL1 and with the SL1 Agent, including definitions of each metric type and the collection methods that are and are not supported for each.

Metric Descriptions

The following table describes the system vital metrics that can be collected with SL1 and the SL1 Agent:

Metric	Type	Description
Availability	Performance	The ability to communicate with the managed entity or device.
File Systems	Configuration	The configuration of the file systems found within a managed entity that can include attributes like name, size, and type.
File Systems	Performance	Time series data associated with file system utilization that can include metrics like free space, size, and usage percentage.
Installed	Configuration	The software found on a managed entity that can include attributes like name,

Metric	Type	Description
Software		version, and installation date.
Network Interfaces	Configuration	The configuration of the network interface found within a managed entity that includes attributes like MAC address, IP address, position, and speed.
Network Interfaces	Performance	Time series data associated with physical memory utilization that includes metrics like inbound and outbound utilization, number of errors, and discard and usage percentage.
Physical Memory	Configuration	The configuration of the physical memory found within a managed entity that can include attributes like memory size.
Physical Memory	Performance	Time series data associated with physical memory utilization that can include metrics like memory used.
Ports	Configuration	The ports discovered on a managed entity.
Ports	Performance	Time series data associated with port availability.
Ports (Illicit)	Performance	An analysis of ports. When a port from the illicit port list is found on a managed system, the system will trigger an event indicating an illicit port has been found.
Processes	Configuration	The processes found on a managed entity that can include attributes like name, process ID (PID), and state.
Processes	Performance	Time series data associated with process performance that can include metrics like availability percentage.
Processor	Configuration	The configuration of the processor found within a managed entity that can include attributes like number of cores, processor model, processor speed, cache size, and CPU ID.
Processor	Performance	Time series data associated with processor utilization that can include metrics like CPU idle time, CPU wait time, and overall CPU time.
Restarts	Performance	An analysis of uptime. When uptime is less than 15 minutes, the system triggers an event indicating the system was restarted.
SSL Certificates	Configuration	The certificates found on a managed system.
SSL Certificates	Performance	An analysis of certificate expiration date. The system will trigger an event when certificates are nearing expiration.
Uptime	Performance	The timespan since the managed entity was last initialized.
Virtual Memory (Swap)	Configuration	The configuration of the virtual memory found within a managed entity.
Virtual Memory (Swap)	Performance	Time series data associated with virtual memory utilization.
Windows Services	Configuration	The services found on a managed entity that can include attributes like name and state.
Windows Services	Performance	Time series data associated with service performance that can include metrics like availability percentage.

Supported Data Collection Methods for Monitoring Windows

The following table describes which methods of data collection are supported when running SL1 and the SL1 Agent on monitored Windows systems:

Metric	Type	Agentless			Agent-Based	
		SNMP	WMI	PowerShell	Gen-01	Gen-03
Availability	Performance	Yes	Yes	Yes	Yes	Yes
File Systems	Configuration	Yes	Some	Yes	Some	Yes
File Systems	Performance	Yes	Some	Yes	Some	Yes
Installed Software	Configuration	Yes	No	Yes	No	Yes
Network Interfaces	Configuration	Yes	Some	Yes	Some	Yes
Network Interfaces	Performance	Yes	Some	Yes	Some	Yes
Physical Memory	Configuration	Yes	Yes	Yes	Yes	Yes
Physical Memory	Performance	Yes	Yes	Yes	Yes	Yes
Ports	Configuration	Yes	No	Yes	Yes	No
Ports	Performance	Yes	No	Yes	Yes	No
Ports (Illicit)	Performance	Yes	No	Yes	Yes	No
Processes	Configuration	Yes	Some	Yes	Yes	Yes
Processes	Performance	Yes	No	Yes	Yes	Yes
Processor	Configuration	Yes	Yes	Yes	Yes	Yes
Processor	Performance	Yes	Yes	Yes	Yes	Yes
Restarts	Performance	Yes	No	Yes	Yes	Yes
SSL Certificates	Configuration	Yes	No	No	No	No
SSL Certificates	Performance	Yes	No	No	No	No
Uptime	Performance	Yes	No	Yes	Yes	Yes
Virtual Memory (Swap)	Configuration	Yes	Yes	Yes	Yes	Yes
Virtual Memory (Swap)	Performance	Yes	Yes	Yes	Yes	Yes
Windows Services	Configuration	Yes	Some	Yes	No	Yes
Windows Services	Performance	Yes	Some	Yes	No	Yes

Supported Data Collection Methods for Monitoring Linux

The following table describes which methods of data collection are supported when running SL1 and the SL1 Agent on monitored Linux systems:

Metric	Type	Agentless		Agent-Based	
		SNMP	SSH	Gen-01	Gen-03
Availability	Performance	Yes	Yes	Yes	Yes
File Systems	Configuration	Yes	Yes	Some	Yes
File Systems	Performance	Yes	Yes	Some	Yes
Installed Software	Configuration	Yes	No	No	Yes
Network Interfaces	Configuration	Yes	Yes	Some	Yes
Network Interfaces	Performance	Yes	Yes	Some	Yes
Physical Memory	Configuration	Yes	Yes	Yes	Yes
Physical Memory	Performance	Yes	Yes	Yes	Yes
Ports	Configuration	Yes	Yes	Yes	No
Ports	Performance	Yes	Yes	Yes	No
Ports (Illicit)	Performance	Yes	Yes	Yes	No
Processes	Configuration	Yes	Yes	Yes	Yes
Processes	Performance	Yes	Yes	Yes	Yes
Processor	Configuration	Yes	Yes	Yes	Yes
Processor	Performance	Yes	Yes	Yes	Yes
Restarts	Performance	Yes	Yes	Yes	Yes
SSL Certificates	Configuration	Yes	No	No	No
SSL Certificates	Performance	Yes	No	No	No
Uptime	Performance	Yes	Yes	Yes	Yes
Virtual Memory (Swap)	Configuration	Yes	Yes	Yes	Yes
Virtual Memory (Swap)	Performance	Yes	Yes	Yes	Yes
Windows Services	Configuration	N/A	N/A	N/A	N/A
Windows Services	Performance	N/A	N/A	N/A	N/A

Chapter 3

Viewing Details in the Device Reports Panel

Overview

This chapter describes how to view device details in the Device Reports Panel.

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

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

This chapter covers the following topics:

What is the Device Reports Panel? *18*

Device Dashboards in the Device Summary Page *21*

The Default Device Summary Page *23*

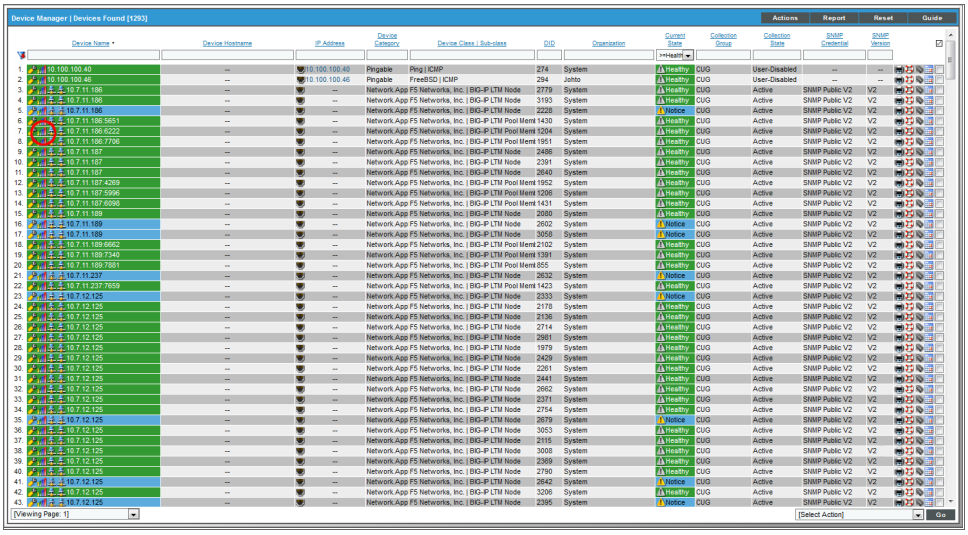
Shortcut Keys for Device Reports Panel *30*

What is the Device Reports Panel?

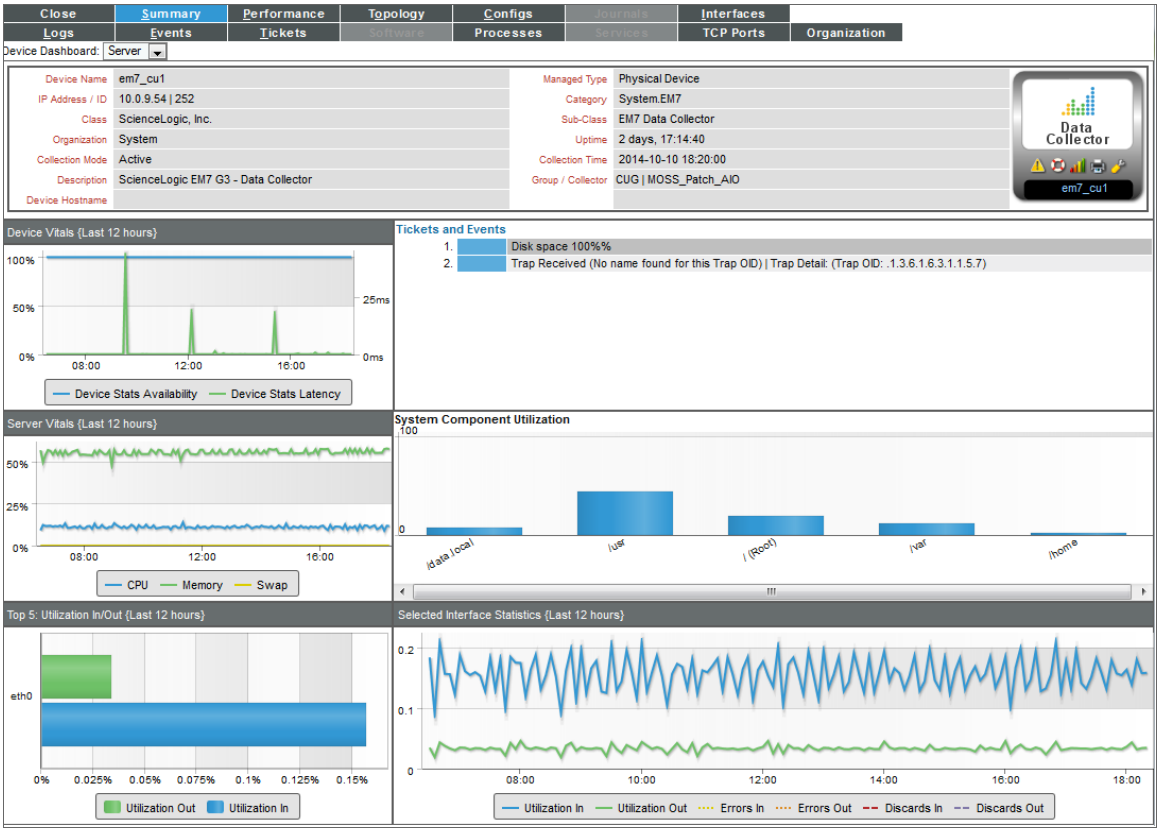
The **Device Reports** panel allows you to view detailed information that SL1 has gathered from each device and view reports generated from that information. The **Device Reports** panel is for viewing information, rather than for administering the device.

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.



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.
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	The **Configuration Report** page displays configuration information collected by Dynamic Applications. All objects of type "config" are included in the **Configuration Report** page. 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. For details on Dynamic Applications and configuration objects, see one of the manuals on ***Dynamic Applications***.
Journals	The **Journal View** page displays journal entry information collected from the device by journal Dynamic Applications. For details on the **Journal View** page, see the ***Snippet Dynamic Application*** manual.
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	The **Viewing Active Events** page displays a list of all events associated with the device. For details on events, see the manual ***Events***.
Tickets	The **Ticket History** page displays a list of all tickets, both open and resolved, associated with the device. For details on tickets and ticket administration, see the manual ***Ticketing***.
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.

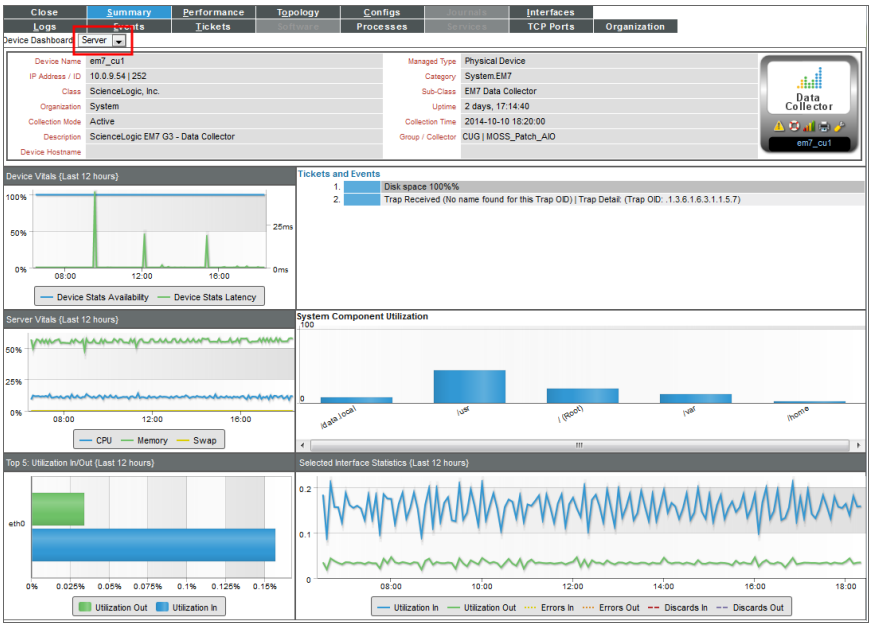
Tab	Description
Services	The **Windows Services** page displays a list of all Windows services enabled on the device.
TCP Ports	The **Port Security** page displays a list of all open ports on a device. Every night, SL1 scans all the ports of each managed device. If any new ports are opened, SL1 adds the port to the list in the **Port Security** page.
Organization	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. For details on organizations and organization administration, see the manual ***Organizations and Users***.
Asset	Leads to the **Asset Properties** page and the **Asset Administration** panel, where you can view and edit the asset record for the device. For details on asset records and asset administration, see the manual ***Asset Management***.

Device Dashboards in the Device Summary Page

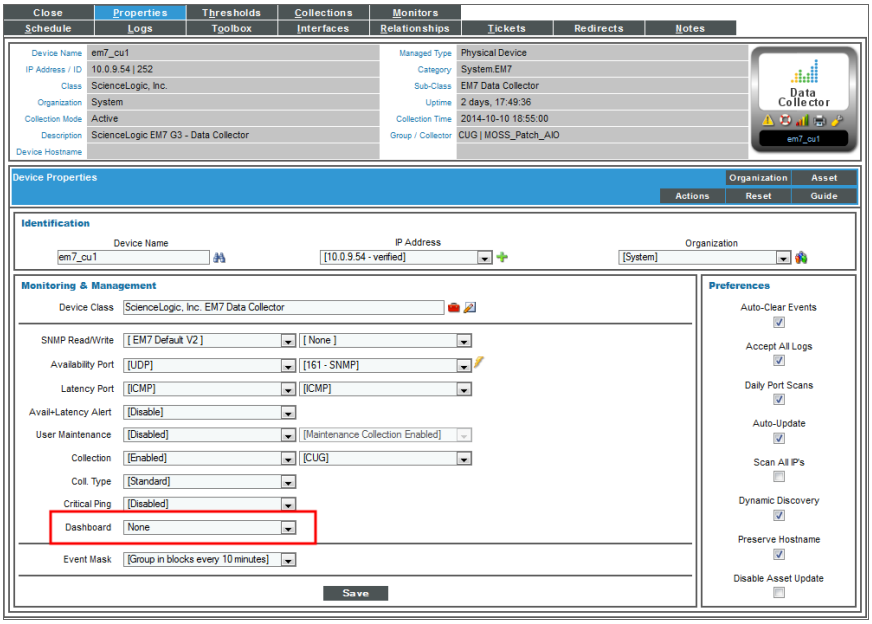
In addition to the default dashboard for a device, you can also view other device dashboards in the **Device Summary** page. The other dashboards that are available for a device are based on the device class and device category assigned to the device and the Dynamic Applications to which the device is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



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 ***Device Management*** manual.

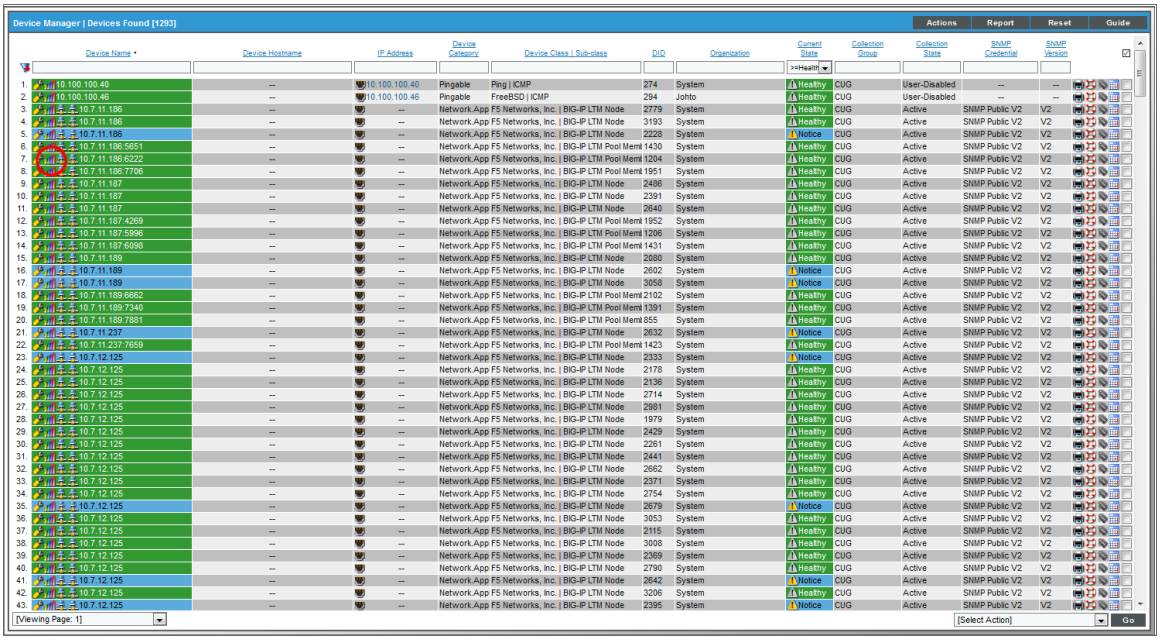
The Default Device Summary Page

This section describes device dashboard that is configured as the global default when SL1is installed. This default device dashboard provides a one-stop overview of a device.

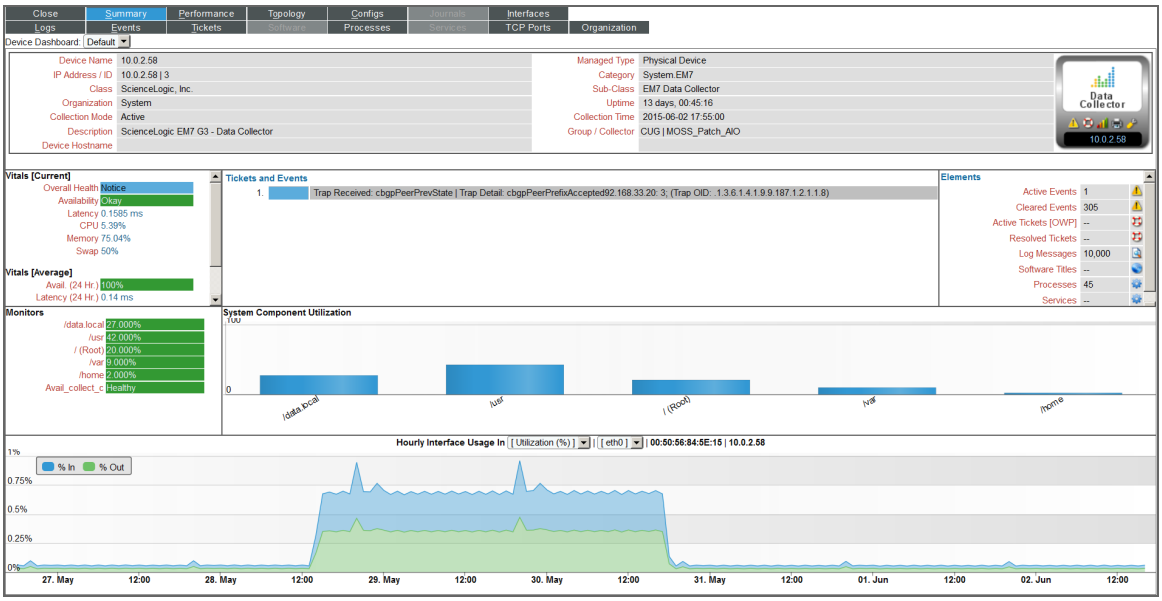
NOTE: The global default dashboard can be changed. The dashboard describes in this section might not be the global default dashboard in your SL1 system.

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

1. Go to the **Device Manager** page (Devices > Device Manager).
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 (along with the tabs for the **Device Reports** panel):



4. 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 in formation 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 the sections on *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 Compute Nodes, 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 Compute Nodes, 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
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

Page or Tab	Shortcut Keys
Device Summary page	Ctrl + Alt + . ("period")
Ticket Editor page	Ctrl + Alt + <Enter>

Chapter 4

Monitoring Device Availability and Latency

Overview

This chapter describes how to monitor device availability and latency.

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

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

This chapter covers the following topics:

Availability *32*

Latency *40*

Viewing Reports on Device Availability and Device Latency *42*

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 SL1 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 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.

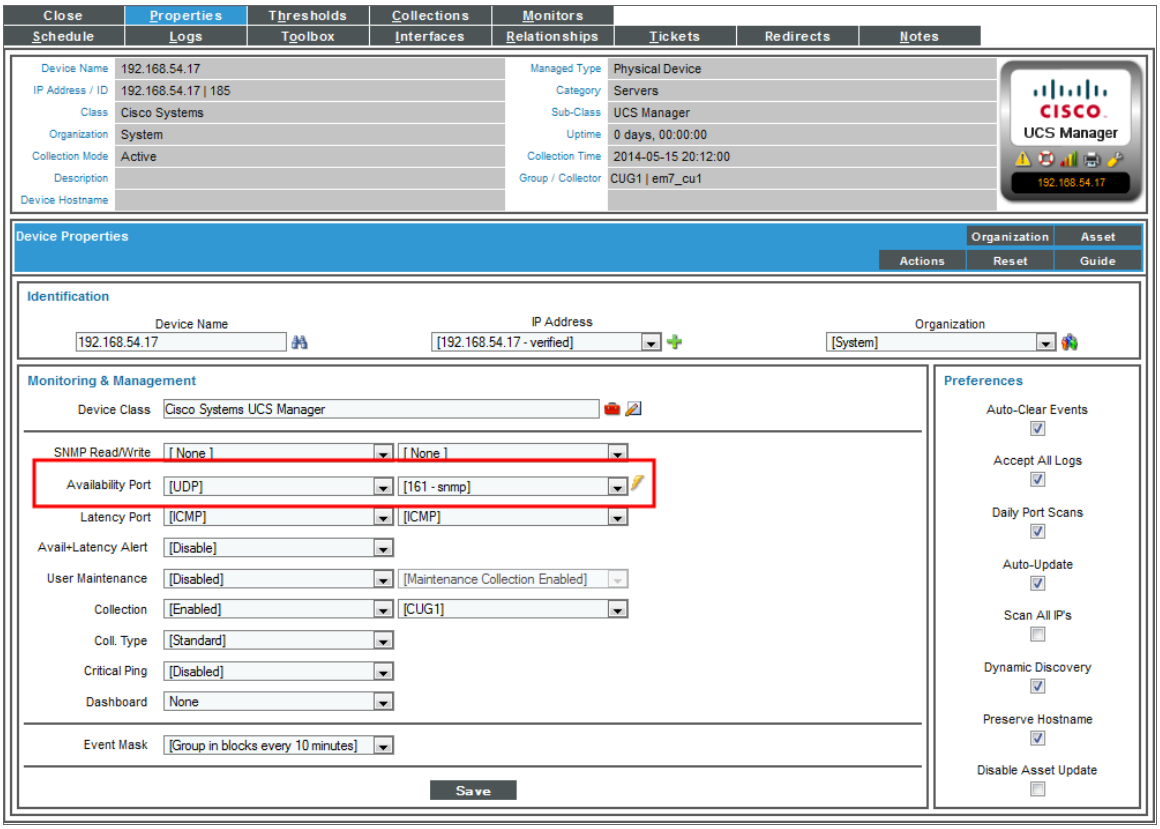
Configuring Availability Monitoring on a Device

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 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 more information, see the section *Configuring Availability for Component Devices*.

To configure availability monitoring 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 configure availability monitoring. Click its wrench icon ( ). The **Device Properties** page displays:



3. 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) that SL1 should monitor to determine if the device is available. The list of ports will contain all the ports discovered by SL1. The data collected from this port will be used in device availability reports. Protocol options include:

     - *TCP*. Availability is based on whether SL1 can connect to the device using the specified TCP port.
     - *ICMP*. Availability is based on whether the device responds to an ICMP ping request from SL1. If you select *ICMP* as the protocol, you can use the ***ICMP Availability Thresholds*** fields in the **Device Thresholds** page to further define how SL1 will test the device's availability.
     - *SNMP*. Availability is based on whether the device responds to an SNMP GET request from SL1.
     - *ScienceLogic Agent*. Availability is based on whether the SL1 Agent is reporting data to SL1. The agent must be installed on the device to use this option.

- ***Avail + Latency Alert***. Specifies how SL1 should respond when the device fails an availability check, a latency check, or 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 the Major event "Device Failed Availability Check: UDP - SNMP". The Minor event "Network Latency Exceeded Threshold: No Response" is rolled up under the availability event.

4. Click **[Save]**.

> **NOTE**: The ***Ping & Poll Timeout (Msec)*** setting in the **Behavior Settings** page (System > Settings > Behavior) affects how SL1 monitors device availability. This field specifies the number of milliseconds the discovery tool and availability polls will wait for a response after pinging a device. After the specified number of milliseconds have elapsed, the poll will timeout.

Defining Availability Thresholds

SL1 allows you to define global Availability Thresholds that apply to all devices and device-specific Availability Thresholds that apply to 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 ***Device Management*** manual.

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.

Configuring Availability for Component Devices

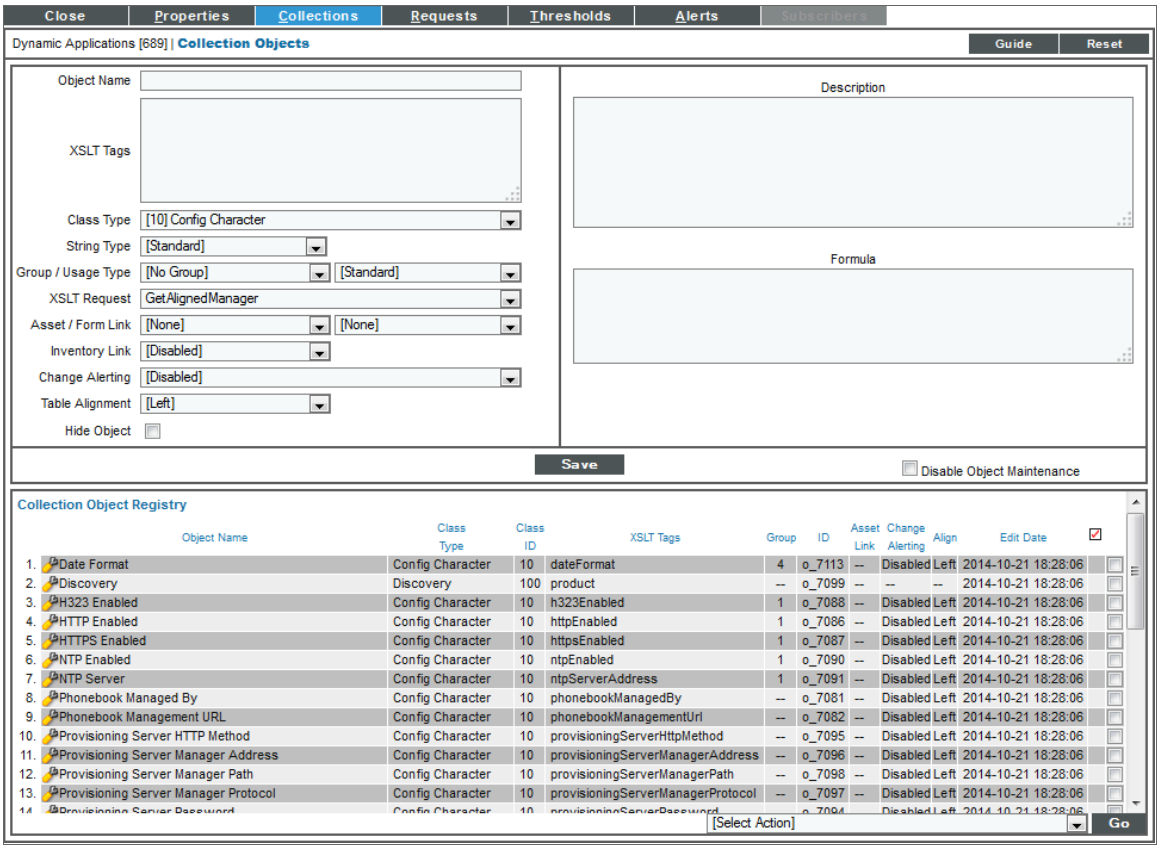
Dynamic Applications that create component devices have the ***Component Mapping*** checkbox selected in the **Dynamic Applications Properties Editor** page and also include the ***Component Identifiers*** field.

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. Click 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. Click the **[Collections]** tab.



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. Click **[Save]**. SL1 will now monitor availability and graph availability statistics for the component devices aligned with the Dynamic Application.

Critical Ping

Critical Ping is a tool that allows you to monitor a device as frequently as every five seconds. If the device does not respond, SL1 creates an event. You can enable or disable critical ping for a device from its **Device Properties** page (Registry > Devices > wrench icon).

SL1 does not use critical ping 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 (System > Settings > Admin Processes).

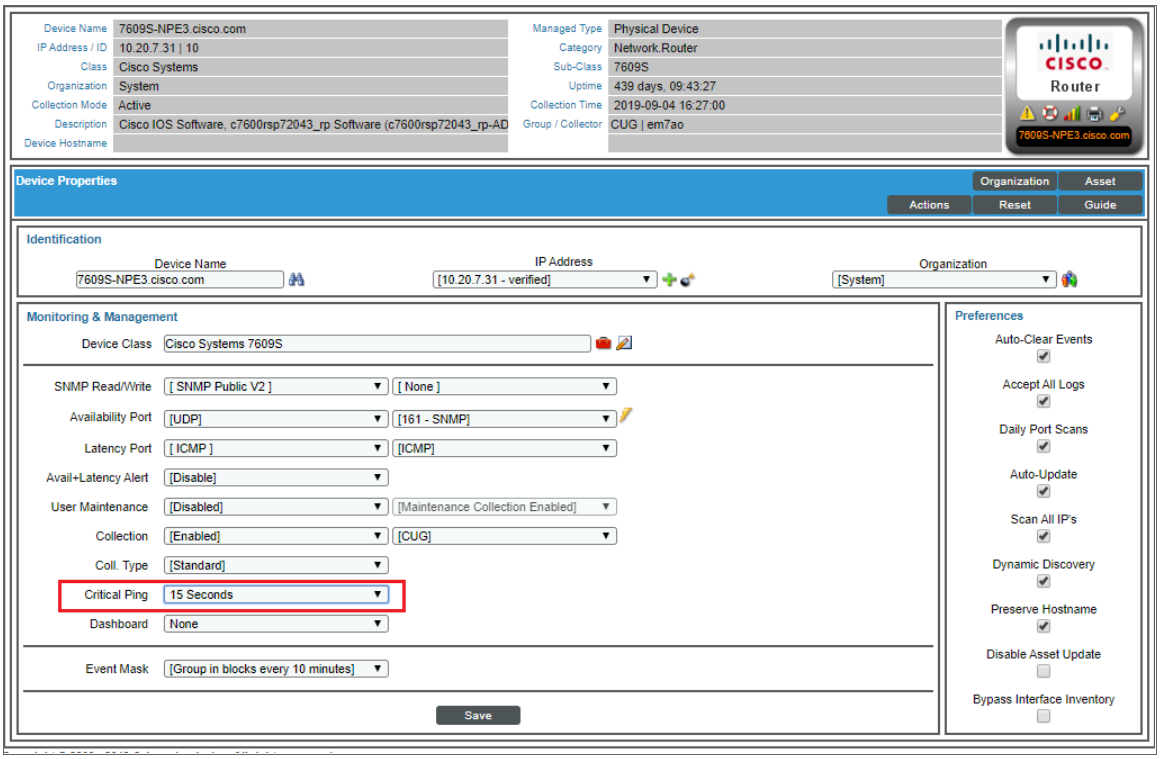
Critical Ping uses the following global default values:

- ***Ping Count***. This field specifies the number of packets that should be sent during each critical ping. The default value is "1".
- ***Required Ping Percentage***. This field specifies the percentage of packets that must be returned during a critical ping before SL1 considers the device available. The default value is "100%".
- ***Packet Size***. This field specifies the size of each packet, in bytes, that is sent during each critical ping. The default value is "56 bytes".

To adjust these global values or to allow Critical Ping to inherit the per-device values for ICMP Availability Thresholds defined in the in the **Device Thresholds** page (Registry > Devices > Device Manager > wrench icon > Thresholds), contact ScienceLogic Customer Support.

To define critical ping 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 configure availability monitoring. Click its wrench icon ( ). The **Device Properties** page displays:



3. In the **Device Properties** page, edit the following fields:

- ***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 (System > Settings > Admin Processes).

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*.

TIP: You might experience some performance issues if you have a large number of devices using critical ping on a short polling interval. If you have a large number of devices and are experiencing a delay in events being generated for a critical ping outage, try increasing the interval time.

4. Click **[Save]**.

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).

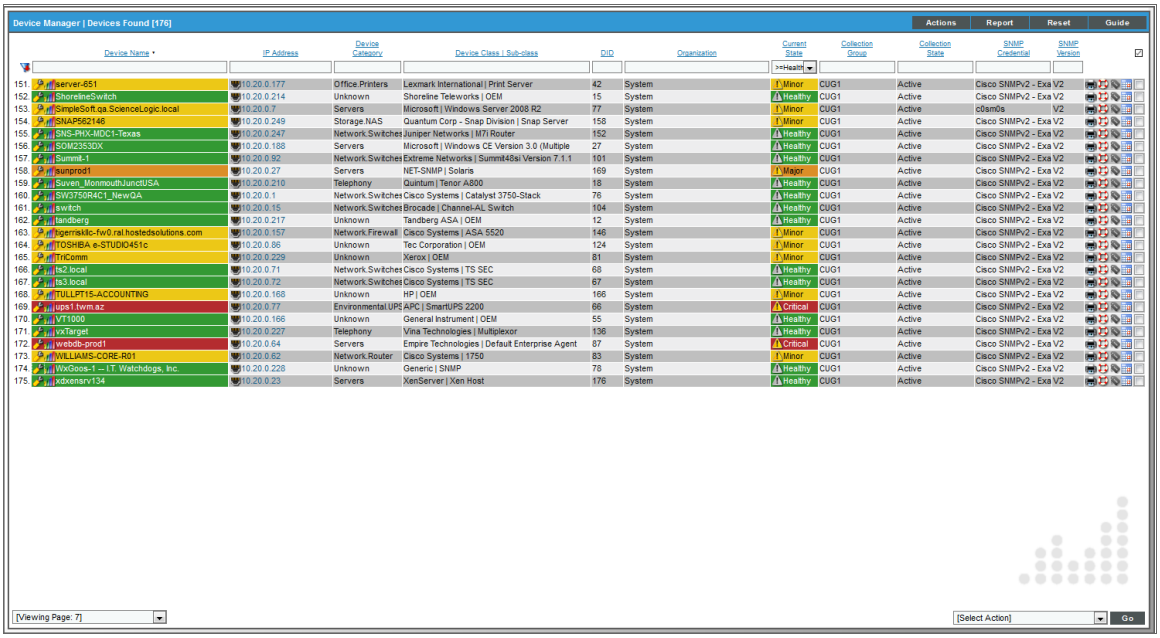
SL1 uses ports to monitor a device's latency. You specify which ports to use for device latency on the **[Settings]** tab of the **Device Investigator** page (or the **Device Properties** page in the classic SL1 user interface).

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).



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 ***Device Management*** manual.

Viewing Reports on Device Availability and Device Latency

See the section on *Viewing Performance Graphs* for information and examples of reports for device availability and device latency.

Chapter 5

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 covers the following topics:

Viewing Device Configuration Data *43*
Viewing Device Journal Data *48*

Viewing Device Configuration Data

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

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.

> **NOTE:** Only those Dynamic Applications that have collected data will appear on the **Configs** tab.

The data displayed on this tab is read-only.

Generating a Device Configuration Report

On the **Device Investigator** page, you can generate a detailed report on the configuration data for that device.

To generate a device configuration report:

1. On the **Device Investigator** page, click the **[Report]** button in the top navigation bar. The **Device Report** modal appears.
2. From the ***Select Type*** drop-down, select *Config*.
3. In the ***Select Format*** drop-down, select the format for the report. Options include *HTML*, *PDF*, *DOC*, *XLS*, or *CSV*.
4. Click **[Create Report]** to generate the report.

Viewing Device Configuration Data in the Classic SL1 User Interface

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.

You can define the layout of the **Configuration Report** page in the **Collection Objects** page for the Dynamic Application. In the **Collection Objects** page, you can use the ***Group*** field and the ***Table Alignment*** fields to define which objects will be grouped together, and which table each object will appear in.

You can enable change detection for an object in the in the **Collection Objects** page for the Dynamic Application, in the ***Change Alerting*** field. If an object's value has changed, it will be highlighted in red in 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.

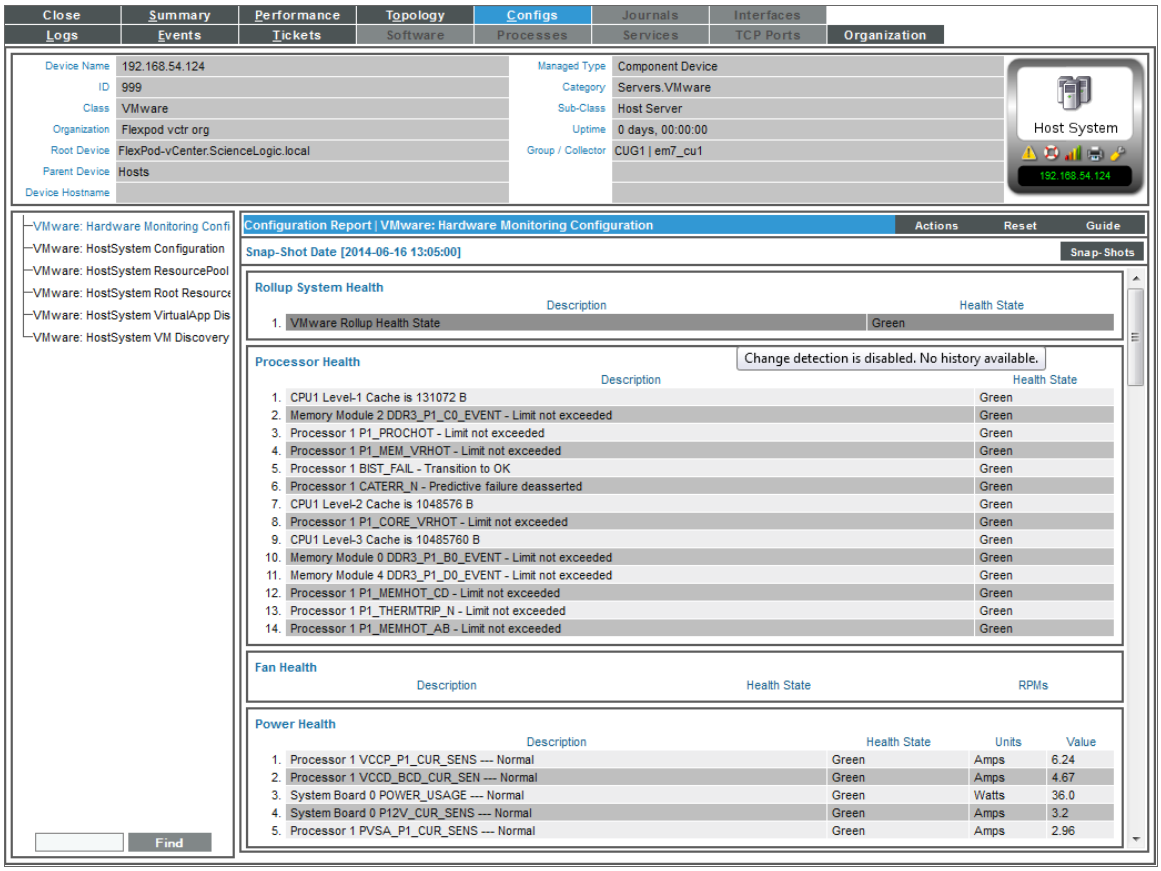
For more information about configuring the table layout and change detection for a configuration Dynamic Application, see the *Collection Objects* chapter in the ***Dynamic Application Development*** manual.

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 and select its bar graph icon ( ).
3. In the **Device Administration** panel, select the **[Configs]** tab. The **Device Configuration** page appears:



Selecting Device Configuration Data to View in the Classic SL1 User Interface

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.

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, where you can view all the values collected from the device for the selected object.

Generating a Device Configuration Report in the Classic SL1 User Interface

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.

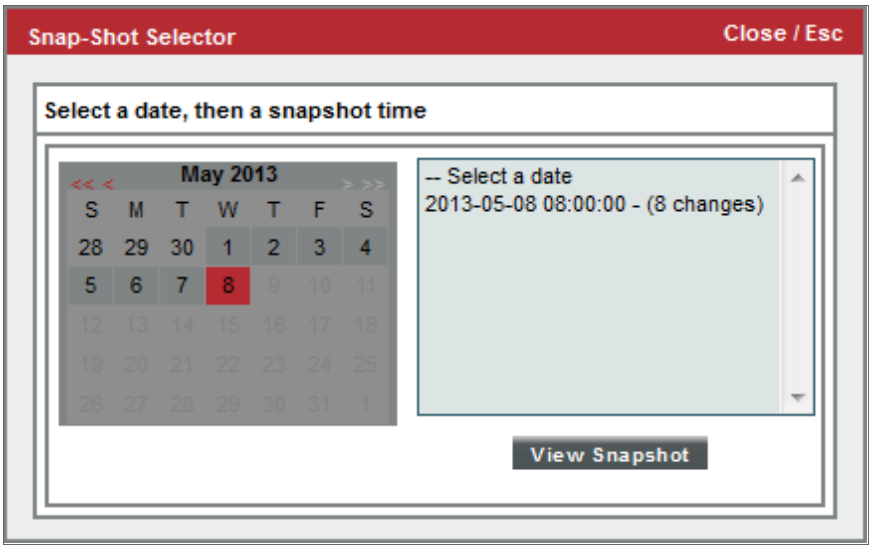
Viewing Historical Device Configuration Data in the Classic SL1 User Interface

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 Configuration Dynamic 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:

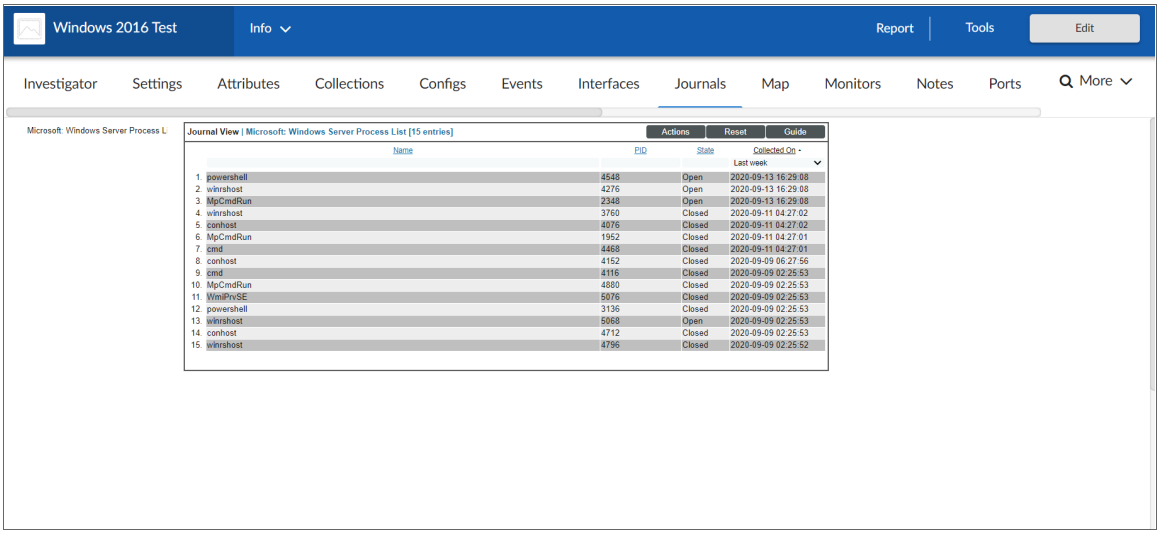
1. In the **Configuration Report** page, in the Navigation Bar (left pane), select the Dynamic Application you want to view and edit.

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.

Viewing Device Journal Data

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



All information from journal Dynamic Applications is included on the **[Journals]** tab.

Journal Dynamic Applications collect and store data in log format. Collected data is stored as a series of journal entries, each entry representing a "log". For example, a journal Dynamic Application might collect telephone call records, where each journal entry represents a single call, or it might collect system access records, where each journal entry represents a user session.

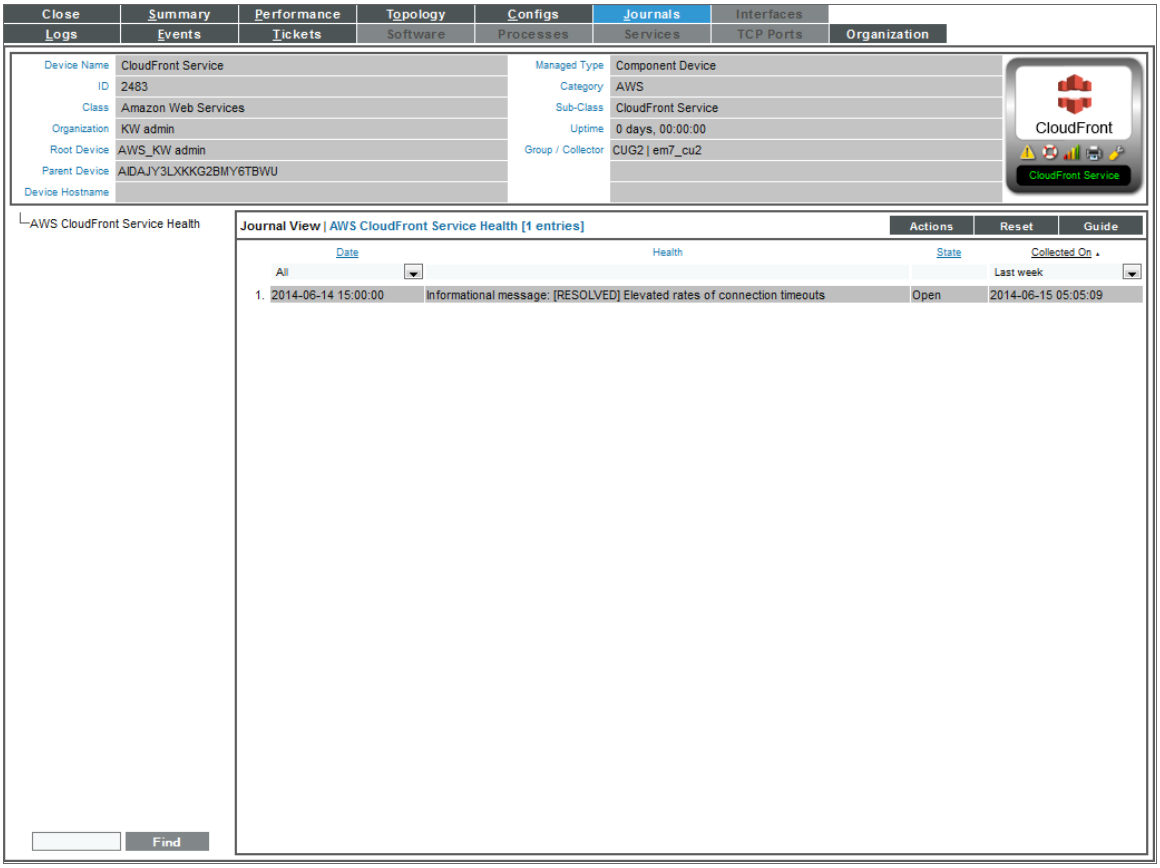
NOTE: For more information about journal Dynamic Applications, see the chapter on "Journal Dynamic Applications" in the ***Snippet Dynamic Application Development*** manual.

Viewing Device Journal Data in the Classic SL1 User Interface

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 and select its bar graph icon ( ).
3. In the **Device Reports** panel, select the **[Journals]** tab. The **Journal View** page appears:



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:

NOTE: You can also use the "!" character in combination with the arithmetical 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.

Examples

- "!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".
- "aio$". Matches only text that ends with "aio".
- " ^ shu". Matches only text that begins with "shu".
- " ^ silo$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contains the characters "silo".
- "! ^ silo". Matches only text that does not start with "silo".
- "!0$". Matches only text that does not end with "0".
- "! ^ silo$". Matches only text that is not the exact text "silo", with no characters before or after.
- "! ^ ". Matches null values, typically represented as "--" in most pages.
- "!$". Matches null values, typically represented as "--" in most pages.
- "! ^ $". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".

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

Selecting Data to View

If one or more journal Dynamic Applications are associated with the device, the **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface) will display that list of Dynamic Applications on the left side of the page.

When you select a Dynamic Application on the left side of the page, the right pane displays data collected from the device by the selected Dynamic Application.

The **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface) 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 **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface) 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.

Generating a Report of the Device Journal Data

You can generate a report about the data in the **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface).

To generate a report about the a device's journal data:

1. Go to the **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface).
2. In the left NavBar, select the Dynamic Application from which you want to generate a report.
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. Click the **[Actions]** button and then select *Generate Report*.
5. The **Export current view as a report** page displays. Select the output format for the report, optionally select if SL1 must force the browser to save the file to disk, and then click **[Generate]**.

Editing the Journal Dynamic Application

From the **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface), 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 journal Dynamic Application:

1. Go to the **[Journals]** tab of the **Device Investigator** (or the **Journal View** page in the classic SL1 user interface).
2. 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, click the **[Actions]** button and then select *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 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 covers the following topics:

Features of the Performance Tab 58
Viewing System Vitals for a Device 60
Viewing Availability Reports for a Device 62
Viewing Latency Reports for a Device 65
Viewing a Report on CPU Usage for a Device 67
Viewing a Report on Physical Memory Usage for a Device 71
Viewing a Report on Virtual Memory Usage for a Device 74
Viewing a Report on File System Usage for a Device 76
Viewing Performance Report Graphs on Network Interfaces 80
Viewing Reports about DNS Servers and DNS Records for a Device 100
Viewing Reports on an Email Round-Trip Monitoring Policy 102
Viewing Reports on a SOAP or XML Transaction Policy 104

Viewing Availability Reports for a Single System Process on a Device *110*
Viewing Port Availability Reports for a Single Device *113*
Viewing Reports for a Web Content Policy *114*
Viewing Availability Reports for a Single Windows Service on a Device *121*

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 section.

- *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.

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

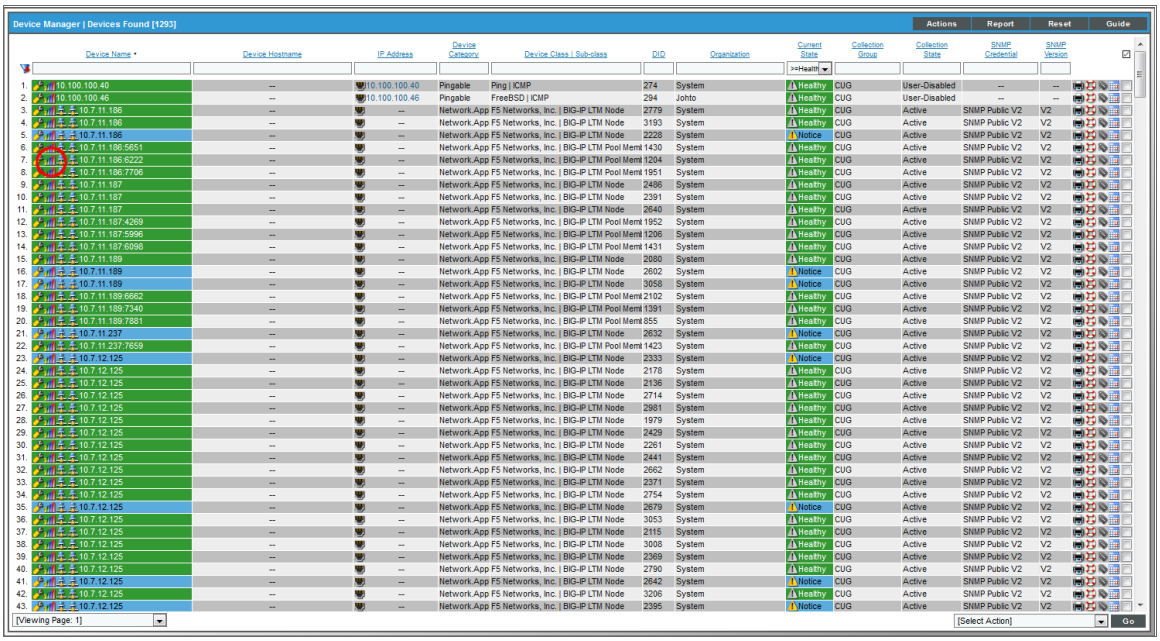
The System Vitals Summary Report displays multiple device-parameters in a single graph. The System Vitals Summary Report trends the following parameters:

- 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.

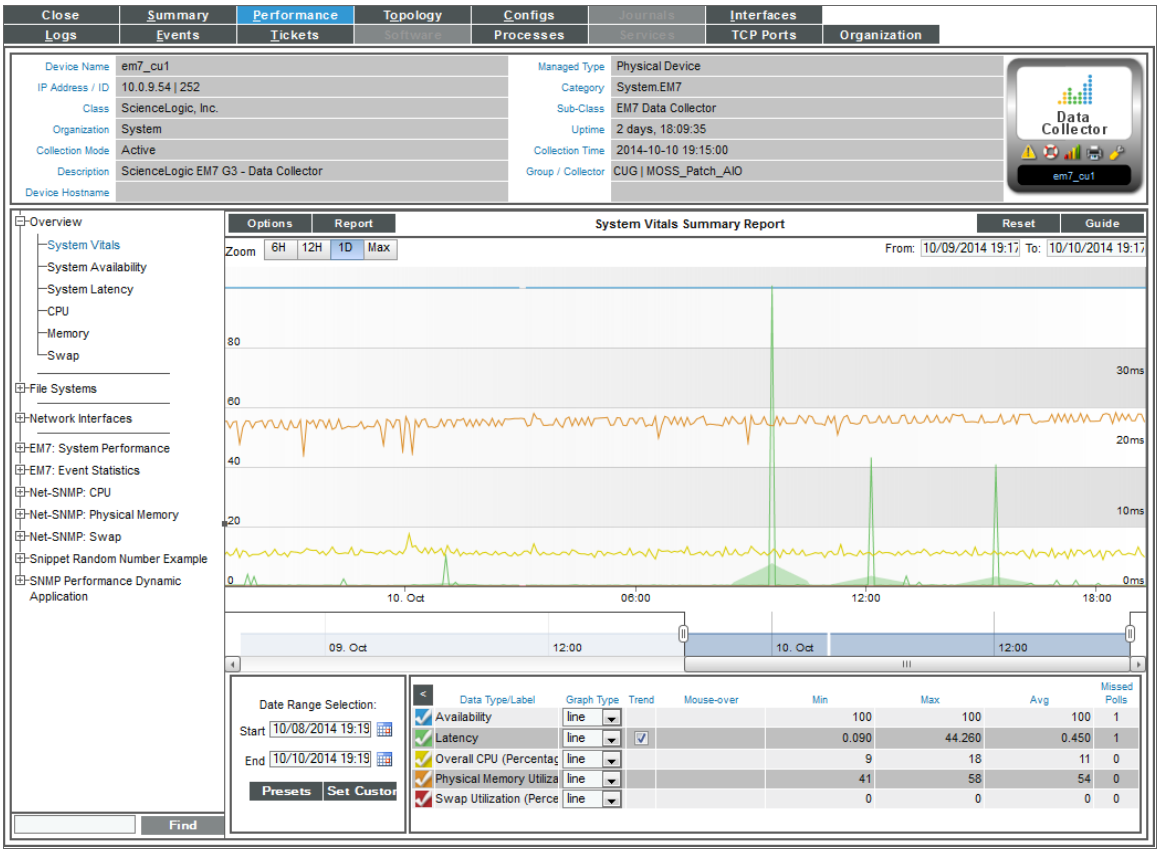
To view the System Vitals report for a device:

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 ( ).



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

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



5. 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.

6. The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
7. 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 SL1 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).

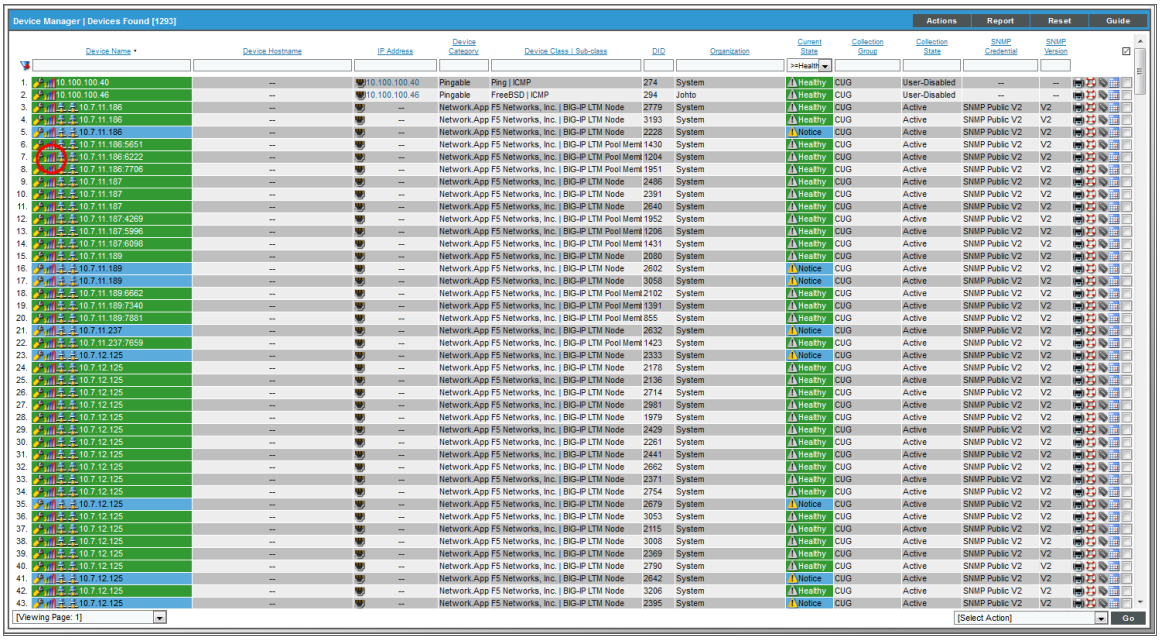
For devices that SL1 discovers with the discovery tool (Devices > Add Devices button, or System > Manage > Classic Discovery in the classic SL1 user interface), SL1 determines availability by checking the status of the port specified in the ***Availability Port*** field in the **Device Properties** page. 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.

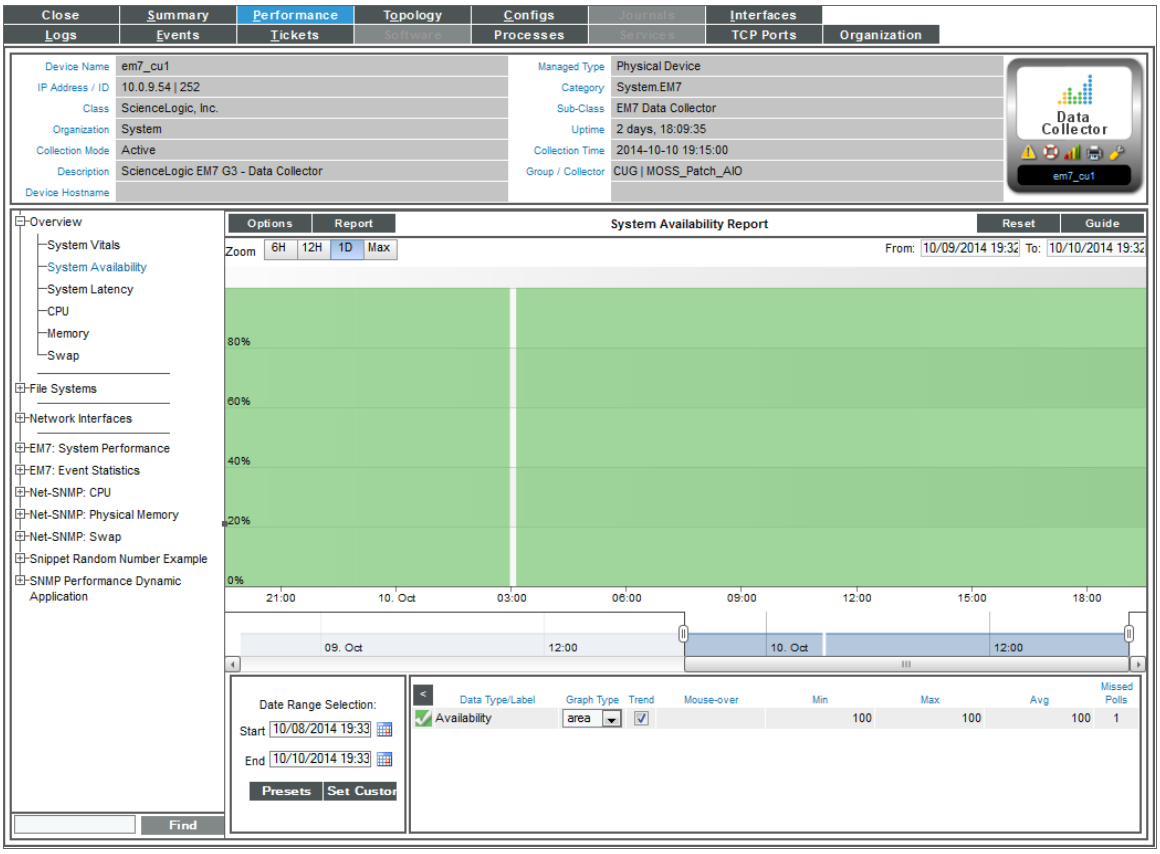
For devices that SL1 discovers with the agent, SL1 collects uptime data from the agent every 5 minutes, and uses this value to determine device availability.

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. Click its bar graph icon ( ).



3. In the **Device Reports** panel, click the Performance tab.



4. In the Performance tab, go to the NavBar (list of links in the left pane), expand the ***Overview*** link, and click ***System Availability***.
5. 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.

6. The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
7. 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:

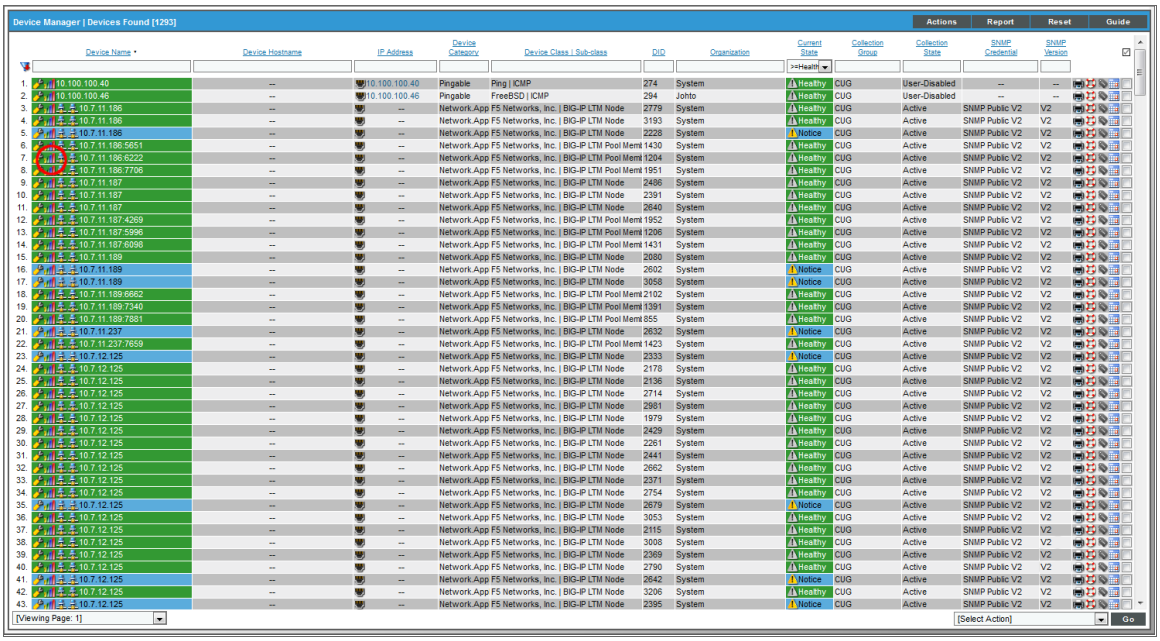
- ***Data Type/Label***. For graphs that include multiple types of data on a single graph (for example, availability and latency), each data type has its own row in this table. This column displays the type of data and how it is color coded in the report. Clicking on the check mark toggles on and off 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 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.

Viewing Latency Reports for a Device

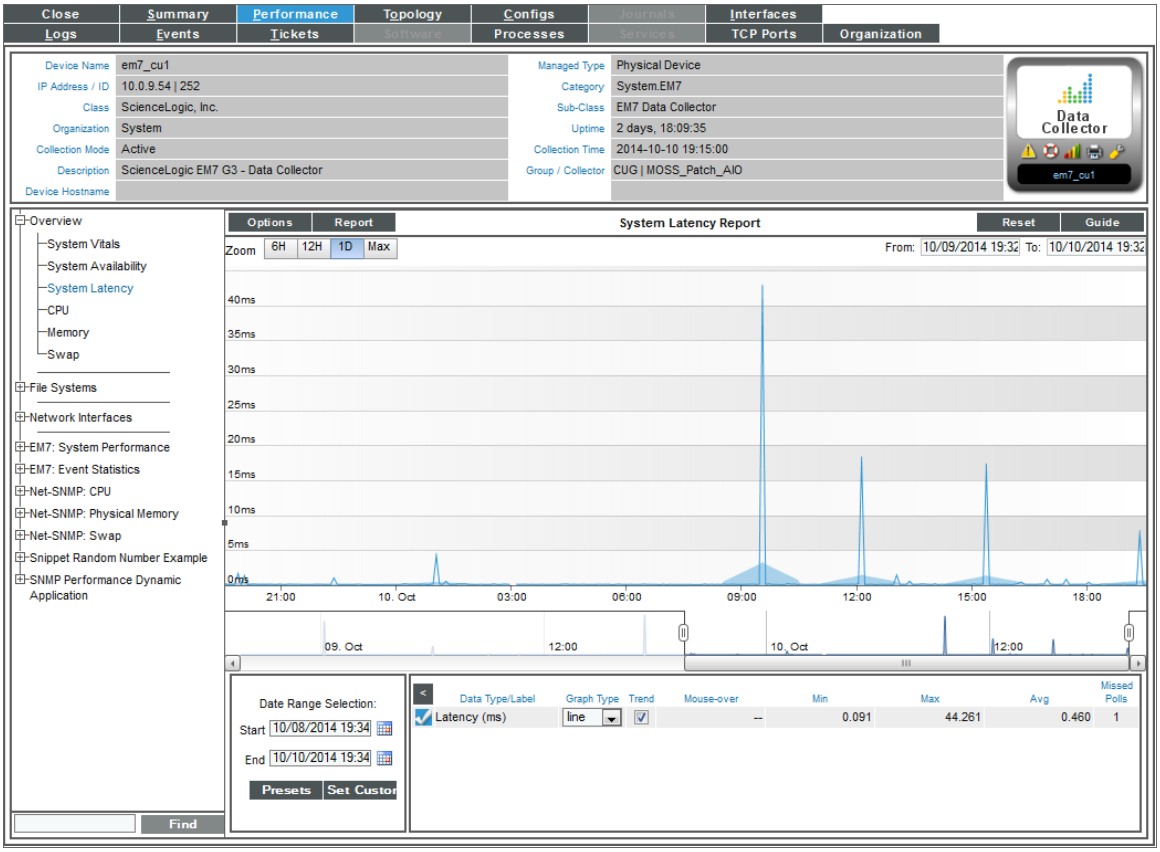
The System Latency report displays a graph with information about a single device's latency over time.

To view the System Latency report for a device:

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



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



4. In the Performance tab, go to the NavBar (list of links in the left pane), expand the ***Overview*** link, and select ***System Latency***.
5. 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.

6. The **[Options]** menu in the upper left of the report displays a menu of options you can apply to data in the current report.
7. 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.

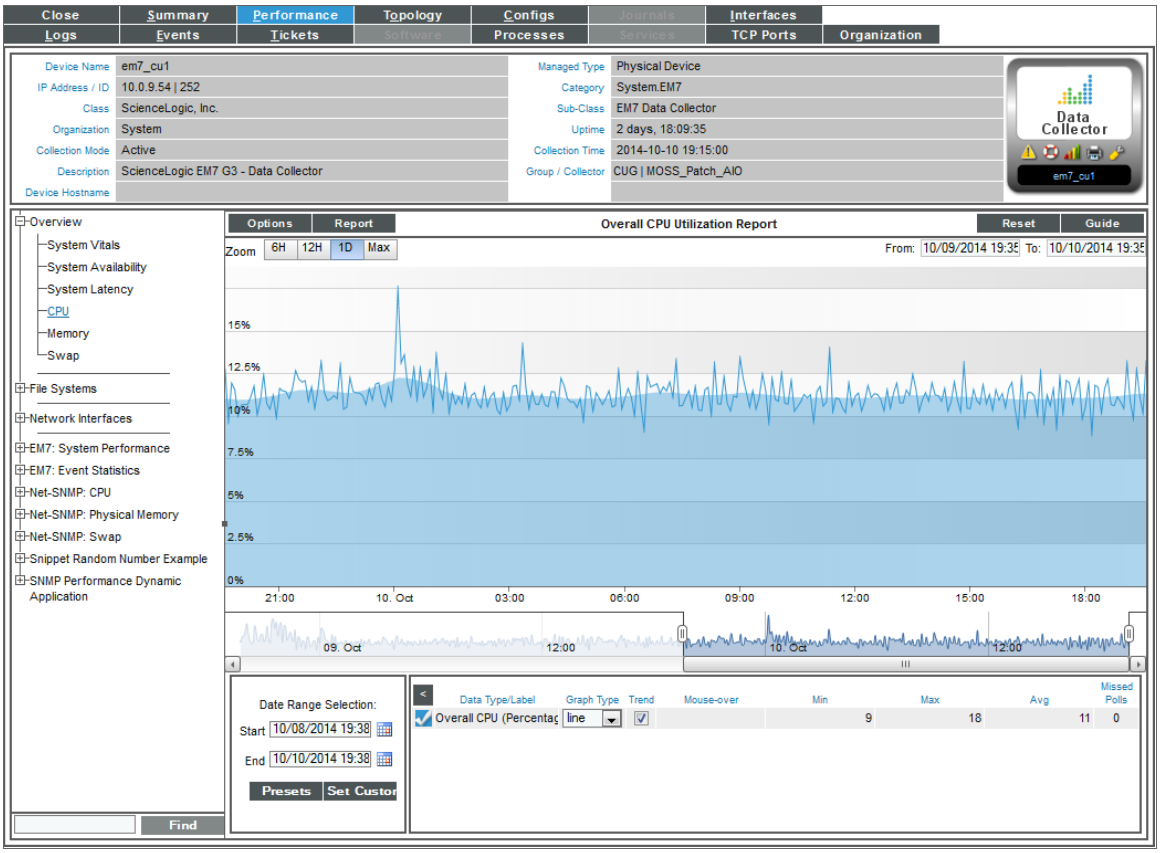
Viewing a Report on CPU Usage for a Device

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, click 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 click ***CPU Utilization***.



4. 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.

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***. 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.

Changing the Dynamic Application Precedence Settings for CPU and Memory Utilization

SL1 collects CPU and memory utilization metrics using Dynamic Applications. If an SNMP device is monitored using the SL1 agent, multiple Dynamic Applications can collect CPU and memory utilization metrics. When multiple Dynamic Applications collect CPU and/or memory utilization for a device, SL1 evaluates precedence settings to determine which Dynamic Application will be used to represent CPU and memory utilization for that device.

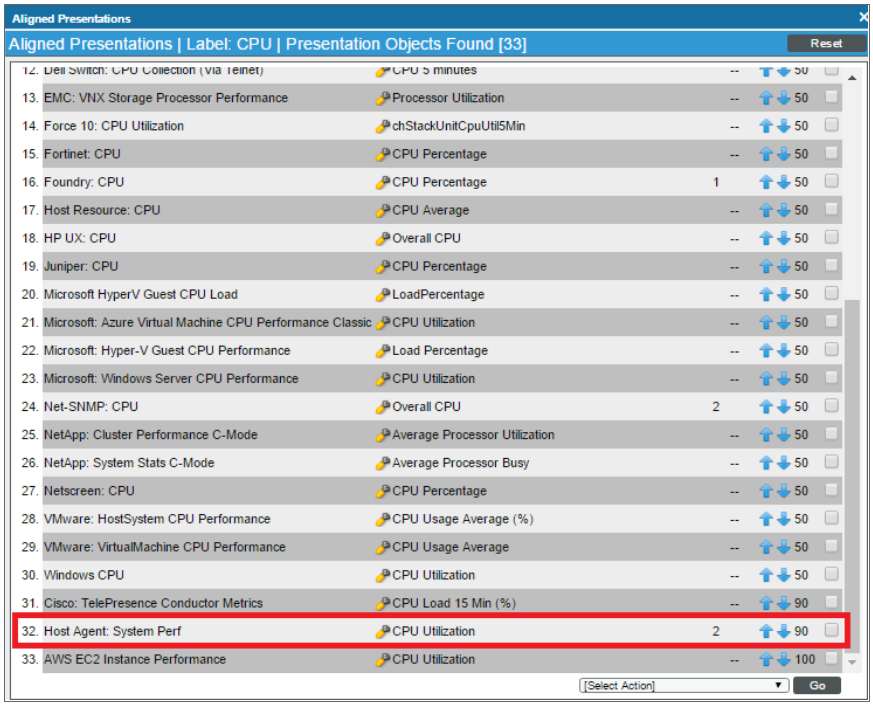
By default, the precedence settings are configured so the Dynamic Applications that poll the device (using methods other than the agent) represent CPU and memory utilization for that device.

You can change the precedence settings so the Dynamic Applications that use data collected by the agent represent CPU and memory utilization:

- For all applicable devices discovered in the future
- Per-device

To change the precedence settings *for all applicable devices discovered in the future*:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).
2. The **Collection Labels** page includes entries for CPU Utilization and Memory Utilization. Select the icon in the **Aligned Presentations** column ( ) for the utilization metric for which you want to adjust precedence. The **Aligned Presentations** page appears.

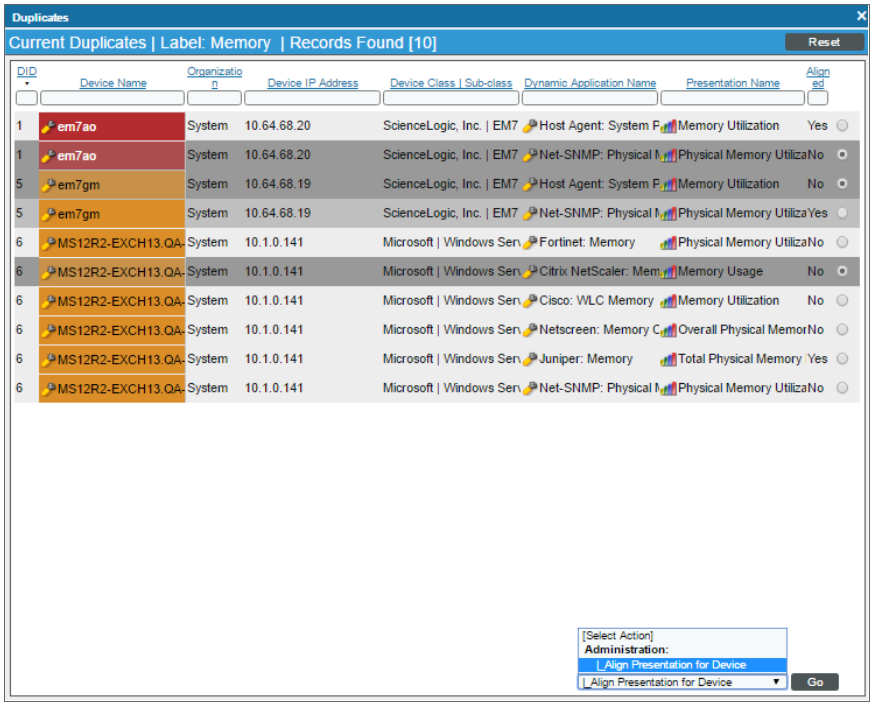


3. Locate the entry for the ***Host Agent: System Perf*** Dynamic Application. Select its checkbox.
4. In the ***Select Action*** drop-down list, select *0* in the *Change Precedence* section.
5. Click **[Go]**.

To change the precedence settings *per-device*:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).

2. The **Collection Labels** page includes entries for CPU Utilization and Memory Utilization. Select the icon in the **Duplicates** column ( ) for the utilization metric for which you want to adjust precedence. The **Current Duplicates** page appears.



3. The **Current Duplicates** page displays multiple rows for each device; each row specifies a device and Dynamic Application metric pair. For each group of rows for a device, use the radio button to the right of the page to select the Dynamic Application metric you want to use for that device.
4. In the ***Select Action*** drop-down list, select *Align Presentation for Device*.
5. Click **[Go]**.

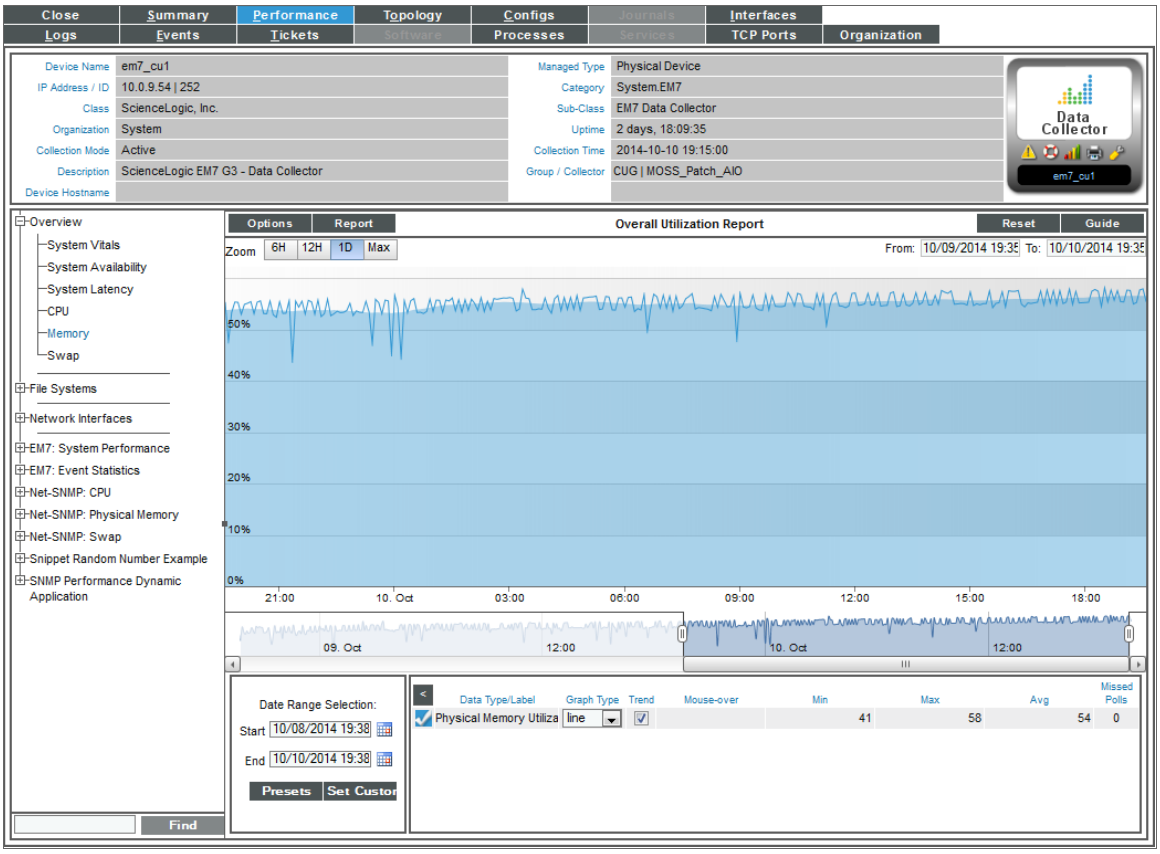
Viewing a Report on Physical Memory Usage for a Device

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.

NOTE: If an SNMP device is monitored using the SL1 agent, multiple Dynamic Applications can collect CPU and memory utilization metrics. When multiple Dynamic Applications collect CPU and/or memory utilization for a device, SL1 evaluates precedence settings to determine which Dynamic Application will be used to represent CPU and memory utilization for that device. By default, the precedence settings are configured so the Dynamic Applications that poll the device using methods other than the agent represent CPU and memory utilization for that device. However, you can change the precedence settings so the Dynamic Applications instead use data collected by the agent to represent CPU and memory utilization. For more information, see the section on *Changing the Dynamic Application Precedence Settings for CPU and Memory Utilization*.

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 SL1 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.

> **NOTE:** If an SNMP device is monitored using the SL1 agent, multiple Dynamic Applications can collect CPU and memory utilization metrics. When multiple Dynamic Applications collect CPU and/or memory utilization for a device, SL1 evaluates precedence settings to determine which Dynamic Application will be used to represent CPU and memory utilization for that device. By default, the precedence settings are configured so the Dynamic Applications that poll the device using methods other than the agent represent CPU and memory utilization for that device. However, you can change the precedence settings so the Dynamic Applications instead use data collected by the agent to represent CPU and memory utilization. For more information, see the section on *Changing the Dynamic Application Precedence Settings for CPU and Memory Utilization*.

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.

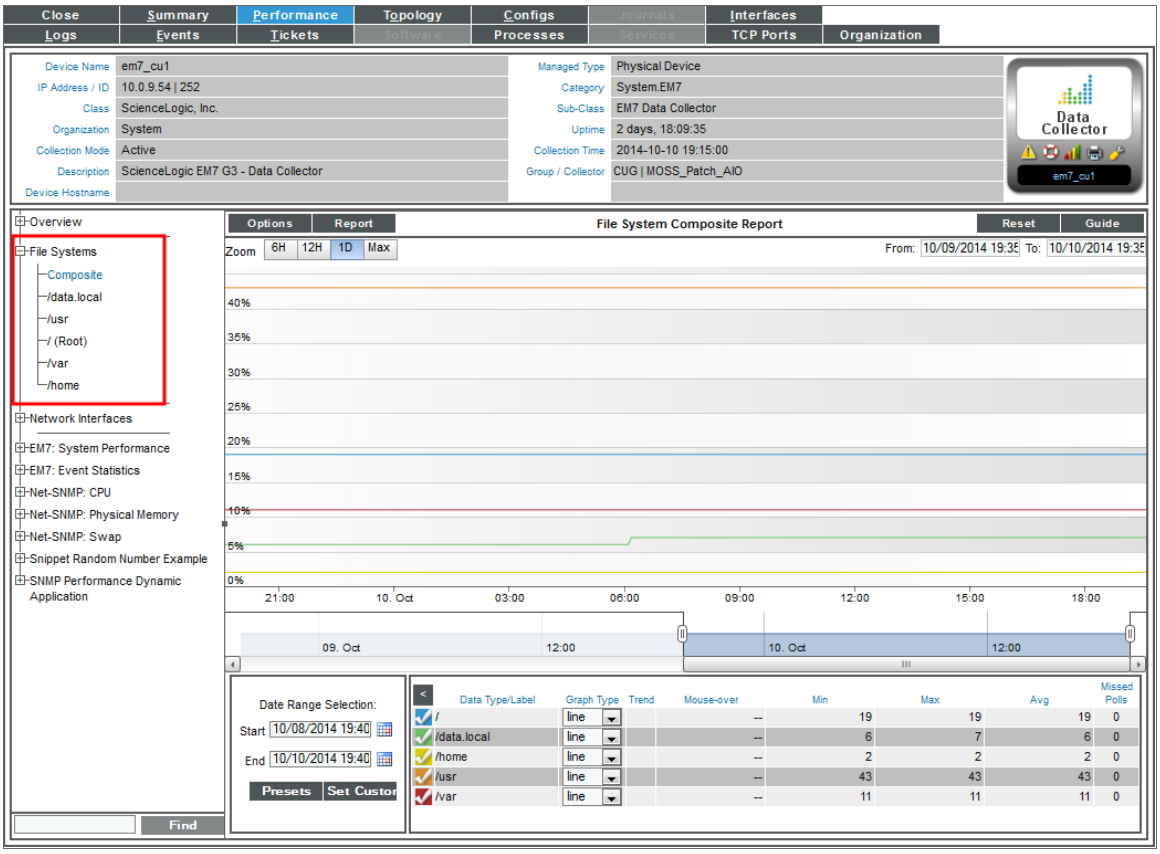
Viewing a Report on File System Usage for a Device

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:

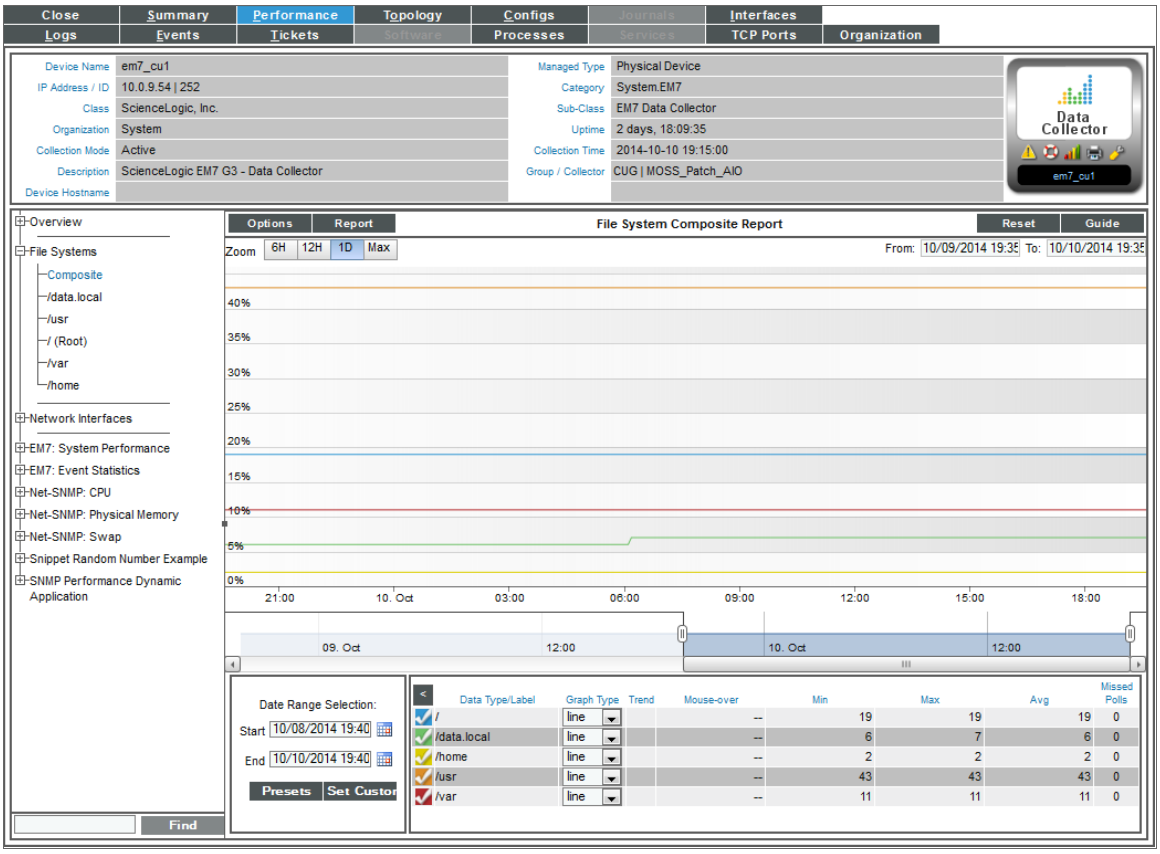
1. You can access the File System reports from two places:
    - Go to the **Device Manager** page (Devices > Device Manager), find the device where the file system resides, and select its bar graph icon ( ).
    - Go to the **Device Hardware** page (Devices > Hardware), filter by CPU, find the device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

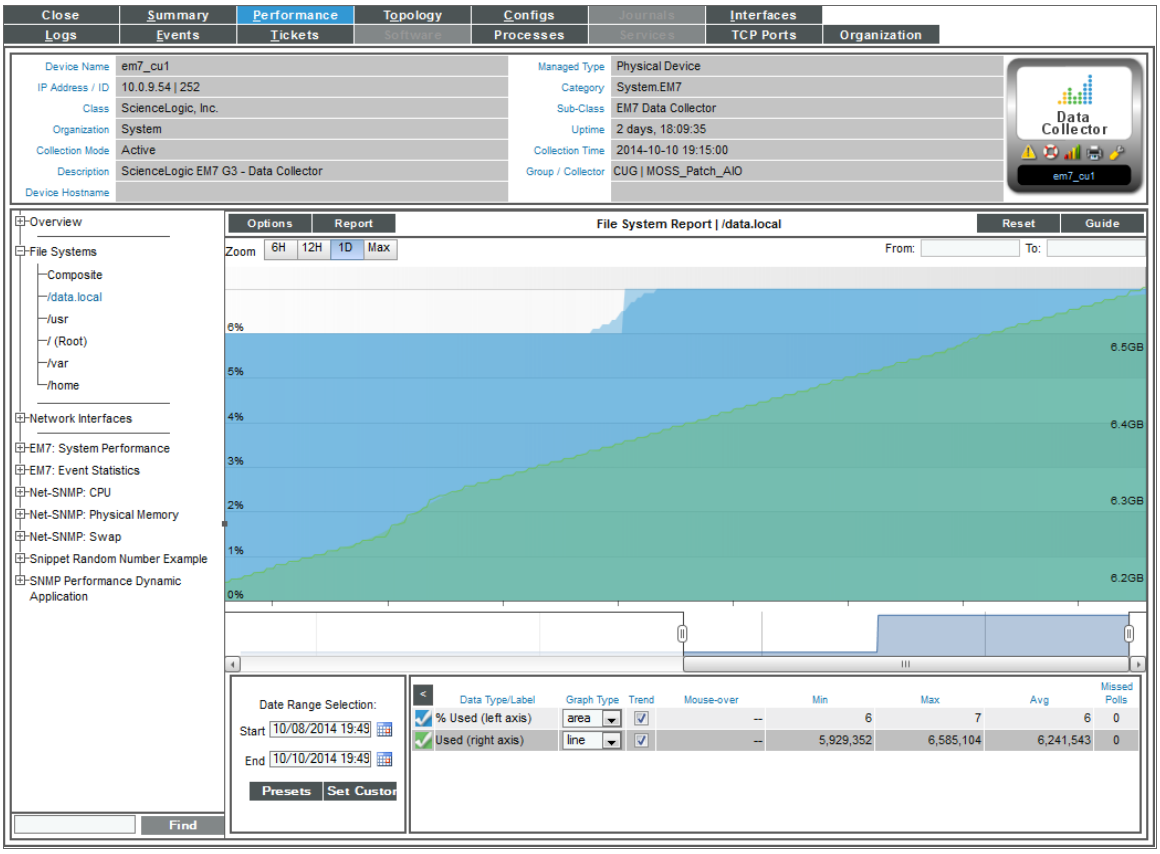
5. The File System Composite Report displays percent of disk-space used for all file systems on the device.



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 Performance Report Graphs on Network Interfaces

For each network interface discovered on a device, SL1 generates five network interface performance report graphs. These five graphs 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 performance report graphs. For each CBQoS Policy and each class map under that policy, SL1 can generate graphs on the following based on the CBQoS configuration:

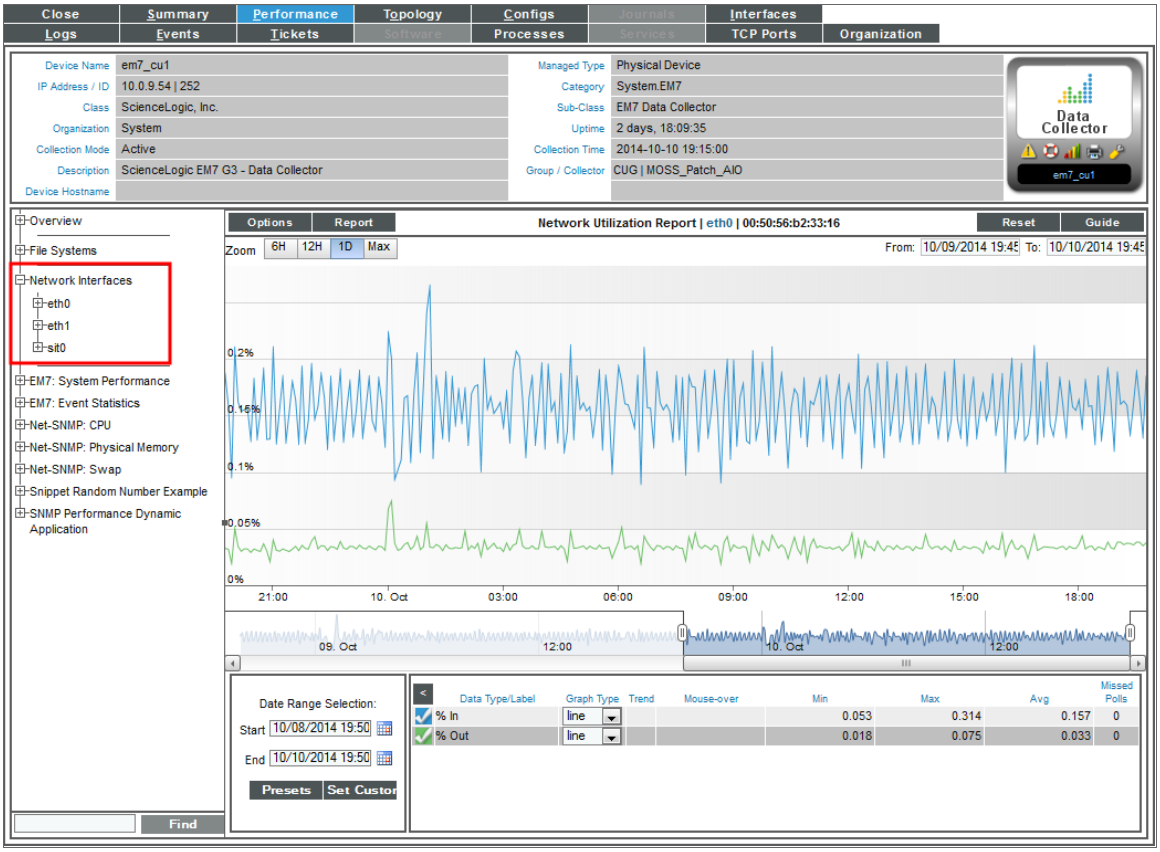
- Class Maps
- Policing
- Sets
- Match Statements

- Queuing
- Sets
- Traffic Shaping
- WRED

Default Performance Graph Reports for Network Interfaces

To view the five default network interface performance report graphs for a device:

1. You can access the network interface performance report graphs 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.



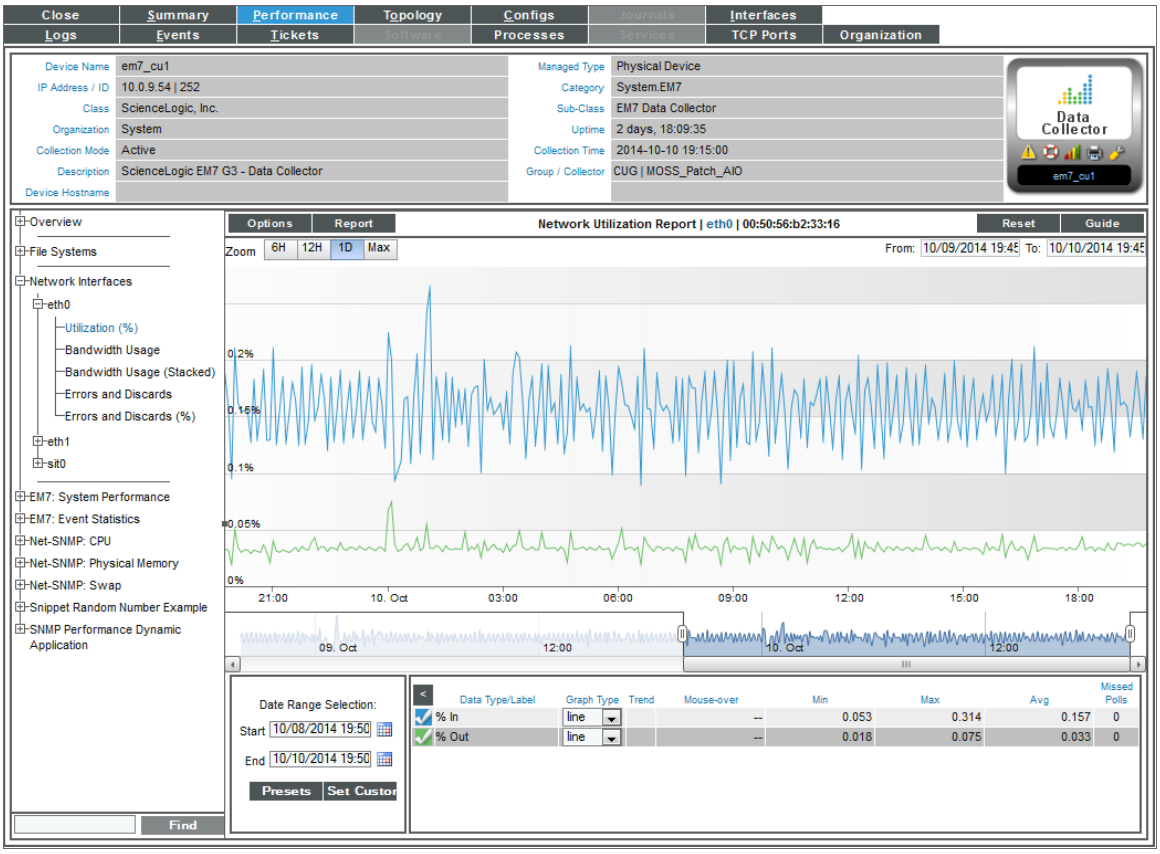
4. When you expand a network interface, links to each network interface report appear under that interface. Each report is described in the sections below.
5. In all of the network interface reports, the **[Options]** menu in the upper left of the report displays a menu of options you can apply to data 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



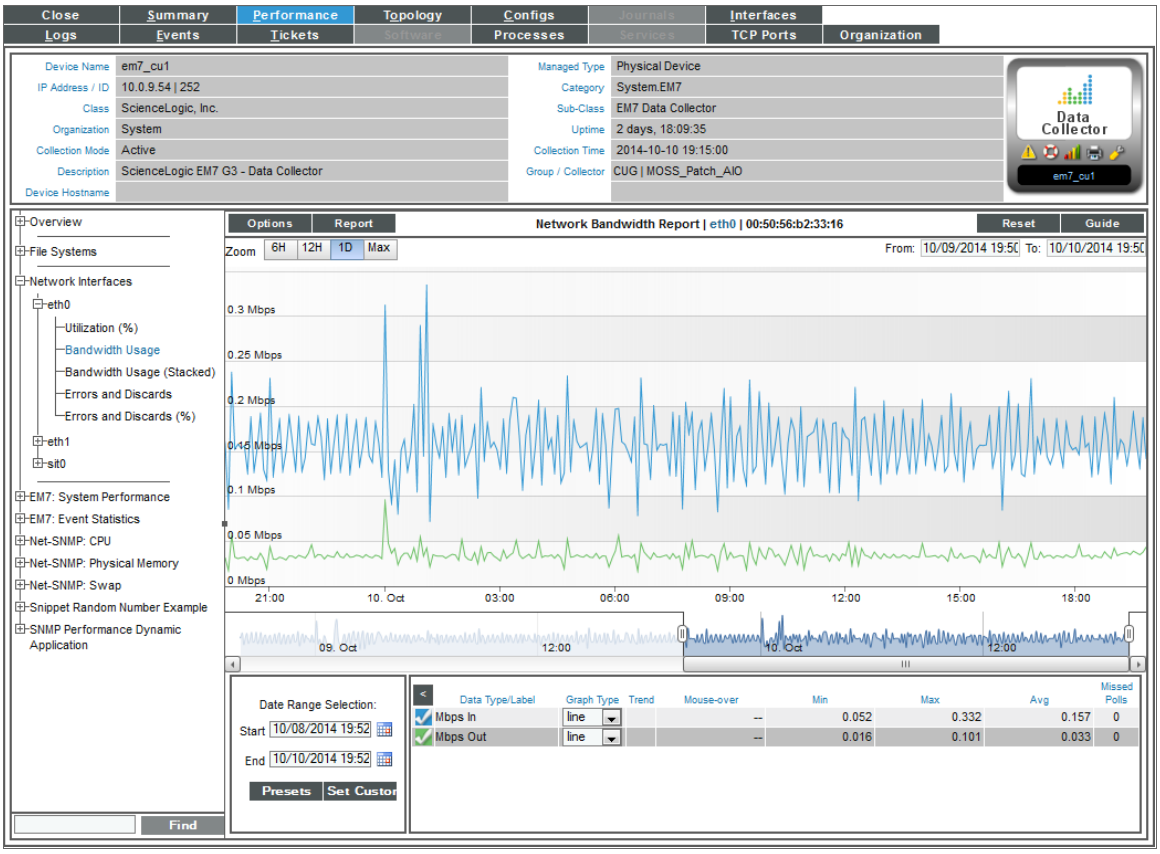
The **Network Utilization Report** displays a color-coded line for percentage in and a color-coded line for percentage out.

- 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



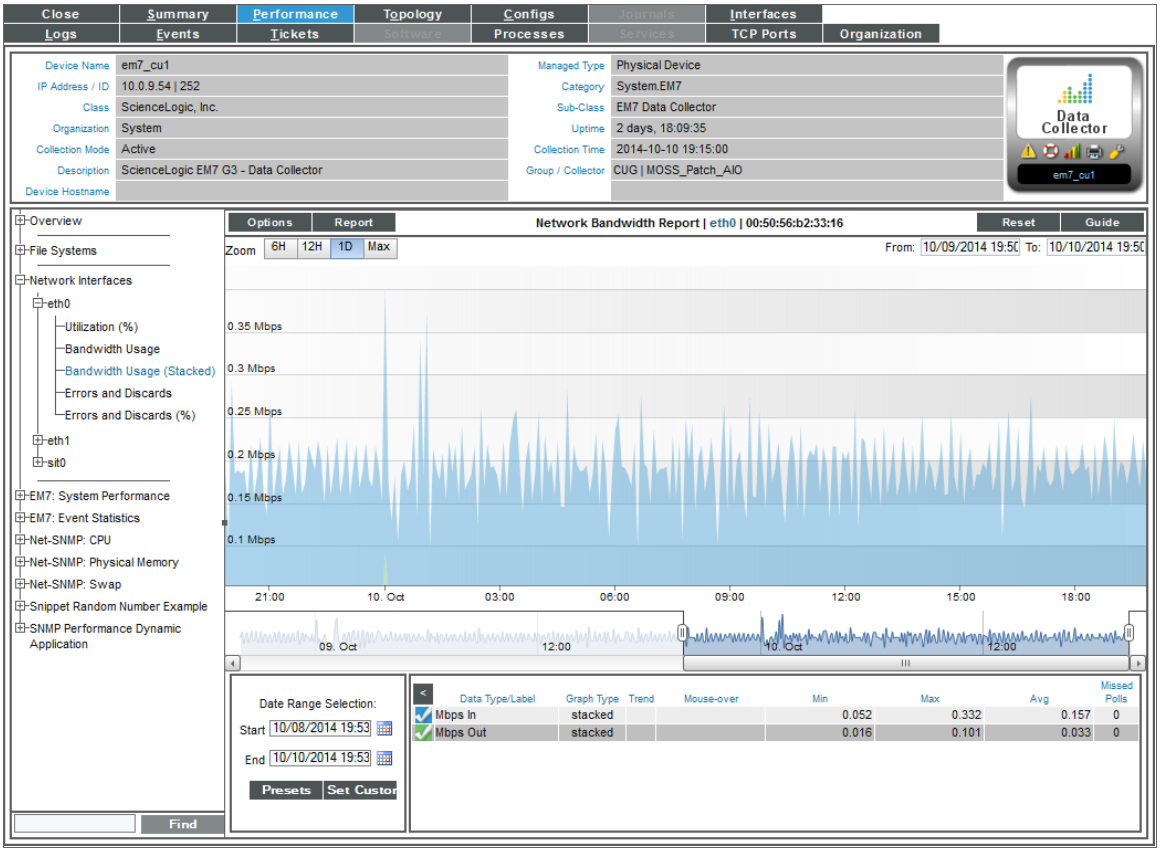
The **Network Bandwidth Usage Report** graph displays a color-coded line for octets in and a color-coded line for octets out.

- 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.

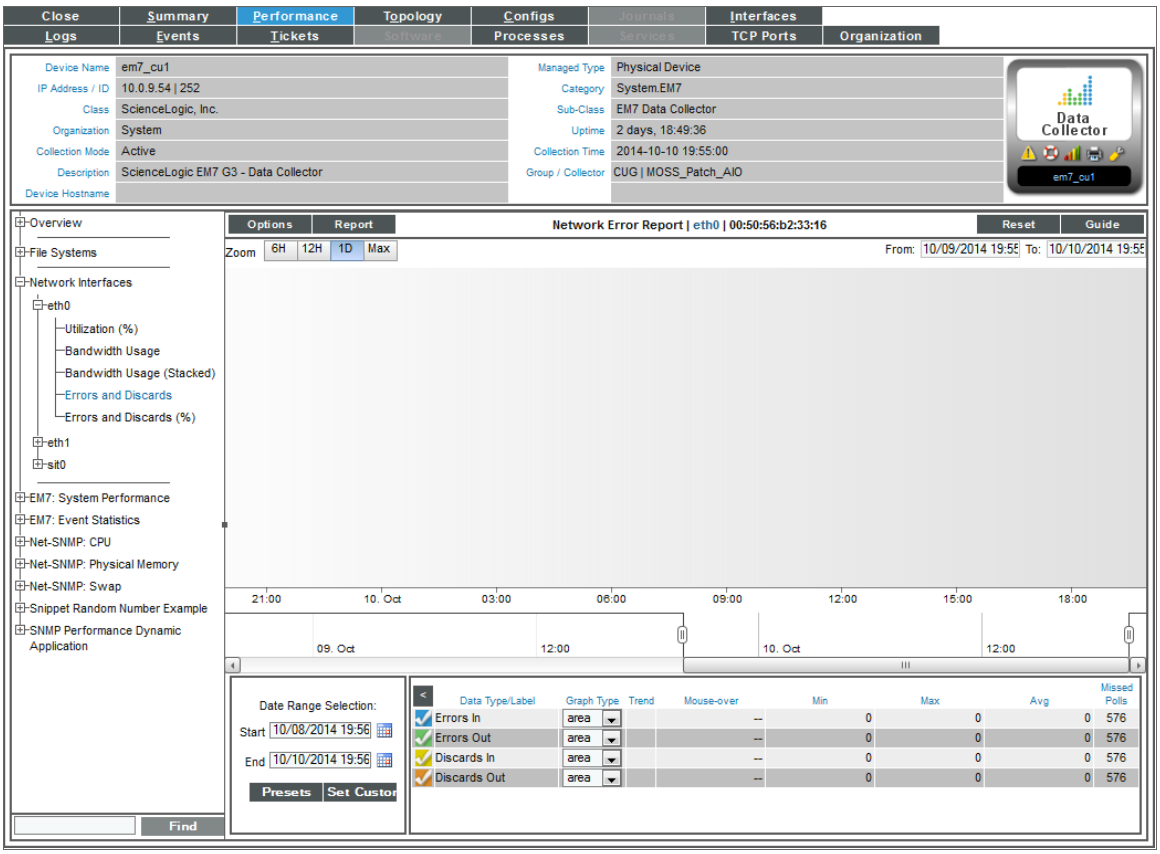
Network Error Report

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.

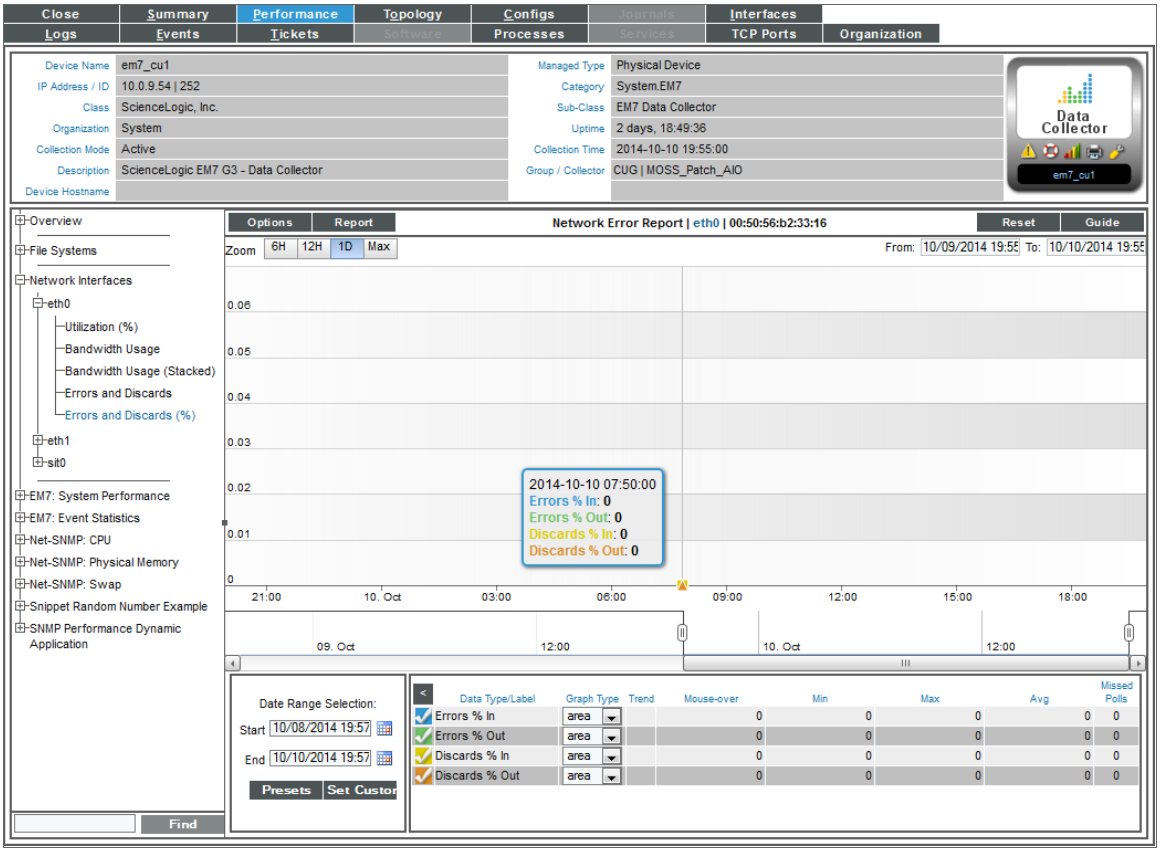
Network Error Report (Percent)

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.



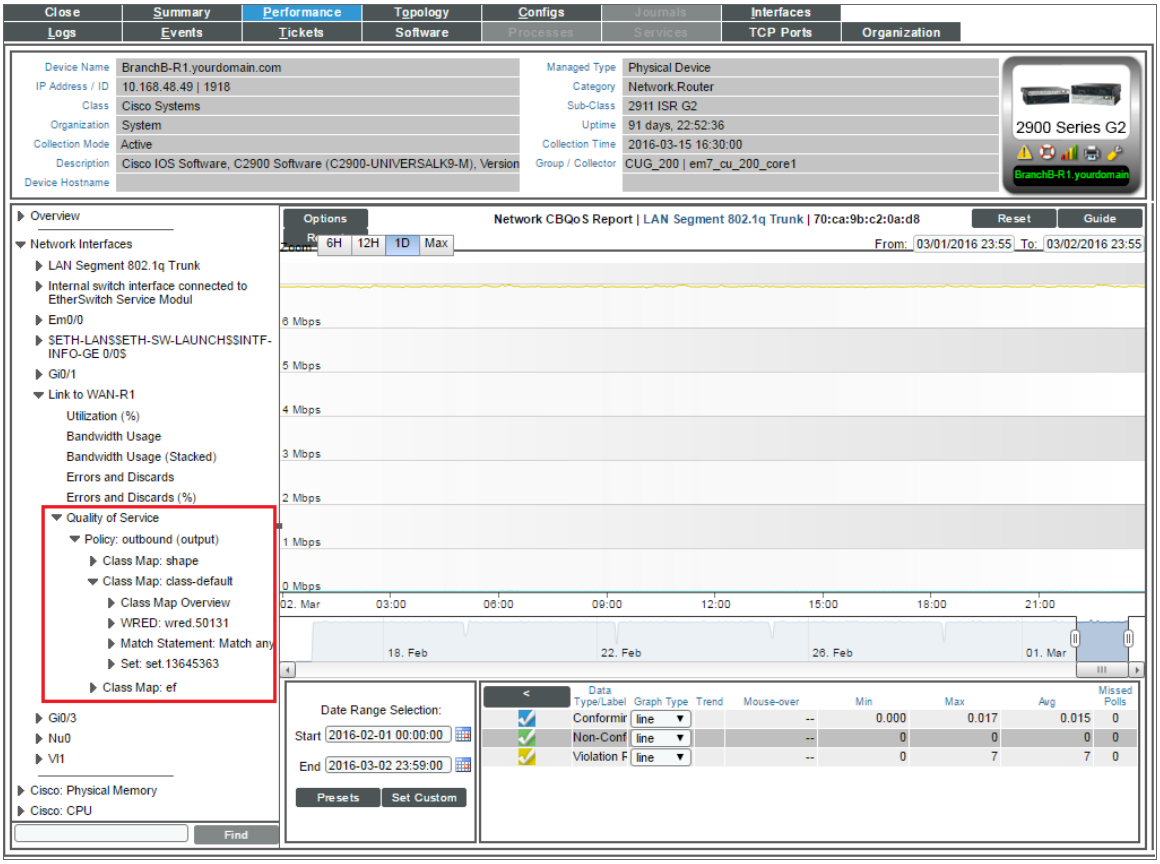
The **Network Error Report (%)** graph displays a color-coded line for errors % in, errors % out, discards % in, and discards % out.

- 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.

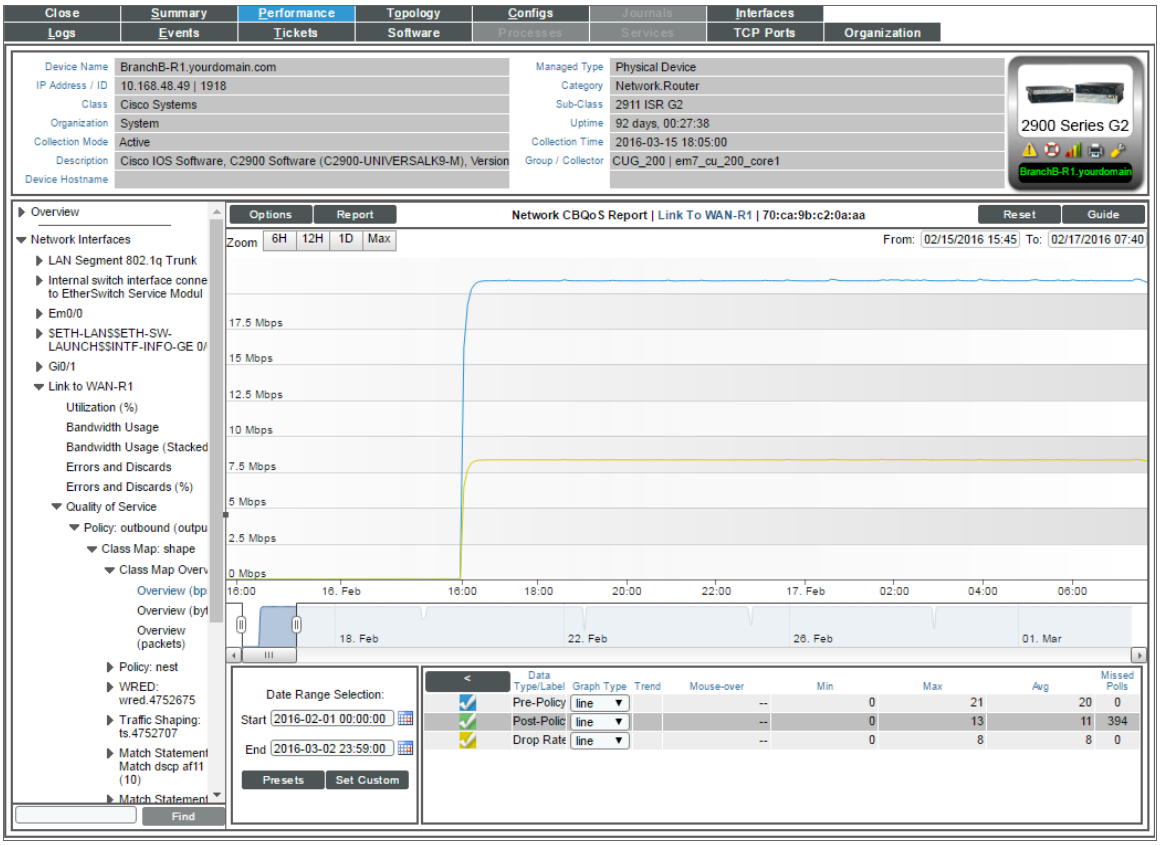
7. In all of the network interface reports, the **Data Table** at the bottom of each report enables you to view details about each data point and view overview information about the entire report. The data table includes the following:

    - ***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 SL1 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



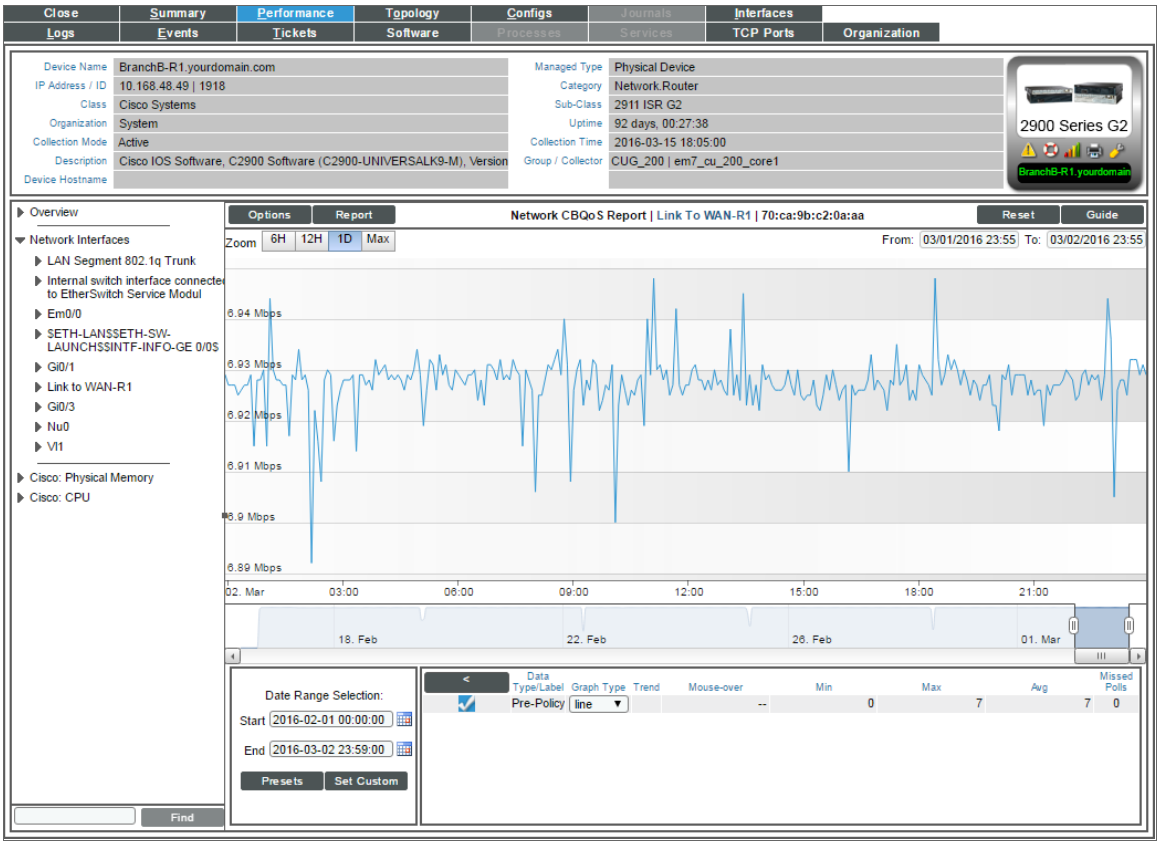
The graph displays a color-coded line for Pre-Policy, Post-Policy, and Dropped.

- 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



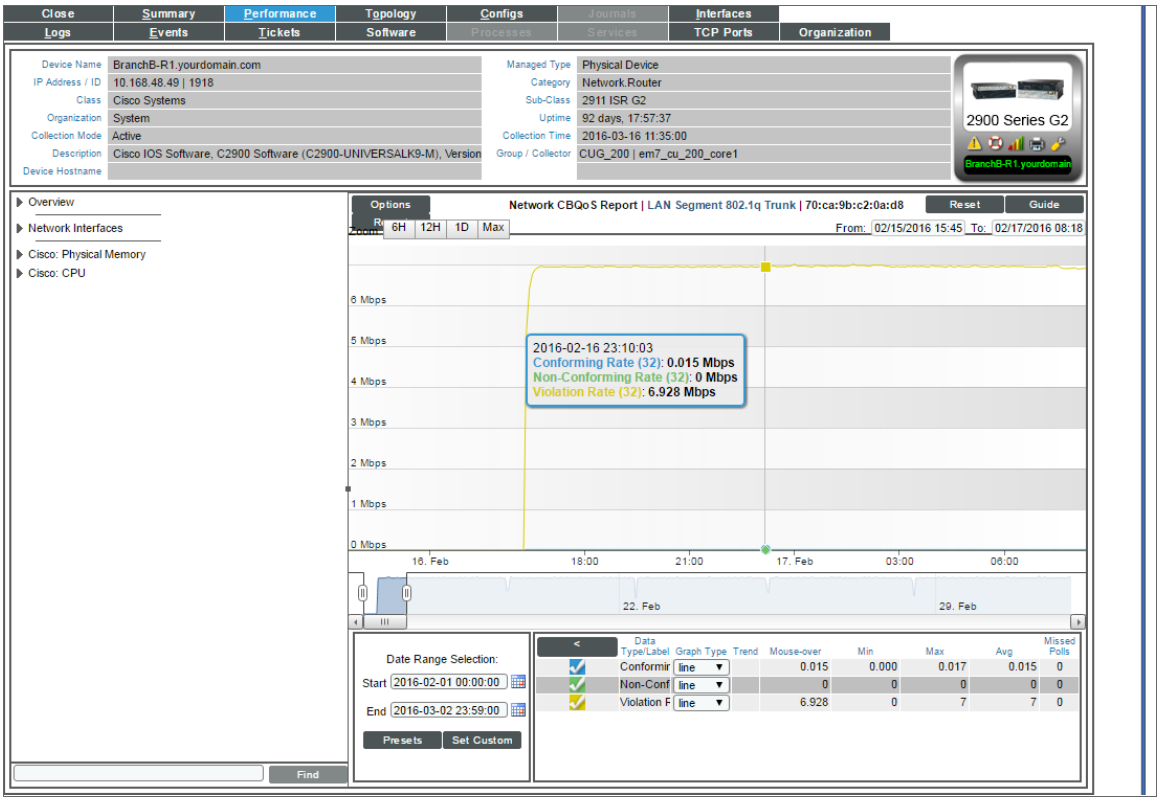
The graph displays a color-coded line for Pre-Policy Inbound (U32), Pre-Policy Inbound (L32), and Pre-Policy Inbound.

- 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.

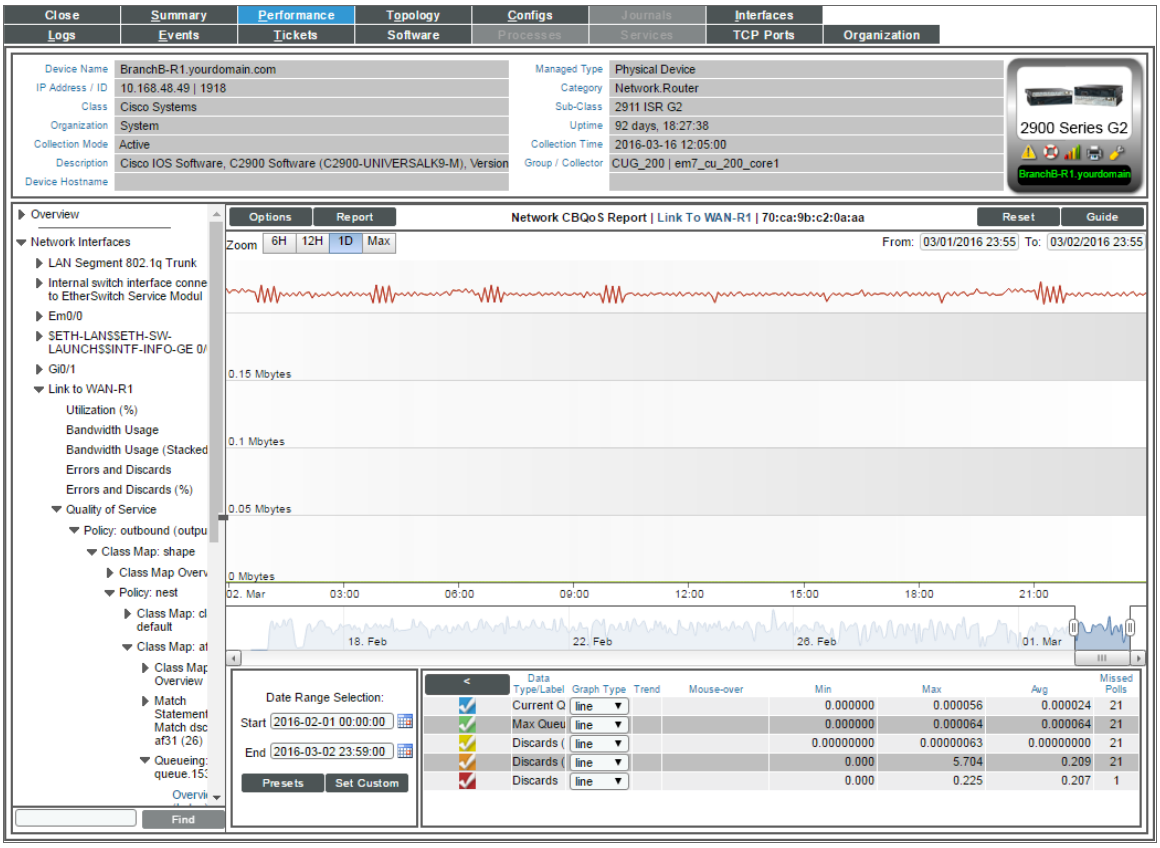
- The y-axis displays volume in either Mbytes, bps, or packets.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the Conforming, 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 Queuing 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:

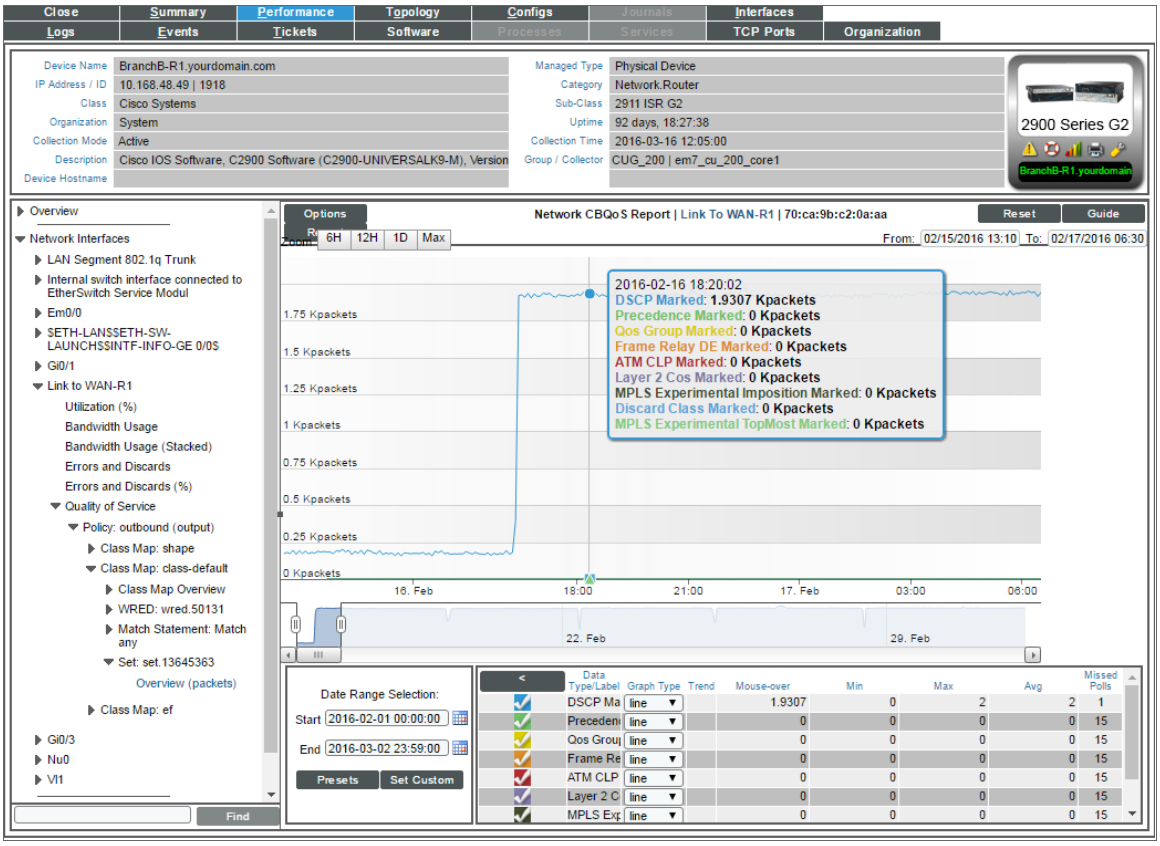
- The y-axis displays volume in either bytes or bps.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays the number or discards at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

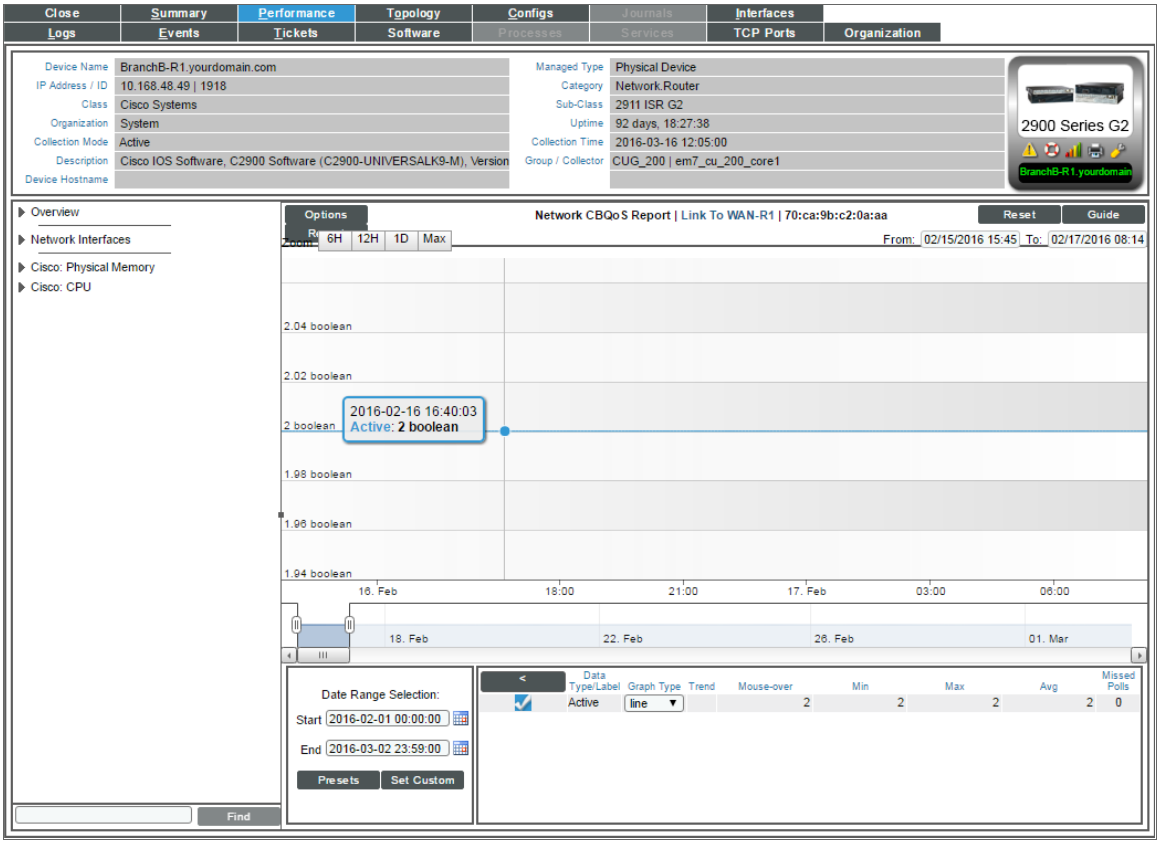
For the selected interface, the **Traffic Shaping Overview Report** for each traffic shaping policy includes two reports:

- Overview (boolean)
- Overview (in either byes 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):

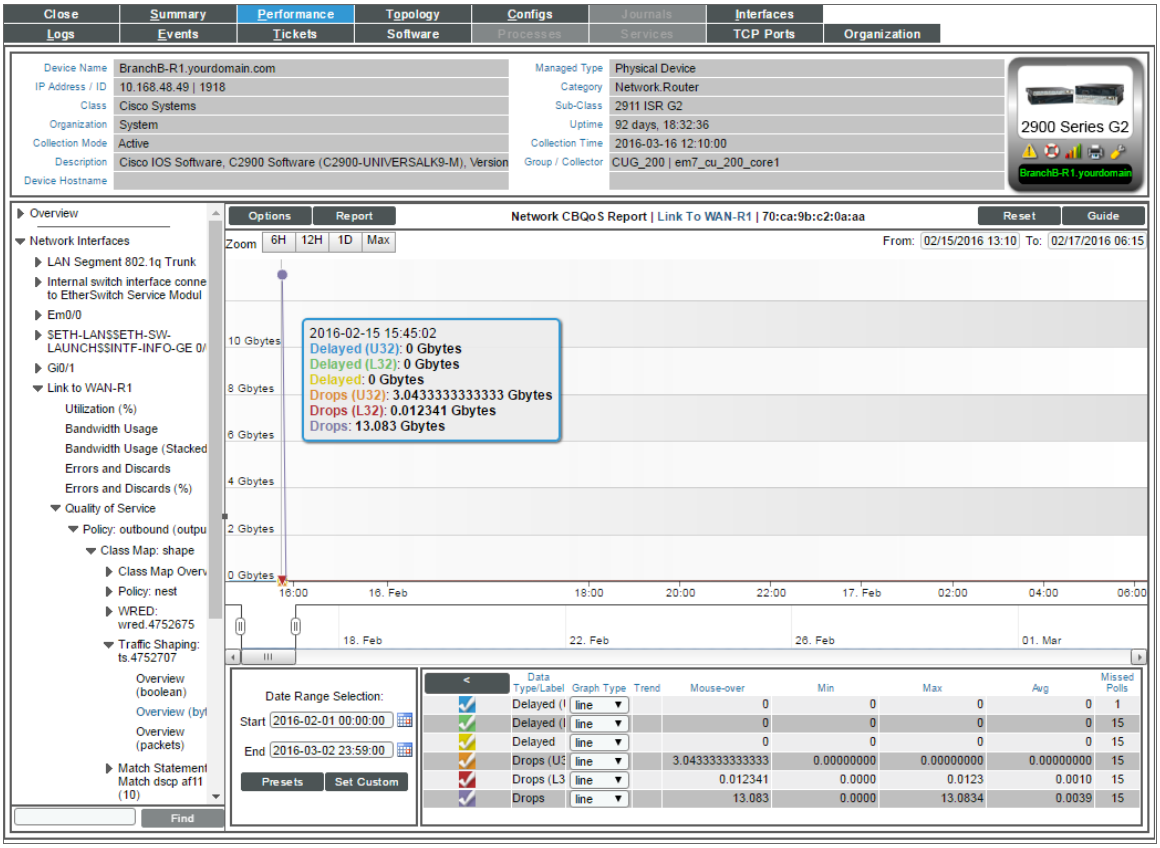
- The y-axis displays volume in either Mbytes or packets.

- 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.

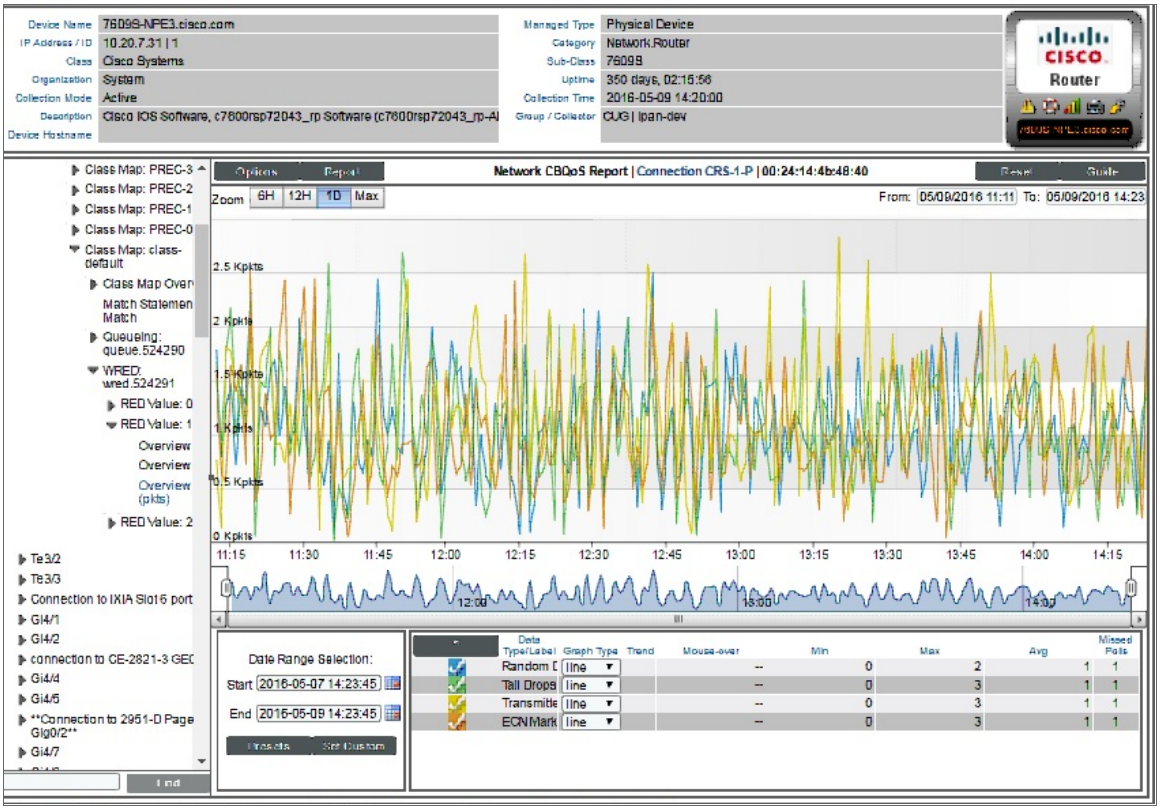
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the **Date Range Selection** pane).
- Mousing over any point in any line displays a value for each of the metrics described above at that time-point.
- You can 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:

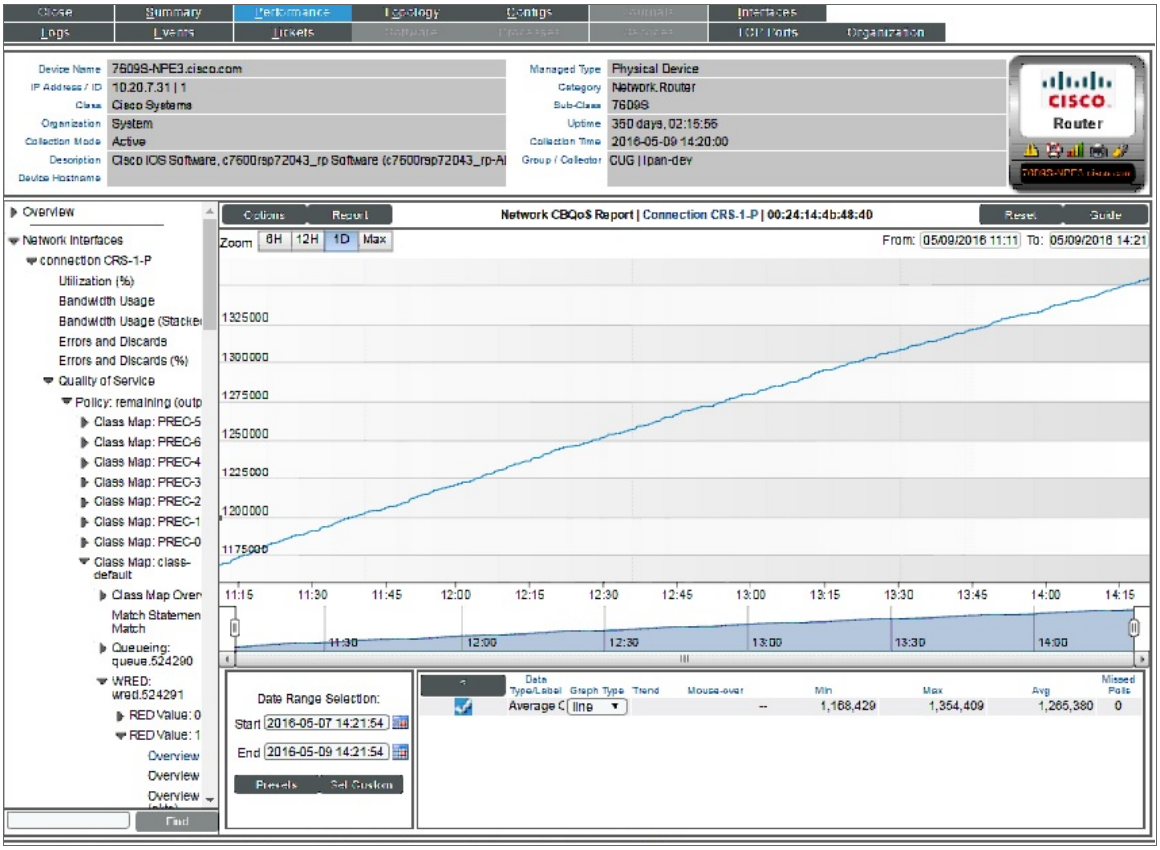
- Random drops (in either bytes or packets) over time for the RED policy
- Random drops (in either bytes or packets) over time that match the U32 filter for the RED policy
- Random drops (in either bytes or packets) over time that match the L32 filter for the RED policy
- Tail drops (in either bytes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

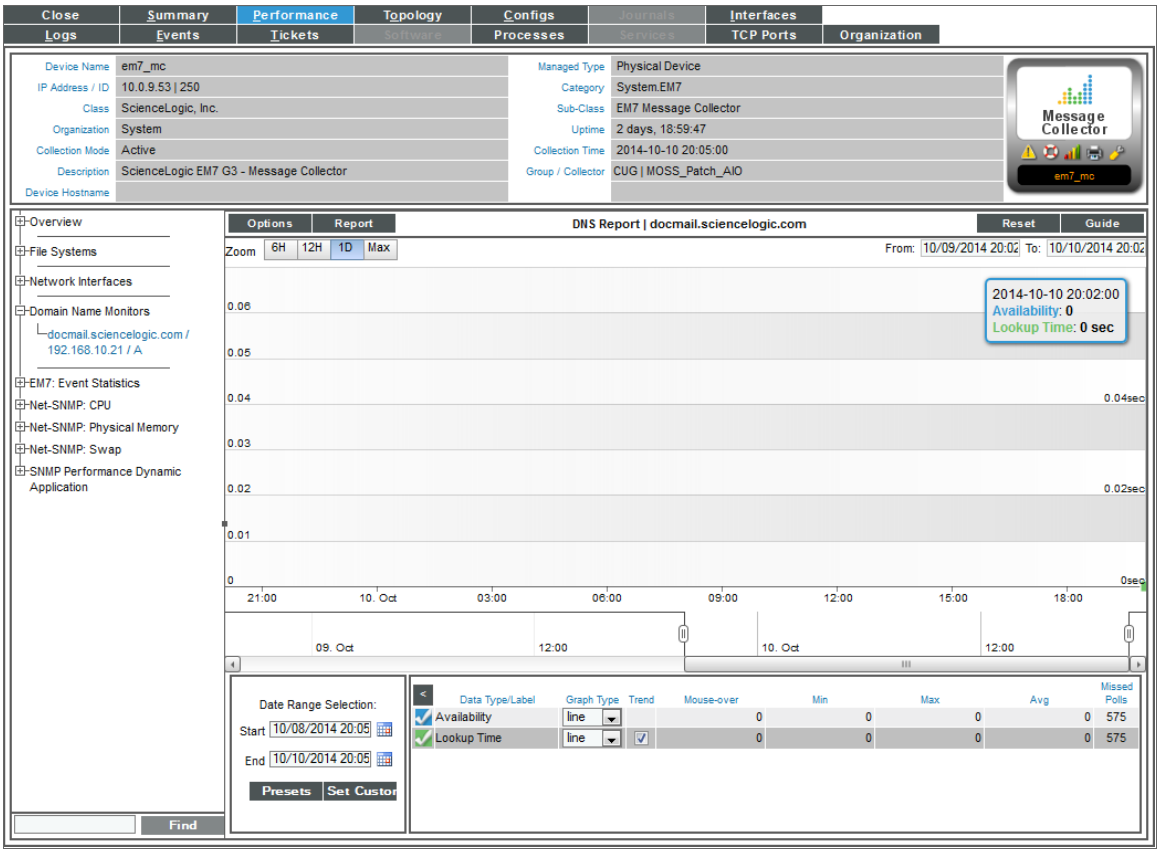
When you define a domain-name monitoring policy, SL1 automatically collects data associated with the policy. SL1 graphs that data in the **Performance** tab for the device associated with the policy.

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:

1. 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( ).
2. The **Device Performance** page appears, with the DNS Report displayed.



3. 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):

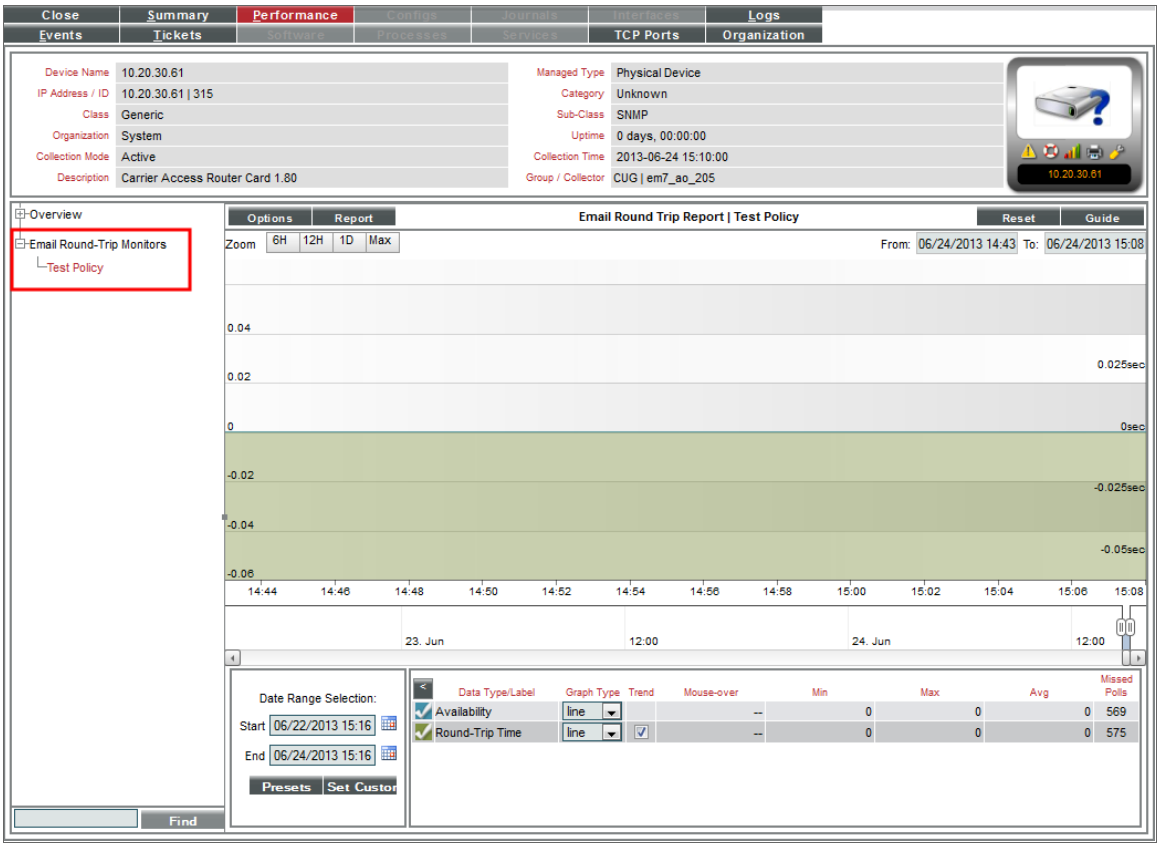
    - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon ( ) for the device.
    - In the **Device Reports** panel, select the **Performance** tab.
    - In the NavBar, expand Email Round-Trip Monitors and select the policy for which you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

Or:

1. 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 ( ).

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



3. 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 a SOAP or XML Transaction Policy

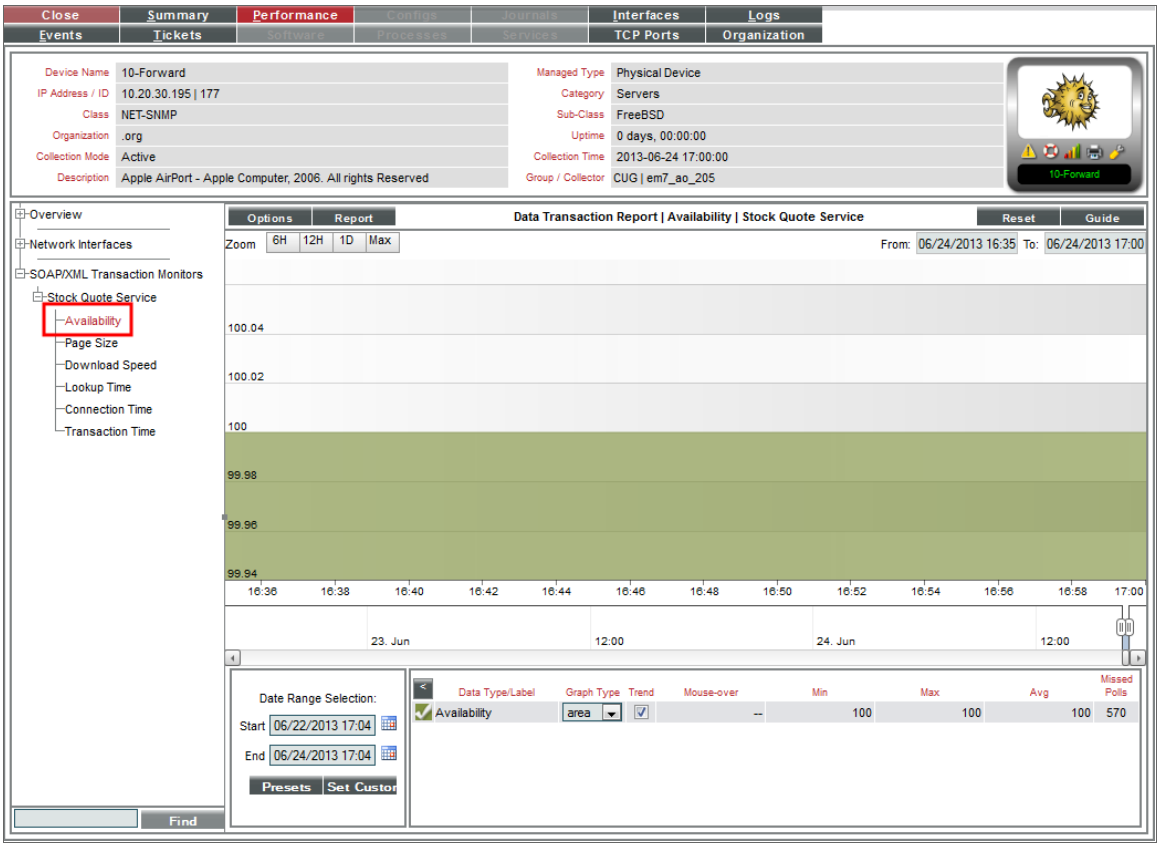
The **Data Transaction Reports** page display results from a SOAP/XML transaction policy. Each of these policies monitors a server-to-server transaction that uses HTTP and can post files or forms (for example, SOAP/XML or Email). SL1 sends a request and some data and then examines the result of the transaction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

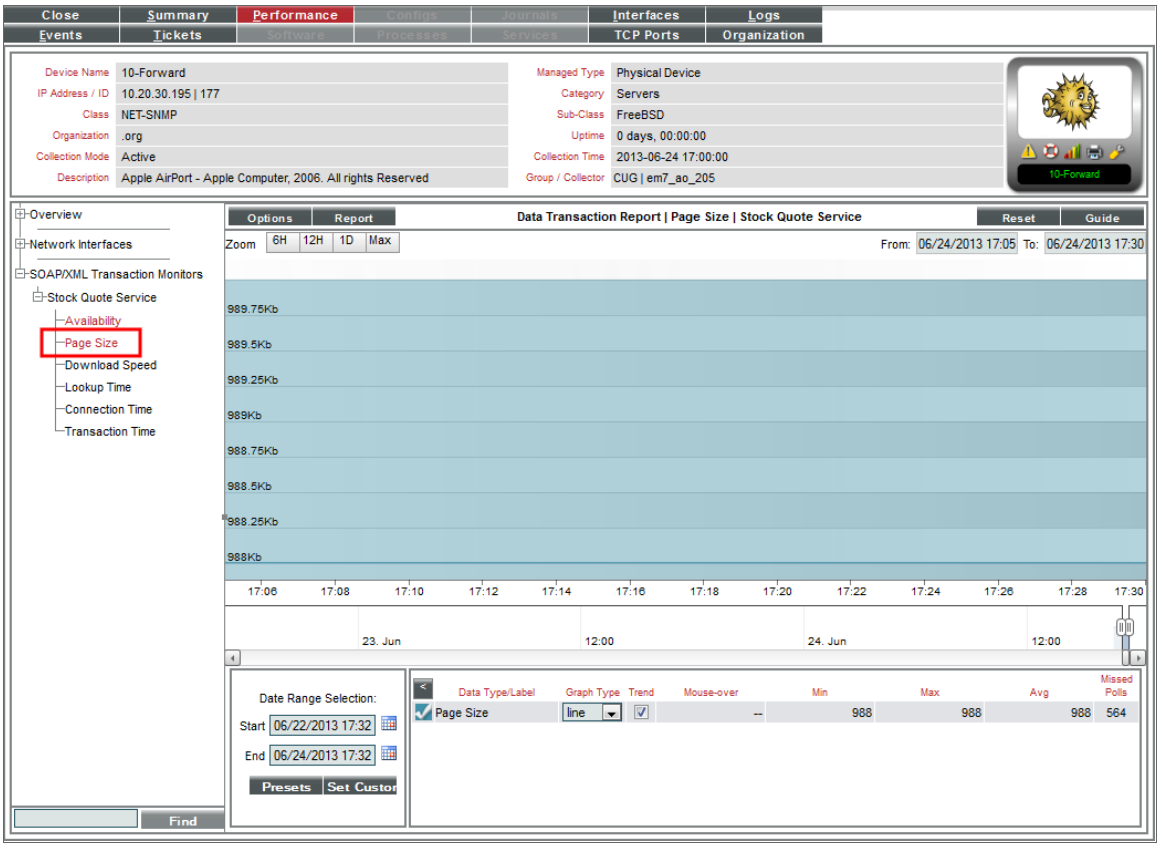


4. The Data Transaction Report | Availability report displays results from a SOAP/XML Transaction policy. The report trends the parameters described below. The Data Transaction Report | Availability report displays the availability of the external server and the availability of the specified data.

    - 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.

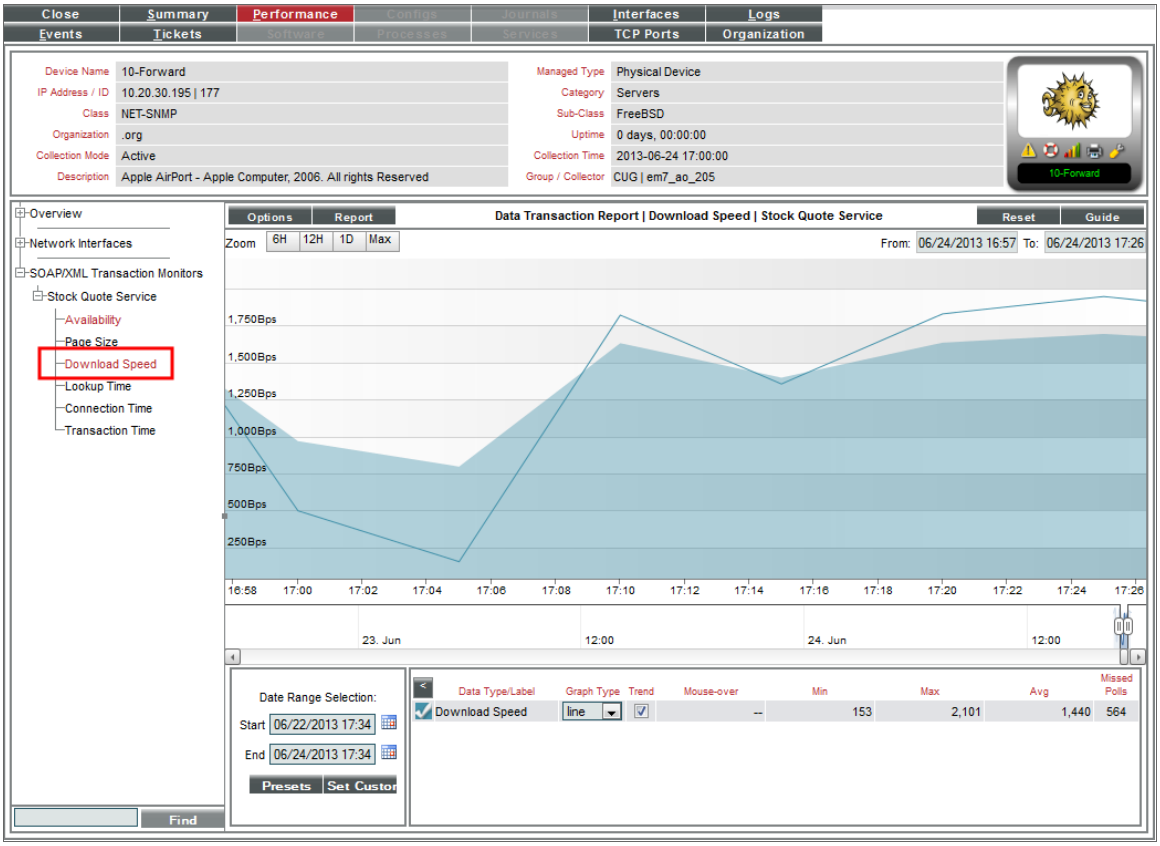
5. For each SOAP/XML Transaction policy, you can also view the following additional reports. To view them, select the appropriate entries in the NavBar:

    - ***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.



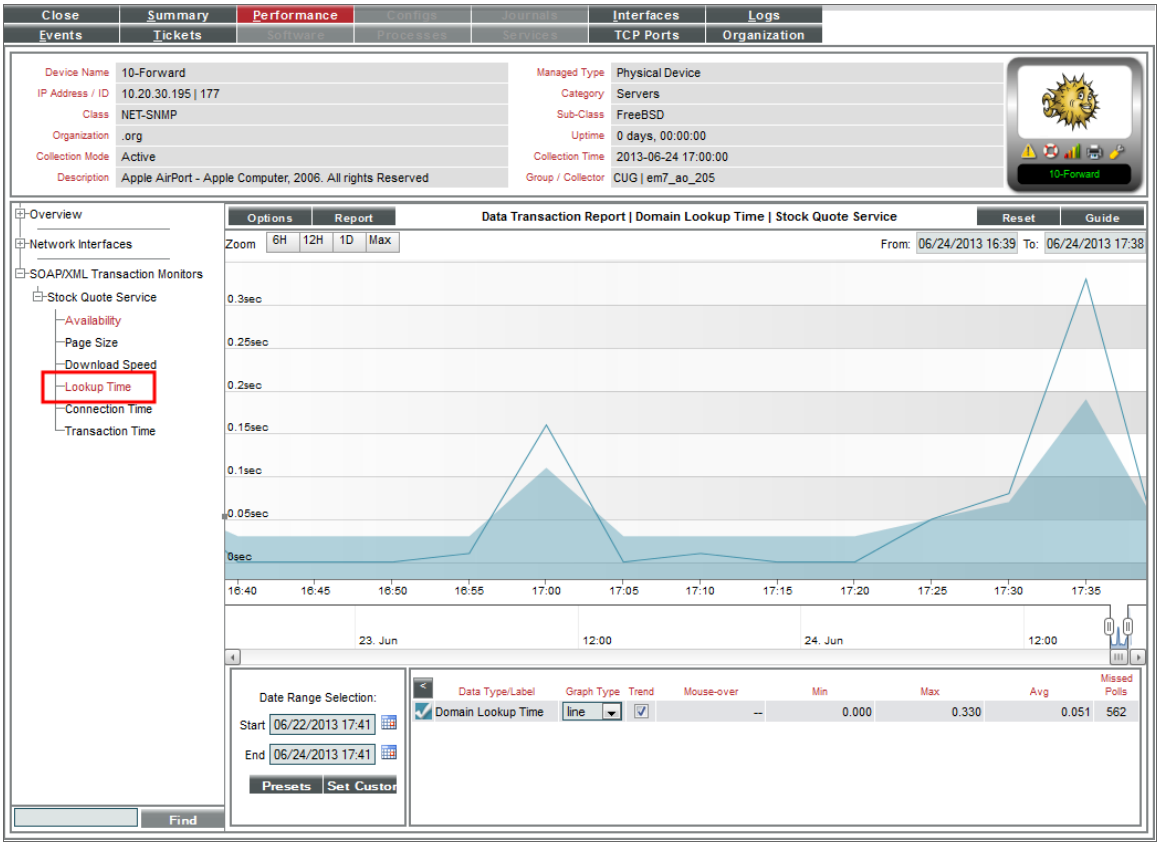
- The y-axis displays size in kilobytes per second (Kb).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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.



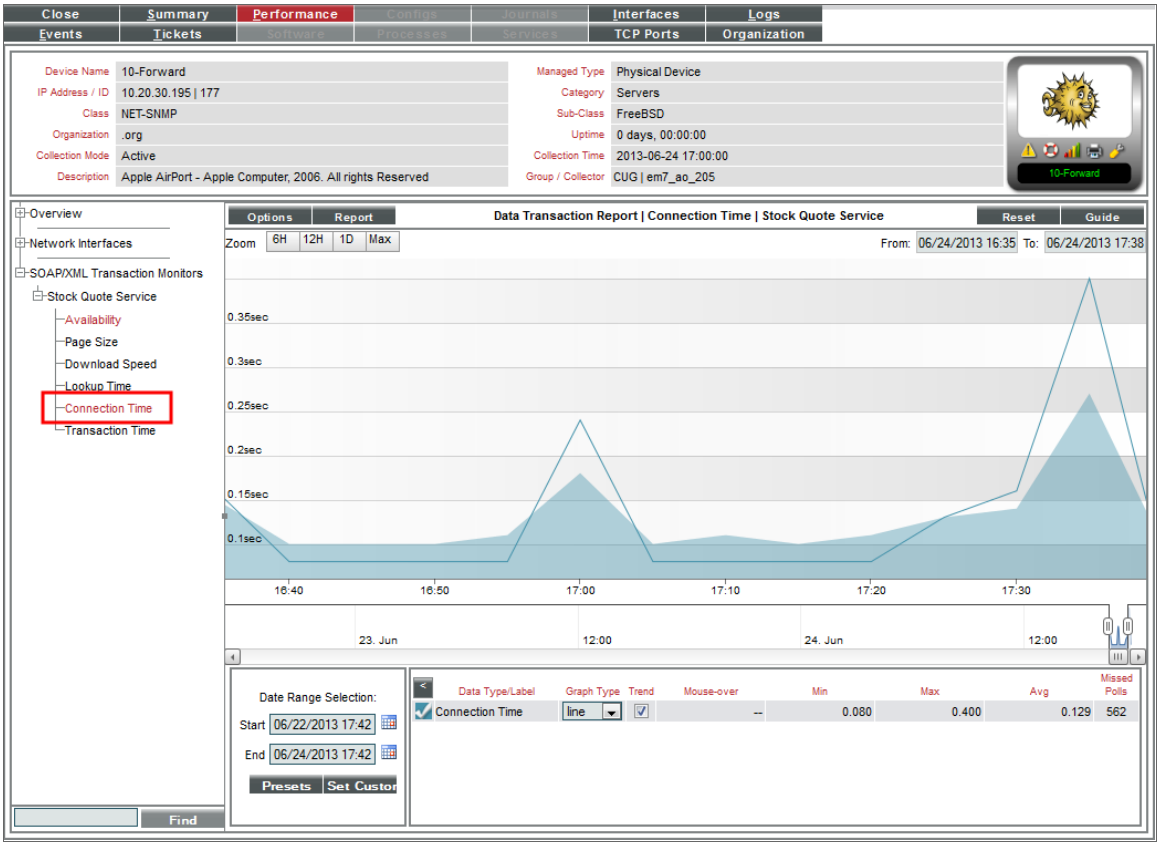
  - The y-axis displays the speed at which data was downloaded from the server to SL1, in (bits per second) Bps.
  - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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.



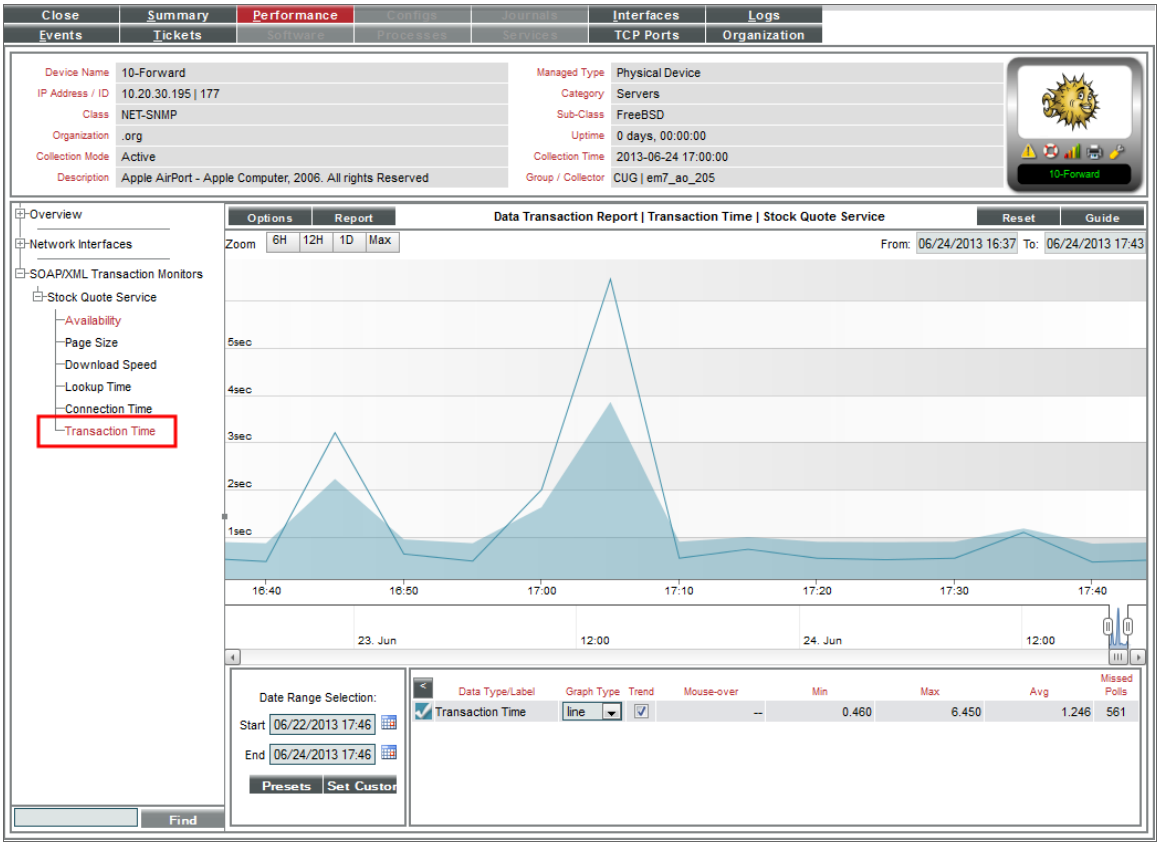
  - The y-axis displays the speed at which your DNS system was able to resolve the name of the server, in seconds.
  - The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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.

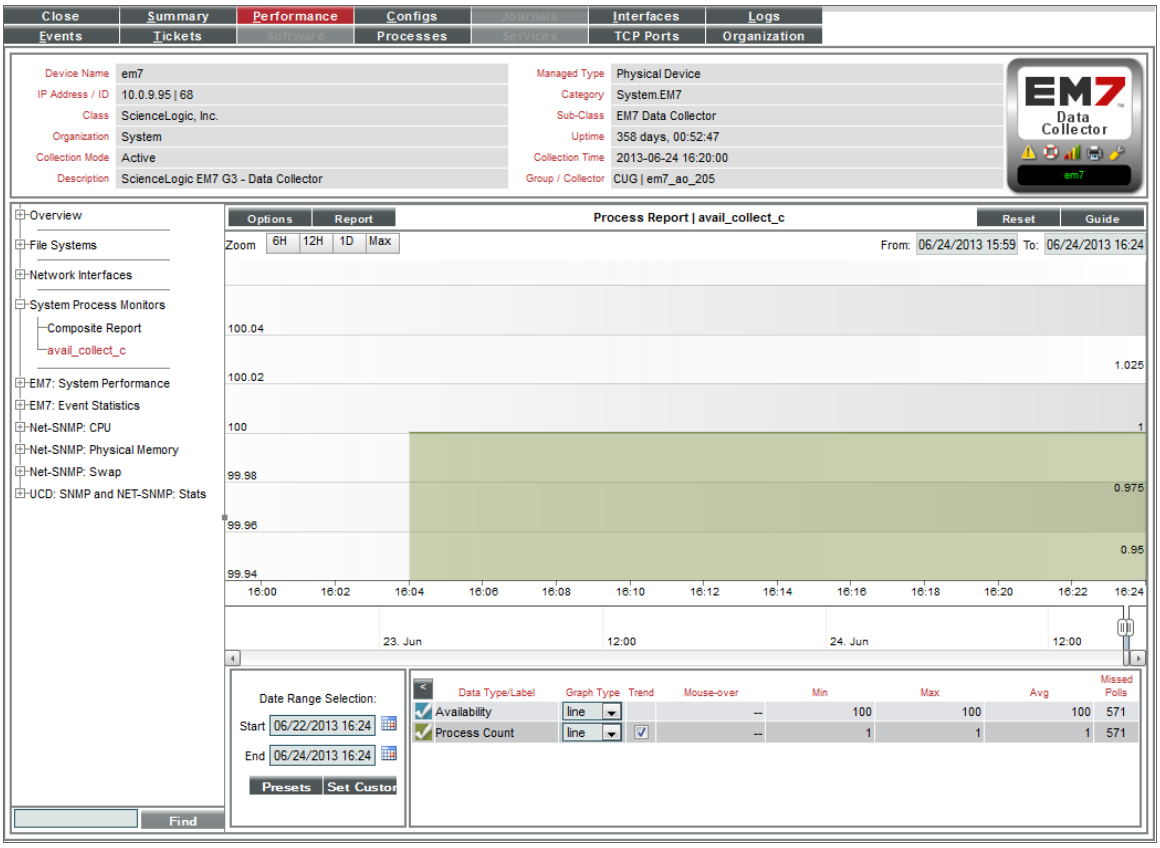
However, you might see values other than 100 or 0 in an availability report. If a report contains any other percentage, it is an average of multiple readings. For example, if SL1 gathered five readings and during one of those readings, a process was unavailable, the average would be 80% (100 + 100 + 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:

1. 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( ).
2. The **Device Performance** page appears, with the Process Report displayed.



3. 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).

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

5. 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.

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):

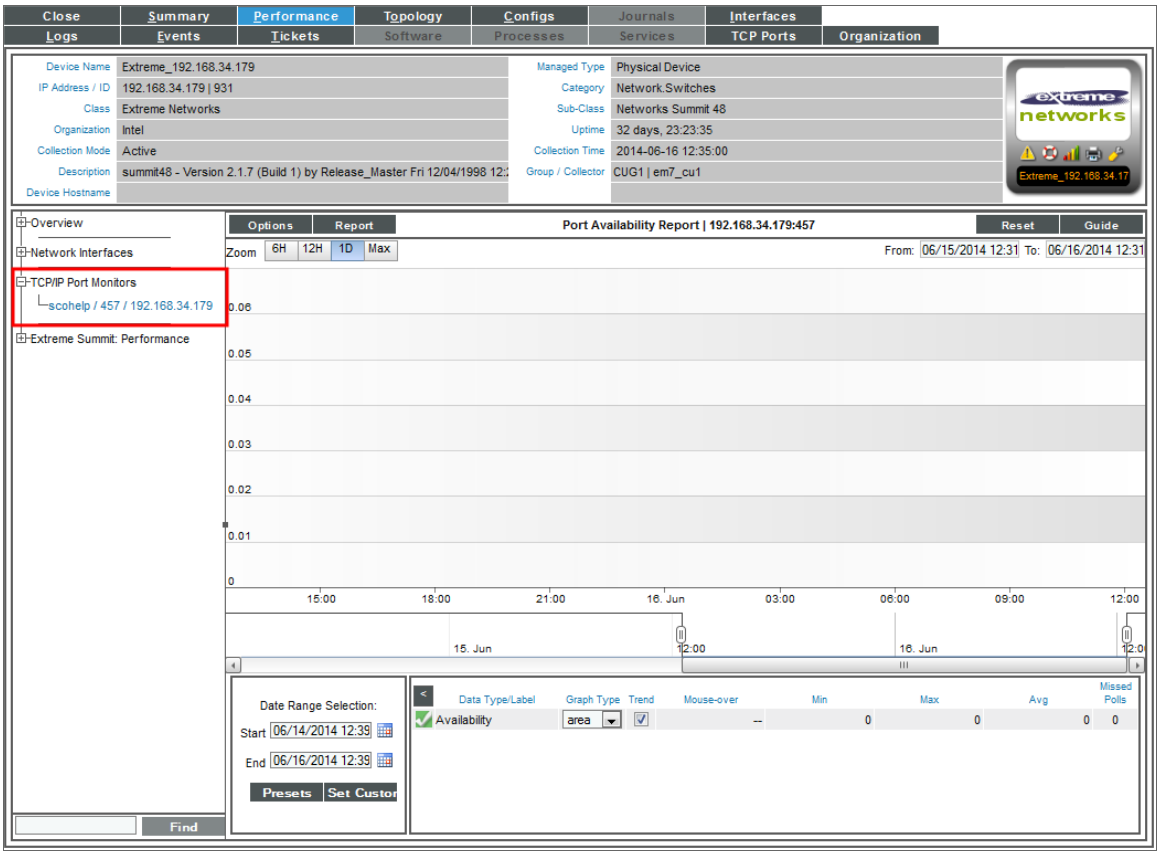
    - In the **Device Manager** page, find the device that is associated with the monitoring policy. Click the bar graph icon ( ) for the device.
    - In the **Device Reports** panel, click the **Performance** tab.
    - In the NavBar, expand TCP/IP Port Monitors and select the policy for which you want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

Or:

1. 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.
    - Click its bar graph icon ( ) in the *Port Number* field.

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



3. 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):

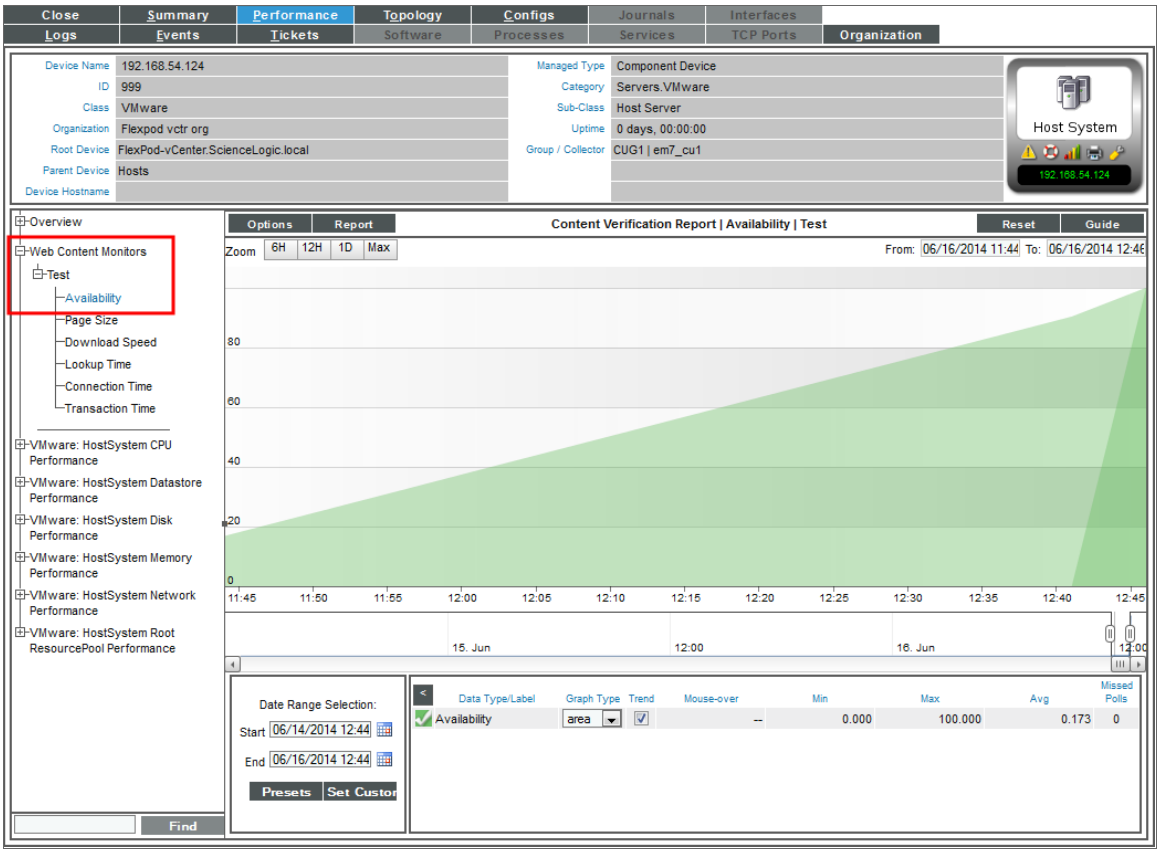
    - In the **Device Manager** page, find the device that is associated with the monitoring policy. Select the bar graph icon ( ) for the device.
    - In the Device Reports panel, select the **Performance** tab.
    - In the NavBar, expand Web Content Monitors and select the policy for which you want to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

Or:

1. 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 ( ).

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

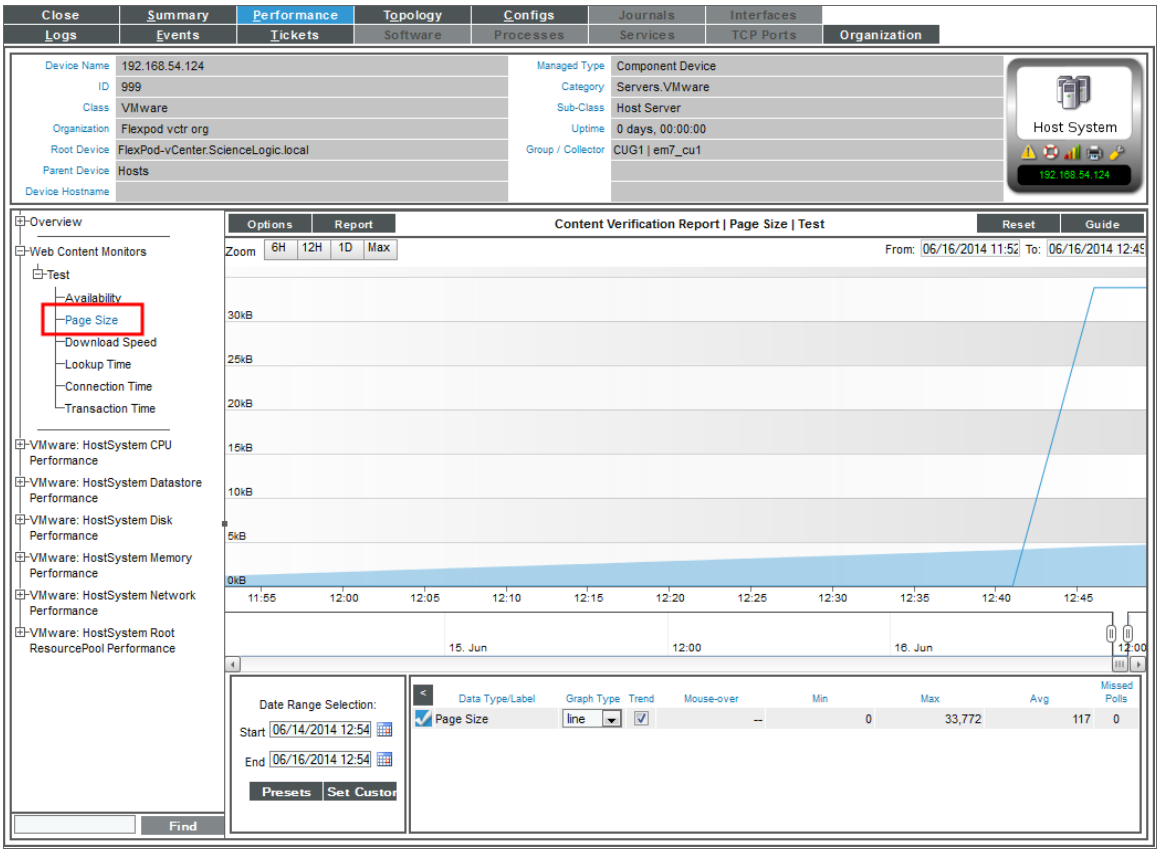


3. The Content Verification Report | Availability report displays the availability of the specified content on the specified web-server for the selected duration.

    - 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).

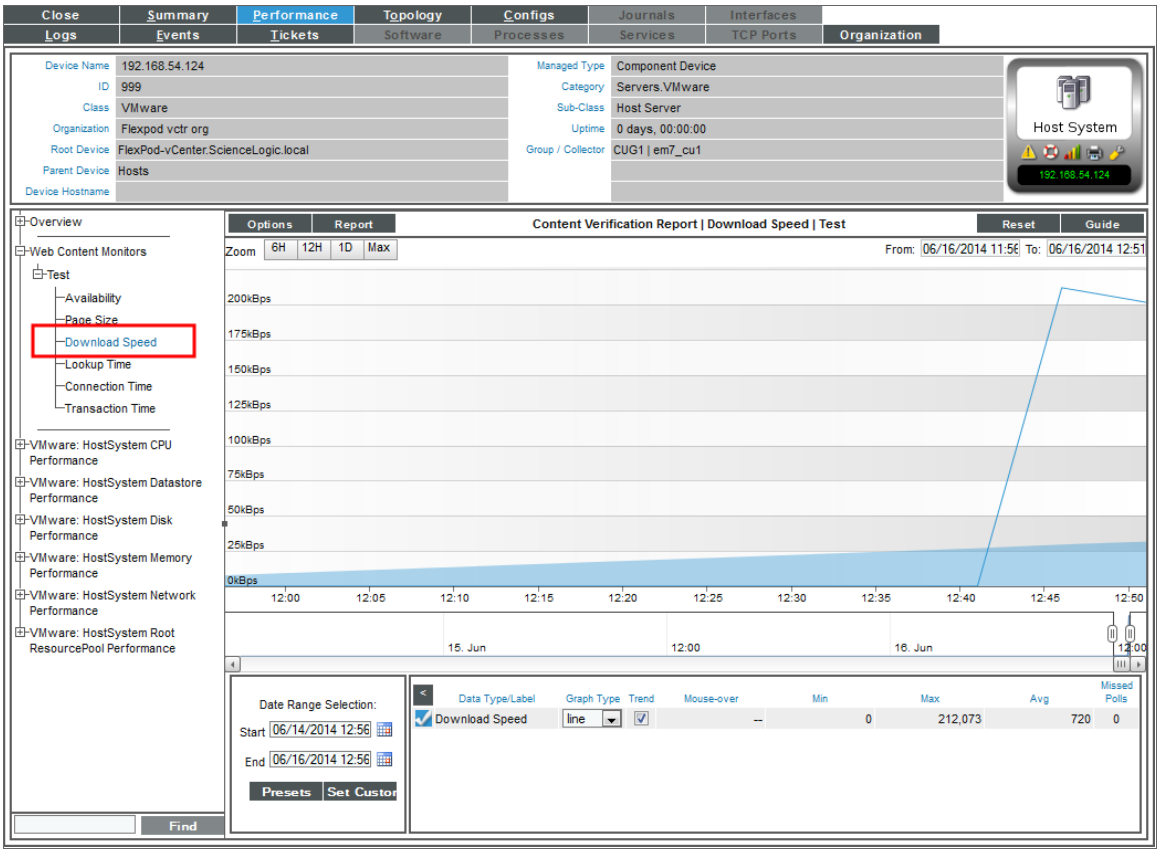
5. For each Web Content policy, you can also view the following additional reports. To view them select the entries in the NavBar:

    - ***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.



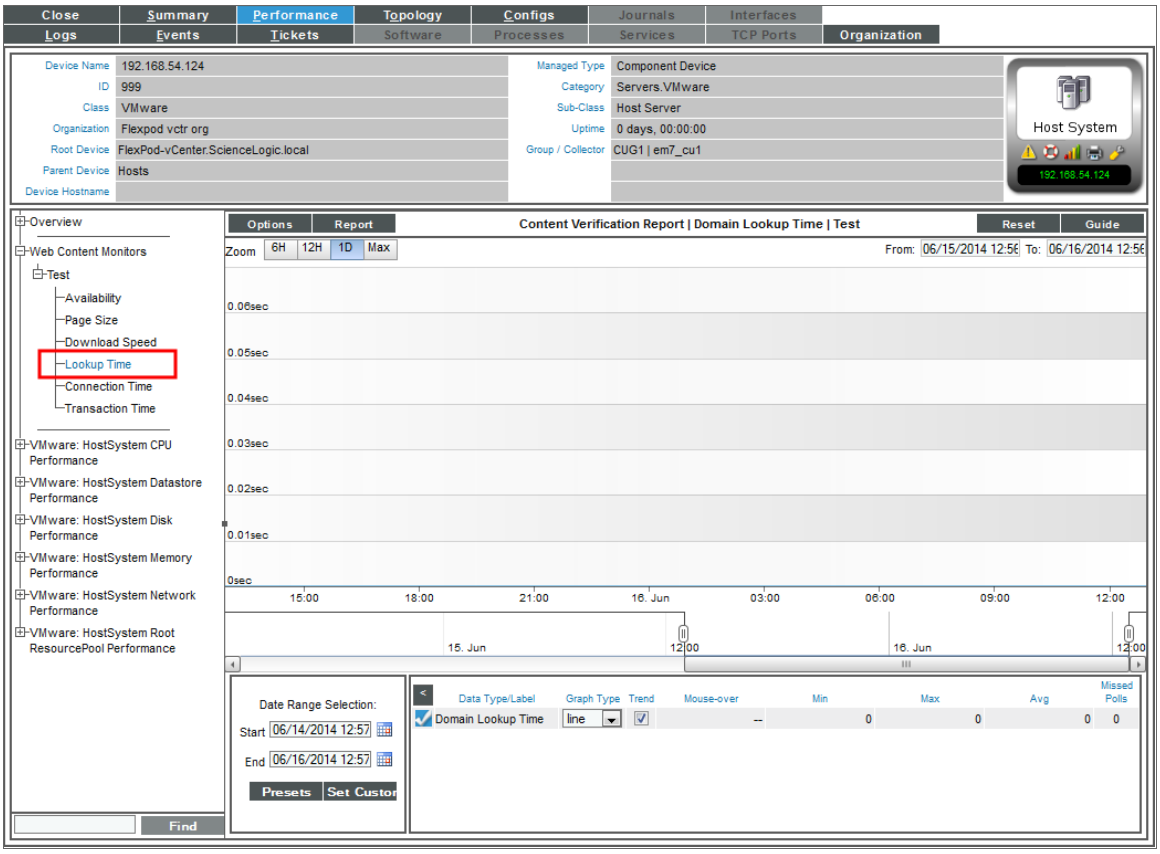
- The y-axis displays size in kilobytes (Kb).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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.



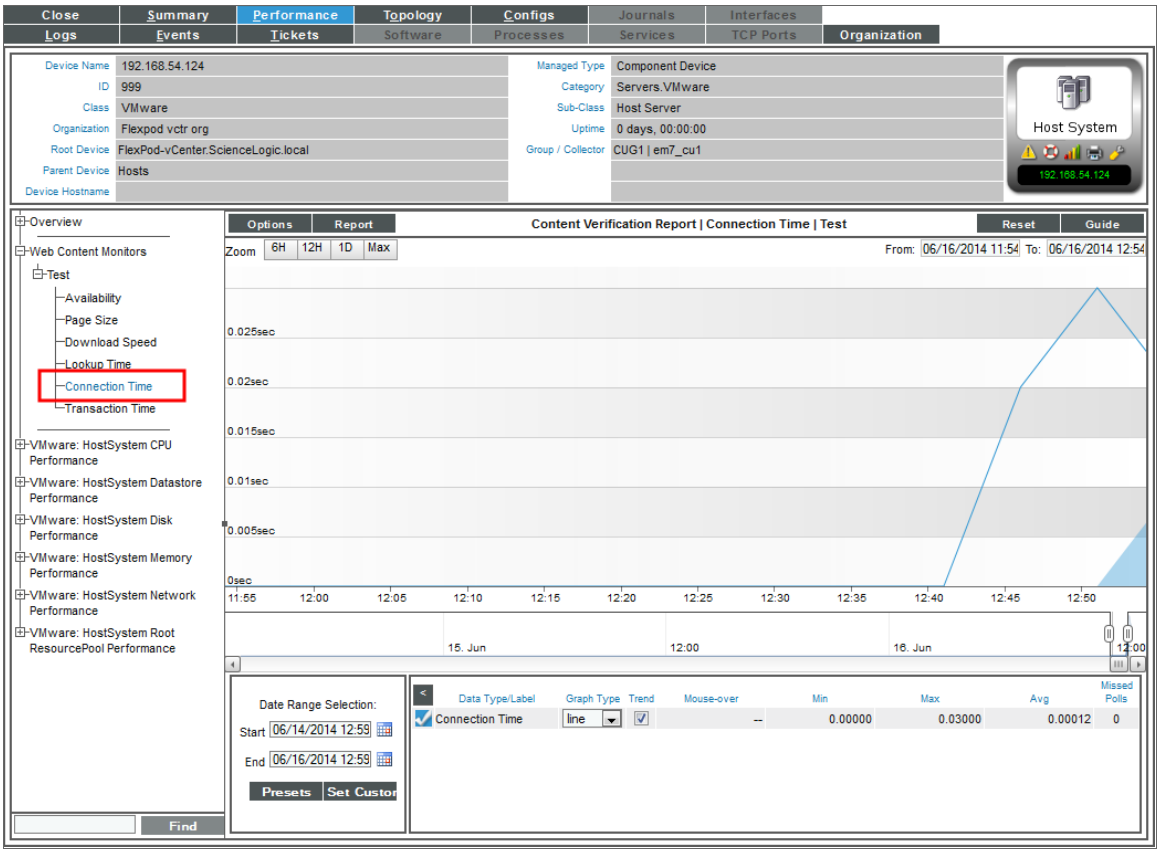
- The y-axis displays the speed at which data was downloaded from the website to SL1, in bits per second (Bps).
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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.



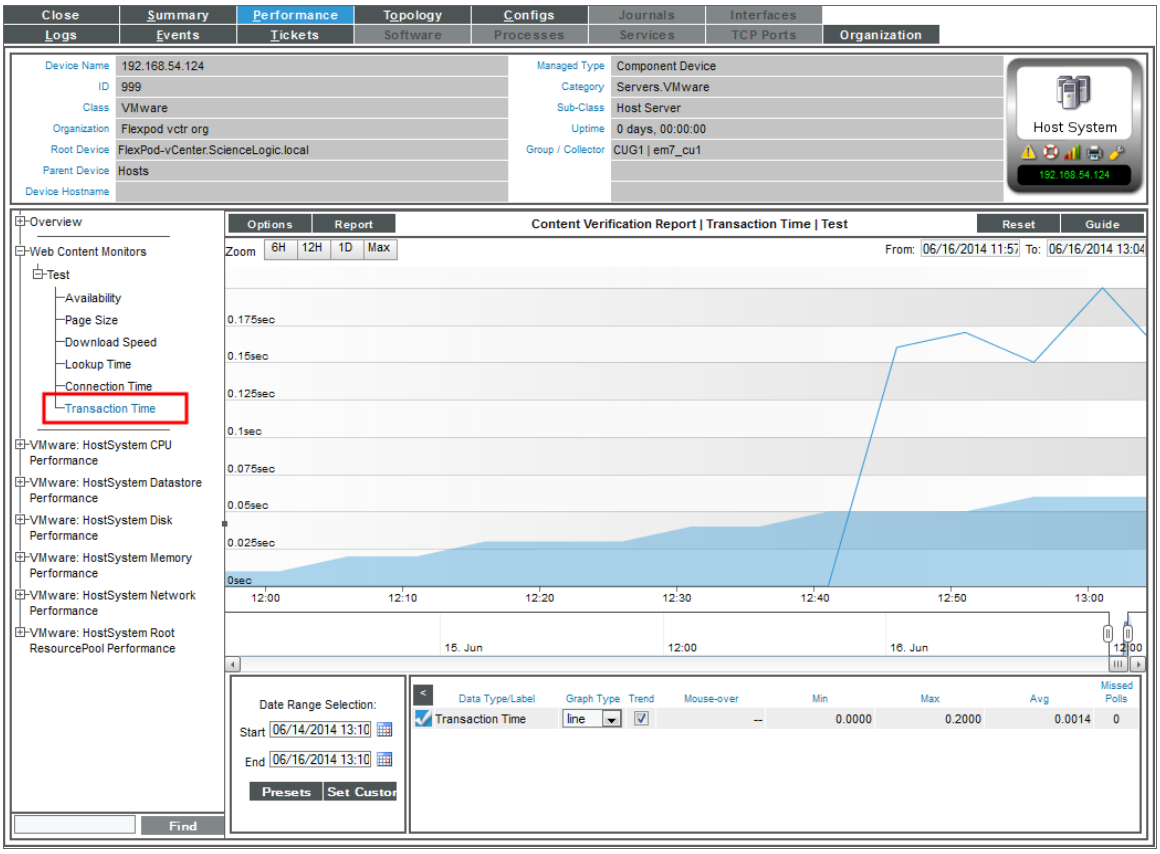
- The y-axis displays the speed at which your DNS system was able to resolve the name of the website, in seconds.
- The x-axis displays time. The increments vary, depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).

- ***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

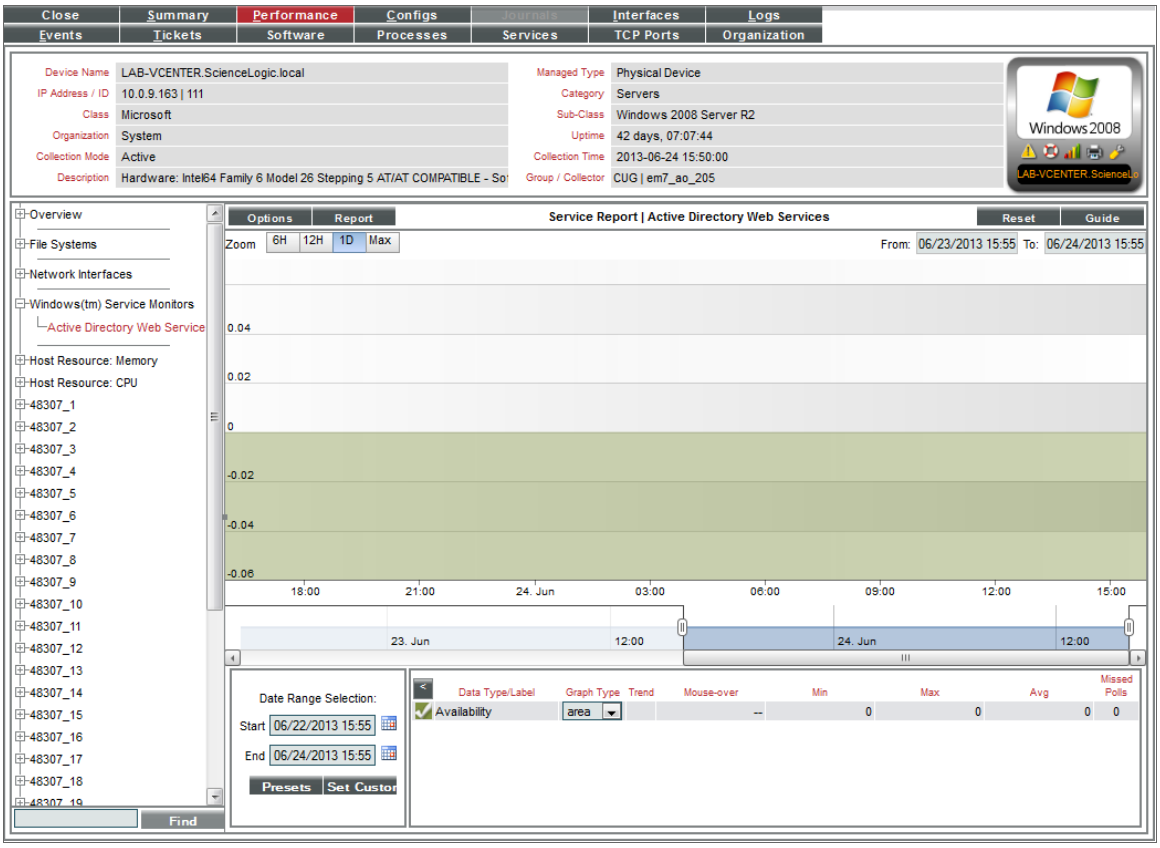
However, you might see values other than 100 or 0 in an availability report. If a report contains any other percentage, it is an average of multiple readings. For example, if SL1 gathered five readings and during one of those readings, a service was unavailable, the average would be 80% (100 + 100 + 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:

1. 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( ).
2. The **Device Performance** page appears, with the Service Report displayed.



3. 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).

Chapter 7

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 covers the following topics:

IPv4 Networks 125
Viewing the List of IPv4 Networks 126
Browsing a Network 130
Viewing Used and Unused IP Addresses in a Network 131
Viewing Devices Aligned with a Network 131
Viewing Interfaces Aligned with a Network 131
Viewing a Map of a Network 132
Generating a Report for a Network 132
Defining a New Network 133
Merging One or More Networks 134
Synchronizing One or More Networks 135

Editing a Network's Properties *136*
Performing Dynamic Discovery for a Network *136*
Creating a Ticket About a Network *137*
Deleting One or More IPv4 Networks *138*

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.

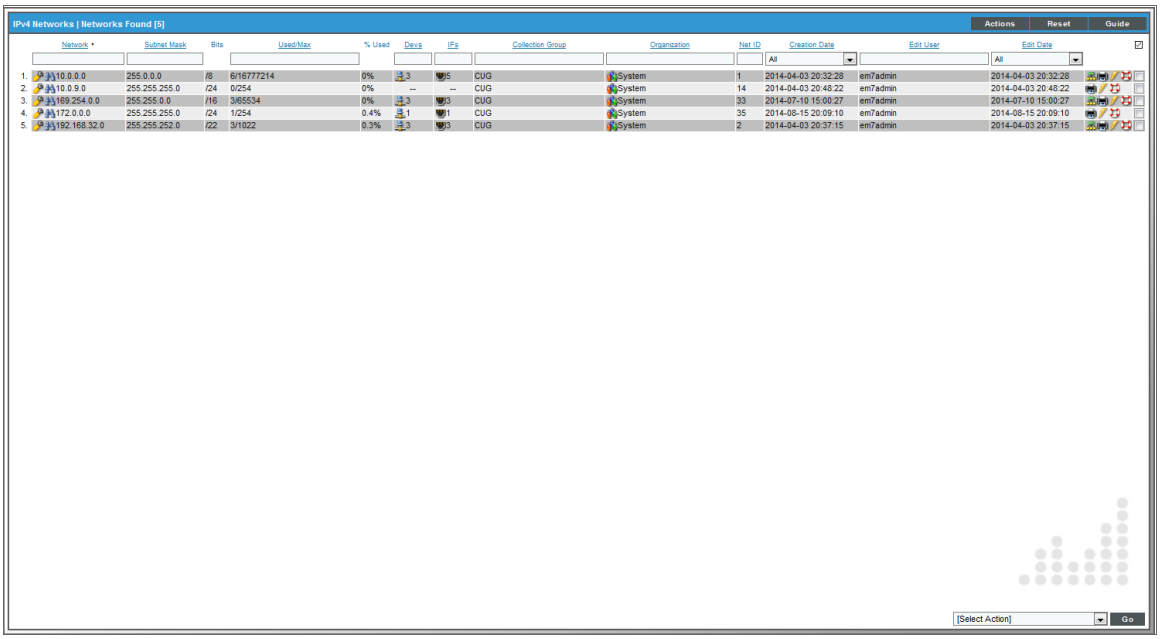
The **IPv4 Networks** page allows you to easily manage networks and IP addresses. From the **IPv4 Networks** page, you can view detailed data about the network, keep records of subnets, and determine which IP addresses are in use and which IP addresses are available.

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 **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.

Filtering the List of Networks

You can filter the list on the **IPv4 Networks** page by one or more parameters. Only IPv4 subnets that meet all the filter criteria will be displayed in the **IPv4 Networks** page.

To filter by parameter, enter text into the desired filter-while-you-type field. The **IPv4 Networks** page searches for IPv4 subnets 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:

- ***Network***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching network IP.
- ***Subnet Mask***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching subnet mask.
- ***Bits***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching number of bits in the network address.
- ***Used/Max***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching number of monitored IP addresses and/or a matching number of maximum allowed IP addresses.
- ***% used***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching percentage of monitored IP addresses in the subnet.
- ***Devs***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching number of discovered devices in the subnet.
- ***IFs***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching number of discovered network interfaces in the subnet.
- ***Collection Group***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching collector group.
- ***Organization***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that are associated with a matching organization.
- ***Net ID***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching network ID.
- ***Creation Date***. Only those subnets that match all of the previously selected fields and have the specified creation date will be displayed. The choices are:

    - *All*. Display all subnets that match the other filters.
    - *Last Minute*. Display only subnets that have been created within the last minute.
    - *Last Hour*. Display only subnets that have been created within the last hour.
    - *Last Day*. Display only subnets that have been created within the last day.
    - *Last Week*. Display only subnets that have been created within the last week.
    - *Last Month*. Display only subnets that have been created within the last month.
    - *Last Year*. Display only subnets that have been created within the last year.

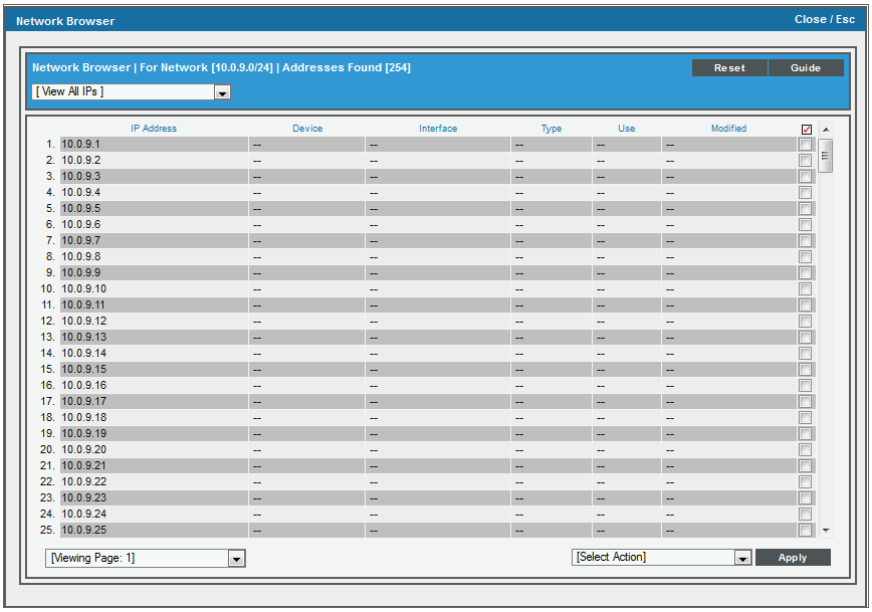
- ***Edit User***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **IPv4 Networks** page will display only subnets that have a matching username in the ***Edit User*** field.
- ***Edit Date***. Only those subnets that match all of the previously selected fields and have the specified last-edited date will be displayed. The choices are:

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

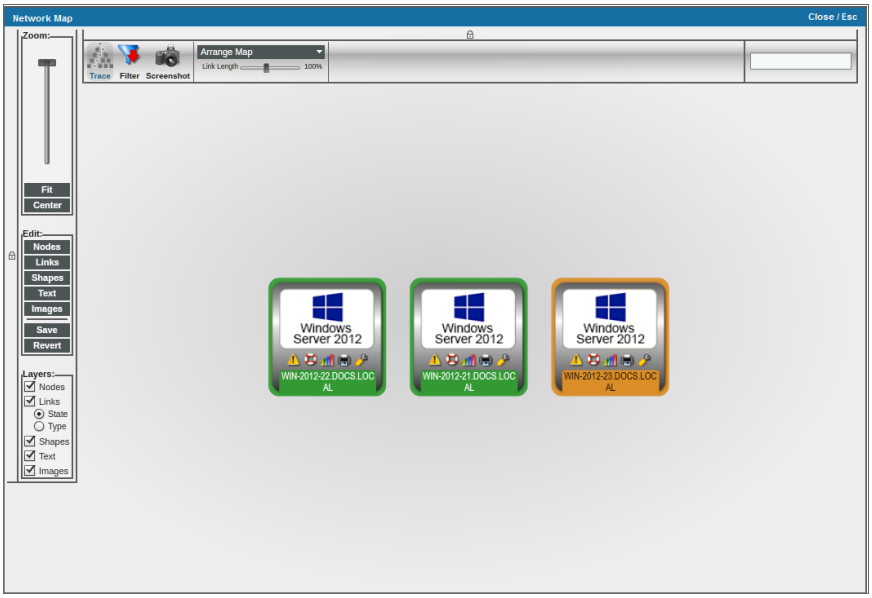
From the **IPv4 Networks** page, you can view a list of all interfaces in a network To do this:

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.

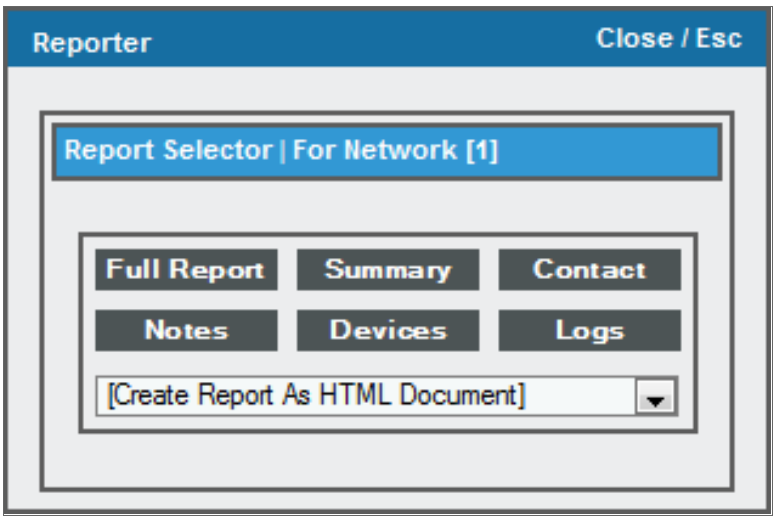


Generating a Report for a Network

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.

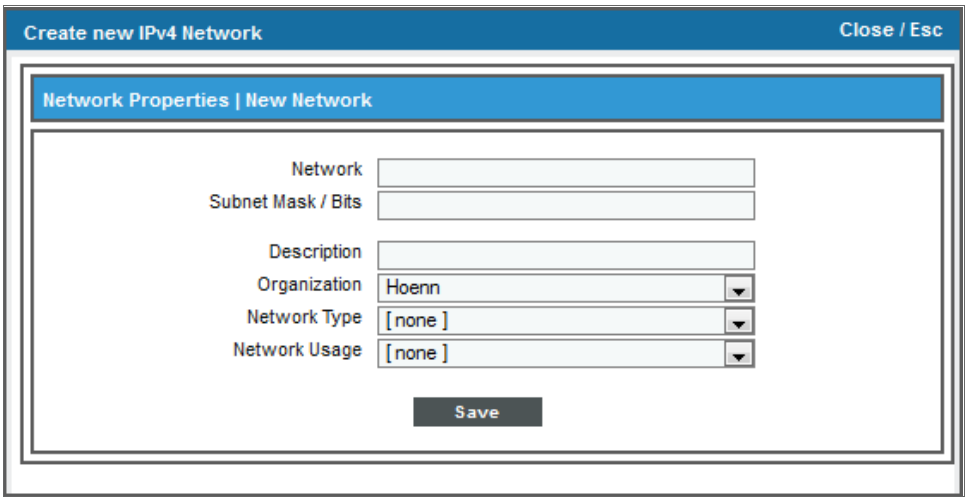
4. The **Report Creator** modal page appears. In this page, you can specify information to include in the report and the format in which to generate the report.



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:



- ***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.

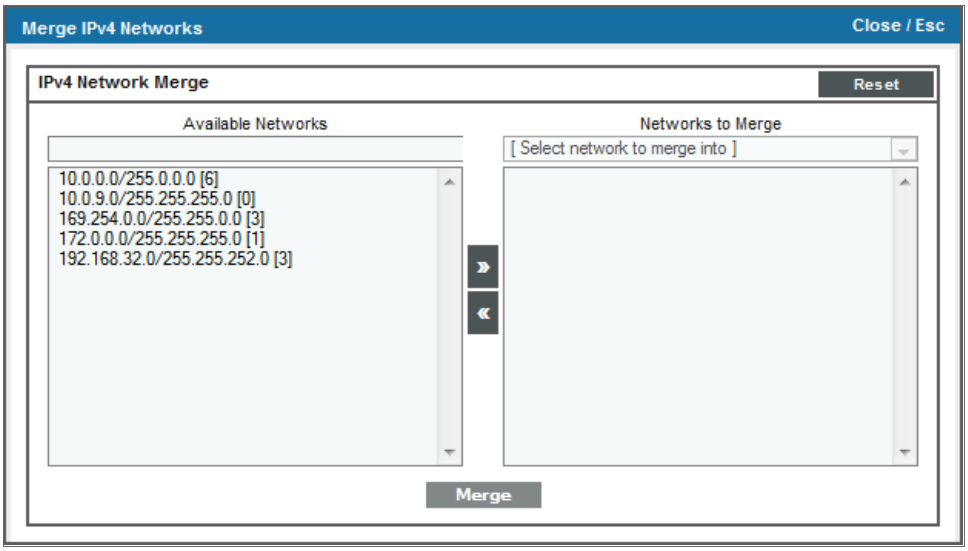
Merging One or More Networks

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.

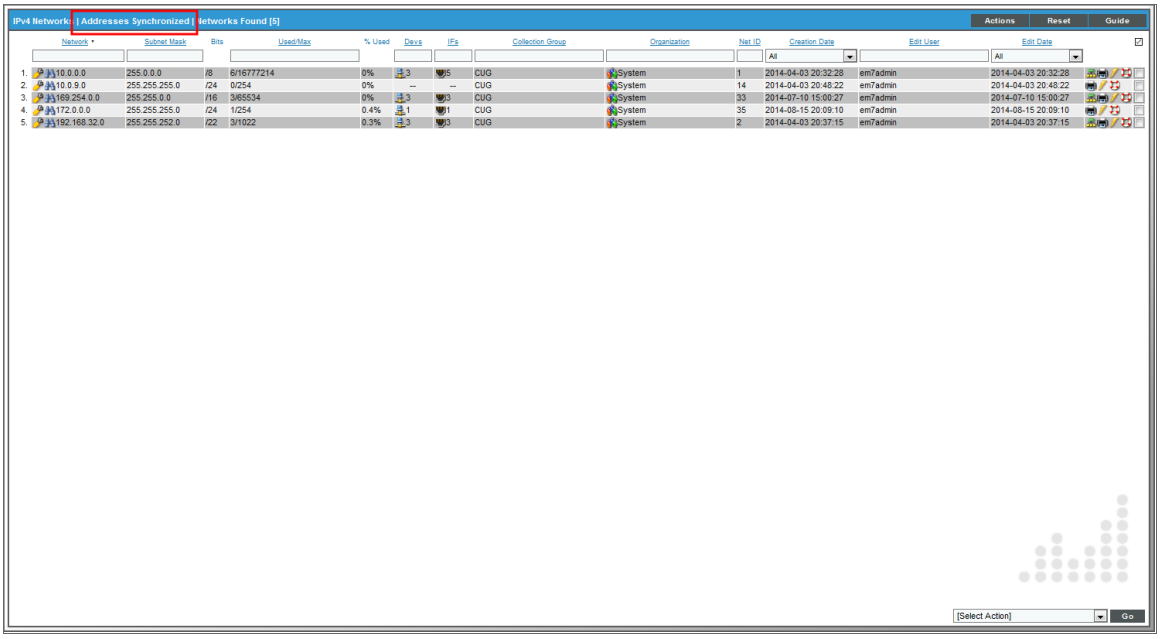
5. Click the **[Merge]** button to save the newly merged network.

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*.

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



Editing a Network's Properties

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

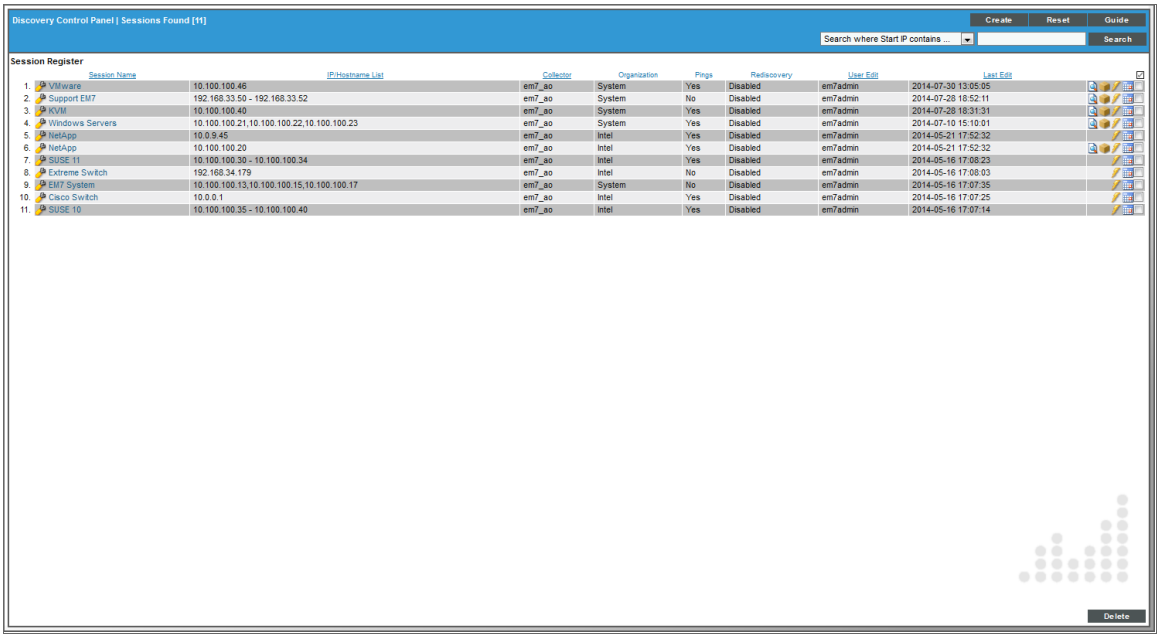
1. Go to the **IPv4 Networks** page (Registry > Networks > IPv4 Networks).
2. In the **IPv4 Networks** page, find the network you want to edit.
3. Click the wrench icon ( ) for that network. The **Network Properties** modal page appears.
4. In the **Network Properties** modal page, you can edit the *values for one or more parameters*.
5. 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:

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 perform dynamic discovery. Click the lightning bolt icon ( ) for that network.

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

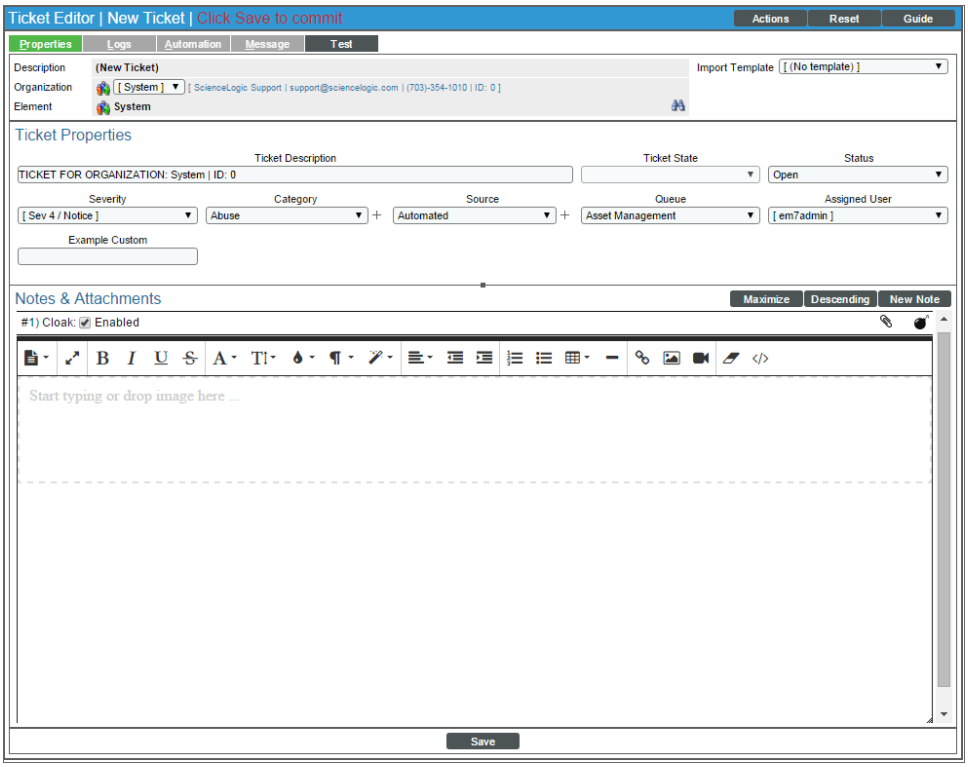


Creating a Ticket About a Network

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:

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 create a ticket.
3. Click the ticket icon ( ) for that network.
4. 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.



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 8

Monitoring Network Interfaces

Overview

This chapter describes how to monitor network interfaces in SL1.

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

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

This chapter covers the following topics:

Discovering Interfaces 139
Viewing a List of All Interfaces Discovered by SL1 140
Viewing Interfaces for a Single Device 143
Global Settings that Affect Interfaces 148
Defining Interface Monitoring Policies and Thresholds 162
Class-Based Quality of Service (CBQoS) 178
Concurrent Network Interface Collection 184
Viewing Performance Graphs and Reports About Interfaces 187

Discovering Interfaces

During the discovery process, SL1 discovers all interfaces on each discovered device. 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 (Registry > Networks > Interfaces) allows you to view a list of all discovered interfaces, view details about each interface, edit the monitoring policy for an interface, and view bandwidth reports for each interface.

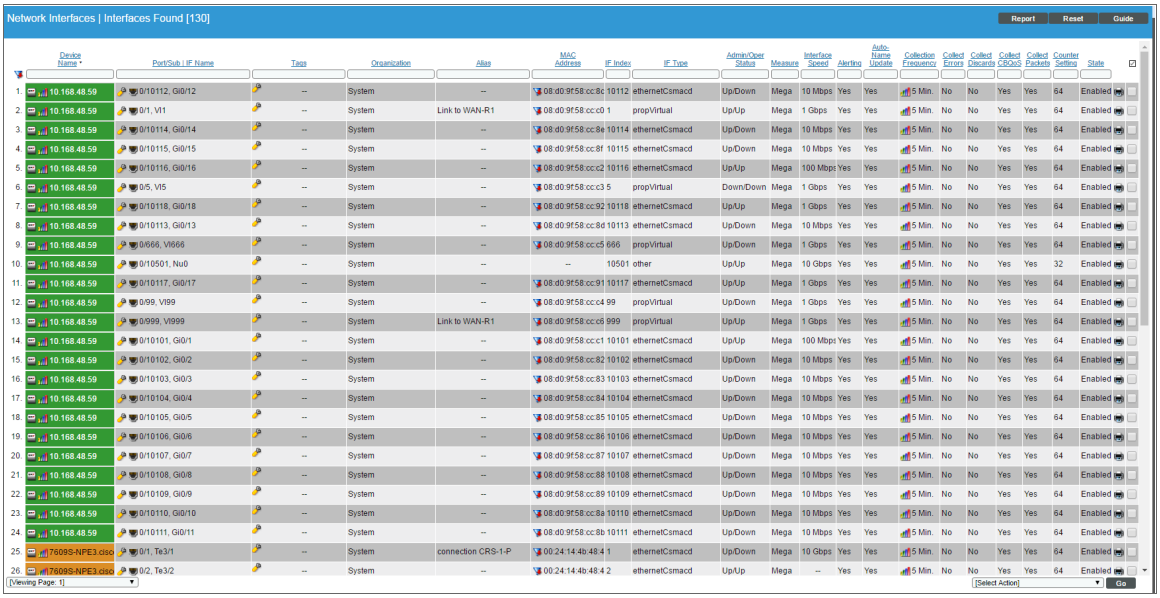
Viewing a List of All Interfaces Discovered by SL1

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 about each interface, define a monitoring policy for an interface, and view bandwidth reports for 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.



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. You 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 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***. 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 (IANA).
- ***Status***. Consists of two parts:
    - *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.
        - Down. Network interface has been 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 or 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 overwrite the interface name during auto-discovery.

    - *Yes*. SL1 can update and/or overwrite the interface name during auto-discovery.
    - *No*. SL1 will not update and/or overwrite 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 about packet errors on the interface. Packet errors can occur when packets are lost due to network outages 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 about interface discards. Discards can occur when an interface receives more traffic than it can handle. Discards can also occur when an interface has been specifically configured to discard packets. For example, a network administrator might configure a router's interface to discard packets from an unauthorized IP. Your choices are:

    - *Yes*. SL1 will collect data about packet discards that occur on the interface.
    - *No*. SL1 will not collect data about 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.

  For more information about CBQoS, see the ***Infrastructure Health*** manual.
- ***Collect Packets***. Specifies whether SL1 will collect network traffic data, 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.

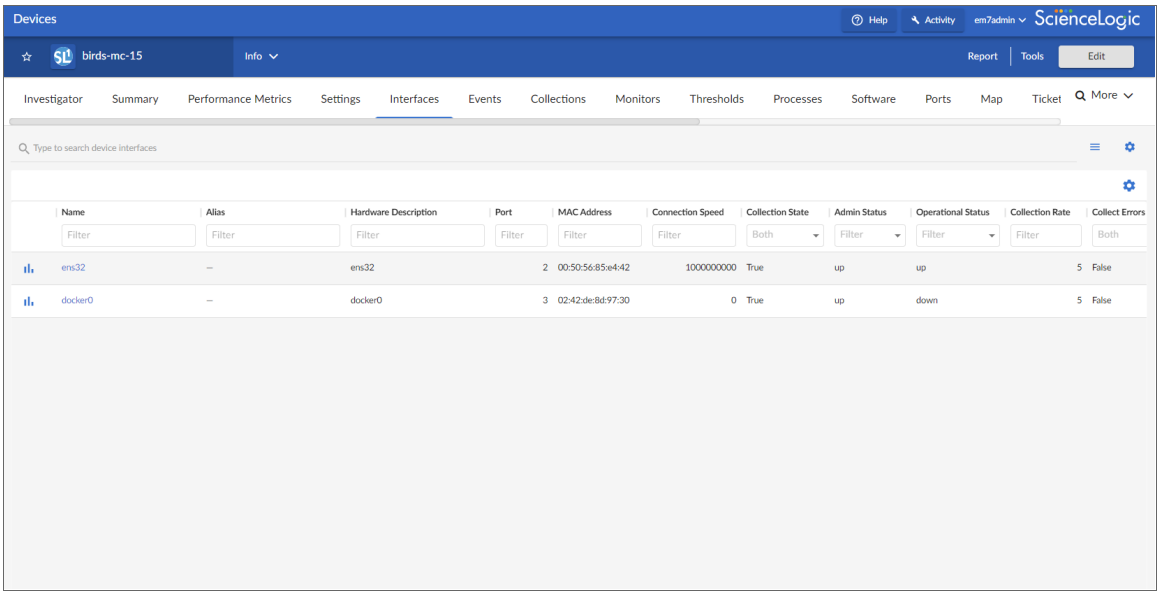
NOTE: If an interface has a status of "down" during initial discovery, SL1 will discover the interface but assign the interface the default Counter Setting of "32". During re-discovery or nightly auto-discovery, SL1 will update Counter Setting to "64" if applicable.

- ***State***. Specifies whether SL1 monitors the network interface and collects data about the network interface for reports. Can be either *Enabled* or *Disabled*.
- ***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

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.

On the **[Interfaces]** tab of the **Device Investigator** page, you can view information about each network interface on the device. From this tab, you can also *define monitoring policies for interfaces on the device*.



NOTE: You can view an interface's network utilization graph in a new window by clicking the bar graph icon ( ) next to the name of the interface.

NOTE: The data displayed on this tab is read-only.

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

- ***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.
- ***Hardware Description***. Description of the network interface. Usually a description of a network interface card.
- ***Port***. The interface port.
- ***MAC Address***. A unique number that identifies the interface. MAC Addresses are defined by the hardware manufacturer.
- ***Connection Speed***. The amount of data, in Megabytes per second, that the interface can process.
- ***Collection State***. Specifies whether the platform monitors the network interface and collects data from the network interface for reports. Can be either *Enabled* or *Disabled*.

- ***Admin Status***. Specifies how the network interface has been configured on the device. Can be one of the following:
    - *Up*. Network interface has been enabled.
    - *Down*. Network interface has been 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 or receive data.
- ***Collection Rate***. Specifies (in minutes) how often SL1 collects data from the interface.
- ***Collect Errors***. Specifies whether SL1 will collect data about packet errors on the interface. Packet errors can occur when packets are lost due to network outages or faulty adapter hardware.
- ***Collect Discards***. Specifies whether SL1 will collect data about interface discards. Discards occur when an interface receives more traffic than it can handle. Discards can also occur when an interface has been specifically configured to discard. For example, a network administrator might configure a router's interface to discard packets from an unauthorized IP address.
- ***Alerts***. Specifies whether SL1 will generate events for the interface. Can be *Enabled* or *Disabled*. 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.
- ***Index***. A unique number greater than zero that identifies each interface on a device. These numbers are defined by the device.

Clicking an interface ***Name*** opens the **Interface Properties** page for that interface. This page enables you to view the properties for that interface and ***define a monitoring policy for the interface***.

> **NOTE:** You can also access the **Interface Properties** page by clicking the **[Actions]** button (···) for that interface and selecting *Manage Interface*.

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.

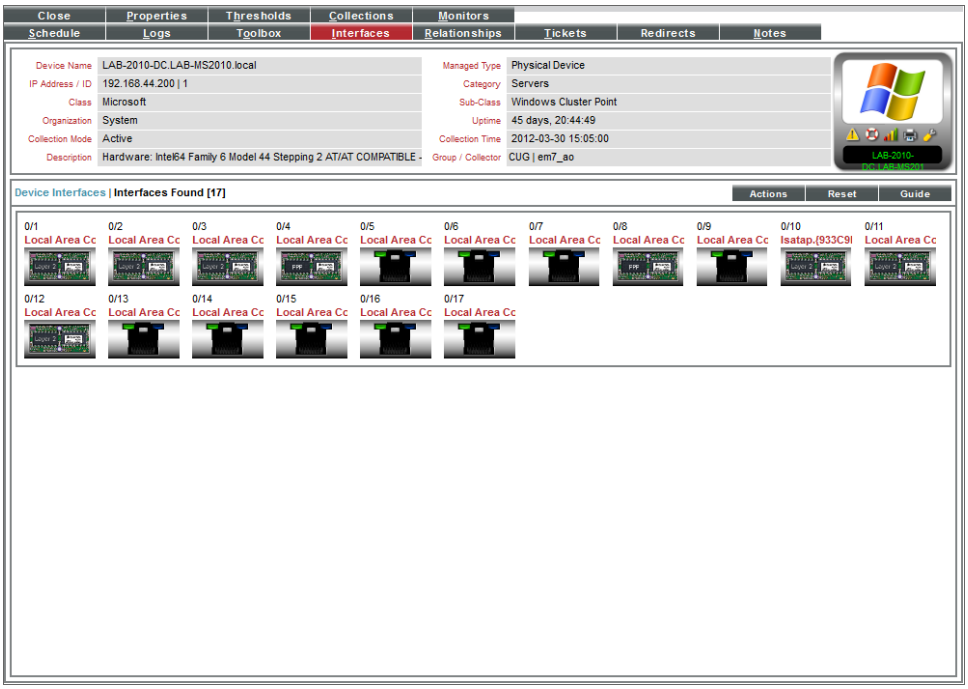
Viewing Interfaces for a Single Device in the Classic User Interface

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.

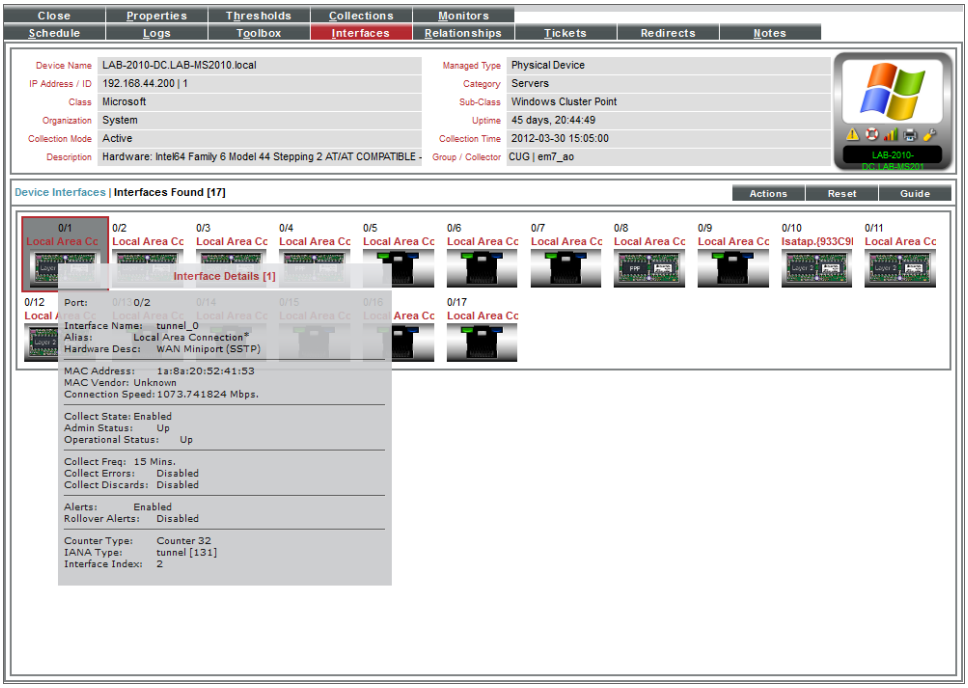
To view details about the network interfaces on a device:

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.
3. Both pages display icons to represent the interfaces on the device:



4. The page displays an icon for each interface on the device. Each icon provides a visual overview of the interface.
5. 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** pop-up window appears. This window displays details about the interface and its current monitoring policy.



7. The **Interface Details** pop-up window 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***. 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 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 or 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 about packet errors on the interface. Packet errors occur when packets are lost due to hardware problems such as network outages or faulty adapter hardware.
- ***Collect Discards***. Specifies whether or not SL1 will collect data about interface discards. Discards occur when an interface receives more traffic than it can handle. Discards can also occur when an interface has been specifically configured to discard. For example, a network administrator might configure a router's interface to discard packets from an unauthorized 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.
9. In the **Interfaces Found** page, clicking on an interface icon leads to the Network Bandwidth Usage report in the **Device Performance** page.

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 you can override these settings for a specific device on the **Settings** tab of the **Device Investigator** page or the **Device Properties** page (Devices> Device Manager > wrench icon) in the classic user interface.

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 all 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 CBQoS, see the section on *Class-Based Quality of Service*.)
- ***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.
- ***Enable Concurrent Network Interface Collection***. If selected, enables asynchronous concurrent SNMP collection for all network interfaces. This provides better scalability for large networks by allowing multiple collection tasks to run at the same time with a reduced load on Data Collectors. (For more information, see the section on *Concurrent Network Interface Collection*.)

NOTE: You can also enable or disable concurrent network interface collection for individual collector groups using the ***Enable Concurrent Network Interface Collection*** field on the **Collector Group Management** page (System > Settings > Collector Groups). This setting overrides the global setting for concurrent network interface collection for the selected collector group. For more information, see the section on *Configuring Concurrent Network Interface Collection for a Collector Group*.

NOTE: If you do not enable concurrent network interface collection, then ScienceLogic recommends that you maintain a limit of no more than 10,000 interfaces per SL1 Data Collector; there is no recommended limit to the number of interfaces you can monitor per Data Collector if concurrent network interface collection is enabled.

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

Interface Threshold Defaults

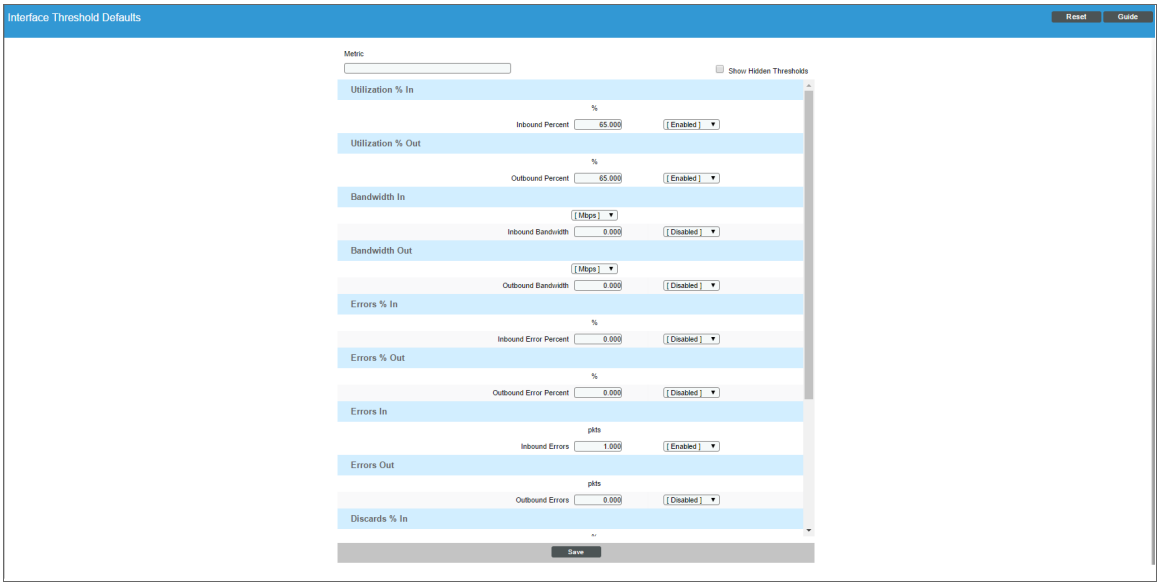
The **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) allows you to define global thresholds for interfaces.

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**, **kbps**, **Mbps** (the default), or **Gbps**.

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

Threshold	Default Value	Default Status
Errors Out > Outbound Errors	1000.000	Enabled
Discard % In > Inbound Discard Percent	1.000	Enabled
Discards % Out > Outbound Discard Percent	1.000	Enabled
Discards In > Inbound Discards	1000.000	Enabled
Discards Out > Outbound Discards	1000.000	Enabled
Multicast % In > Rising Medium	30.000	Disabled
Multicast % In > Rising Low	20.000	Disabled
Broadcast % Out > Rising Medium	30.000	Disabled
Broadcast % Out > Rising Low	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
Utilization % In > Rising High	0.000	Hidden
Utilization % In > Rising Medium	0.000	Hidden
Utilization % In > Rising Low	0.000	Hidden
Utilization % In > Falling Low	0.000	Hidden
Utilization % In > Falling Medium	0.000	Hidden
Utilization % In > Falling High	0.000	Hidden
Utilization % In > Inbound Percent	65.000	Enabled
Utilization % Out> Rising High	0.000	Hidden
Utilization % Out > Rising Medium	0.000	Hidden
Utilization % Out > Rising Low	0.000	Hidden
Utilization % Out > Falling Low	0.000	Hidden
Utilization % Out > Falling Medium	0.000	Hidden
Utilization % Out > Falling High	0.000	Hidden
Utilization % Out > Outbound Percent	65.000	Enabled

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

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

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

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

Threshold	Default Value	Default Status
Multicast Out > Falling Medium	0.000	Hidden
Multicast Out > Falling High	0.000	Hidden
Unicast % In > Rising High	0.000	Hidden
Unicast % In > Rising Medium	00.000	Hidden
Unicast % In > Rising Low	00.000	Hidden
Unicast % In > Falling Low	0.000	Hidden
Unicast % In > Falling Medium	0.000	Hidden
Unicast % In > Falling High	0.000	Hidden
Unicast % Out > Rising High	0.000	Hidden
Unicast % Out > Rising Medium	00.000	Hidden
Unicast % Out > Rising Low	00.000	Hidden
Unicast % Out > Falling Low	0.000	Hidden
Unicast % Out > Falling Medium	0.000	Hidden
Unicast % Out > Falling High	0.000	Hidden
Unicast In > Rising High	0.000	Hidden
Unicast In > Rising Medium	0.000	Hidden
Unicast In > Rising Low	0.000	Hidden
Unicast In > Falling Low	0.000	Hidden
Unicast In > Falling Medium	0.000	Hidden
Unicast In > Falling High	0.000	Hidden
Unicast Out > Rising High	0.000	Hidden
Unicast Out > Rising Medium	0.000	Hidden
Unicast Out > Rising Low	0.000	Hidden
Unicast Out > Falling Low	0.000	Hidden
Unicast Out > Falling Medium	0.000	Hidden
Unicast Out > Falling High	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:
  - kbps
  - Mbps
  - Gbps

Quality of Service Threshold Defaults

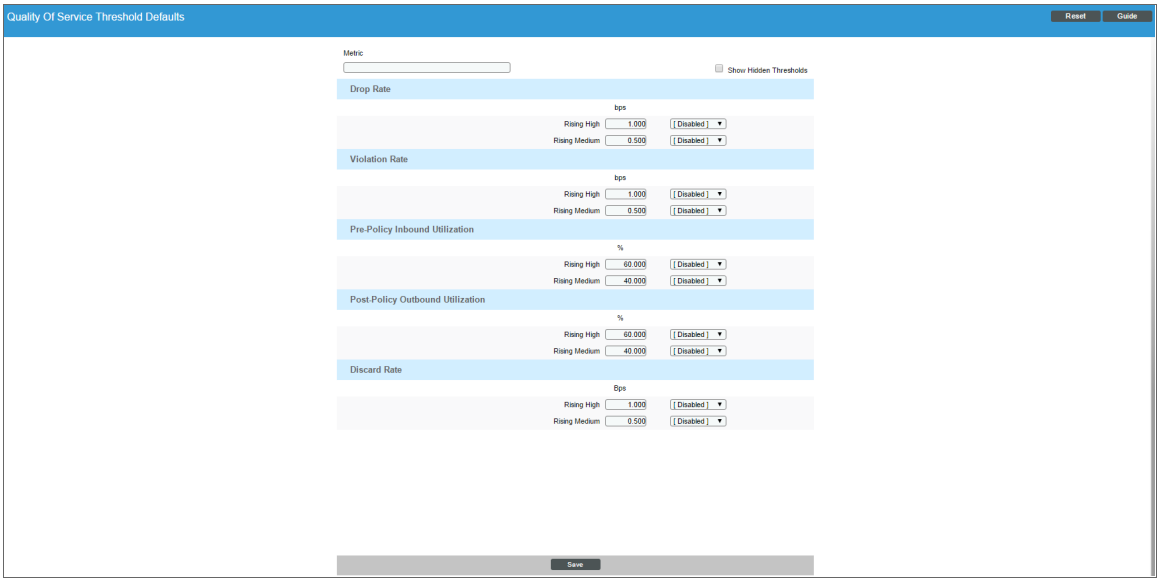
The **Quality of Service Threshold Defaults** page (System > Settings > Thresholds > Quality of Service) allows you to define global thresholds for CBQoS objects.

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
Drop Rate > Rising High	1.000	Disabled
Drop Rate > Rising Medium	0.500	Disabled
Violation Rate > Rising High	1.000	Disabled
Violation Rate > Rising Medium	0.500	Disabled
Pre-Policy Inbound Utilization % > Rising High	60.000	Disabled
Pre-Policy Inbound Utilization % > Rising Medium	40.000	Disabled
Pre-Policy Outbound Utilization % > Rising High	60.000	Disabled
Pre-Policy Outbound Utilization % > Rising Medium	40.000	Disabled
Discard Rate > Rising High	1.000	Disabled
Discard Rate > Rising Medium	0.500	Disabled

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

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

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

Threshold	Default Value	Default Status
Discard Rate > Falling Low	0.000	Hidden
Discard Rate > Falling Medium	0.000	Hidden
Discard Rate > Falling High	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 **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).

Defining Interface Monitoring Policies and Thresholds

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:

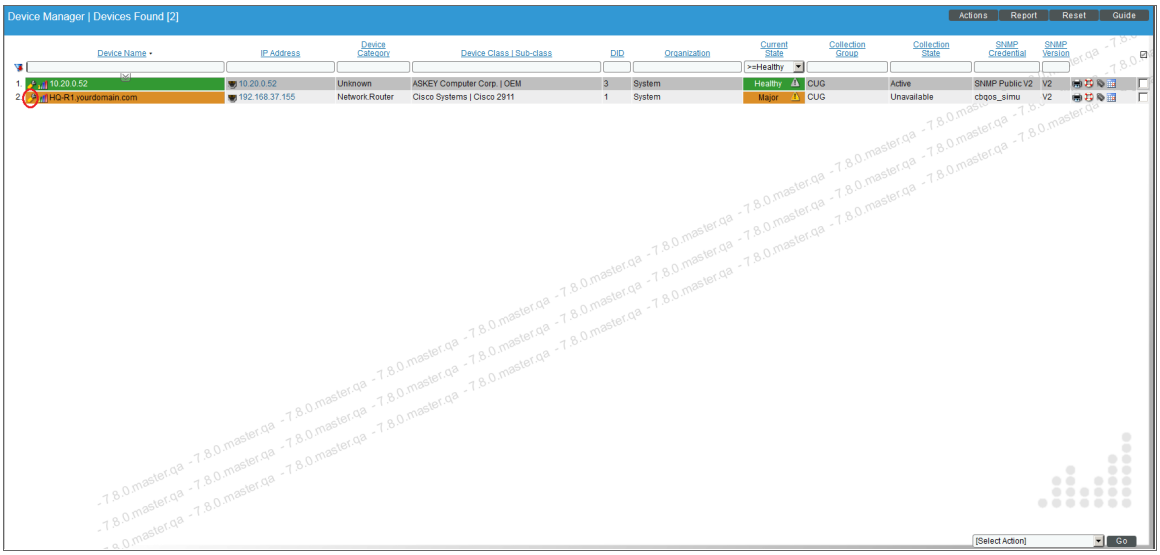
- Define a detailed policy for a single interface at a time.
- Define a single policy setting for multiple interfaces at a time.

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



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

4. 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. In this page, you can define a detailed monitoring policy for the selected interface.

6. 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 set ***Collect State*** to *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.

NOTE: In the **Network Interfaces** page (Registry > Networks > Interfaces), the option "***Select Action > Auto-Name Update*** > *Enable*" will unselect the ***Disable Discovery Name Update*** field for each interface selected in the **Network Interfaces** page.

- ***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 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.

NOTE: In the **Network Interfaces** page (Registry > Networks > Interfaces), the option "***Select Action > Interface Speed / Counter Type Update*** > *Enable*" will unselect the ***Disable Discovery Name Update*** field for each interface selected in the **Network Interfaces** page.

- ***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 let you 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.
- ***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. For more information about CBQoS, see the section on *Class-Based Quality of Service (CBQoS)*.

- ***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.

- ***Emissary***. Select an organization from the list to enable all users in that organization to view this interface. 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.

7. Click **[Save]**.

Defining Thresholds for a Single Interface

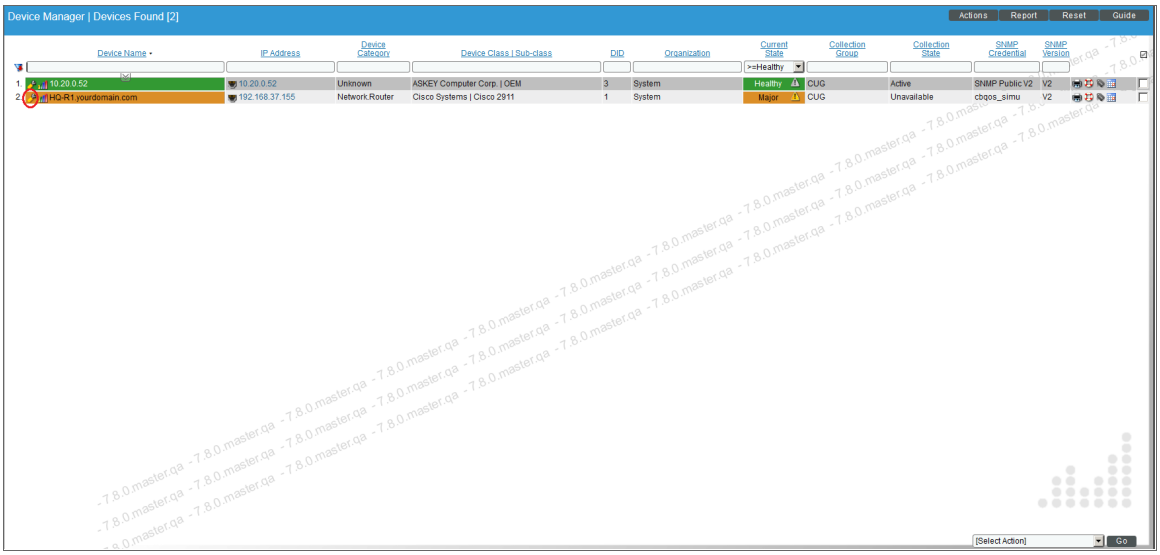
The **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) allows you to define custom thresholds for the monitored interface. If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor 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*.

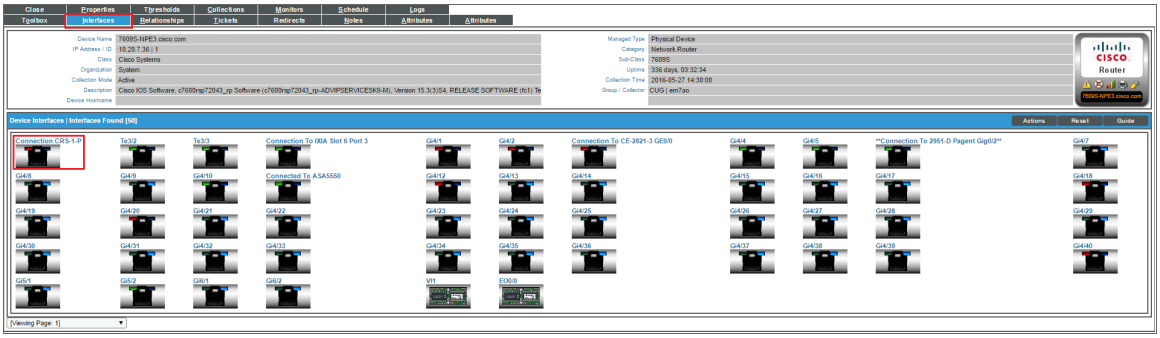
NOTE: The thresholds defined for a specific interface in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) override the global thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface.

To define custom thresholds for an interface:

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



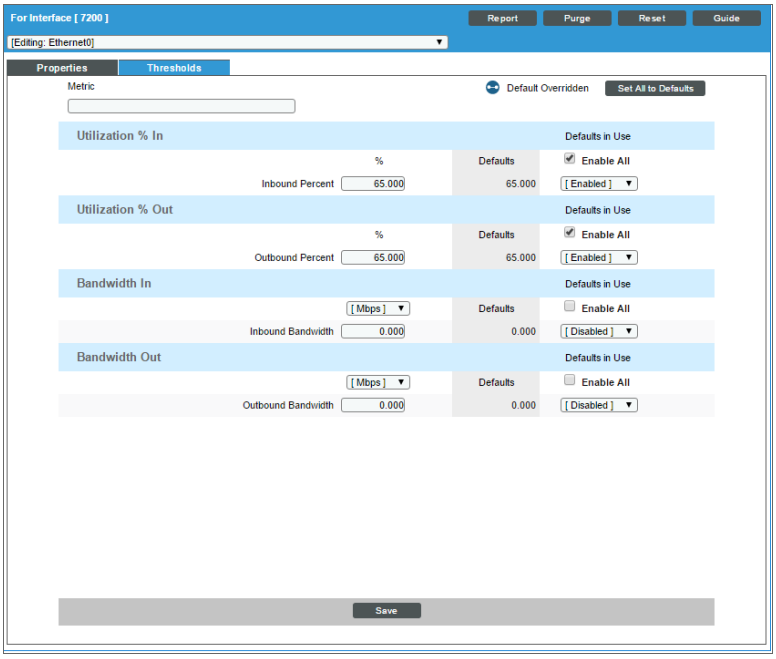
3. In the **Device Administration** panel, click the **[Interfaces]** tab.



4. 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.

6. Click the **Thresholds** tab.



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***, ***kbps***, ***Mbps*** (the default), or ***Gbps***.

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

Threshold	Default Value	Default Status
Discards In > Inbound Discards	1000.000	Enabled
Discards Out > Outbound Discards	1000.000	Enabled
Multicast % In > Rising Medium	30.000	Disabled
Multicast % In > Rising Low	20.000	Disabled
Broadcast % Out > Rising Medium	30.000	Disabled
Broadcast % Out > Rising Low	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 the **[Properties]** tab for the interface.

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

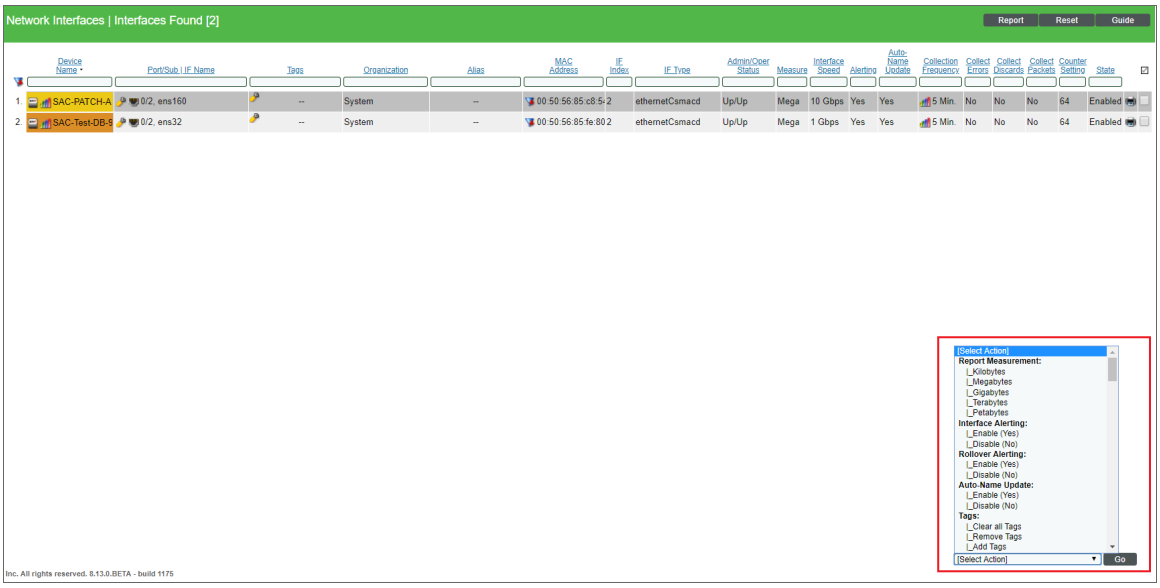
   - ***Value***. The value at which the threshold will trigger an event.
     - For thresholds that include the word *Rising*, when a value exceeds the specified value, SL1 triggers an event.
     - For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers 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

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.



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:

  - *Enable*. Allows nightly auto-discovery to update the interface name of each selected interface. For each interface selected in the **Network Interfaces** page, the ***Disable Discovery Name Update*** fieldfield will be unselected in the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).
  - *Disable*. Does not allow nightly auto-discovery to update the interface name of each selected interface. For each interface selected in the **Network Interfaces** page, the ***Disable Discovery Name Update*** field will be selected in the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).

- ***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, where you can remove one or more tags from the selected interfaces. In the **Bulk Remove Network Interface Tags** modal, 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, where you can add one or more tags to the selected interfaces. In the **Bulk Add Network Interface Tags** modal, 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.

- ***Interface Speed / Counter Type Update***. Specifies whether SL1 can update or over-write the interface name during nightly auto-discovery. This field also specifies whether nightly auto-discovery can update the interface speed and counter type of an interface. Options are:

    - *Enable*. Allows nightly auto-discovery to update the interface speed and counter type of each selected interface. For each interface selected in the **Network Interfaces** page, the ***Disable Interface Speed Update*** field will be unselected in the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).
    - *Disable*. Does not allow nightly auto-discovery to update the interface speed and counter type of each selected interface. For each interface selected in the **Network Interfaces** page, the ***Disable Interface Speed Update*** field will be selected in the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).

- ***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.

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 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.

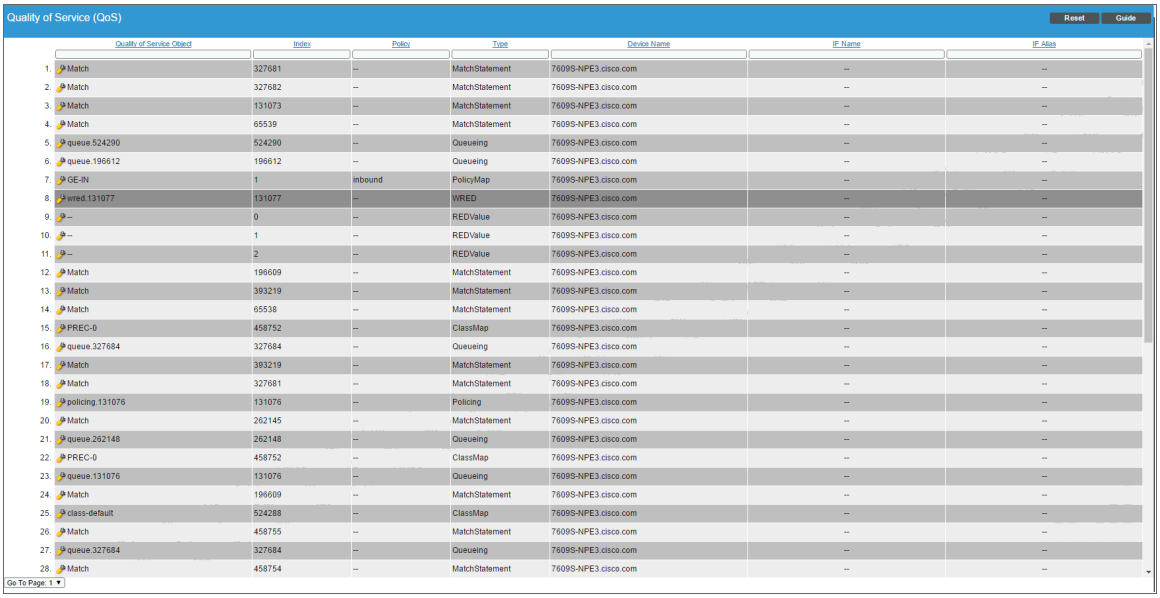
SL1 collects CBQoS data only if you have enabled the field ***Enable CBQoS Collection*** in the **Behavior Settings** page (System > Settings > Behavior).

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).



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
  - Queuing
  - 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.

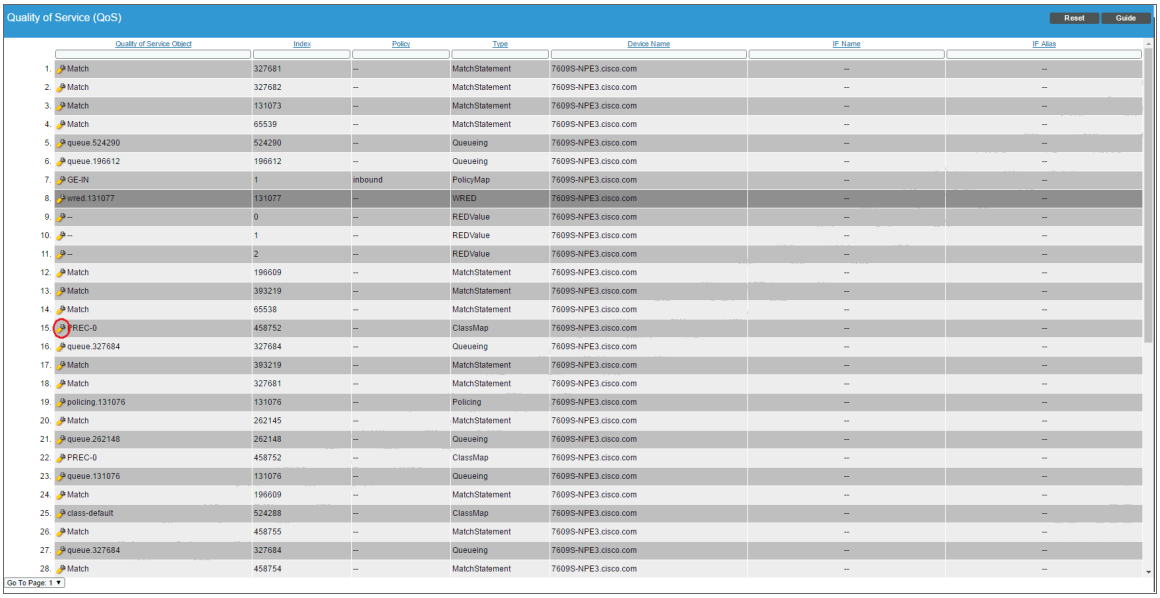
If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. For interfaces that are part of a CBQoS class, SL1 will use either the global CBQoS thresholds defined in the **Quality of Service Threshold 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).

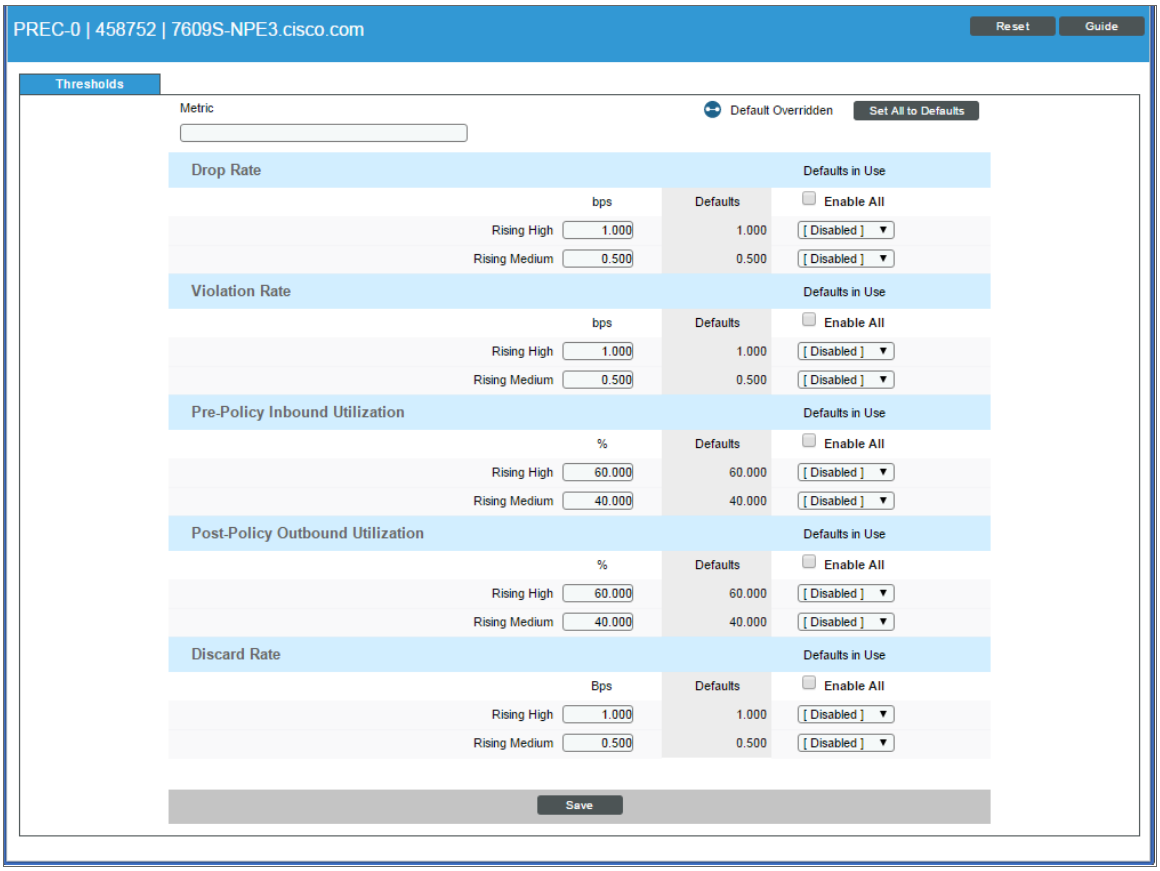
To edit the interface thresholds for a CBQoS object on a specific device and specific interface:

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



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

3. Click the wrench icon ( ).



4. 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*.

5. 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
Drop Rate > Rising High	1.000	Disabled

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

Concurrent Network Interface Collection

The standard network interface collection process uses the SL1 SNMP API to collect data directly from interfaces, one device at a time. Because this data is collected in a serial fashion, any issue or delay in collecting metrics can have a domino effect. For this reason, you should monitor no more than 10,000 interfaces per SL1 Data Collector using this standard interface collection process.

However, to increase the scale at which you can collect data for network interfaces, you can enable ***Concurrent Network Interface Collection***. Concurrent network interface collection uses asynchronous SNMP collection for all network interfaces. This provides better scalability for large networks by allowing multiple collection tasks to run at the same time with a reduced load on Data Collectors.

With concurrent network interface collection, SL1 can run thousands of SNMP collection tasks in parallel and wait for the results to be returned independently. A single failed task will not prevent other tasks from completing. Therefore, there is no recommended limit to the number of interfaces you can monitor per Data Collector with concurrent network interface collection enabled.

TIP: Because concurrent network interface collection requires each Data Collector to do additional work, you should consider device latency when determining whether to enable concurrent network interface collection. Generally speaking, if your device latencies are under 10 ms, then legacy network interface collection will likely outperform concurrent collection across vital key performance measures such as CPU, memory utilization, and elapsed time.

Enabling Concurrent Network Interface Collection for All Interfaces

NOTE: This feature is disabled by default.

To enable concurrent network interface collection for all interfaces:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. Select the ***Enable Concurrent Network Interface Collection*** checkbox.
3. Click **[Save]**.

Configuring Concurrent Network Interface Collection for a Collector Group

You can enable or disable concurrent network interface collection for individual collector groups on the **Collector Group Management** page (System > Settings > Collector Groups). When you do so, this setting overrides the global setting for concurrent network interface collection for the selected collector group.

To configure concurrent network interface collection for a collector group:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).
2. Click the wrench icon ( ) for the collector group you want to edit. The fields at the top of the page are updated with the data for that collector group.
3. Select an option in the ***Enable Concurrent Network Interface Collection*** field:
   - *Use system-wide default*. Select this option if you want this collector group to use or not use concurrent network interface collection based on the ***Enable Concurrent Network Interface Collection*** field on the **Behavior Settings** page (System > Settings > Behavior). This is the default.
   - *Yes*. Select this option to enable concurrent network interface collection for this collector group, even if you did not enable it on the **Behavior Settings** page.
   - *No*. Select this option to prevent this collector group from using concurrent network interface collection, even if you did enable it on the **Behavior Settings** page.
4. Click **[Save]**.

Additional Configuration for Concurrent Network Interface Collection

There are several configuration settings that can affect the concurrent network interface collection performance.

By default, the asynchronous SNMP service will send a single SNMP OID per PDU request. While asynchronous collection will generally perform well without it, you can improve your chances of better performance by packing more than one SNMP OID in a PDU.

Several methods for doing so are described below.

Enabling PDU Packing

You can enable the asynchronous SNMP service to pack up to five OIDs into a single PDU by enabling PDU packing in SNMP-enabled device classes.

To do so:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes).
2. Click the wrench icon ( ) for the SNMP-enabled device class that you want to edit. The fields at the top of the page are updated with the properties for that device class.
3. Select the ***PDU Packing*** checkbox.
4. Click **[Save]**.

Increasing the Maximum Number of PDUs in a Single SNMP Request

When an SNMP device class has PDU packing enabled, the default maximum number of OIDs that the asynchronous SNMP service will pack up into a single PDU is five. However, you can change the maximum number of PDUs that are packed into a single SNMP GET request by editing the `GETMULTI_CHUNK_SIZE` value in the `/opt/em7/services/snmp_collector/snmp_collector_shared.env` file.

To set the maximum number of PDUs in a single SNMP request:

1. Either go to the console of the SL1 server or use SSH to access the SL1 appliance.
2. Log in as user **em7admin**.
3. At the command line, use the vi editor to edit the SNMP collector file for one of the SNMP collectors (containers) on your Data Collector:
   - `sudo vi /opt/em7/services/snmp_collector/snmp_collector_shared.env`, to set the value across all service replicas on the Data Collector and for all devices with PDU packing enabled.
   - `sudo vi /opt/em7/services/snmp_collector/snmp_collector<collector_number>.env`, where you replace `<collector_number>` with the number of the container, to set the value over an individual service replica's PDU packing limit.

NOTE: If you set the value across all service replicas, then you cannot customize the `GETMULTI_CHUNK_SIZE` setting per device. On the other hand, if you set the value for an individual service replica, you cannot control which device uses which PDU packing limit.

4. Edit the value for the `GETMULTI_CHUNK_SIZE` setting to represent the maximum number of PDUs you want the asynchronous SNMP service to pack into a single SNMP GET request. This value must be an integer. The default value is `5`.
5. Optionally, you can update the `USE_GETMULTI` setting to `True` to pack multiple PDUs into a single SNMP GET request for all devices, regardless of the ***PDU Packing*** setting for each device class. The default value is `False`, which causes the service to consider the ***PDU Packing*** setting for each device class.
6. Save your changes and exit the file (`:wq`).

Troubleshooting Concurrent Network Interface Collection

For information about troubleshooting concurrent network interface collection, which uses asynchronous SNMP collection, see the section on Troubleshooting Concurrent SNMP Collection in the ***SNMP Dynamic Application Development*** manual.

Viewing Performance Graphs and Reports About Interfaces

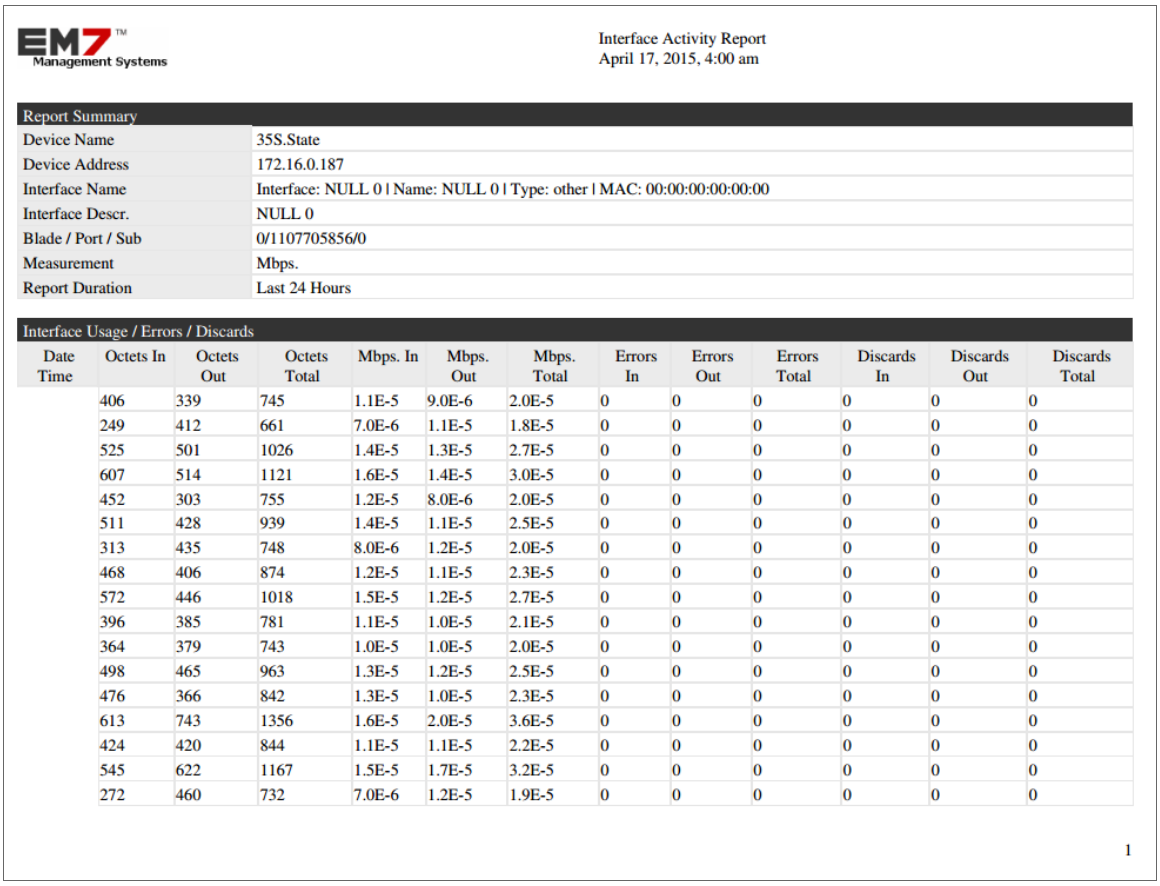
SL1 enables you to view a number of performance graphs and generate text-based reports about interfaces.

The following sections describe how to generate the text-based reports that are available for interfaces.

For information about interface performance graphs, see the chapter on *Viewing Performance Graphs*.

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.



EM7 Management Systems

Interface Activity Report
April 17, 2015, 4:00 am

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

1

To generate the report:

1. Go to **Network Interfaces** (Registry > Networks > Interfaces).
2. In the **Network Interfaces** page, find the interface for which you want to generate a bandwidth report. Click its printer icon (). The **Report Creator** modal page is displayed.
3. 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
4. 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.

5. SL1 will generate the report. You can immediately view the report or save it to your local computer.

Generating a Report for Multiple Network Interfaces

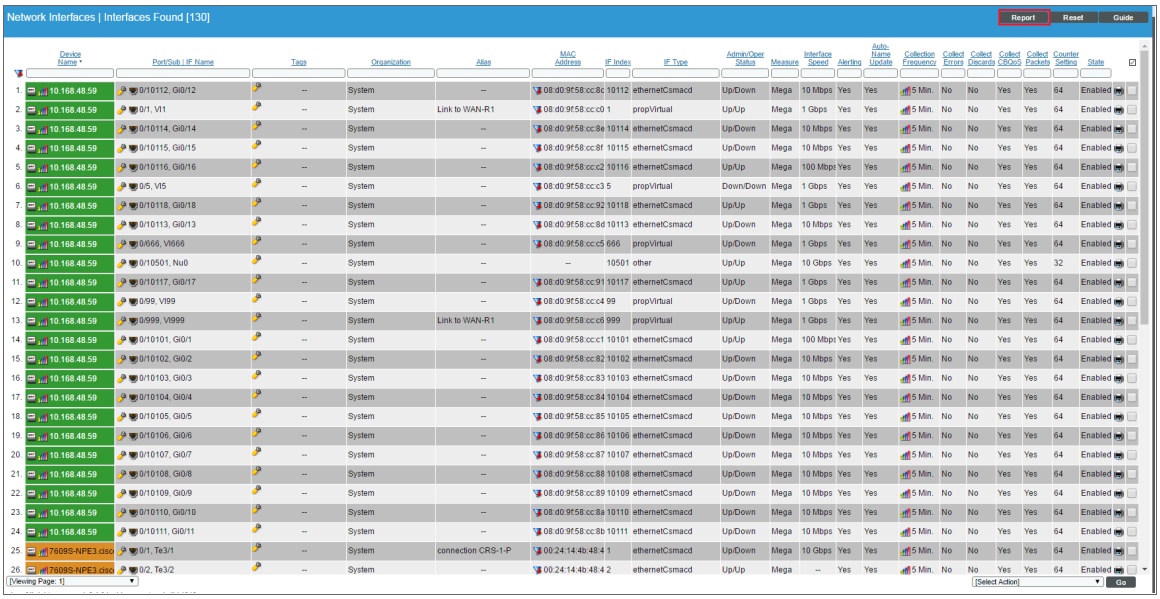
On the **Network Interfaces** page (Registry > Networks > Interfaces) you can generate a report on all, multiple, or a single interface in SL1. The report will contain all the information displayed in the **Network Interfaces** page.

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	0/10112, Gi0/12		08:d0:9f:58:cc:8c	10112	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
2.	10.168.48.59	0/1, Vl1	Link to WAN-R1	08:d0:9f:58:cc:c0	1	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
3.	10.168.48.59	0/10114, Gi0/14		08:d0:9f:58:cc:8e	10114	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
4.	10.168.48.59	0/10115, Gi0/15		08:d0:9f:58:cc:8f	10115	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
5.	10.168.48.59	0/10116, Gi0/16		08:d0:9f:58:cc:c2	10116	ethernetCsmacd	/	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
6.	10.168.48.59	0/5, Vl5		08:d0:9f:58:cc:c3	5	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
7.	10.168.48.59	0/10118, Gi0/18		08:d0:9f:58:cc:92	10118	ethernetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
8.	10.168.48.59	0/10113, Gi0/13		08:d0:9f:58:cc:8d	10113	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
9.	10.168.48.59	0/666, Vl666		08:d0:9f:58:cc:c5	666	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
10.	10.168.48.59	0/10501, Nu0			10501	other	/	Mega	10 Gbps	Yes	Yes	5 Min.	No	No	32 bits	Enabled
11.	10.168.48.59	0/10117, Gi0/17		08:d0:9f:58:cc:91	10117	ethernetCsmacd	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
12.	10.168.48.59	0/99, Vl99		08:d0:9f:58:cc:c4	99	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
13.	10.168.48.59	0/999, Vl999	Link to WAN-R1	08:d0:9f:58:cc:c6	999	propVirtual	/	Mega	1 Gbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
14.	10.168.48.59	0/10101, Gi0/1		08:d0:9f:58:cc:c1	10101	ethernetCsmacd	/	Mega	100 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
15.	10.168.48.59	0/10102, Gi0/2		08:d0:9f:58:cc:82	10102	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
16.	10.168.48.59	0/10103, Gi0/3		08:d0:9f:58:cc:83	10103	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
17.	10.168.48.59	0/10104, Gi0/4		08:d0:9f:58:cc:84	10104	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
18.	10.168.48.59	0/10105, Gi0/5		08:d0:9f:58:cc:85	10105	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
19.	10.168.48.59	0/10106, Gi0/6		08:d0:9f:58:cc:86	10106	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
20.	10.168.48.59	0/10107, Gi0/7		08:d0:9f:58:cc:87	10107	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
21.	10.168.48.59	0/10108, Gi0/8		08:d0:9f:58:cc:88	10108	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
22.	10.168.48.59	0/10109, Gi0/9		08:d0:9f:58:cc:89	10109	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
23.	10.168.48.59	0/10110, Gi0/10		08:d0:9f:58:cc:8a	10110	ethernetCsmacd	/	Mega	10 Mbps	Yes	Yes	5 Min.	No	No	64 bits	Enabled
24.	10.168.48.59	0/10111, Gi0/11		08:d0:9f: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 SI	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-282	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 ASA555	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).



> **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.

2. Click the **[Report]** button. The **Export current view as a report** modal page appears.
3. Select the format in which SL1 will generate the report. Your choices are:

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

4. 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.

Chapter 9

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 covers the following topics:

Viewing the List of All Discovered Hardware Components 192
Generating a Report for Multiple Hardware Components on Multiple Devices 195
Hiding a File System 195
Changing Thresholds for One or More File Systems 196
Viewing the List of All Discovered Software Titles 197
Viewing a List of Software Titles for a Single Device 199
Generating a Report on All Software on All Devices 202
Generating an Exclusion Report for a Single Software Title 204

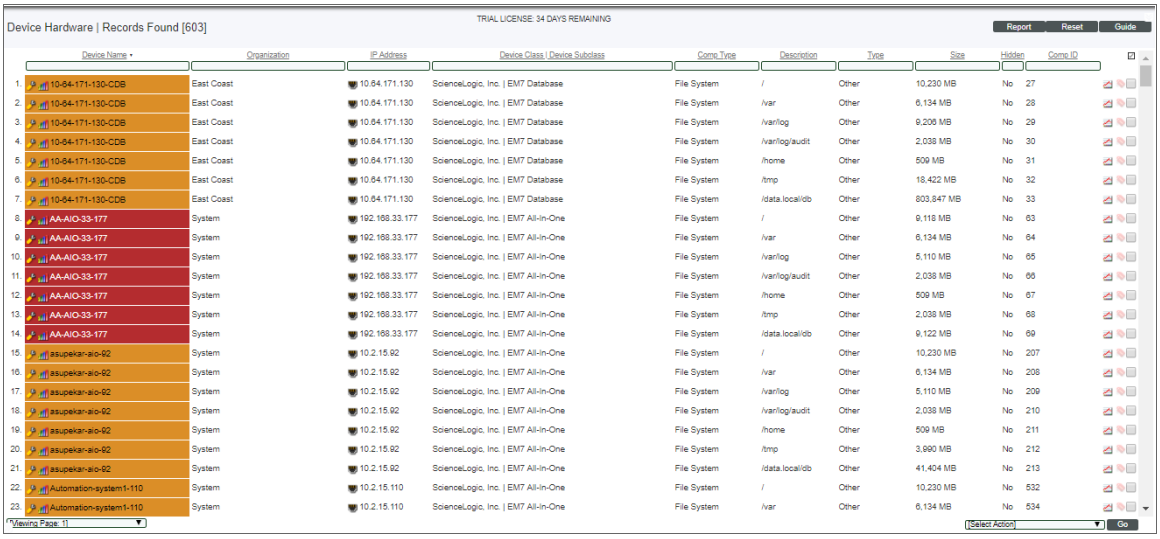
Viewing the List of All Discovered Hardware Components

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).



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 menu to the hardware component. To select all the checkboxes, select the checkmark 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 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.

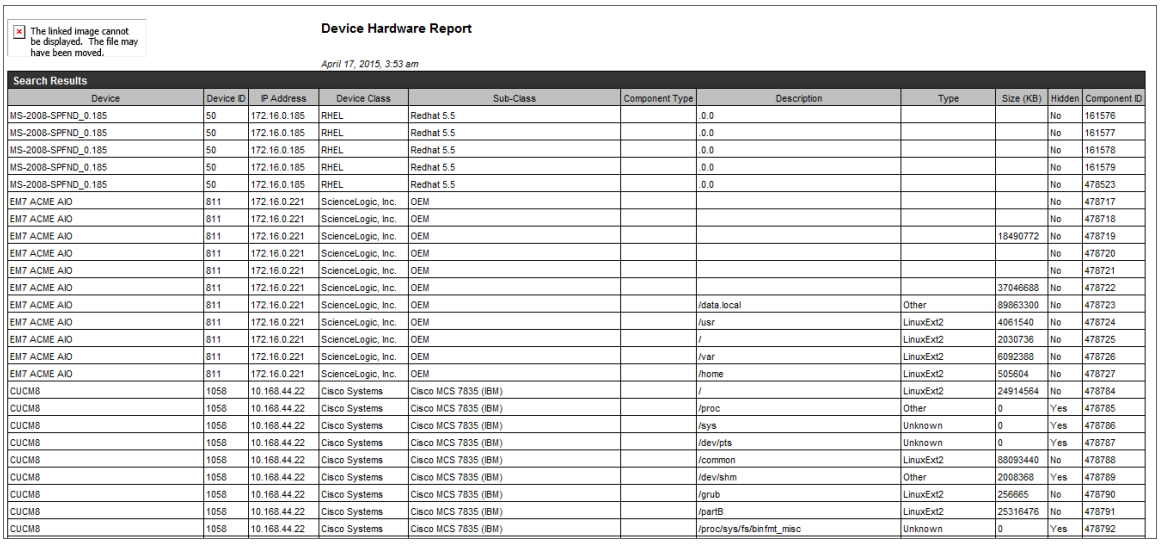
You can also use special characters to filter each parameter.

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-SPFND_0.185	50	172.16.0.185	RHEL	Redhat 5.5		.0.0			No	161576
MS-2008-SPFND_0.185	50	172.16.0.185	RHEL	Redhat 5.5		.0.0			No	161577
MS-2008-SPFND_0.185	50	172.16.0.185	RHEL	Redhat 5.5		.0.0			No	161578
MS-2008-SPFND_0.185	50	172.16.0.185	RHEL	Redhat 5.5		.0.0			No	161579
MS-2008-SPFND_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				18490772	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				37046688	No	478722
EM7 ACME AIO	811	172.16.0.221	ScienceLogic, Inc.	OEM		/data.local	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	6092388	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 (IBM)		/	LinuxExt2	24914564	No	478784
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/proc	Other	0	Yes	478785
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/sys	Unknown	0	Yes	478786
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/dev/pts	Unknown	0	Yes	478787
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/common	LinuxExt2	88093440	No	478788
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/dev/shm	Other	2008368	Yes	478789
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/grub	LinuxExt2	256665	No	478790
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/partB	LinuxExt2	25316476	No	478791
CUCM8	1058	10.168.44.22	Cisco Systems	Cisco MCS 7835 (IBM)		/proc/sys/fs/binfmt_misc	Unknown	0	Yes	478792

To generate a report on all hardware components in SL1:

1. Go to the **Device Hardware** page (Devices > Hardware).
2. In the **Device Hardware** page, click the **[Report]** button.
3. 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.
- 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 MB are automatically hidden during discovery.
- File systems of type "Other" are automatically hidden during discovery.

> **NOTE:** If the type for 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 is 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:

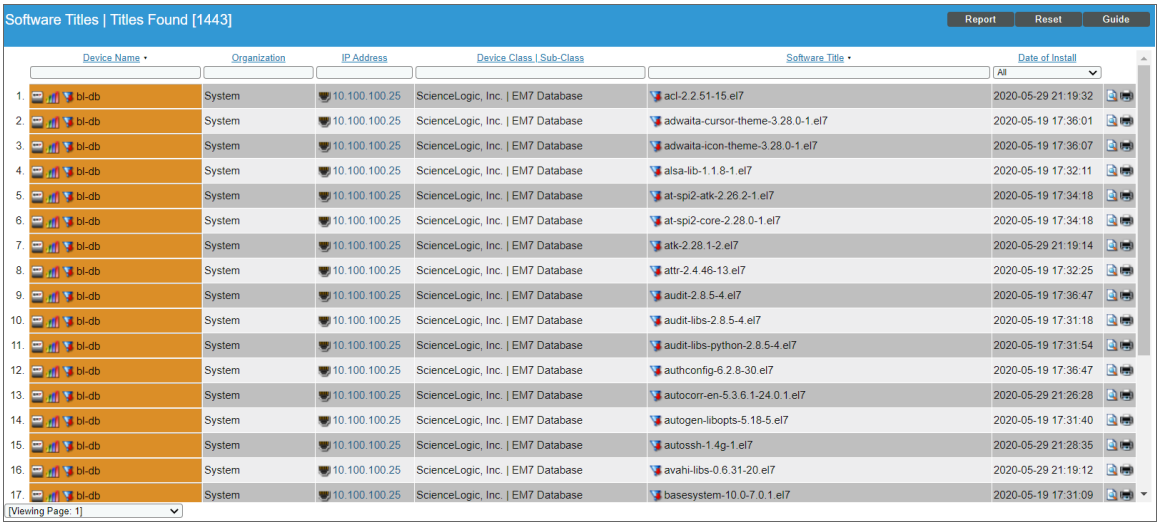
1. Find the file system for which you want to change the Critical threshold. Select its checkbox ( ).
2. Select the checkbox for each additional file system for which you want to change the Critical threshold.
3. In the ***Select Action*** drop-down list, find *Change Critical Threshold* and select a 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** 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** page (Devices > Software).



2. The **Software** 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.

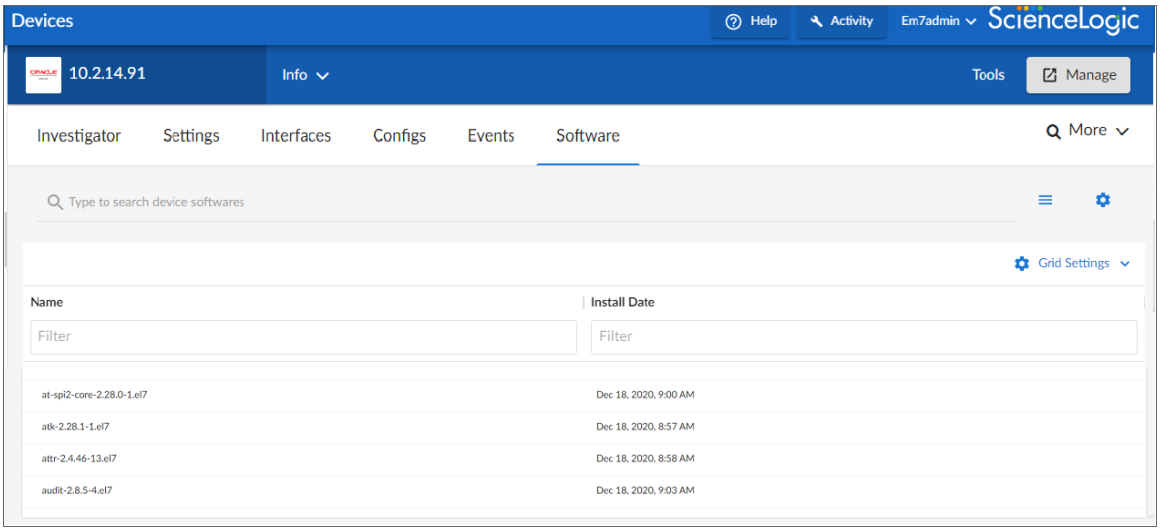
You can also use special characters to filter each parameter.

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

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



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

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

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

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

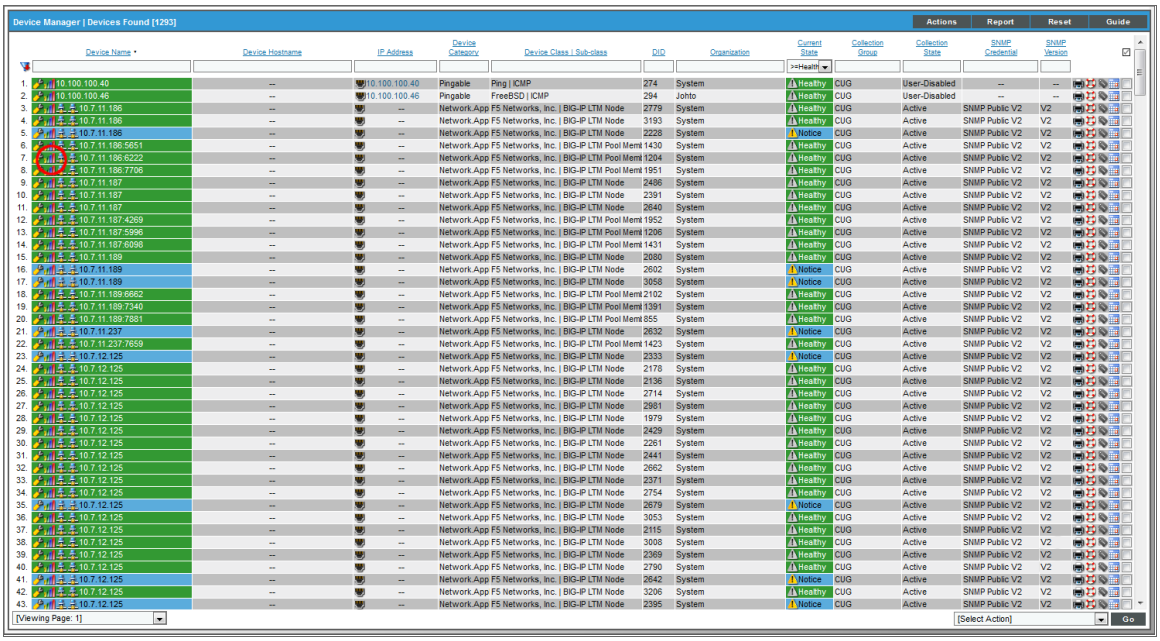
- ***Name***. Name of the software.
- ***Install Date***. Date and time the software was installed on the device.

Viewing a List of Software Titles for a Single Device in the Classic SL1 User Interface

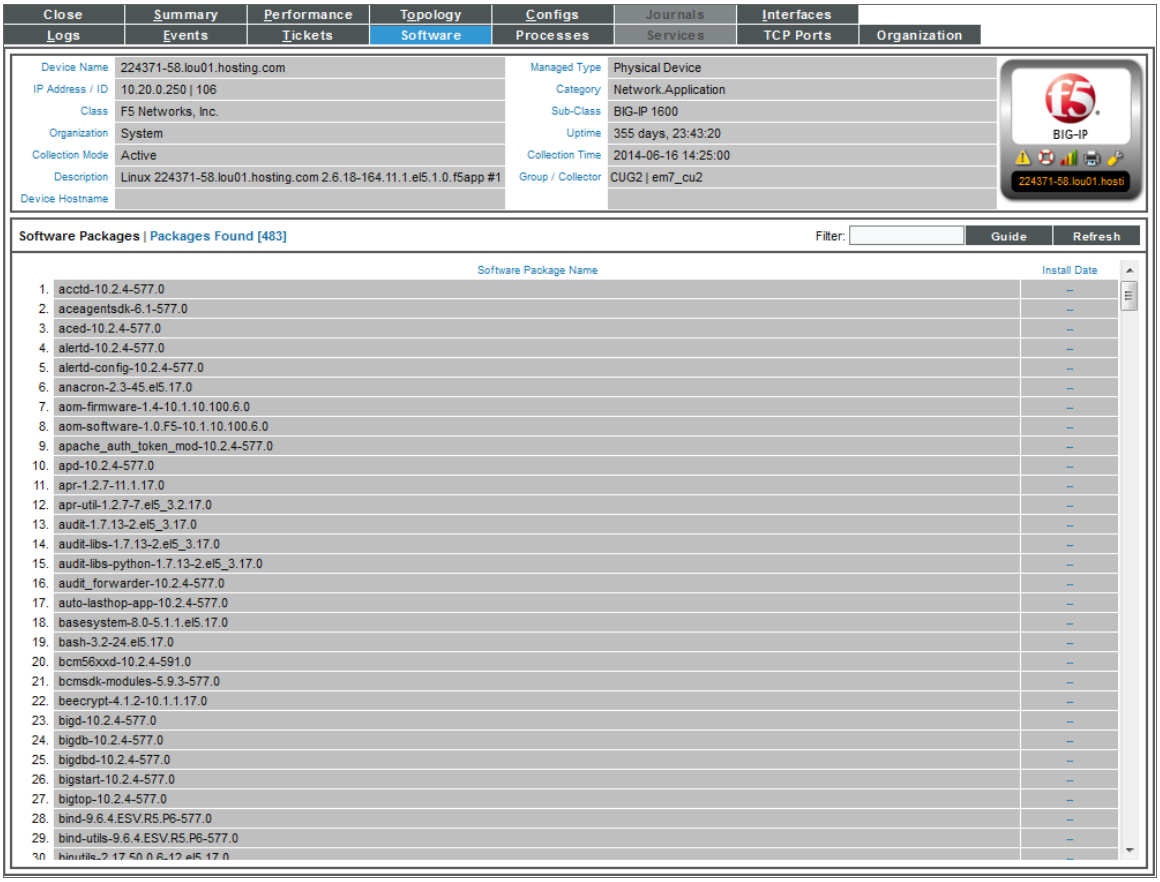
The **Software Packages** page displays a list of all the software installed on the device. If possible, the installation date is also displayed.

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.



3. In the **Device Reports** panel, select the Software tab. The **Software Packages** page appears.



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 - We	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	Microsoft Application Error Reporting	2012-10-03 17:49:50
26.	ACME - DB-MSSQL - We	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 - We	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 - We	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 - We	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 - We	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 - We	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 - We	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 - We	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 - We	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 - We	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 - We	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).
2. On the **Software Titles** page, click the **[Report]** button. The **Export current view as a report** modal appears:

> **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.

3. 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)
4. Click 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 - We	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 - We	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 - Web	ACME	192.168.32.110	Microsoft | Windows Server 2008 R2	BOINC	2012-10-05 07:01:42
1.	ACME - WEB-IIS-1 - Web	ACME	192.168.32.111	Microsoft | Windows Server 2008 R2	BOINC	2012-10-05 10:06:00
2.	DEMO-AP-01.demo.scien	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).
2. On the **Software Titles** page, find an instance of the software title you want to generate an exclusion report for.
3. Click its printer icon ( ). You will be prompted to save or view the generated report.

Chapter 10

Viewing Device Logs

Overview

This chapter describes Device Logs in SL1.

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

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

This chapter covers the following topics:

Viewing Device Logs and Messages *206*

Viewing Events Associated with a Log Entry *210*

Creating an Event Policy from a Log Entry *211*

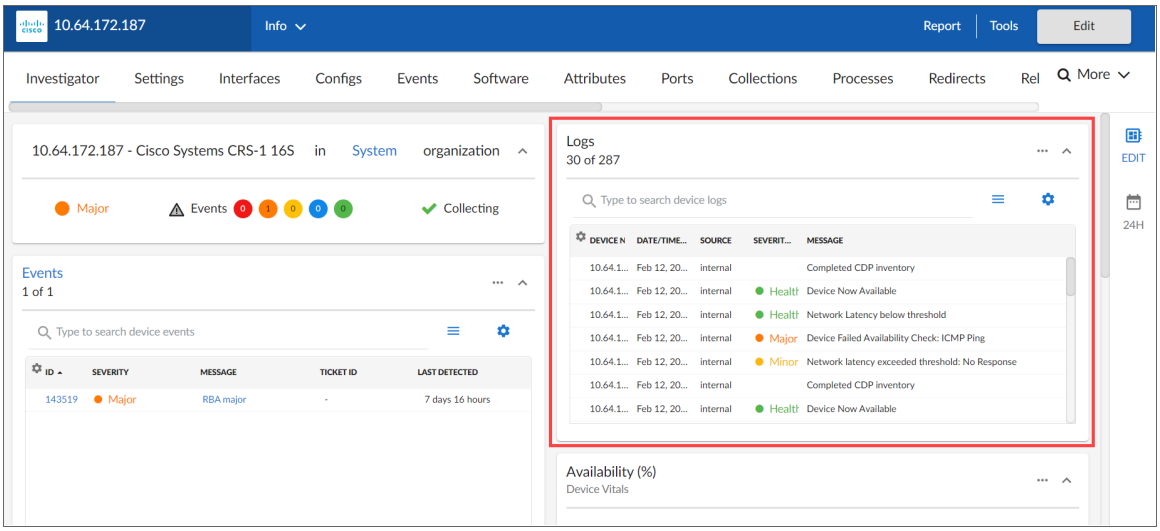
Redirecting Log Data from One Device to Another *212*

Viewing Logs for All Devices *214*

Viewing Device Logs and Messages

You can view logs and messages for a device in the **[Investigator]** tab of the **Device Investigator** page.

The **[Investigator]** tab displays a customizable set of metrics and panels that display information about the selected device. One of those panels is the **Logs** panel:



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

NOTE: For more information about Log File Monitoring Policies and using the SL1 Agent to monitor device logs, see the chapter on "Monitoring Logs Using the SL1 Agent" in the ***Monitoring with the SL1 Agent*** manual.

The **Logs** panel displays the following information about each device log entry:

- ***Device Name***. The name of the device on which the log message was collected.
- ***Date/Time***. The date and time the entry was made in the log.
- ***Source***. The entity or process that generated the message. Options include:
    - *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.
    - *ScienceLogic Agent*. Entry was generated by the SL1 Agent.
- ***Severity***. The color-coded severity of the event that generated the log entry, if applicable. Possible values are:

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

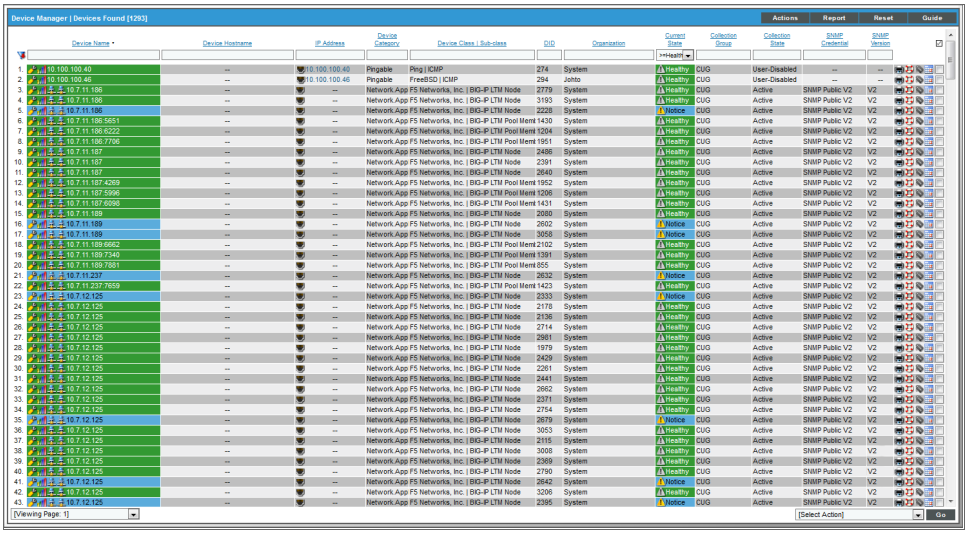
- ***Message***. Text of the log entry.

Viewing Device Logs and Messages in the Classic SL1 User Interface

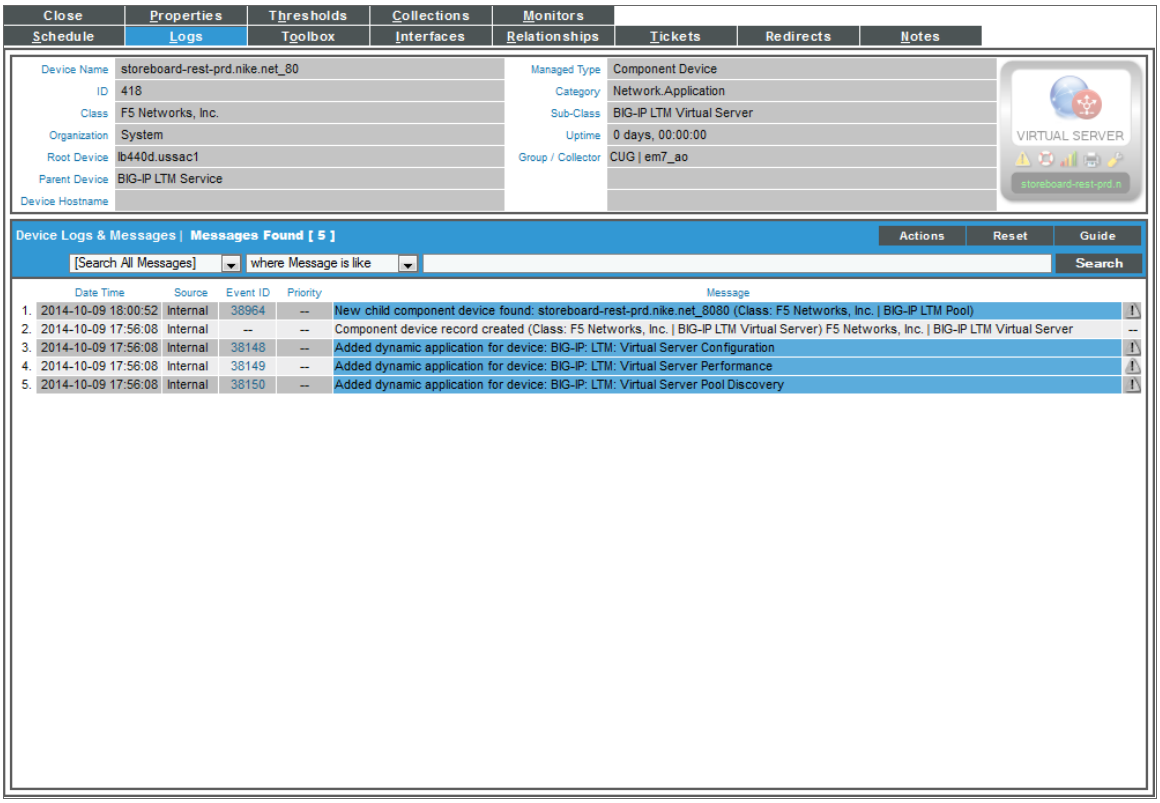
In the **Device Administration** panel, the **Device Logs & Messages** page displays all the messages SL1 and the SL1 agent, if applicable, have collected from the device. You might find it helpful to view these log entries during troubleshooting or to manually check on the status of a device.

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 ( ).



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



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.
     - *ScienceLogic Agent*. Entry was generated by the SL1 Agent.

   - ***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.

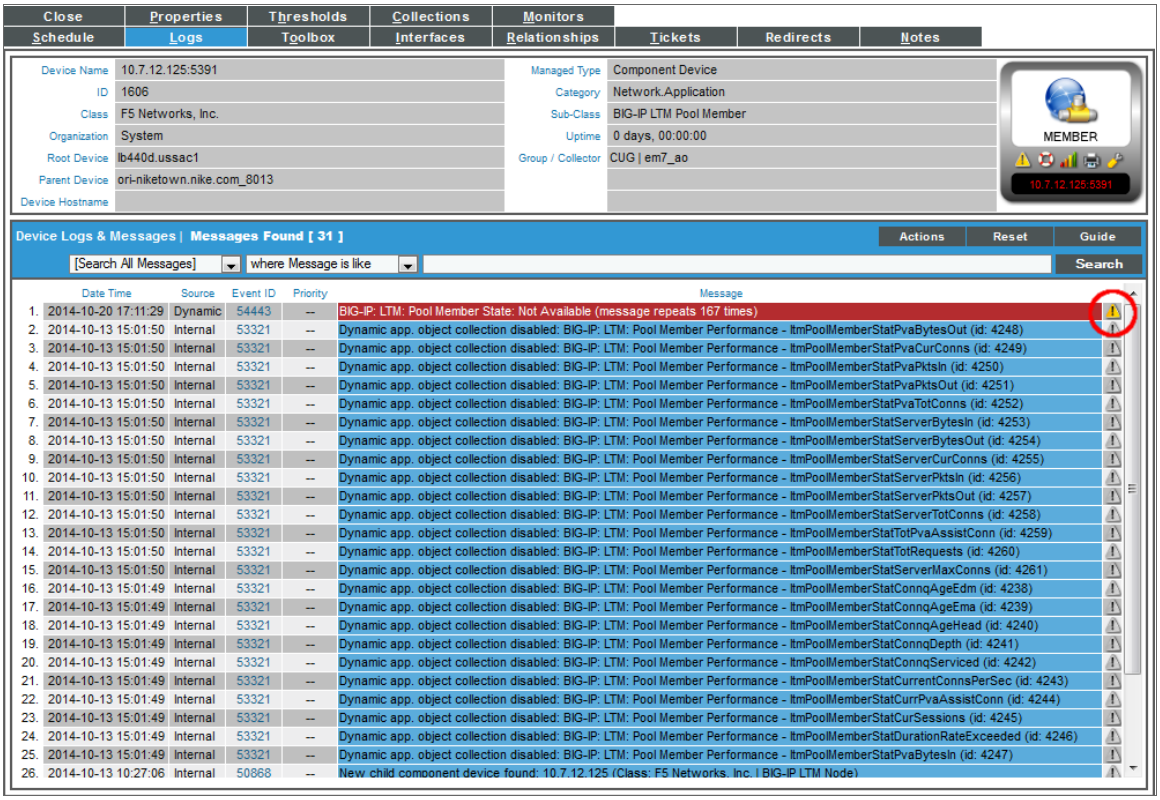
- *Info*. An error occurred.
- *Notice*. An error has not occurred. Entry denotes normal system activity.
- *N / A*. Not applicable. Entry was not generated by syslog.

- ***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.



4. In the **Device Logs & Messages** page, find the log entry you are interested in. Select its event icon ( ).
5. 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

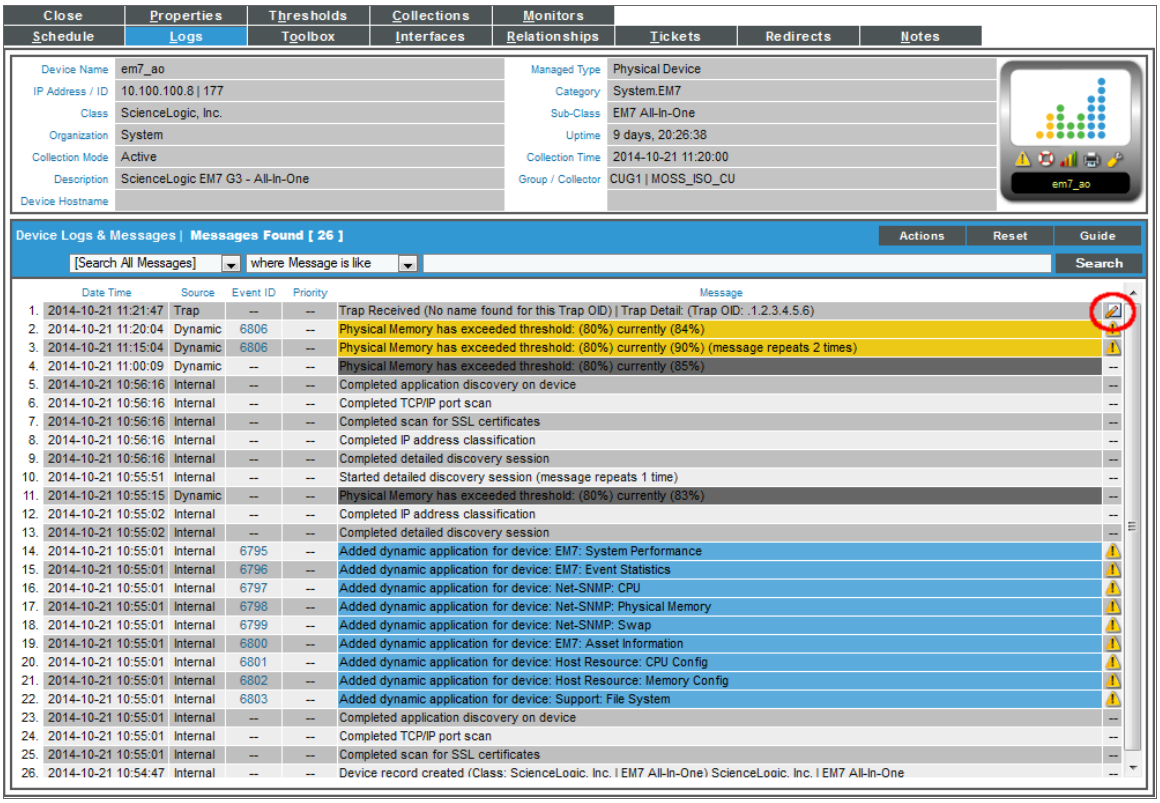
From the **Device Logs & Messages** page, you can create a new event policy based on a log entry. If a log entry does not have an event policy already associated with it, the pencil icon ( ) will appear next to the entry. You can click on this icon to create a new event policy. After you create an event 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, and which lines from those log files the agent should send to the platform. You can define event policies to trigger an event based on Log File Monitoring policies.

NOTE: For more information about Log File Monitoring Policies and using the SL1 Agent to monitor device logs, see the chapter on "Monitoring Logs Using the SL1 Agent" in the ***Monitoring with the SL1 Agent*** manual.

To create an event policy from a log entry:

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.



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***.

Redirecting Log Data from One Device to Another

The **[Redirects]** tab of the **Device Investigator** (or the **Redirect Policy Editor** page in the **Device Administration** panel in the classic SL1 user interface) enables you to redirect log entries from one IP-based device to another IP-based device, or from an IP-based device to a virtual device.

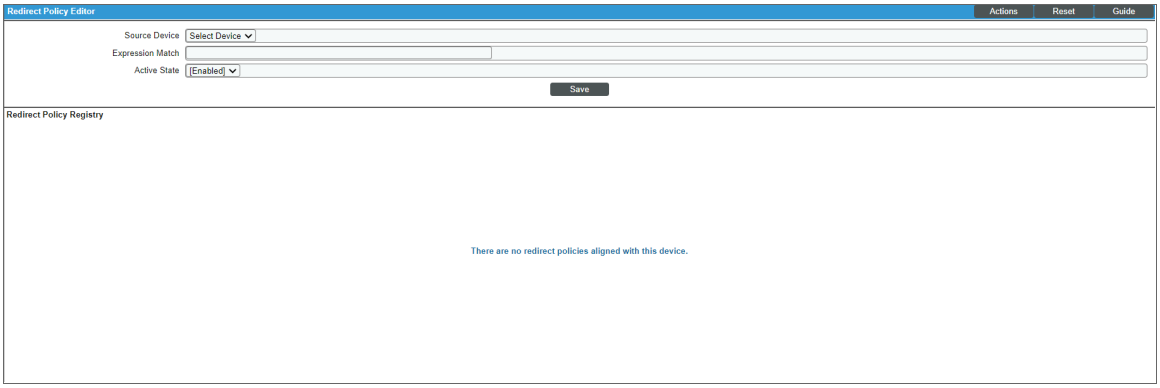
This is perhaps most useful for devices that do not support TCP/IP. Using a redirect, SL1 can push data from a device that does not support TCP/IP to another device that does, and then collect the data from the device that does support TCP/IP.

In this scenario, you can create a virtual device in SL1 to represent the device that does not 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 **[Redirects]** tab of the **Device Investigator** (or the **Redirect Policy Editor** page in the **Device Administration** panel in the classic SL1 user interface) allows you to move data and log entries generated by inbound SNMP Trap, Syslog, or Email messages from the TCP/IP device to the virtual device. However, if you do so, be aware of the following:

- 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 one IP-based device to another IP-based device or a virtual device:

1. Go to the **[Redirects]** tab of the **Device Investigator** for the virtual or IP-based device to which you want to redirect data. (Alternatively, in the classic SL1 user interface, go to the **Redirect Policy Editor** page in the **Device Administration** panel. To do so, go to the **Device Manager** page Devices > Device Manager), find the device to which you want to direct data, click its wrench icon (), and then click the **[Redirects]** tab.)



2. 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 current 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. This 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.

3. Click **[Save]**.
4. You can repeat steps 2 and 3 to redirect data from more than one device or from more than one type of log message.

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 11

Monitoring SSL Certificates

Overview

This chapter describes how to monitor SSL certificates in SL1.

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 "2" 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.

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

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

This chapter covers the following topics:

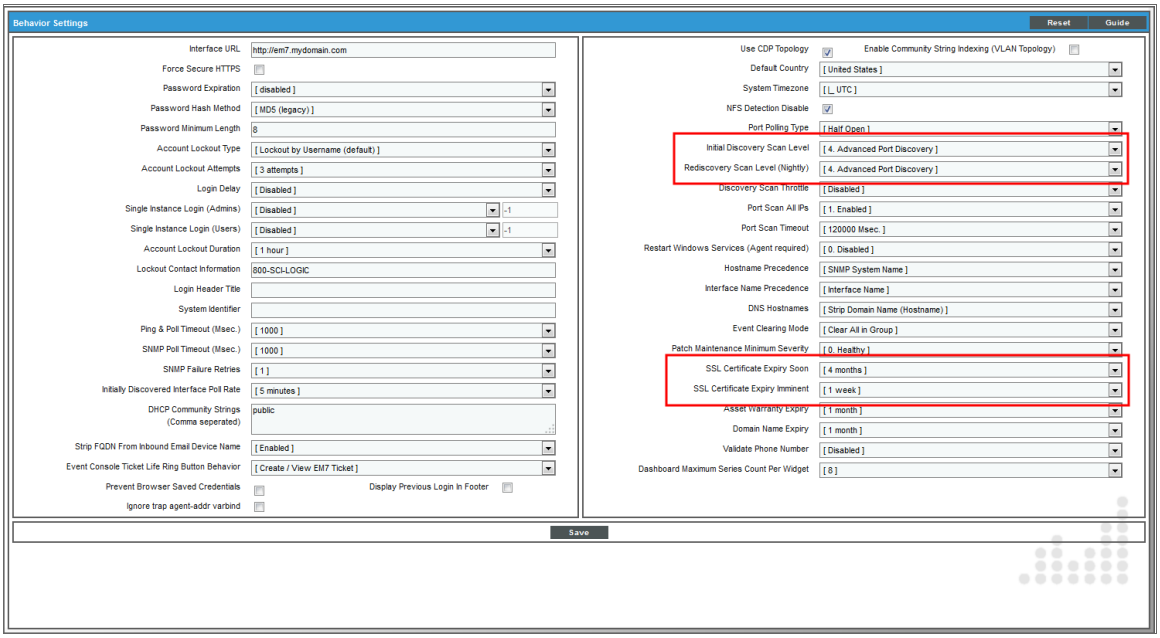
System Settings that Affect SSL Certificates in SL1 ..... *216*

Viewing the List of SSL Certificates *217*

Filtering the List of SSL Certificates *219*

System Settings that Affect SSL Certificates in SL1

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.

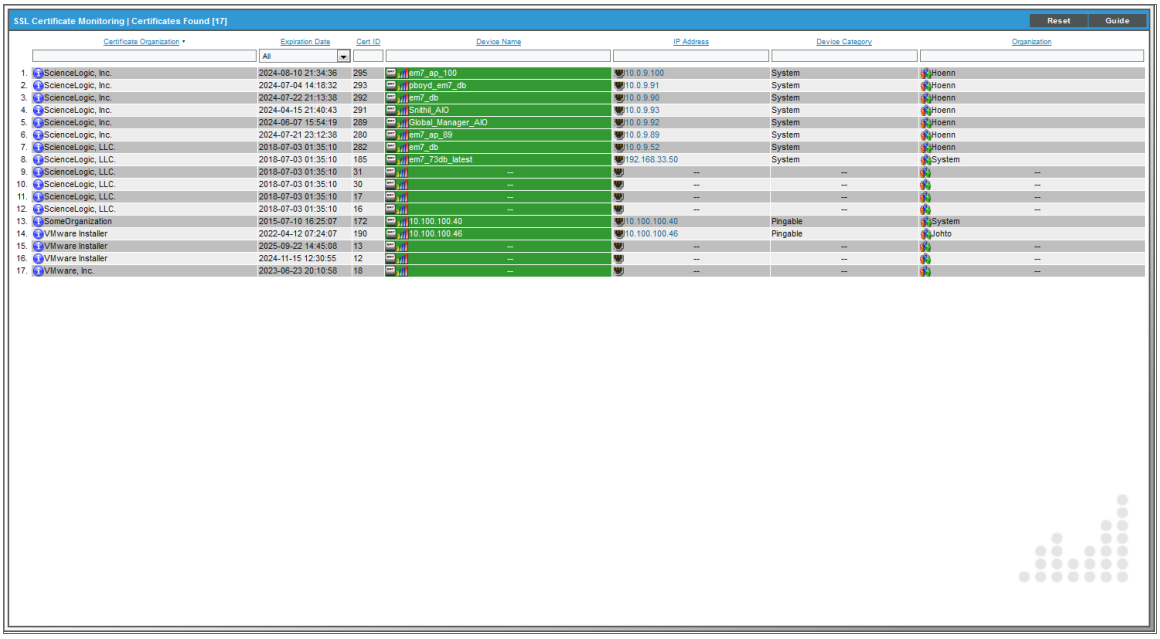
- ***Rediscovery Scan Level (Nightly)***. Specifies the data to be gathered/updated each night during the rediscovery process. The Rediscovery process will find any changes to previously discovered devices and will also find any new devices added to the network. The options are the same as those described 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.



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 12

Monitoring Domain Servers and DNS Records

Overview

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 "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.

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

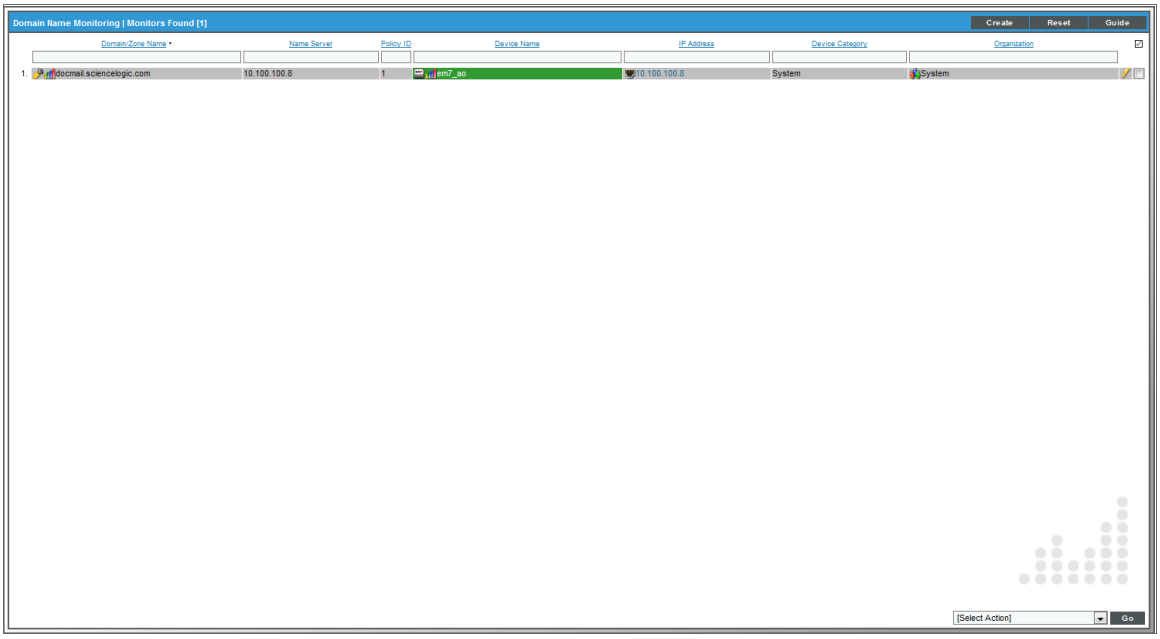
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Viewing the List of Domain Name Monitoring Policies 221
Defining a Monitoring Policy for a Domain Name 223
Editing a Monitoring Policy for a Domain Name 226
Executing the Domain Name Monitoring Policy 227
Deleting a Domain Name Policy 227
Viewing Reports for a Domain Name Monitoring Policy 228

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:



- ***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.
- ***State***. Whether the policy is enabled or disabled.
- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.

- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

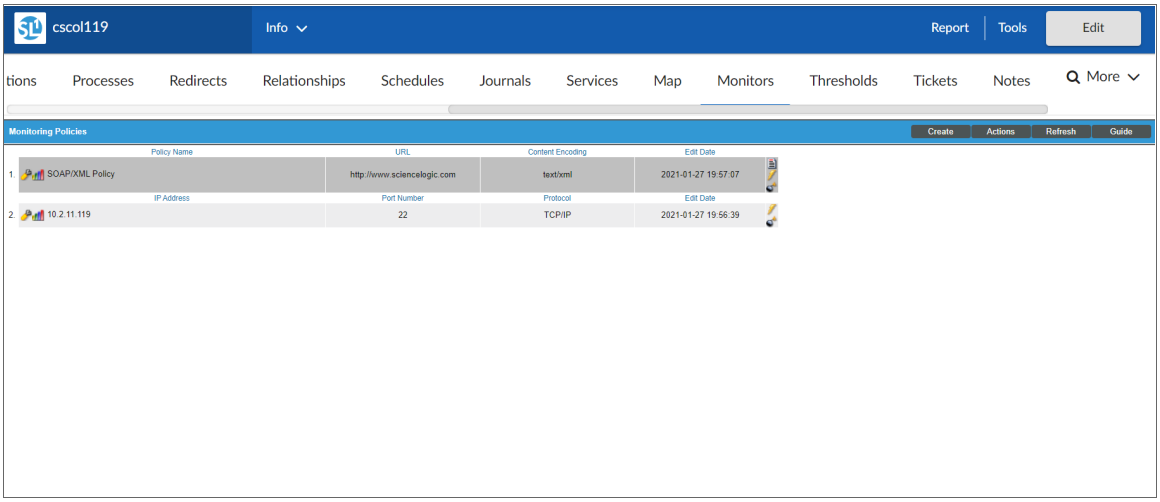
You can also use ***special characters*** to filter each parameter.

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.

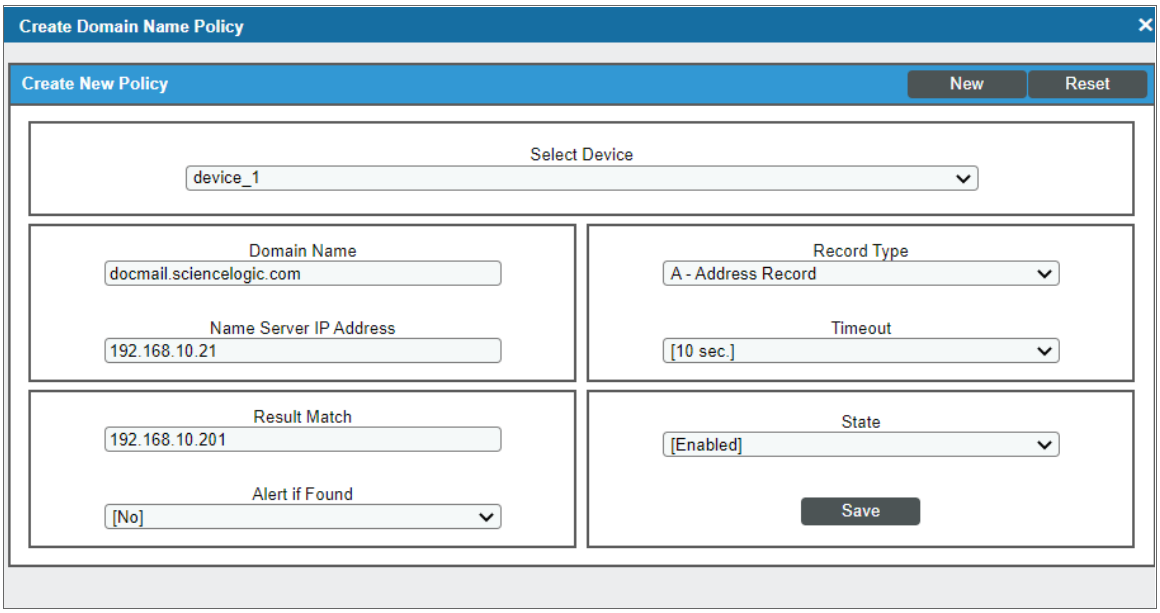
Defining a Monitoring Policy for a Domain Name

You can define a domain name monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define a domain name monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a domain name monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Click **[Create]**, and then select *Create Domain Name Policy*. The **Create Domain Name Policy** modal appears:



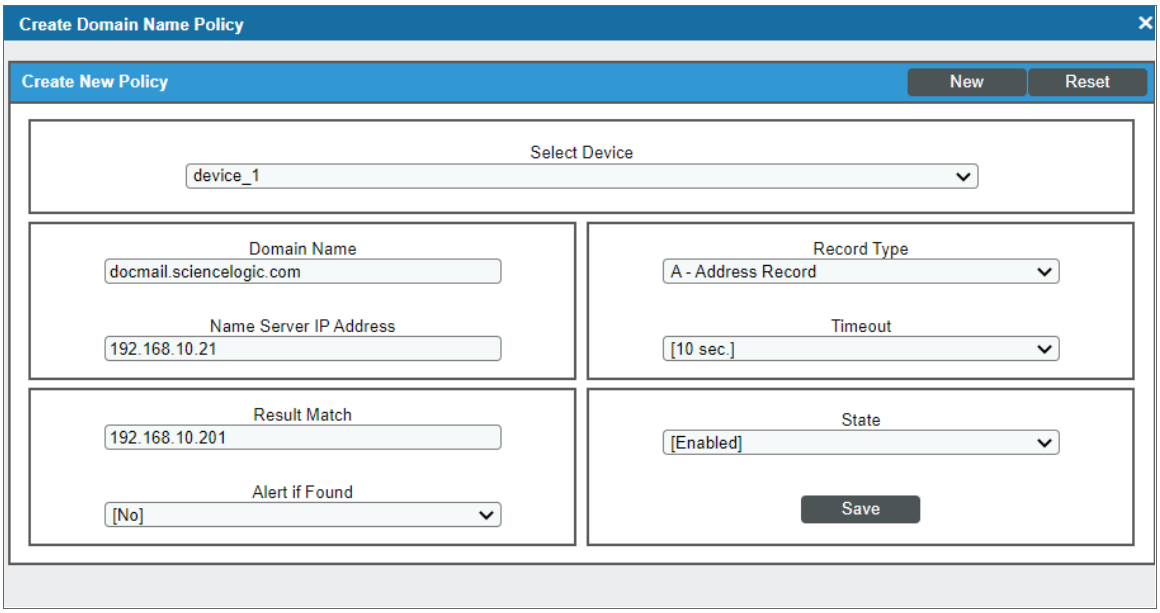
4. In the **Create Domain Name Policy** modal, supply a value in each of the following fields:
    - ***Select Device***. Select a device from the drop-down list to align with this policy. By default, the current device is selected in this field.

> **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 DNS you will be monitoring with the policy, but you aren't required to do so. The requests to the DNS will be sent from an 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 DNS. 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. Click **[Save]**.

Example Policy for Domain Name



- 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.

Defining a Monitoring Policy for a Domain Name in the Classic SL1 User Interface

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.
- Click the **[Create]** button.

3. The **Create Domain Name Policy** modal page appears.

For information about completing the fields in the **System Process Policy** modal page, see the section on *Defining a Monitoring Policy for a Domain Name*.

Editing a Monitoring Policy for a Domain Name

To edit a domain name monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **Domain Name Policy** modal appears.
4. In the **Domain Name Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Monitoring Policy for Domain Names*.
5. Click **[Save]**.

Editing a Monitoring Policy for a Domain Name in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
   - In the **Device Administration** panel, click the **[Monitors]** tab.
   - In the **Monitoring Policies** page, find the policy you want to edit and click its wrench icon ( ).

Or:

2. From the **Domain Name Monitoring** page (Registry > Monitors > Domain Name):
   - In the **Domain Name Monitoring** page, find the policy you want to edit and click that policy's wrench icon ( ).
3. The **Domain Name Policy** modal appears.
4. In the **Domain Name Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Monitoring Policy for Domain Name*.
5. Click **[Save]**.

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.

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.

To execute a domain name monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).
4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is helpful for diagnosing possible problems with a policy.

Executing the Domain Name Monitoring Policy in the Classic SL1 User Interface

To execute a domain name monitoring policy in the classic SL1 user interface:

1. In the **Domain Name Monitoring** (Registry > Monitors > Domain Name) page, find the policy you want to run manually.
2. Click the lightning bolt icon ( ) to manually execute the policy.
3. While the policy is executing, SL1 opens a modal 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.

Deleting a Domain Name Policy

You can delete a domain name policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a domain name monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.

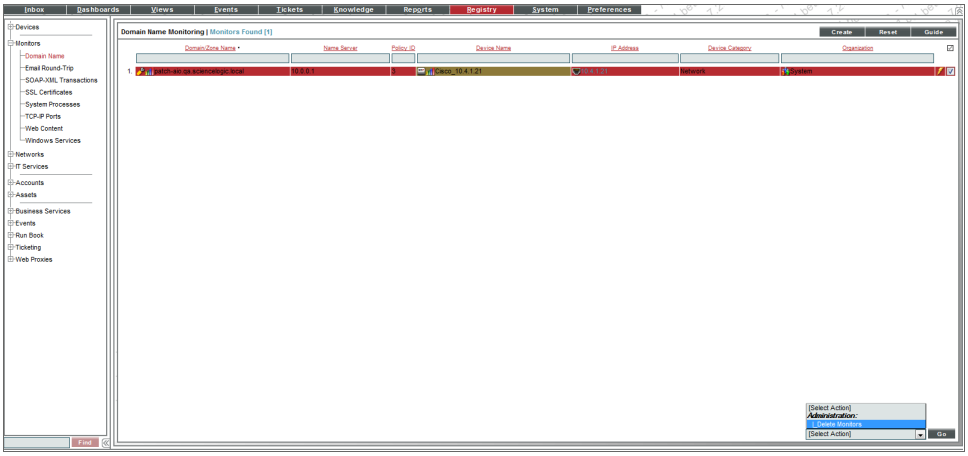
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

Deleting a Domain Name Policy in the Classic SL1 User Interface

You can delete one or more domain-name policies from the **Domain Name Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a domain name monitoring policy in the classic SL1 user interface:

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.

Viewing Reports for a Domain Name Monitoring Policy

See the section *Viewing Performance Graphs* to view information and examples of reports for domain name monitoring.

Chapter 13

Monitoring Email Round-Trips

Overview

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.

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

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

This chapter covers the following topics:

Required Settings and Configuration 230
How SL1 Collects and Calculates Round-Trip Time 232
Viewing the Email Round-Trip Monitoring Policies 232
Defining an Email Round-Trip Monitoring Policy 234
Events for Email Round-Trip Policies 237
Editing an Email Round-Trip Monitoring Policy 238
Deleting an Email Round-Trip Monitoring Policy 239
Viewing Reports on an Email Round-Trip Monitoring Policy 240

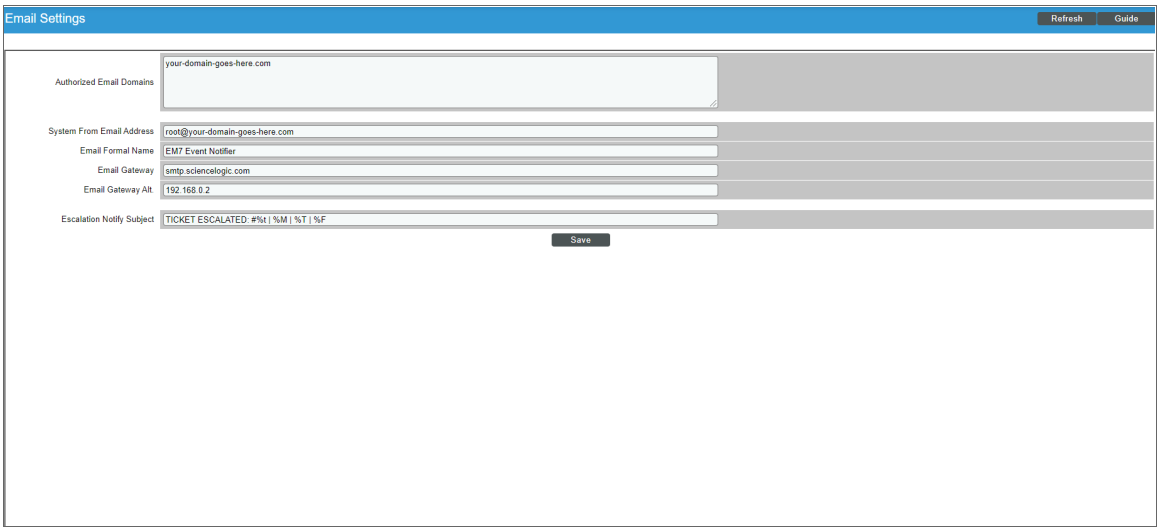
Required Settings and Configuration

The following sections describe the system settings you must define in SL1 and the required configuration that must happen on the external email client before you can define an email round-trip monitoring policy.

Required System Settings in SL1

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).



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 domain name of the Database Server or the fully-qualified domain 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 domain 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 domain 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 domain 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. Click **[Save]**.

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. The following guidelines apply:

- 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 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.

How SL1 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.

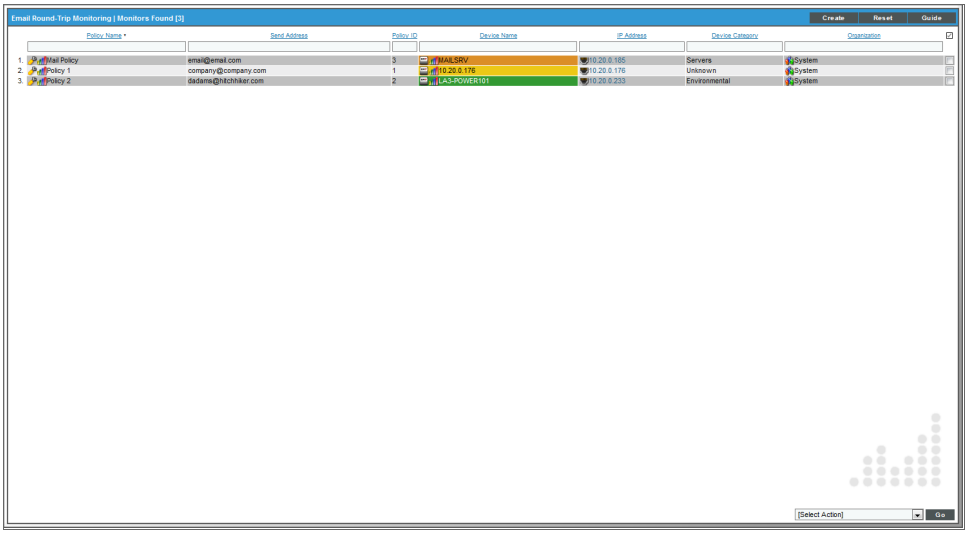
The response email that SL1 receives must contain the body of the email that was sent by SL1, which contains a unique ID number. SL1 compares the unique ID in the response email to the record of emails that SL1 sent. By matching the response to the original email using the unique ID, SL1 can handle cases 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 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:



- ***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.
- ***State***. Whether the policy is enabled or disabled.
- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.
- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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:

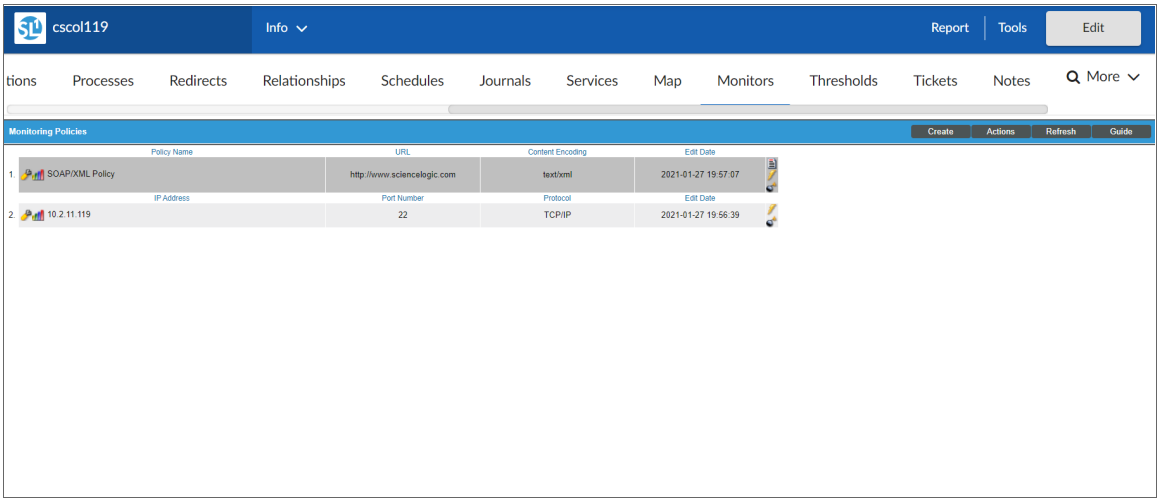
- ***Policy Name***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching name.
- ***Send Address***. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page 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. For more information, see the section on *Required Settings and Configuration*.

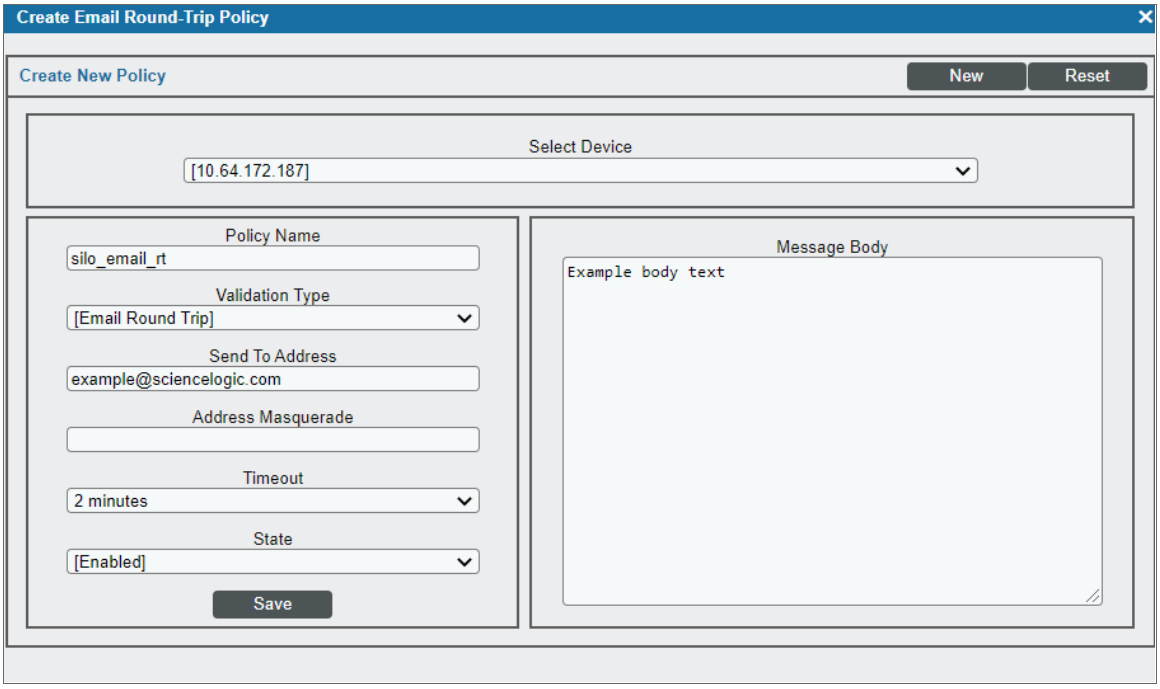
You can define an email round-trip monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define an email round-trip monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define an email round-trip monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.

3. Click **[Create]**, and then select *Create Email Round-Trip Policy*. The **Create Email Round-Trip Policy** modal appears:



4. In the **Email Round-Trip Policy** modal, supply values 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.

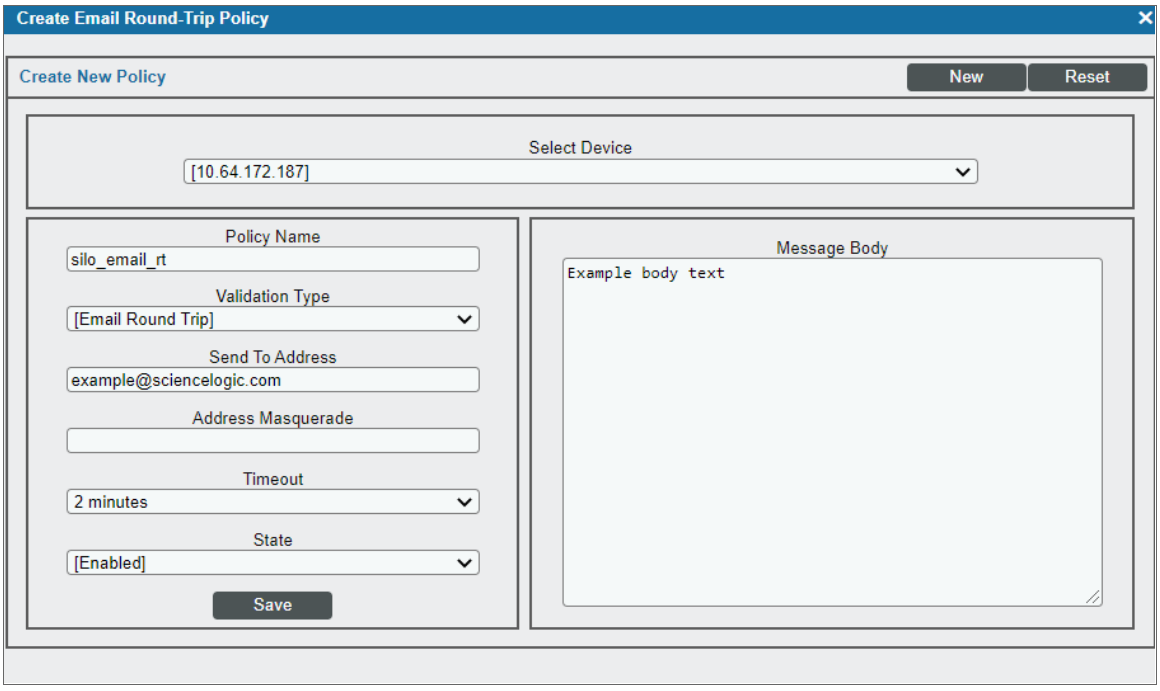
NOTE: Before you can define an email round-trip policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the device to which SL1 will send test messages, but you aren't required to do so. Alternately, you might want to create a virtual device to associate with an 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. This can be any combination of letters and numbers.
   - ***Validation Type***. You can select only *Email Round Trip*.
   - ***Send To Address***. Email address for the external email server. This 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. This 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. Click **[Save]**. SL1 will immediately begin sending email messages to the ***Send To Address***.

Example Email Round-Trip Monitoring Policy



- In this example, we associated the policy with the device "192.168.44.220".
- The policy sent an Email message to "example@sciencelogic.com". The message contained the body "testing Email round trip".
- The mailbox for example@sciencelogic.com included a rule to automatically forward the message back to the original sender.

Defining an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface

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 appears.

For information about completing the fields in the **Email Round-Trip Policy** modal, see the section on *Defining an Email Round-Trip Monitoring Policy*.

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

Event Message	Severity	Description	Cause	Clears Event(s)
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

Editing an Email Round-Trip Monitoring Policy

To edit an email round-trip monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **Email Round-Trip Policy** modal appears.
4. In the **Email Round-Trip Policy** modal, 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. Click **[Save]**.

Editing an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface

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. Click wrench icon ( ) for the device.
   - In the **Device Administration** panel, click the **[Monitors]** tab.
   - In the **Monitoring Policies** page, find the policy you want to edit and click 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 click its wrench icon ( ).
3. The **Email Round-Trip Policy** modal appears.
4. In the **Email Round-Trip Policy** modal, 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. Click **[Save]**.

Deleting an Email Round-Trip Monitoring Policy

You can delete an email round-trip policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

> WARNING: Deleting a monitoring policy will also remove all data that was previously collected by the policy. SL1 also deletes the reports associated with the policy.

To delete an email round-trip monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

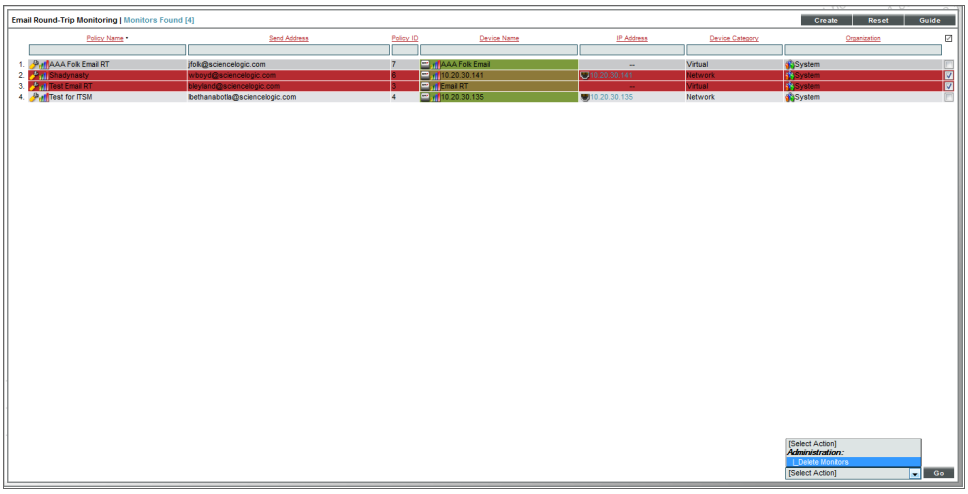
Deleting an Email Round-Trip Monitoring Policy in the Classic SL1 User Interface

You can delete one or more email round-trip policies from the **Email Round-Trip Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device.

> WARNING: Deleting a monitoring policy will also remove all data that was previously collected by the policy. SL1 also deletes the reports associated with the policy.

To delete an email round-trip monitoring policy in the classic SL1 user interface:

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. Click 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.

Viewing Reports on an Email Round-Trip Monitoring Policy

See the section *Viewing Performance Graphs* to view information and examples of reports for email round-trip monitoring.

Chapter 14

Monitoring Ports

Overview

This chapter describes how to create policies that monitor ports in SL1 using NMAP or the SL1 agent.

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

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

This chapter covers the following topics:

What is a Port? 242
Port Security 242
Port Availability 242
System Settings that Affect Port Availability Monitoring 243
Viewing the List of TCP/IP Port Monitoring Policies 244
Defining a Port Monitoring Policy 245
Editing a Port Monitoring Policy 248
Executing a Port Monitoring Policy 249
Deleting a Port Monitoring Policy 250
Viewing a List of All TCP/IP Ports 251
Viewing a List of All Open Ports on All Devices 254
Viewing a List of All Open Ports on a Single Device 257

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 > TCP/UDP Ports tab) 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 SL1 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.

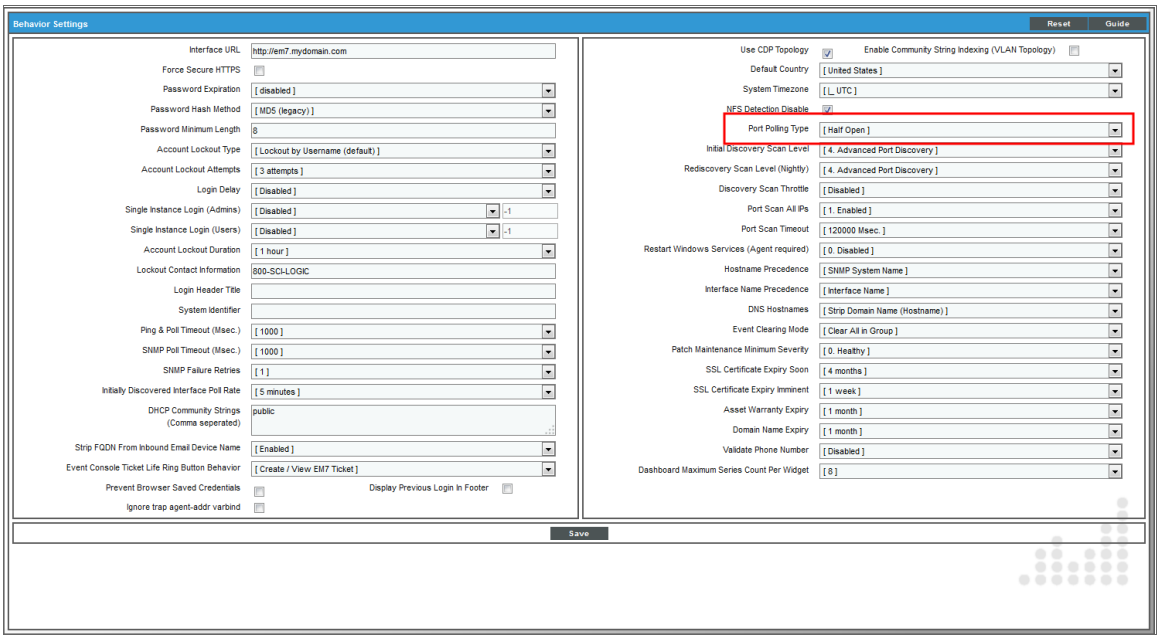
If a port is not available, SL1 creates an event with the message "port not responding to connection".

To monitor port availability, you must define a port monitoring policy. This is described in the following sections.

System Settings that Affect Port Availability Monitoring

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:



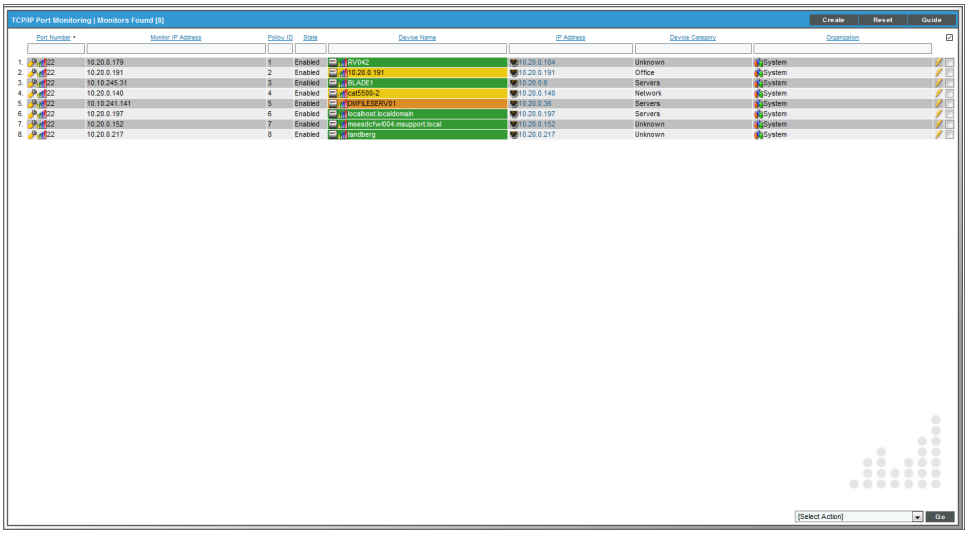
- ***Port Polling Type***. Specifies how SL1 should poll ports for availability using NMAP. The choices are:
    - *Half Open*. Uses a faster TCP/IP connection method (a TCP SYN scan, nmap -sS) and does not appear on device's logs.
    - *Full Connect*. Uses the standard TCP/IP connection (TCP connect() scan, nmap -sT) to detect open ports.

Viewing the List of 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.



- ***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.
- ***State***. Whether the policy is enabled or disabled.
- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.
- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

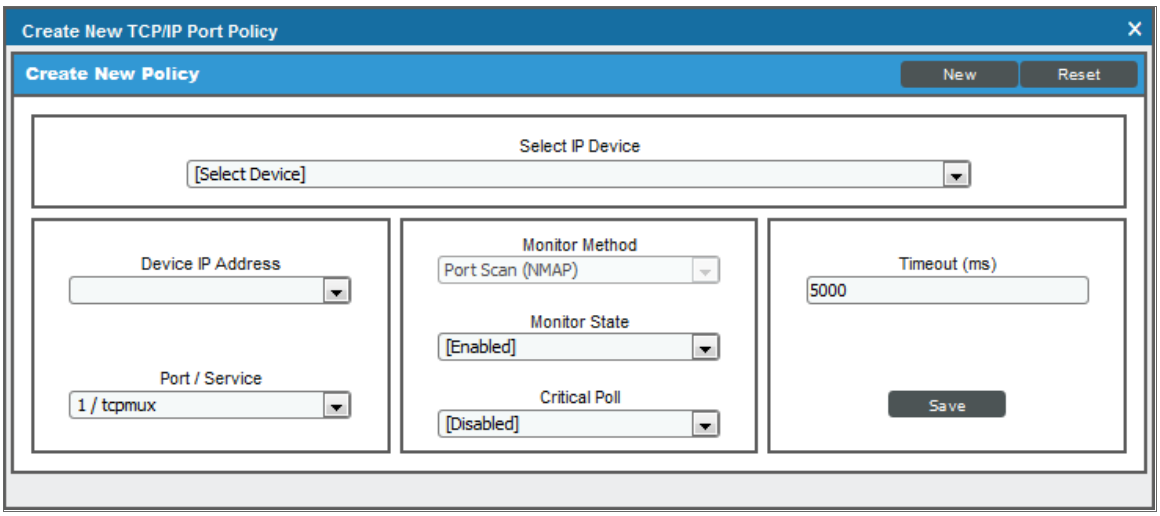
Defining a Port Monitoring Policy

SL1 enables you to create policies that monitor ports. When a port monitoring policy is created, SL1 monitors the port for availability every 5 minutes. You can choose whether a policy monitors port availability.

NOTE: Non-administrator users 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. Administrator users can view all IP ports.

To define a port monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a port monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Click **[Create]**, and then select *Create TCP/IP Port Policy*. The **TCP/IP Port Policy** modal appears:



4. In the **TCP/IP Port Policy** modal, supply a value in each of the following fields:

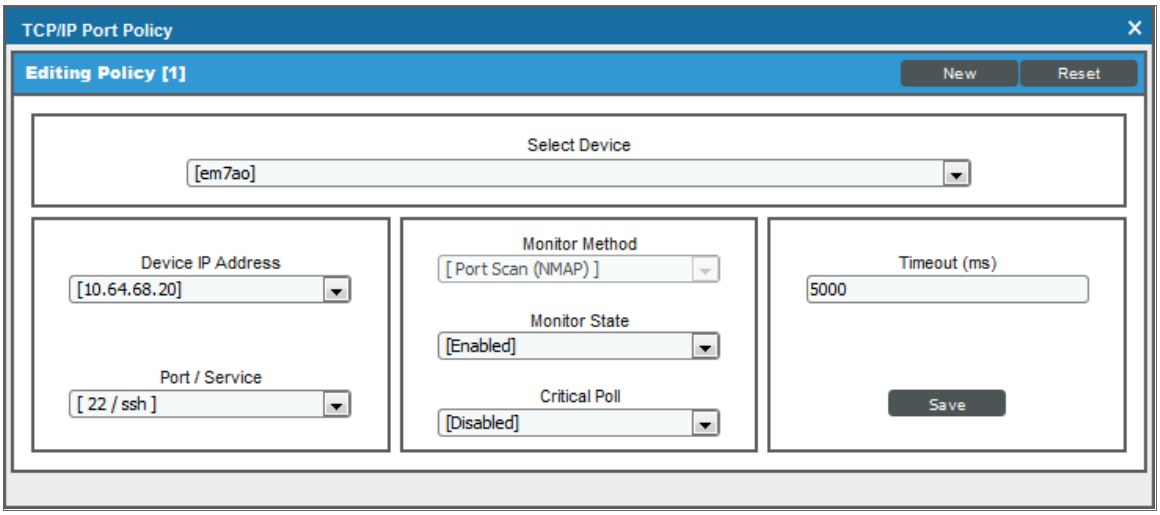
   - ***Select IP Device***. Select a device from this drop-down list to align with this policy. By default, the current device is selected in this field.
   - ***Device IP Address***. IP address through which SL1 communicates with the device.
   - ***Port/Service***. Port number and the corresponding service running on the port.
   - ***Monitor Method***. Select whether the policy will be executed using NMAP or using the SL1 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.

5. Click **[Save]**.

Example Policy for TCP/IP Port Availability



- 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.

Defining a Port Monitoring Policy in the Classic SL1 User Interface

You can define a port monitoring policy in the **TCP/IP Port Policy** modal. 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 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. Click the wrench icon ( ) for the device.
3. In the **Device Administration** panel for the device, click 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 appears.

To access the **TCP/IP Port Policy** modal from the **TCP/IP Port Monitoring** page:

1. Go to the **TCP/IP Port Monitoring** page (Registry > Monitors > TCP-IP Ports).
2. Click the **[Create]** button.
3. The **TCP/IP Port Policy** modal appears.

For information about completing the fields in the **TCP/IP Port Policy** modal, see the section on *Defining a Port Monitoring Policy*.

Editing a Port Monitoring Policy

To edit a port monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **TCP/IP Port Policy** modal appears.
4. In the **TCP/IP Port Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Port Monitoring Policy*.
5. Click **[Save]**.

Editing a Port Monitoring Policy in the Classic SL1 User Interface

You can edit a port monitoring policy on the **TCP/IP Port Policy** modal. You can access the **TCP/IP Port Policy** modal 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 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. Click the wrench icon ( ) for the device.
3. In the **Device Administration** panel, click the **[Monitors]** tab.
4. In the **Monitoring Policies** page, find the port policy you want to edit and click its wrench icon ( ).
5. The **TCP/IP Port Policy** modal appears.
6. In the **TCP/IP Port Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Port Monitoring Policy*.
7. Click **[Save]**.

To access the **TCP/IP Port Policy** modal 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. Click the wrench icon ( ) for the port.
3. The **TCP/IP Port Policy** modal appears.
4. In the **TCP/IP Port Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Port Monitoring Policy*.
5. Click **[Save]**.

Executing a 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.

> **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.

To manually execute a port monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).
4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is helpful for diagnosing possible problems with a policy.

Executing a Port Monitoring Policy in the Classic SL1 User Interface

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. Click the lightning bolt icon ( ) to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal 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.

Deleting a Port Monitoring Policy

You can delete a port monitoring policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a port monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

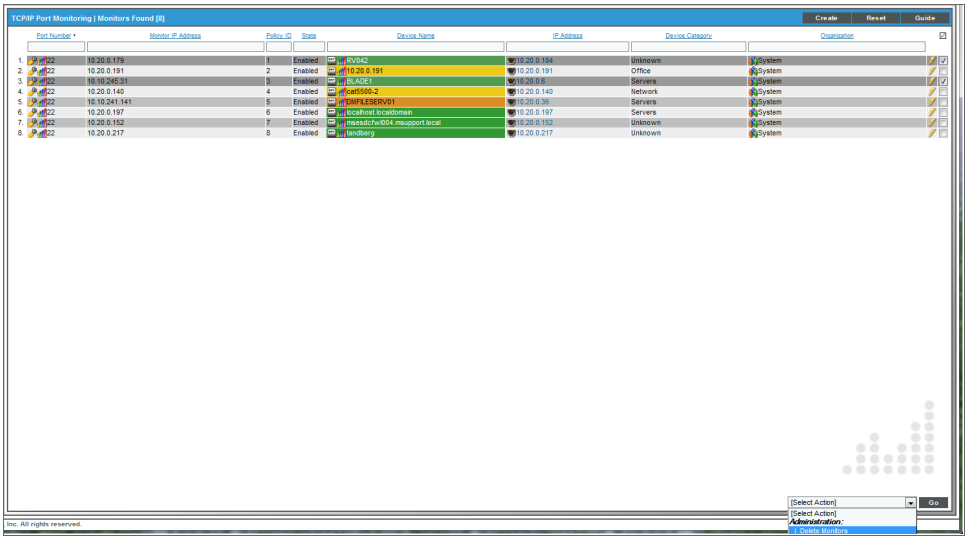
Deleting a Port Monitoring Policy in the Classic SL1 User Interface

You can delete one or more port monitoring policies from the **TCP/IP Port Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a port monitoring policy in the classic SL1 user interface:

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.

3. In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.



4. Click **[Go]** to delete the port monitoring policy.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Viewing a List of All TCP/IP Ports

The **TCP/IP Port Editor** page (System > Customize > TCP-IP Ports) allows you to view the properties of TCP ports. SL1 uses this list of ports and their definitions when scanning devices to discover open ports.

For each port defined in the **TCP/IP Port Editor** page, SL1 can search each device to see if the port exists and if it is operational. For each device, SL1 displays the list of discovered, open ports in the **Port Security** page.

NOTE: TCP ports are logical connections that applications use to communicate between computers. TCP ports are not to be confused with interfaces, which are hardware based.

SL1 includes definitions of all IANA "well-known ports" (0 - 1023) as well as many IANA registered ports (1024 - 49151) and application-specific or user-defined dynamic ports (49152 and greater). If your network includes a port that is not already defined in the **TCP/IP Port Editor** page, you can define the port manually.

The **TCP/IP Port Editor** page contains a pane at the bottom of the page called the **Registry of Manageable Ports**. This pane displays all the ports defined in SL1. These are the ports that SL1 can scan for and manage. For each port, the **TCP/IP Port Editor** page displays the following:

- ***Name***. Name or alias of the port. For well-known ports, use the IANA port name.
- ***Port Number***. Port number for the TCP port.

- ***Protocol***. Currently SL1 scans only TCP ports.
- ***Description***. A brief description of the port, including the service/application that uses the port.
- ***Poll State***. Specifies whether SL1 should poll this port for availability data. This data is used by SL1 in availability reports. Choices are *Enabled* or *Disabled*.
- ***Illicit Port Alarm***. Specifies whether SL1 will generate an event if the port is discovered. This option should be enabled only for unauthorized ports. Choices are *On* or *Off*.
- ***GUI Feature***. For devices that include this port, specifies the tools that should appear in the **Device Toolbox** page to perform diagnostics and administration on the port.

Defining a New TCP/IP Port

If your network includes one or more ports that aren't defined in the **TCP/IP Port Editor** page, you can define these ports manually. To manually define a port:

1. Go to the **TCP/IP Port Editor** page (System > Customize > TCP-IP Ports) .
2. In the **TCP/IP Port Editor** page, go to the registry pane at the bottom of the page. Find the port definition you want to edit. Select its wrench icon ( ).
3. In the editor pane (at the top of the page), supply a value in each of the following fields:

    - ***Description***. A brief description of the port, including the service/application that uses the port. Can be any combination of alpha-numeric characters, up to 128-characters in length.
    - ***Port Name***. Name or alias of the port. For well-known ports, use the IANA port name. Can be any combination of alpha-numeric characters, up to 48-characters in length.
    - ***Port Number***. Port number for the TCP port. Can be any combination of numbers, up to 5-digits in length.
    - ***Poll State***. Specifies whether SL1 should poll this port for availability data. This data is used by SL1 in availability reports. Choices are:

        - *Enabled*. Poll this port to gather availability data.
        - *Disabled*. Don't poll this port to gather availability data.

    - ***Illicit Port Alarm***. Specifies whether SL1 should generate an event if the port is discovered. This option should be enabled only for unauthorized ports. Choices are:

        - *Enabled*. Generate an event if SL1 discovers this port on a device.
        - *Disabled*. Do not generate an event if SL1 discovers this port on a device.

    - ***Toolbox Feature***. For devices that include this port, specifies the tools that should appear in the **Device Toolbox** page. Choices are:

        - *None*
        - *Web*. Opens a new browser window and attempts to make an HTTP connection to the current device.
        - *FTP*. Opens a new browser window and attempts to make an FTP connection to the current device.

- *Secure Web*. Opens a new browser window and attempts to make an https connection to the current device.
- *Telnet*. Opens a browser session or terminal session using the IP address of the current device and prompts you for the telnet user name and password.
- *Terminal*. Opens the **Terminal Services Client Web Connection** modal page, where you can enter the login information for the terminal services session.
- *SSH*. Opens a browser session for a secure SSH connection to the device.

4. Click **[Save]**.

Editing the Properties of a Port

You can edit one or more parameters of a port definition. When you edit a port's properties, you change how SL1 manages the port on each device where the port is discovered.

To edit a port definition:

1. Go to the **TCP/IP Port Editor** page (System > Customize > TCP-IP Ports).
2. Click the **[Refresh]** button to clear any values from the editor pane.
3. Locate the TCP/IP port definition that you want to edit and click its wrench icon ( ). The editor pane (at the top of the page) is populated with values from the port definition.

TIP: You can use the search fields immediately below the editor pane to help you locate the port definition that you want to edit.

4. Edit the values in one or more of the fields in the editor pane.
5. Click **[Save]** to save any changes to the port definition.

Deleting a Port Definition

From the **TCP/IP Port Editor** page, you can delete the definitions for one or more TCP ports.

CAUTION: If you delete the definition of a TCP port, SL1 will not be able discover that port on any devices in the network. To discover open ports and to monitor ports for availability, SL1 must include a definition of the port in the **TCP/IP Port Editor** page.

To delete one or more port definitions from SL1:

1. Go to the **TCP/IP Port Editor** page (System > Customize > TCP-IP Ports).
2. In the **TCP/IP Port Editor** page, go to the registry pane at the bottom of the page. Locate the port definition you want to delete and select its checkbox ( ).

TIP: You can use the search fields immediately above the registry pane to help you locate the port definition that you want to delete.

3. Repeat step 2 to select any additional port definitions you want to delete.
4. Click **[Delete]**. All selected port definitions are deleted.

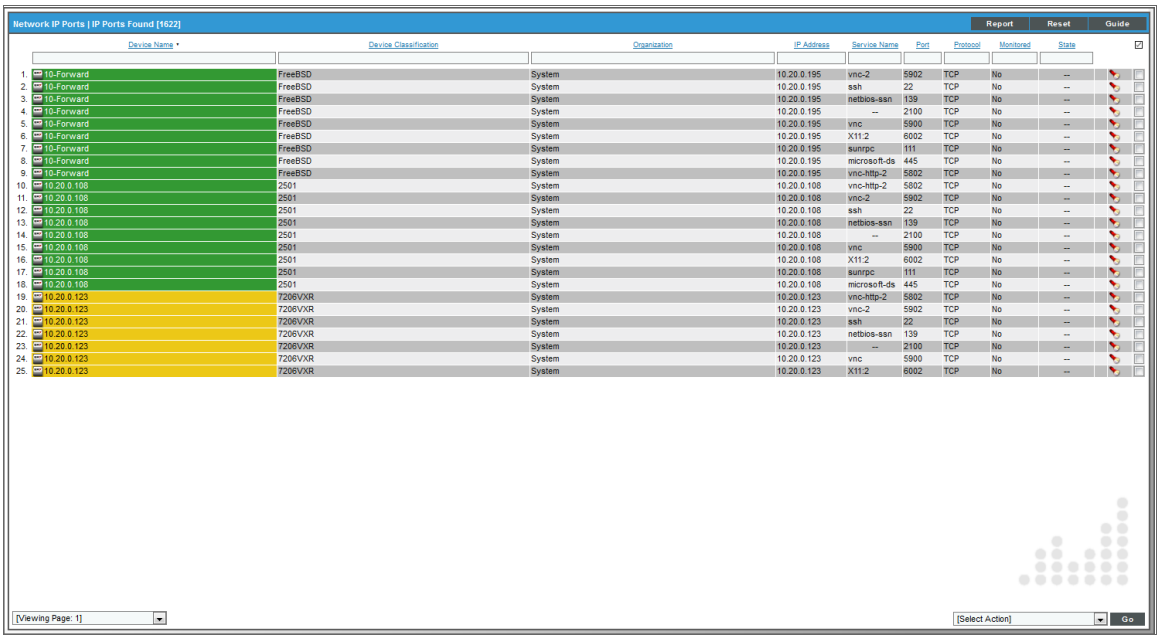
Viewing a List of All Open Ports on All Devices

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).



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 Network 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.

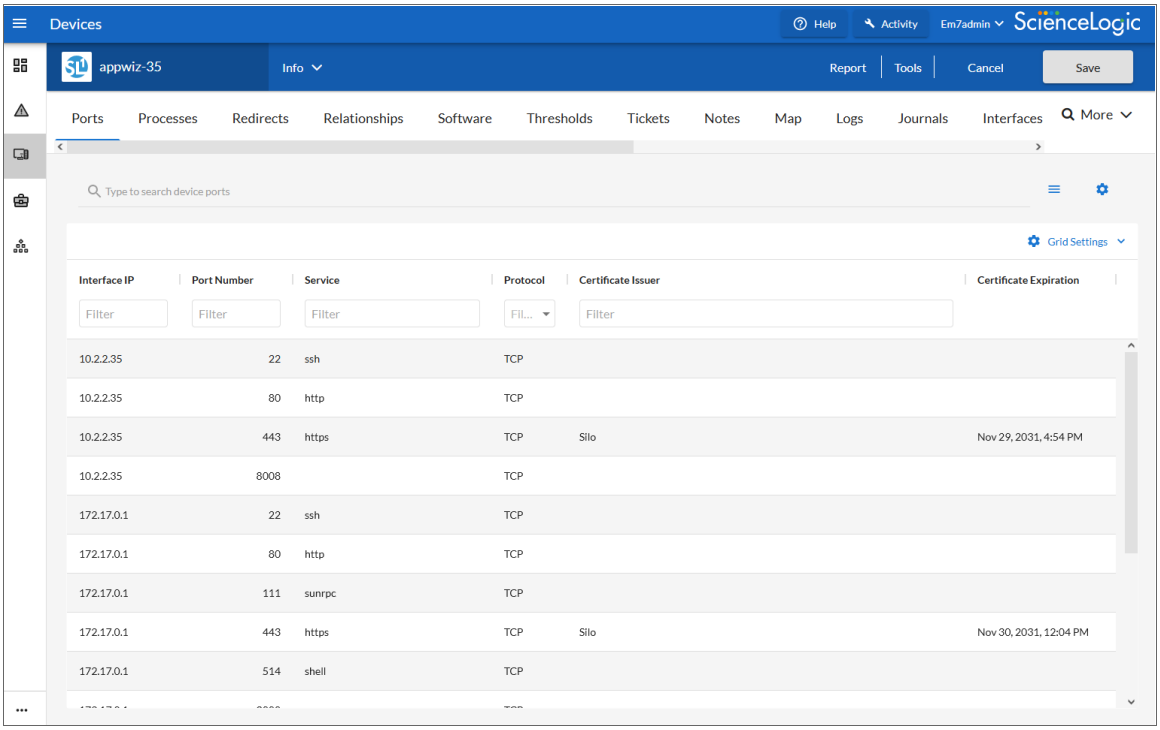
Filter by one or more of the following parameters:

- ***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

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



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

NOTE: 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.

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.

Viewing a List of All Open Ports on a Single Device in the Classic SL1 User Interface

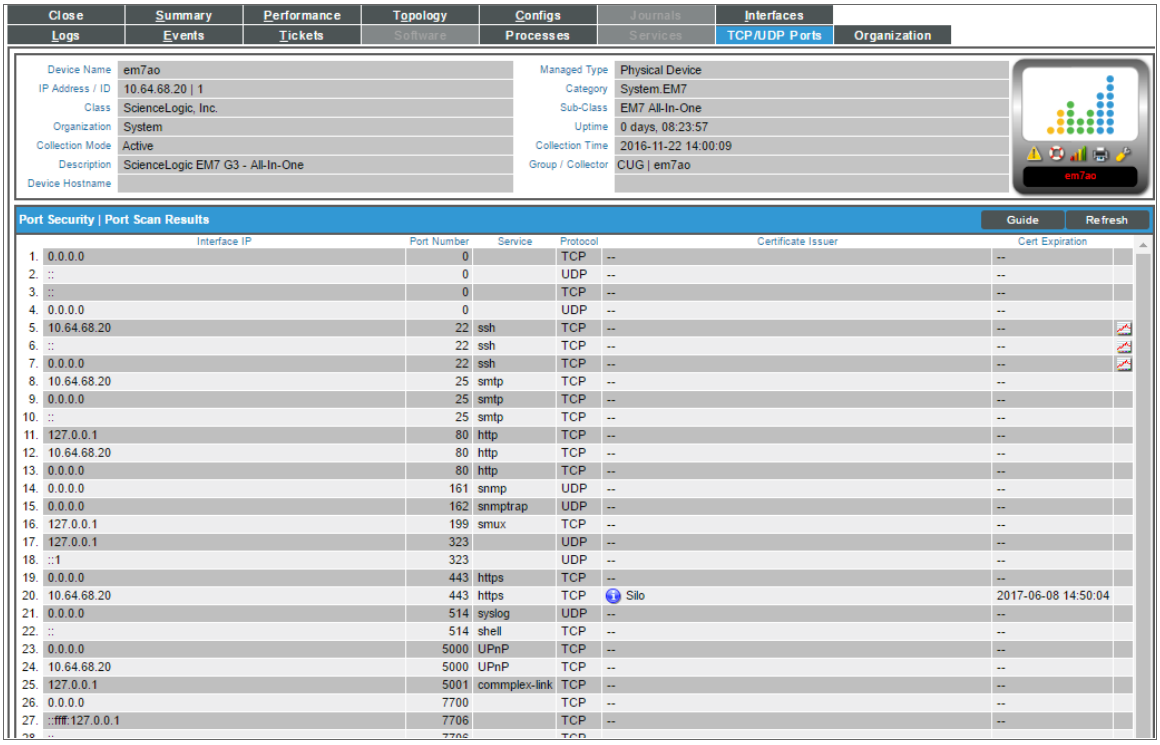
NOTE: Users of type "user" can view only IP ports that are aligned with the same organization(s) to which the user is aligned. This means that the device associated with the port(s) must be aligned with one of the organizations to which the user is aligned. Users of type "administrator" can view all 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.



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.

Viewing Port Availability Reports for a Single Device

See the section on *Viewing Performance Graphs* for information and examples of reports for port availability.

Chapter 15

Monitoring SOAP and XML Transactions

Overview

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.

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

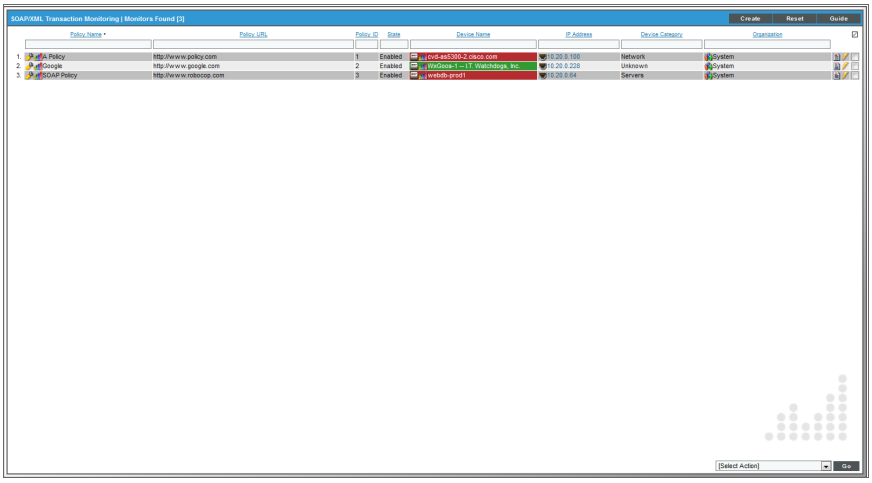
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

This chapter covers the following topics:

Viewing the SOAP/XML Transaction Monitoring Policies *261*
Defining a SOAP/XML Transaction Monitoring Policy *262*
Editing a SOAP/XML Transaction Monitoring Policy *268*
Executing a SOAP/XML Transaction Monitoring Policy *269*
Deleting a SOAP/XML Transaction Monitoring Policy *269*
Viewing Reports on a SOAP/XML Transaction Policy *271*
Viewing Raw Data from a SOAP/XML Policy *271*

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:



- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.
- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

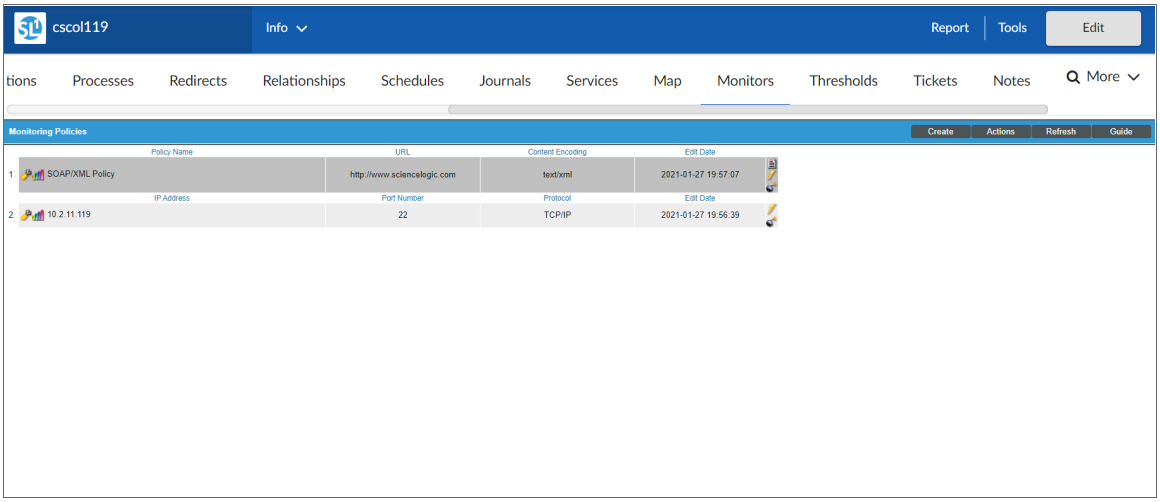
You can also use *special characters* to filter each parameter.

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.

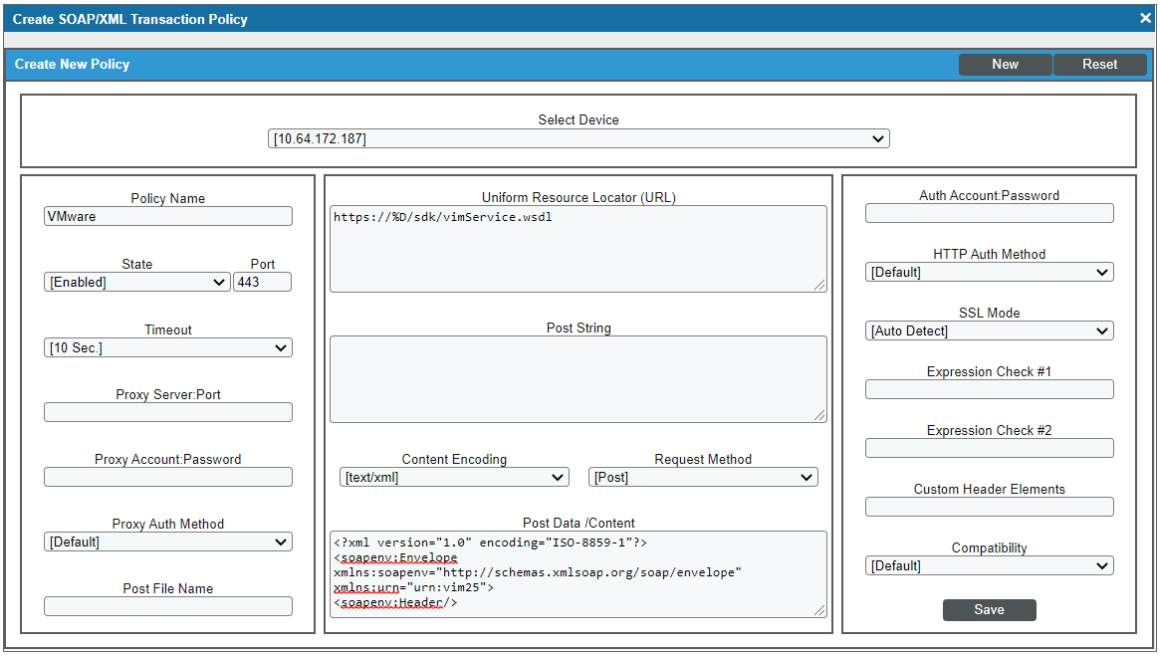
Defining a SOAP/XML Transaction Monitoring Policy

You can define a SOAP/XML transaction monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define a SOAP/XML transaction monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a SOAP/XML transaction monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Click **[Create]**, and then select *Create System Process Policy*. The **SOAP/XML Transaction Policy** modal appears:



4. In the **SOAP/XML Transaction Policy** modal, 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. This 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

- ***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, such as ***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 username and password in clear text.
  - *Digest*. Password is transmitted as encrypted text, but the username 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 username, 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 username 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*.

- ***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 fields "Birthyear" and "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.

- ***HTTP Auth Method***. For websites that require authentication, use one of the selected methods:

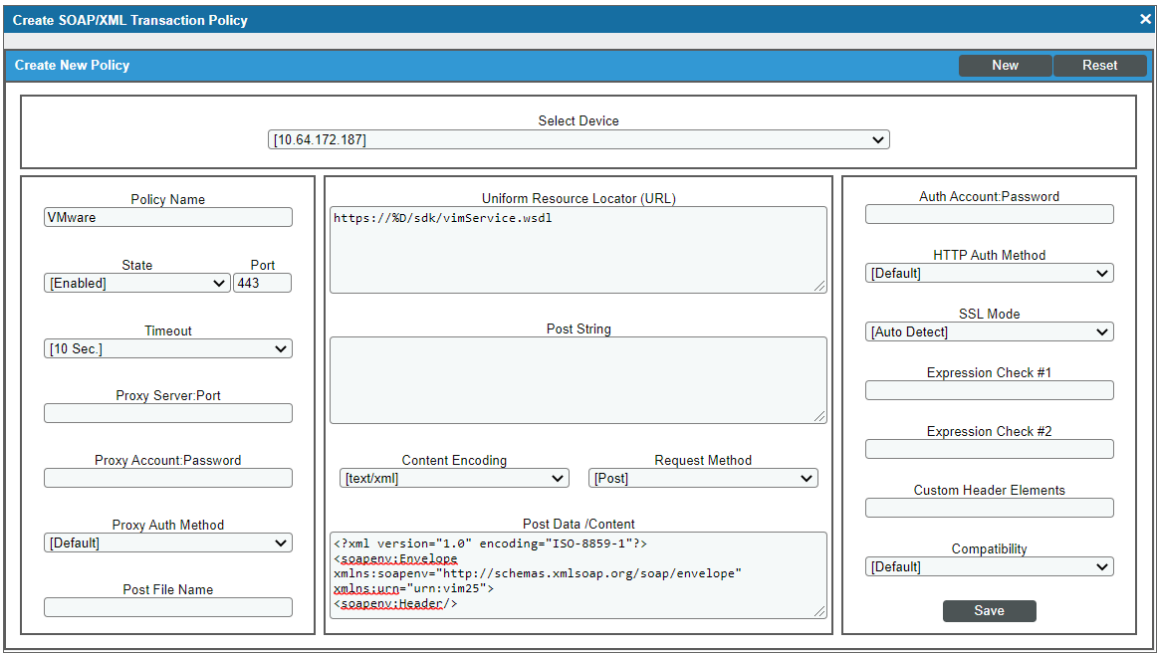
    - *Default*. By default, no authentication parameters are sent. Use this option for websites that do not require authentication. However, if you supply a value in another field that requires authentication, such as ***HTTP Auth Username:Password***, the *Any* authentication parameter will be used.
    - *Basic*. Most widely compatible authentication across platforms. Sends a Base64-encoded string that contains a username and password for the client. Base64 is not a form of encryption and should be considered the same as sending the username and password in clear text.
    - *Digest*. Password is transmitted as encrypted text, but the username 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 username, 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 username 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 Mode***. Specifies whether SL1 should use SSL when communicating with the httpd service.
- ***Expression Check #1***. Regular expression to search for. This 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. Click **[Save]**.

Example SOAP/XML Transaction Monitoring Policy



- In this example, the policy monitors SOAP transactions 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 that SL1 can communicate with the VMware server and returns information about the services available on the VMware server.

Defining a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - From the **[Create]** menu in the upper right, click ***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, click the **[Create]** button.
3. The **SOAP/XML Transaction Policy** modal appears.

For information about completing the fields in the **SOAP/XML Transaction Policy** modal, see the section on *Defining a SOAP/XML Transaction Policy*.

Editing a SOAP/XML Transaction Monitoring Policy

To edit a SOAP/XML transaction monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **SOAP/XML Transaction Policy** modal appears.
4. In the **SOAP/XML Transaction Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a SOAP/XML Transaction Policy*.
5. Click **[Save]**.

Editing a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - In the **Monitoring Policies** page, find the policy you want to edit and click 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 click its wrench icon ( ).

3. The **SOAP/XML Transaction Policy** modal appears.
4. In the **SOAP/XML Transaction Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a SOAP/XML Transaction Monitoring Policy*.
5. Click **[Save]**.

Executing a SOAP/XML Transaction Monitoring 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.

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.

To execute a system process monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).
4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Executing a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface

To execute a SOAP/XML transaction monitoring policy in the classic SL1 user interface:

1. In the **SOAP/XML Transaction Monitoring** page, find the policy you want to run manually.
2. Click the lightning bolt icon ( ) to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal 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.

Deleting a SOAP/XML Transaction Monitoring Policy

You can delete a SOAP/XML policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a SOAP/XML transaction monitoring policy:

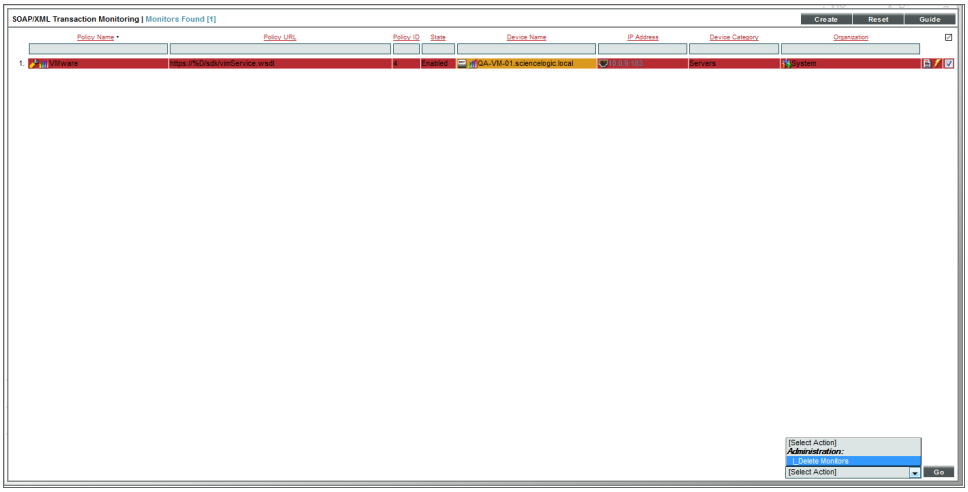
1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

Deleting a SOAP/XML Transaction Monitoring Policy in the Classic SL1 User Interface

You can delete one or more SOAP/XML transaction monitoring policies from the **SOAP/XML Transaction Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a SOAP/XML transaction monitoring policy in the classic SL1 user interface:

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. Click 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.

Viewing Reports on a SOAP/XML Transaction Policy

See the section on *Viewing Performance Graphs* for information and examples of reports for monitoring SOAP/XML transactions.

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. Click the page icon ( ) to the far left in the table.
3. The **Results Page Dump** modal appears. This page displays the raw data sent to the external URL and the raw data returned to SL1.

Chapter 16

Monitoring System Processes

Overview

This chapter describes how to view system processes for devices in SL1 using SNMP or the SL1 Agent. It also describes creating monitoring policies to monitor system processes and using system process reports.

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

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

This chapter covers the following topics:

What is a Process? 273
Viewing the List of System Processes on All Devices 273
Viewing a List of System Processes on a Single Device 276
Viewing the System Process Monitoring Policies 279
Defining a System Process Monitoring Policy 281
Editing a System Process Monitoring Policy 285
Executing a System Process Monitoring Policy 286
Deleting a System Process Monitoring Policy 287
Generating a Report on Multiple System Processes 288
Generating an Exclusion Report for a Single System Process 290
Viewing Reports for a System Process Policy 291

What is a Process?

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:

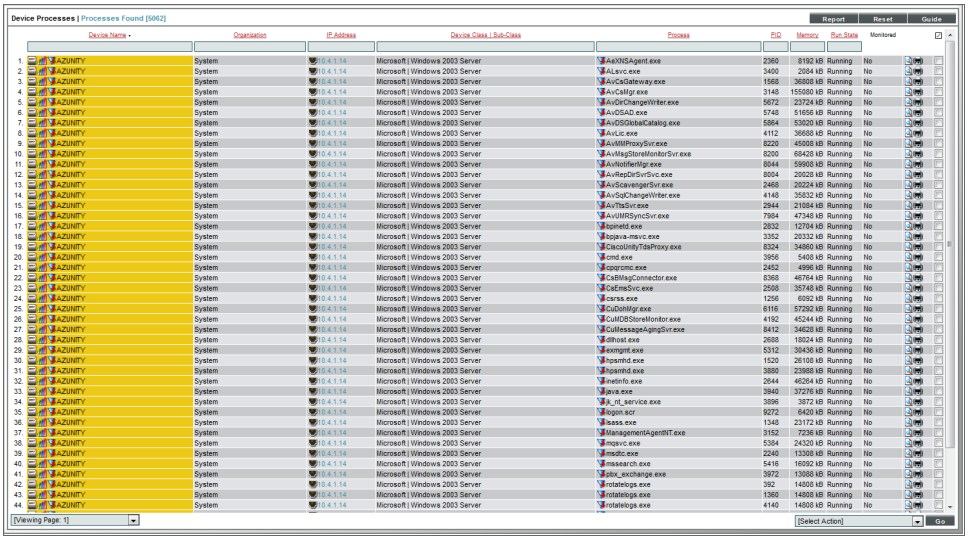
- Whether or not to generate an event if the process is running.
- How much memory each instance of a process can use.
- How many instances of a process can run simultaneously.
- If policy collection is performed by the agent, how much memory all instances of a process can use in total.
- If policy collection is performed by the agent, how much CPU all instances of a process can use in total.

Viewing the List of System Processes on All Devices

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).



2. The **Device Processes** page displays the following about each process:

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.

- ***Device Name***. Name of the device where the process 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.
- ***Organization***. Organization associated with the device where the process resides.
- ***IP Address***. IP address of the device where the process resides.
- ***Device Classification / Sub-Class***. The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during auto-discovery.
- ***Process***. The name of the process. A single process name can have multiple entries.
- ***PID***. A unique ID for the process. The device's operating system assigns this value.
- ***Memory***. The amount of memory currently used/reserved for the process.
- ***Run State***. The current state of the process:
    - *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 monitors the process:
  - *Yes*. SL1 currently monitors this process.
  - *No*. SL1 does not currently monitor this process.

Filtering the List of System 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.

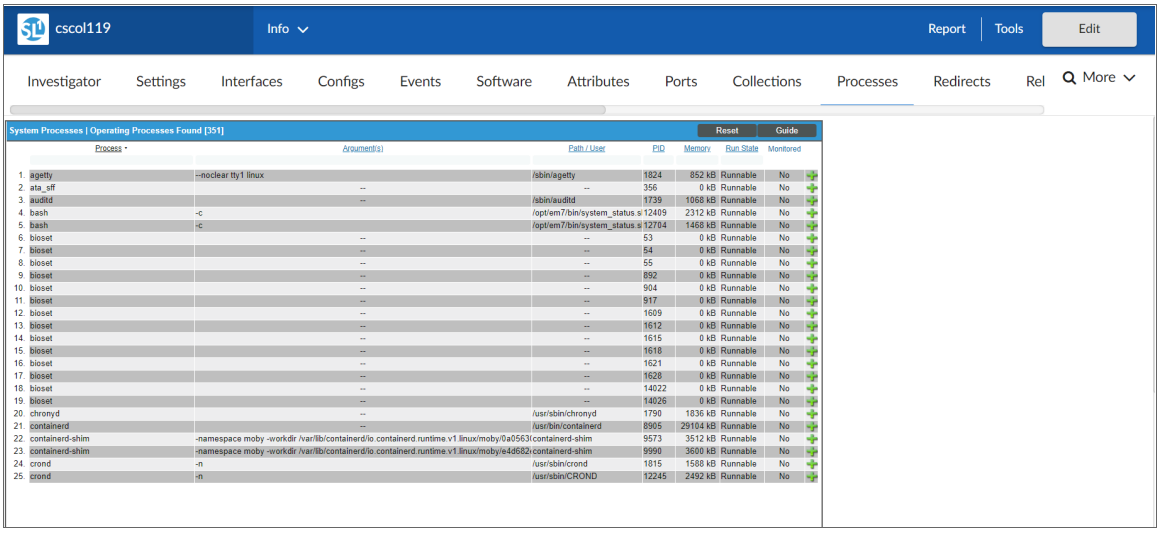
Filter by one or more of the following parameters:

- ***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

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



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.

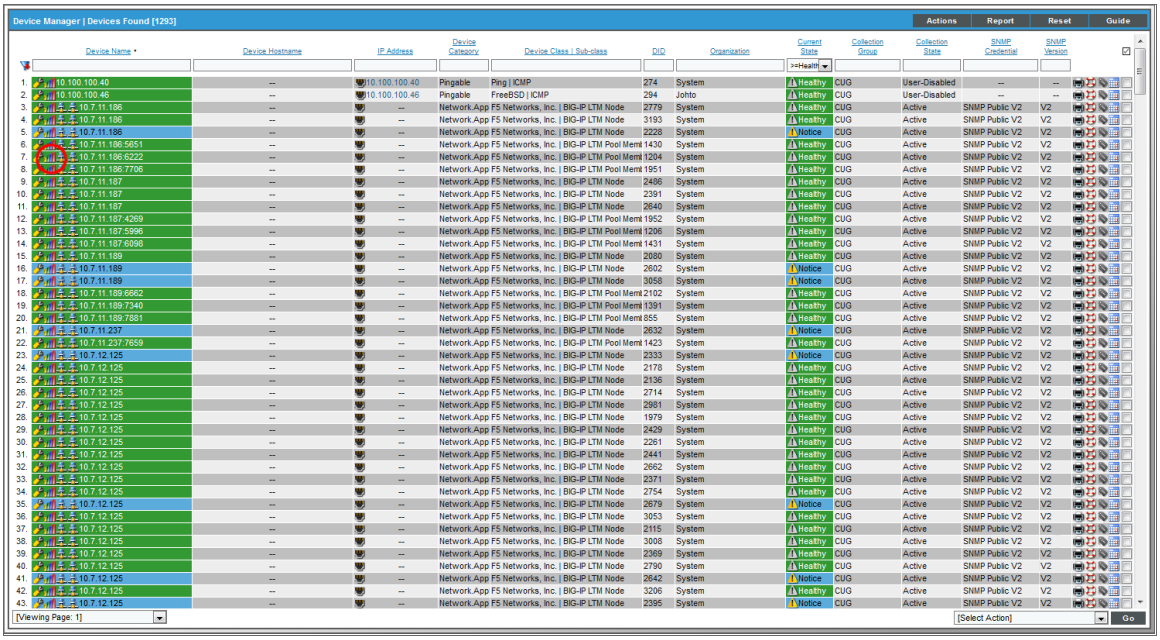
- ***Monitored***. Specifies whether or not SL1 is monitoring this process.

Viewing a List of System Processes on a Single Device in the Classic SL1 User Interface

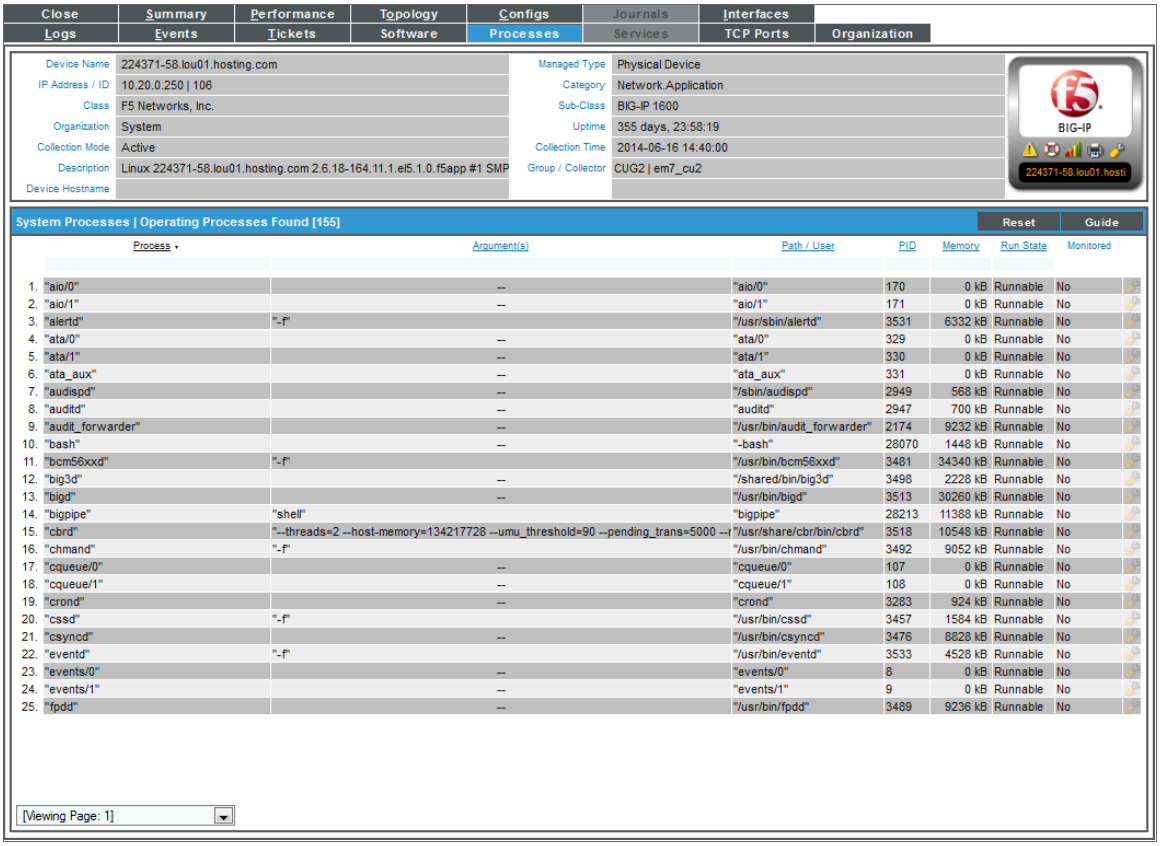
The **System Processes** page displays a list of all of the processes that are running on a single device. The **System Processes** page displays a combined list of processes collected via SNMP and the agent, where applicable.

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.



3. In the **Device Reports** panel, select the Processes tab. The **System Processes** page appears.



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.

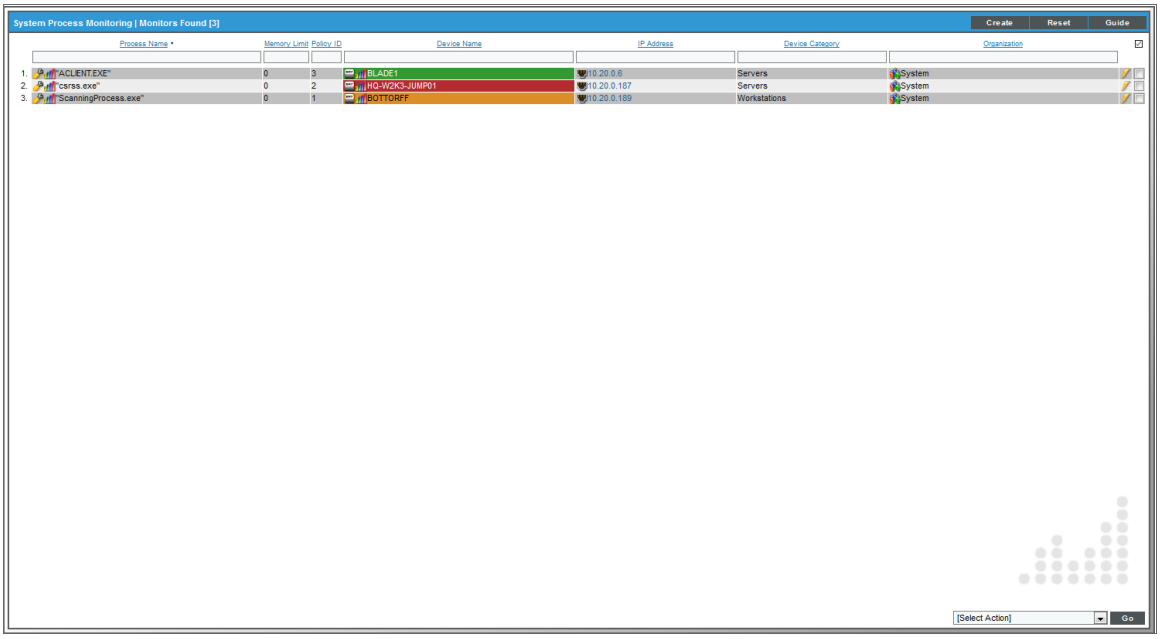
- *Not Running*. Process is in a "waiting" state.
- *Invalid*. Process is part of an operation that failed. Process was not ended gracefully.

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.

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:



- ***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.
- ***State***. Whether the policy is enabled or disabled.
- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.
- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

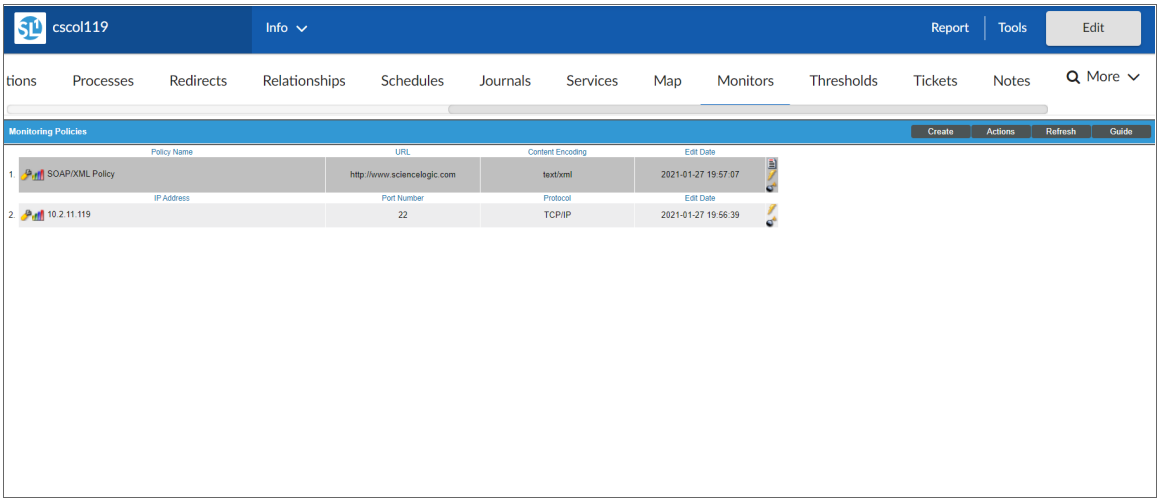
You can also use ***special characters*** to filter each parameter.

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 System Process Monitoring Policy

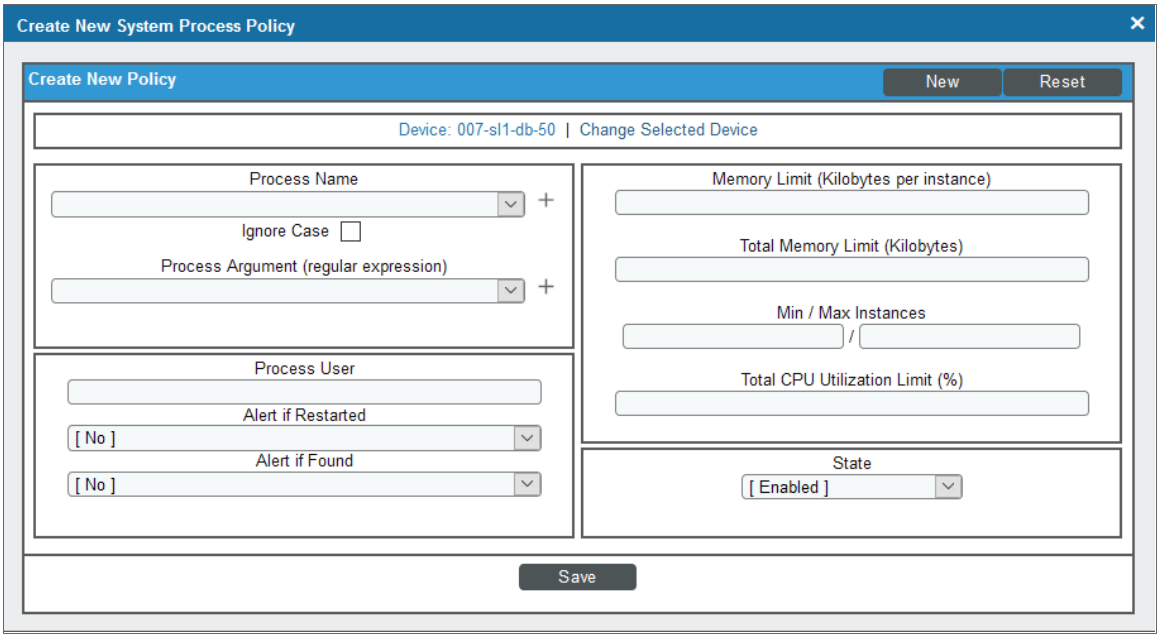
You can define a system process monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define a system process monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a system process monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.

3. Click **[Create]**, and then select *Create System Process Policy*. The **System Process Policy** modal appears:



4. In the **System Process Policy** modal, 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.
- ***Ignore Case***. Select this option if you want SL1 to ignore case-sensitivity in this process name when determining whether to run the system process policy.
- ***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 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 that 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).

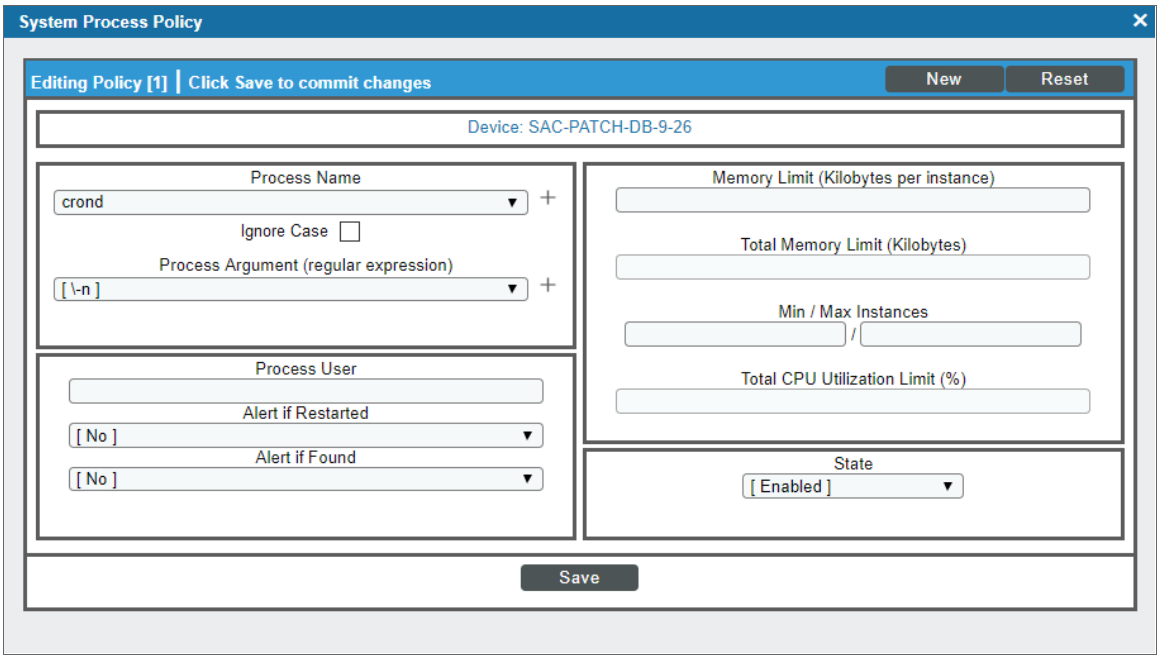
NOTE: In some cases, this alert might appear if a device is restarted.

- ***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 modifiable only if the SL1 Agent is running on the selected device. The amount of memory, in kilobytes, you will 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 modifiable only if the SL1 Agent is running 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*.

5. Click **[Save]**.

Example Policy for a System Process



- 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.

Defining a Monitoring Policy for a System Process in the Classic SL1 User Interface

You can define a process monitoring policy in the **System Process Policy** modal. 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 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 appears.

To access the **System Process Policy** modal 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 appears.

For information about completing the fields in the **System Process Policy** modal, see the section on *Defining a Monitoring Policy for a System Process*.

Editing a System Process Monitoring Policy

To edit a system process monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **System Process Policy** modal appears.
4. In the **System Process Policy** modal, 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. Click **[Save]**.

Editing a Monitoring Policy for a System Process in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - In the **Monitoring Policies** page, find the policy you want to edit and click 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 click its wrench icon ( ).
3. The **System Process Policy** modal appears.
4. In the **System Process Policy** modal, 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. Click **[Save]**.

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. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).
4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Executing a System Process Monitoring Policy in the Classic SL1 User Interface

To execute a system process monitoring policy in the classic SL1 user interface:

1. In the **System Process Monitoring** page (Registry > Monitors > System Processes), find the policy you want to run manually.
2. Click 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.

Deleting a System Process Monitoring Policy

You can delete a system process monitoring policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a system process policy:

1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

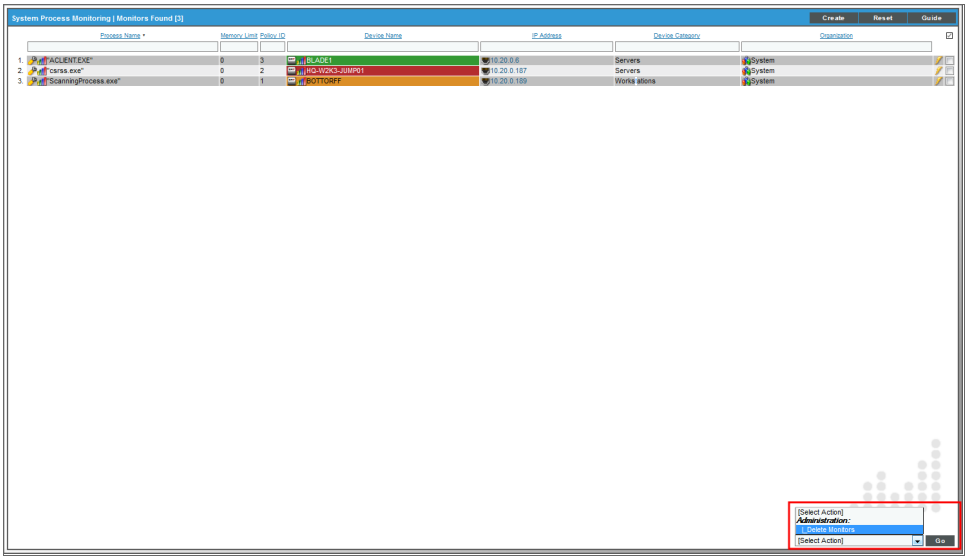
Deleting a System Process Monitoring Policy in the Classic SL1 User Interface

You can delete one or more system process policies from the **System Process Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a system process policy in the classic SL1 user interface:

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*.

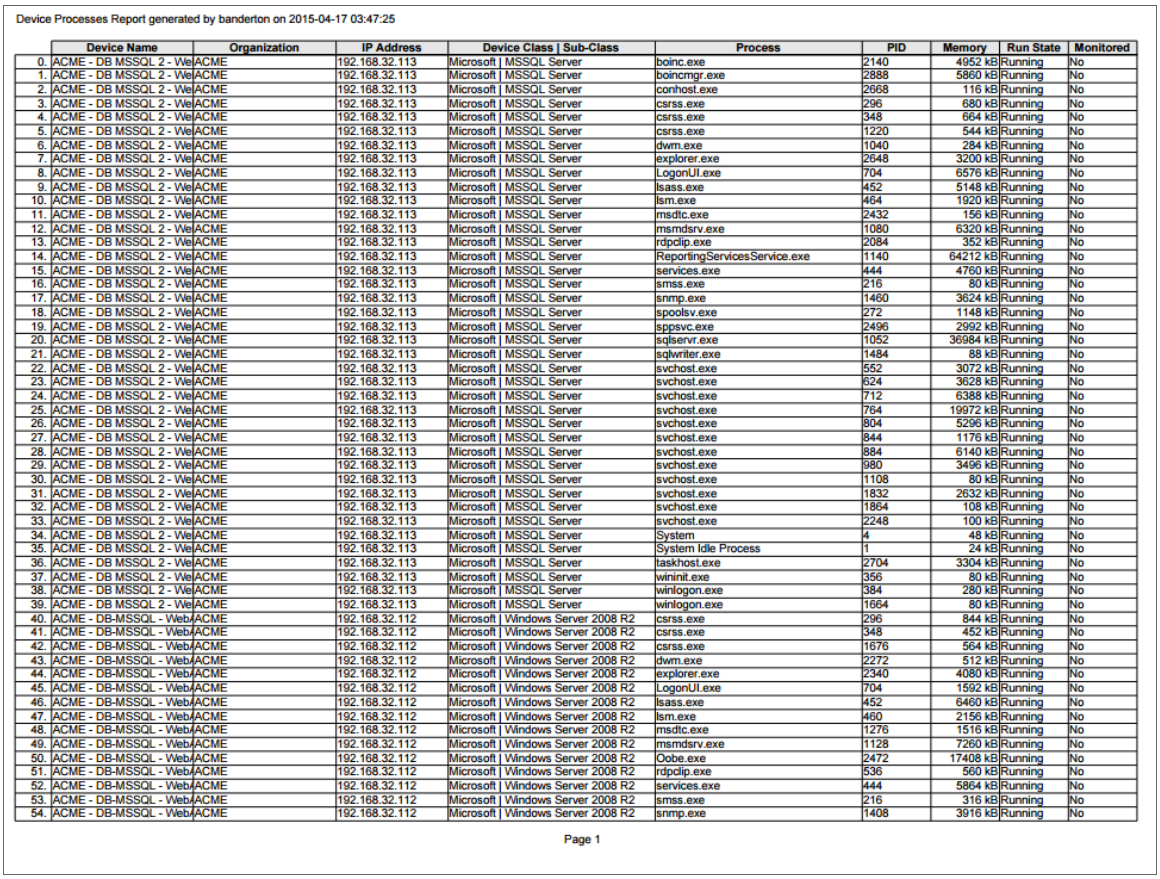


4. Click **[Go]**.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

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.



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 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	boinc.exe	2140	4952 kB	Running	No
1.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	boincmgr.exe	2888	5860 kB	Running	No
2.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	conhost.exe	2668	116 kB	Running	No
3.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	csrss.exe	296	680 kB	Running	No
4.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	csrss.exe	348	664 kB	Running	No
5.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	csrss.exe	1220	544 kB	Running	No
6.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	dwm.exe	1040	284 kB	Running	No
7.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	explorer.exe	2648	3200 kB	Running	No
8.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	LogonUI.exe	704	6576 kB	Running	No
9.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	lsass.exe	452	5148 kB	Running	No
10.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	lsm.exe	464	1920 kB	Running	No
11.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	msdtc.exe	2432	156 kB	Running	No
12.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	msmdsrv.exe	1080	6320 kB	Running	No
13.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	rdpclip.exe	2084	352 kB	Running	No
14.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	ReportingServicesService.exe	1140	64212 kB	Running	No
15.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	services.exe	444	4760 kB	Running	No
16.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	smss.exe	216	80 kB	Running	No
17.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	snmp.exe	1460	3624 kB	Running	No
18.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	spoolsv.exe	272	1148 kB	Running	No
19.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	sppsvc.exe	2496	2992 kB	Running	No
20.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	sqlservr.exe	1052	36984 kB	Running	No
21.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	sqlwriter.exe	1484	88 kB	Running	No
22.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	552	3072 kB	Running	No
23.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	624	3628 kB	Running	No
24.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	712	6388 kB	Running	No
25.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	764	19972 kB	Running	No
26.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	804	5296 kB	Running	No
27.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	844	1176 kB	Running	No
28.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	884	6140 kB	Running	No
29.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	980	3496 kB	Running	No
30.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	1108	80 kB	Running	No
31.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	1832	2632 kB	Running	No
32.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	1864	108 kB	Running	No
33.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	svchost.exe	2248	100 kB	Running	No
34.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	System	4	48 kB	Running	No
35.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	System Idle Process	1	24 kB	Running	No
36.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	taskhost.exe	2704	3304 kB	Running	No
37.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	wininit.exe	356	80 kB	Running	No
38.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	winlogon.exe	384	280 kB	Running	No
39.	ACME - DB MSSQL 2 - Web	ACME	192.168.32.113	Microsoft | MSSQL Server	winlogon.exe	1664	80 kB	Running	No
40.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	csrss.exe	296	844 kB	Running	No
41.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	csrss.exe	348	452 kB	Running	No
42.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	csrss.exe	1676	564 kB	Running	No
43.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	dwm.exe	2272	512 kB	Running	No
44.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	explorer.exe	2340	4080 kB	Running	No
45.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	LogonUI.exe	704	1592 kB	Running	No
46.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	lsass.exe	452	6460 kB	Running	No
47.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	lsm.exe	460	2156 kB	Running	No
48.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	msdtc.exe	1276	1516 kB	Running	No
49.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	msmdsrv.exe	1128	7260 kB	Running	No
50.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	Oobe.exe	2472	17408 kB	Running	No
51.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	rdpclip.exe	536	560 kB	Running	No
52.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	services.exe	444	5864 kB	Running	No
53.	ACME - DB-MSSQL - Webb	ACME	192.168.32.112	Microsoft | Windows Server 2008 R2	smss.exe	216	316 kB	Running	No
54.	ACME - DB-MSSQL - Webb	ACME	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. On the **Device Processes** page, click the **[Report]** button. The **Export current view as a report** modal appears.

> **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.

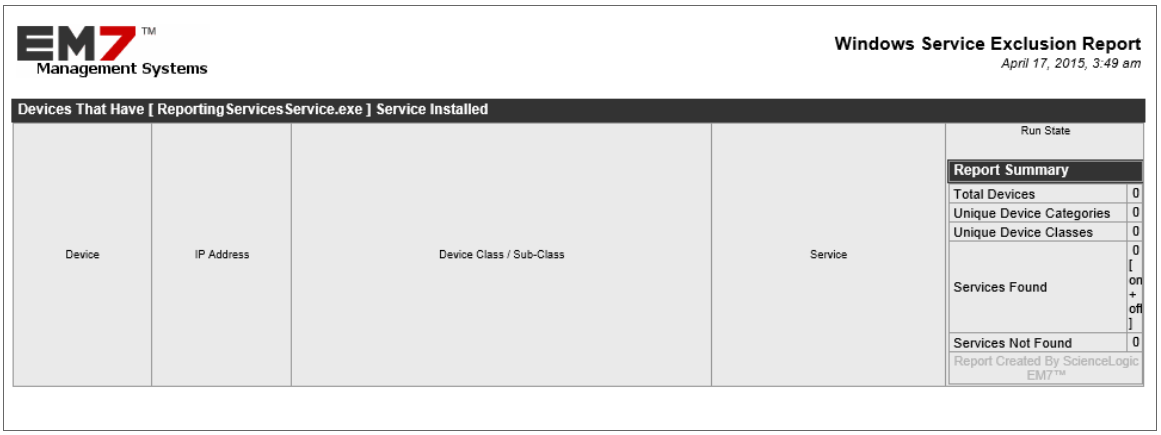
3. In the **Export current view as a report** modal, select the format in which SL1 will generate the report. Your choices are:
    - Comma-separated values (.csv)
    - Web page (.html)
    - OpenDocument Spreadsheet (.ods)

- Excel spreadsheet (.xlsx)
- Acrobat document (.pdf)

4. 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.



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. On the **Device Processes** page (Devices > Processes), find an instance of the process you want to generate an exclusion report for.
2. Click its printer icon ( ). You will be prompted to save or view the generated report.

Viewing Reports for a System Process Policy

See the section on *Viewing Performance Graphs* for information and examples of reports for system processes.

Chapter 17

Monitoring Web Content

Overview

SL1 allows you 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.

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

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

This chapter covers the following topics:

Viewing the Web Content Monitoring Policies *293*

Defining a Web Content Policy *295*

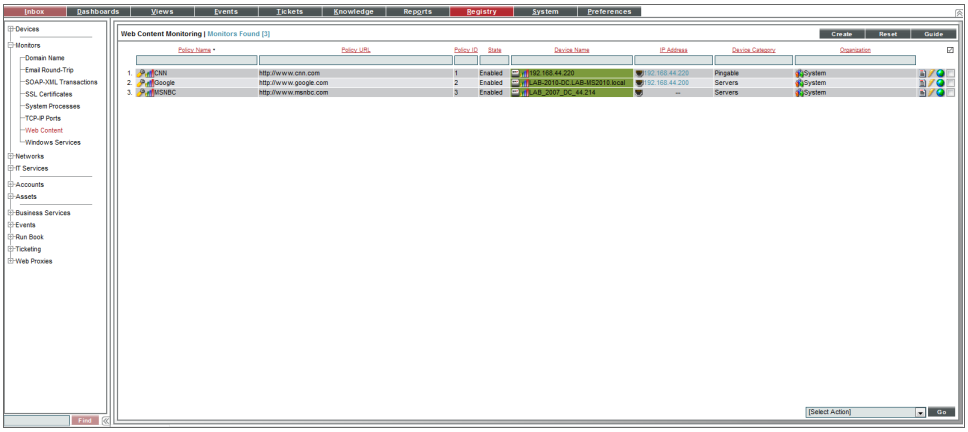
Editing a Web Content Policy *301*

Executing the Web Content Monitoring Policy *302*

Deleting a Web Content Monitoring Policy *302*
Viewing Reports on a Web Content Policy *303*
Viewing ASCII Page Content *304*
Viewing the Monitored Website *305*

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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.

- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

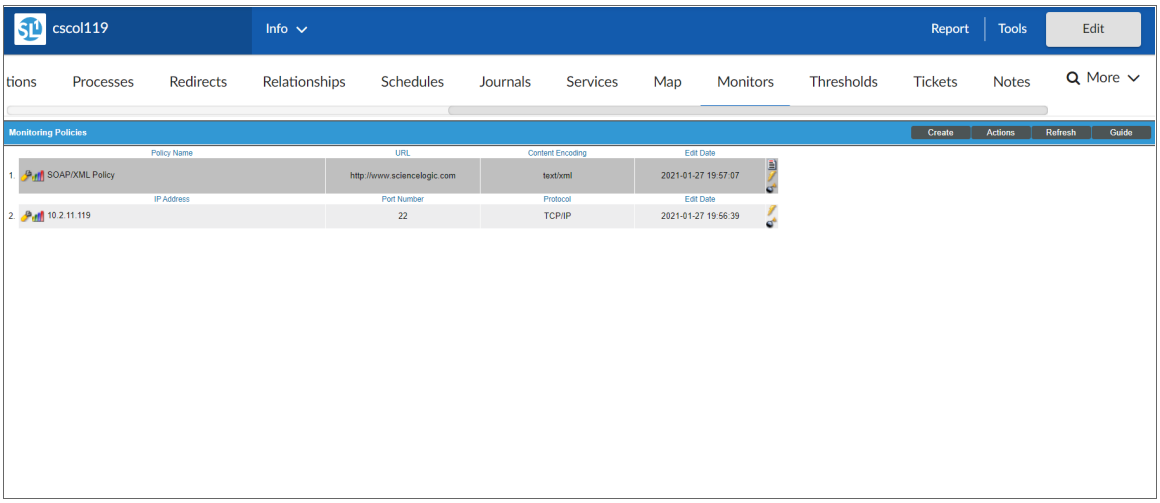
You can also use ***special characters*** to filter each parameter.

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.

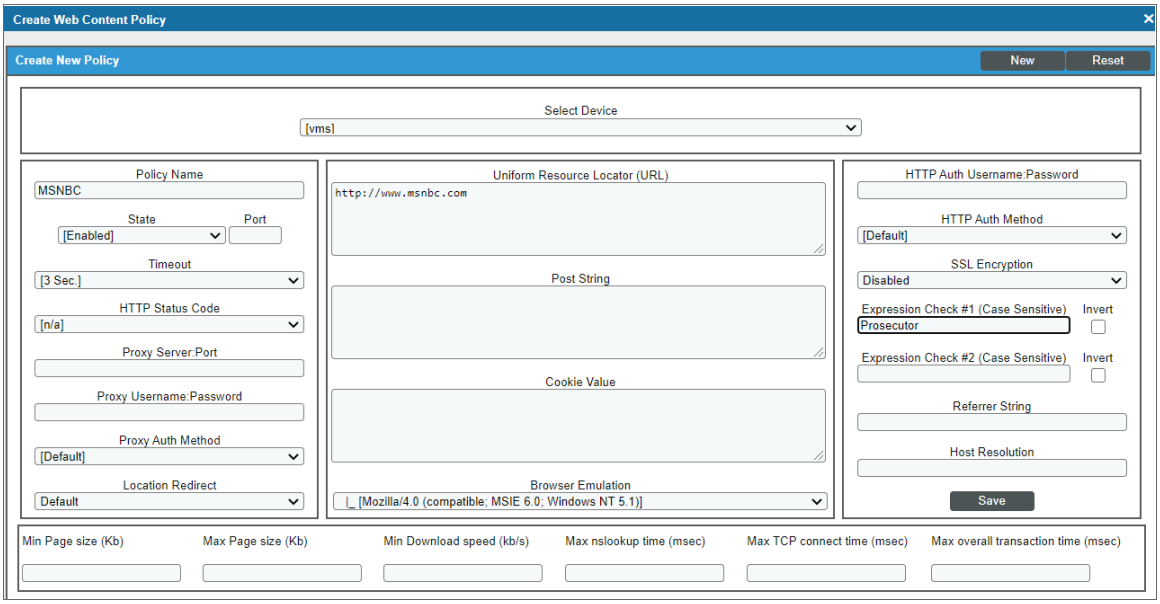
Defining a Web Content Policy

You can define a web content monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define a web content monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a web content monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Click **[Create]**, and then select *Create Web Content Policy*. The **Web Content Policy** modal appears:



4. In the **Web Content Policy** modal, supply values 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. This 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***. Specify the number of seconds after which 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 username and password in clear text.

- *Digest*. Password is transmitted as encrypted text, but the username 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 username, 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 fields "Birthyear" and "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 web server.
- ***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 username and password for the client. Base64 is not a form of encryption and should be considered the same as sending the username and password in clear text.
  - *Digest*. Password is transmitted as encrypted text, but the username 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 username, 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.

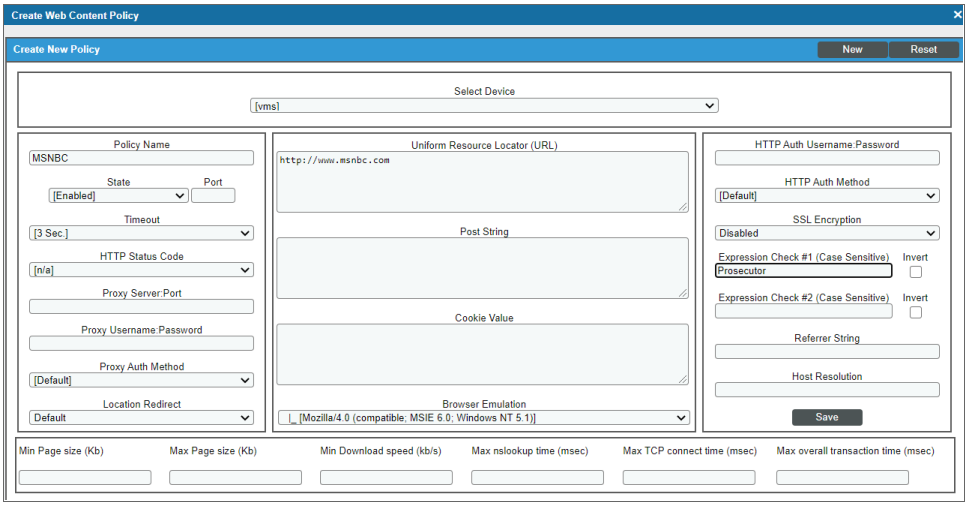
- *NTLM*. NT LAN Manager (NTLM) authentication is a challenge-response scheme that is a more secure variation of Digest authentication. NTLM uses Windows credentials to transform the challenge data instead of the unencoded username and password. NTLM authentication requires multiple exchanges between 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***. Hostname 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 hostname 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. Click **[Save]**.

Example Web Content Policy



- This policy is aligned with the device "vms".
- This policy will search for the expression "Prosecutor", entered in the ***Expression Check #1*** field, in www.msnbc.com ("http://www.msnbc.com/").

Defining a Web Content Policy in the Classic SL1 User Interface

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 appears.

Editing a Web Content Policy

To edit a web content monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **Web Content Policy** modal appears.
4. In the **Web Content Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Web Content Monitoring Policy*.
5. Click **[Save]**.

Editing a Web Content Policy in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - In the **Monitoring Policies** page, find the policy you want to edit and click 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 click its wrench icon ( ).
3. The **Web Content Policy** modal appears.
4. In the **Web Content Policy** modal, you can change the values in one or more of the fields described in the

section on *Defining a Web Content Monitoring Policy*.

5. Click **[Save]**.

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.

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.

To execute a web content monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).
4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is very helpful for diagnosing possible problems with a policy.

Executing the Web Content Monitoring Policy in the Classic SL1 User Interface

To execute a web content monitoring policy in the classic SL1 user interface:

1. In the **Web Content Monitoring** page (Registry > Monitors > Web Content), find the policy you want to run manually.
2. Click 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.

Deleting a Web Content Monitoring Policy

You can delete a web content monitoring policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a web content policy:

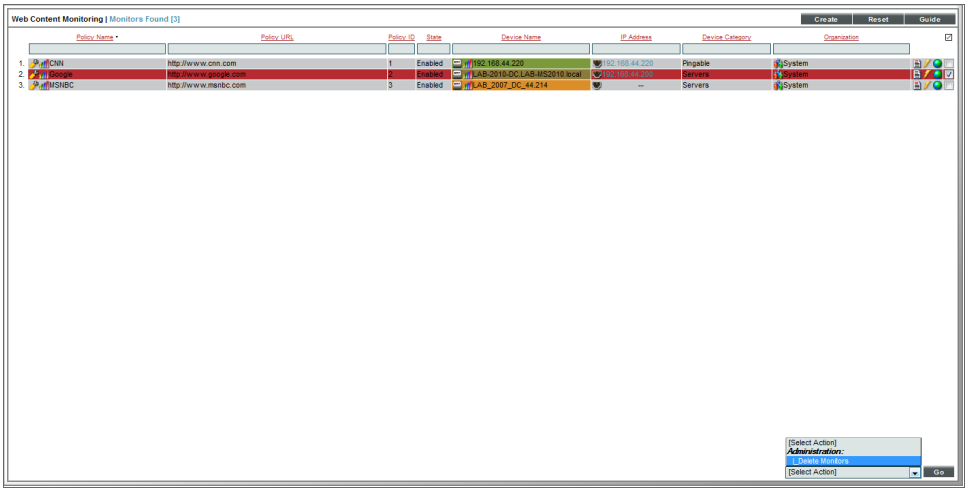
1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

Deleting a Web Content Monitoring Policy in the Classic SL1 User Interface

You can delete one or more web content monitoring policies from the **Web Content Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a web content monitoring policy in the classic SL1 user interface:

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. Click 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.

Viewing Reports on a Web Content Policy

See the section on *Viewing Performance Graphs* for 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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - In the **Monitoring Policies** page, find the policy you want to edit and click the page icon ( ).

Or:

2. From the **Web Content Monitoring** page (Registry > Monitors > Web Content):
    - Click 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.

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. Click its globe icon ( ).
3. SL1 will spawn a new browser page and display the monitored website.

Chapter 18

Monitoring 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.

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

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

This chapter covers the following topics:

Windows Services Monitoring Policies *307*

Viewing the List of Windows Service Monitoring Policies *308*

Prerequisites and Configuration for Windows Service Monitoring Policies *310*

Defining a Monitoring Policy for Windows Services *311*

Editing a Windows Service Monitoring Policy *315*

Executing a Windows Service Monitoring Policy *316*
Deleting a Windows Service Monitoring Policy *317*
Viewing a List of All Windows Services *318*
Viewing a List of Windows Services on a Single Device *321*
Generating and Viewing Reports about Windows Services *324*

Windows Services Monitoring Policies

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:

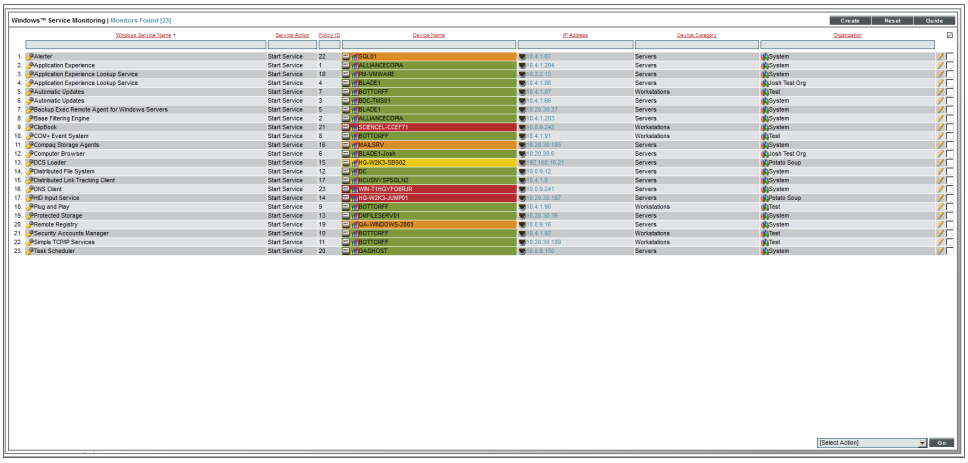
- SL1 generates an event if the service is not running or SL1 generates an event if the service is running.
- Optionally, SL1 starts, pauses, or restarts the service.
- Optionally, SL1 reboots or shuts down the device.
- Optionally, SL1 triggers the execution of a script (script must reside on the device).

NOTE: In addition to using a Windows service monitoring 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.

Viewing the List of 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:



- ***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.
- ***State***. Whether the policy is enabled or disabled.
- ***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.

From the list of policies, you can select the checkbox for one or more policies and choose one of the following bulk actions from the ***Select Action*** drop-down at the bottom right of the page:

- *Delete Monitors*. Deletes the selected policies from SL1. The associated reports (from the Device Reports > Performance tab) are also deleted.
- *Enable Monitors*. Enables the selected policies so that SL1 can collect the data for these policies.
- *Disable Monitors*. Disables the selected policies. SL1 will not collect the data specified in these policies.

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.

Prerequisites and Configuration for Windows Service Monitoring Policies

Before you can define a Windows service monitoring policy that performs actions on the external device, you must perform some required configuration in SL1 and on the external server.

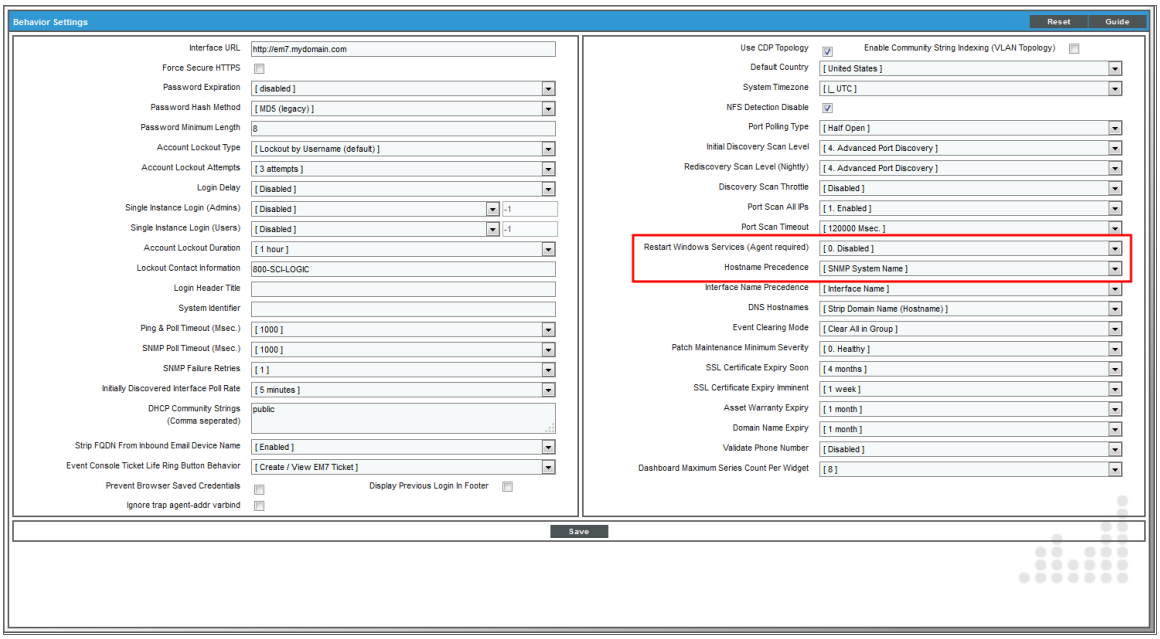
Optional Settings in SL1

If you do not define a Windows service 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 service 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 additional services in this exclusion list, please contact ScienceLogic Customer Support.



Required Configuration

To include any of the optional actions in a Windows service monitoring policy, the external device must meet these requirements:

- The external device must be running the SNMP Informant, WMI Edition agent.
- To execute a script on the external device for monitoring policies, the script must reside on the external device, in the directory:

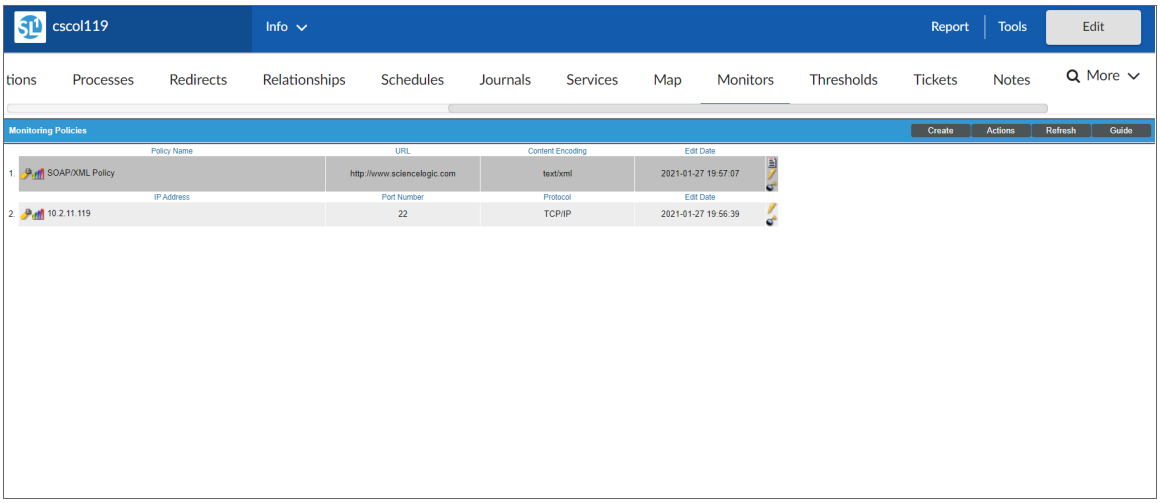
  c:/program files/snmp informant/operating_system/spawn

Additionally, for SL1 to automatically monitor services of type "automatic" and/or execute an action for a Windows service monitoring policy for a device, the device must:

- Be aligned to a device class that has "WMI Informant" configured in the *Service Collection* field.
- Have an SNMP Write credential defined on the **[Settings]** tab of the **Device Investigator** (or in the **Device Properties** page in the classic SL1 user interface).

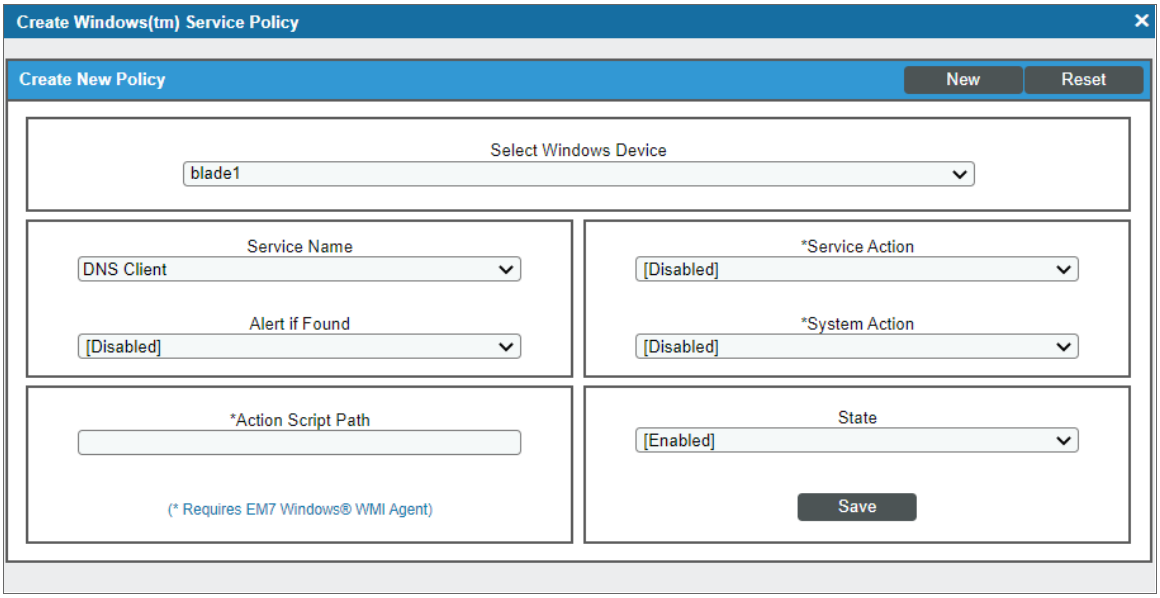
Defining a Monitoring Policy for Windows Services

You can define a Windows service monitoring policy for a device on the **[Monitors]** tab of the **Device Investigator**.



To define a Windows service monitoring policy:

1. Go to the **Devices** page and click the Device Name of the device for which you want to define a Windows service monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Click **[Create]**, and then select *Create Windows service monitoring policy*. The **Windows Service Policy** modal appears:



4. In the **Windows Service Policy** modal, 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 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 until the ***State*** field is set to *Enabled*.

5. Click **[Save]**.

Defining a Monitoring Policy for Windows Services in the Classic SL1 User Interface

There are two places in SL1 from which you can define a monitoring policy for Windows services:

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. Click the wrench icon ( ) for the device.
   - In the **Device Administration** panel, click the **[Monitors]**tab.
   - From the **[Create]** menu in the upper right, select ***Create Windows Services Policy***.

Or:

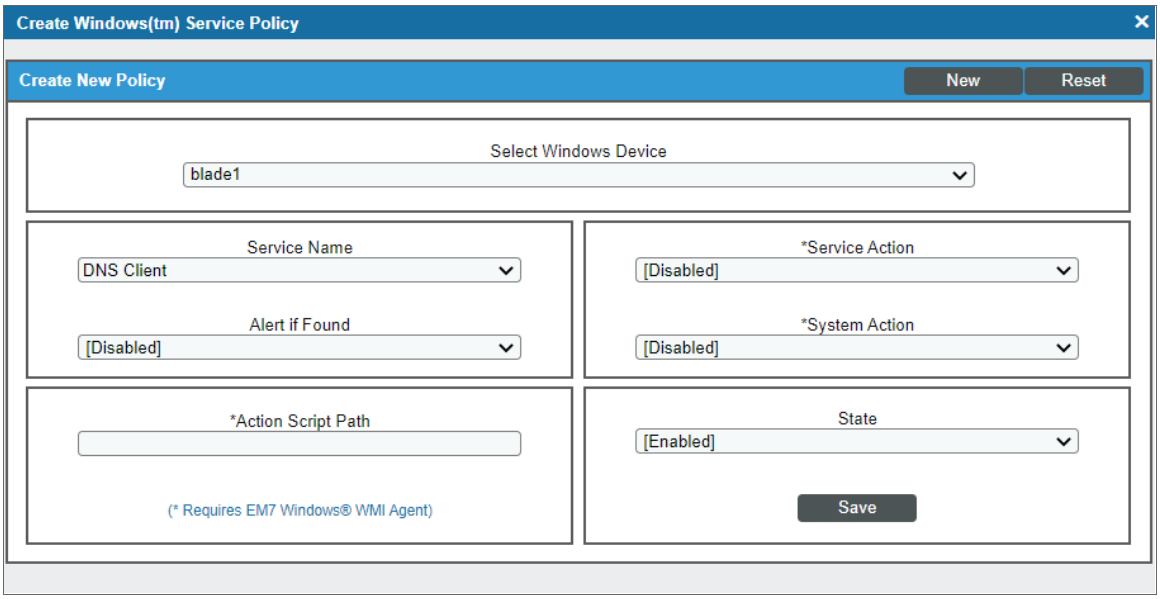
2. From the **Windows Service Monitoring** page (Registry > Monitors > Windows Services):

   - In the **Windows Service Monitoring** page, click the **[Create]** button.

3. The **Windows Service Policy** modal appears.

For information about completing the fields in the **Windows Service Policy** modal, see the section on *Defining a Monitoring Policy for Windows Services*.

Example Policy for Windows Service



- 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.

Editing a Windows Service Monitoring Policy

To edit a Windows service monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to edit a monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to edit and click its wrench icon ( ). The **Windows Service Policy** modal appears.
4. In the **Windows Service Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Monitoring Policy for Windows Services*.
5. Click **[Save]**.

Editing a Windows Service Monitoring Policy in the Classic SL1 User Interface

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. Click the wrench icon ( ) for the device.
    - In the **Device Administration** panel, click the **[Monitors]** tab.
    - In the **Monitoring Policies** page, find the policy you want to edit and click its wrench icon ( ).

Or:

2. From the **Windows Service Monitoring** page (Registry > Monitors > Windows Services):
    - In the **Windows Service Monitoring** page, find the policy you want to edit and click its wrench icon ( ).
3. The **Windows Service Policy** modal appears.
4. In the **Windows Service Policy** modal, you can change the values in one or more of the fields described in the section on *Defining a Monitoring Policy for Windows Services*.
5. Click **[Save]**.

Executing a Windows Service Monitoring Policy

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.

> **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.

To execute a Windows service monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to execute the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to run manually and click its lightning bolt icon ( ).

4. The **Session Logs** modal opens while the policy is executing. The **Session Logs** page provides detailed descriptions of each step during the execution. This is helpful for diagnosing possible problems with a policy.

Executing a Windows Service Monitoring Policy in the Classic SL1 User Interface

To execute a Windows service monitoring policy in the classic SL1 user interface:

1. In the **Windows Service Monitoring** page (Registry > Monitors > Windows Services), find the policy you want to run manually.
2. Click the lightning bolt icon ( ) to manually execute the policy.
3. While the policy is executing, SL1 spawns a modal 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.

Deleting a Windows Service Monitoring Policy

You can delete a Windows service monitoring policy from the **[Monitors]** tab of the **Device Investigator**. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a Windows service monitoring policy:

1. Go to the **Devices** page and click the name of the device for which you want to delete the monitoring policy. The **Device Investigator** displays.
2. Click the **[Monitors]** tab.
3. Find the policy you want to delete and click its bomb icon ( ). A confirmation prompt appears.
4. Click **[OK]**.

Deleting a Windows Service Monitoring Policy in the Classic SL1 User Interface

You can delete one or more Windows service monitoring policies from the **Windows Service Monitoring** page. When you delete a monitoring policy, SL1 no longer uses the policy to collect data from the aligned device. Deleting a monitoring policy will also remove all data that was previously collected by the policy.

To delete a Windows service process policy in the classic SL1 user interface:

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.
3. In the **[Select Action]** menu in the bottom right of the page, select *Delete Monitors*.

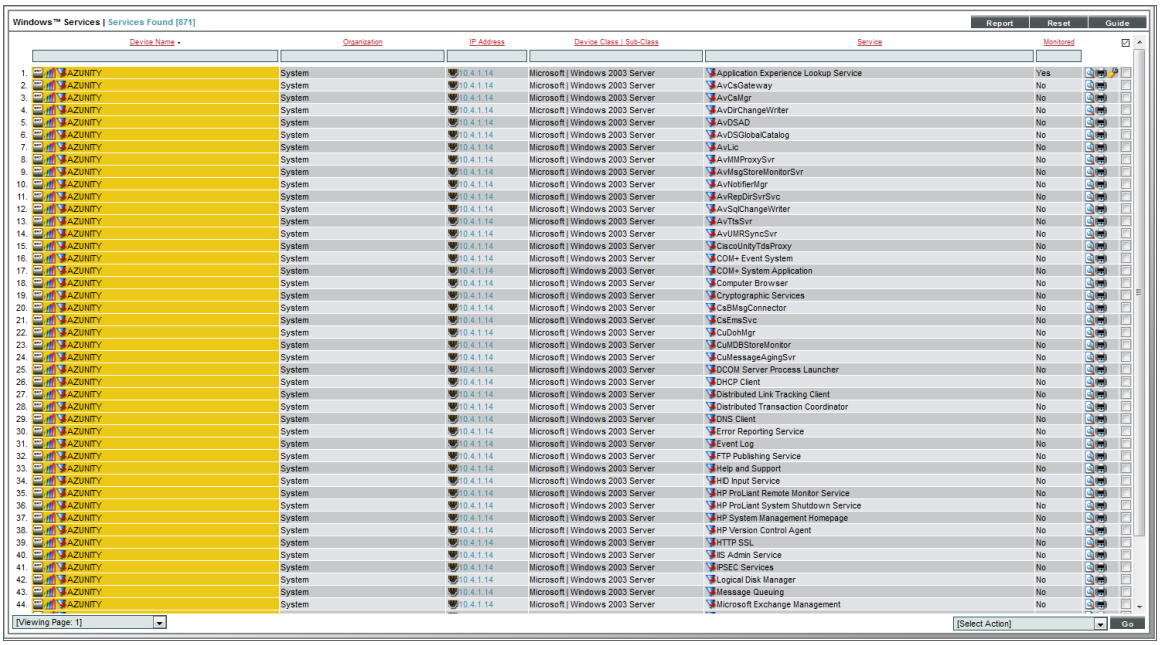
4. Click the **[Go]** button to delete the Windows service policies.
5. The policy is deleted from SL1. The associated reports (from the Device Reports > **[Performance]** tab) are also deleted.

Viewing a List of All 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).



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.

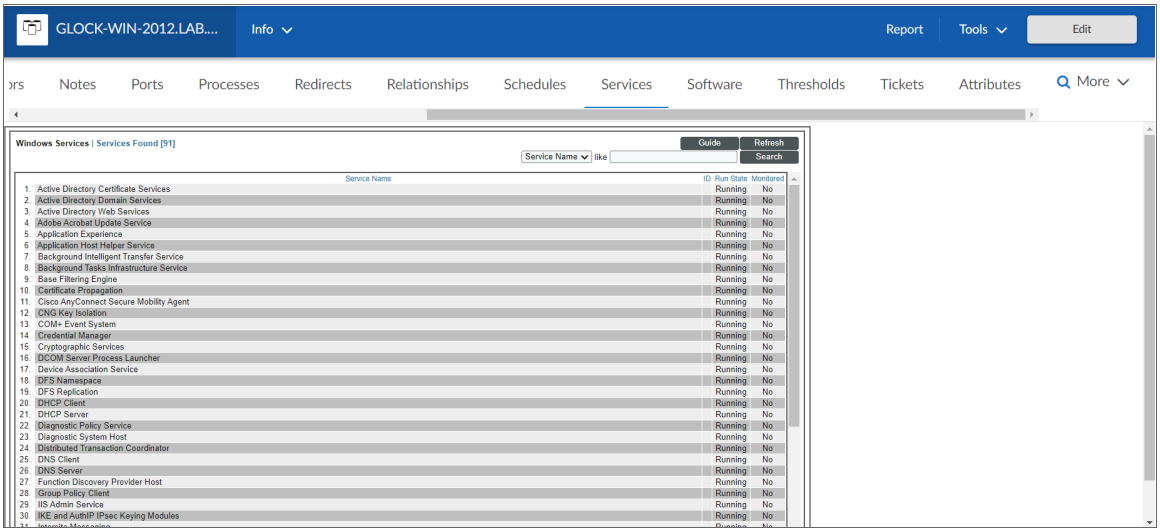
You can also use ***special characters*** to filter each parameter.

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

On the **[Services]** tab of the **Device Investigator**, you can view a list of all Windows services enabled on the device:



To keep your device running efficiently and to maintain security, the **[Services]** tab helps you manage services on your device. For each Windows service running on the device, the **[Services]** tab 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.

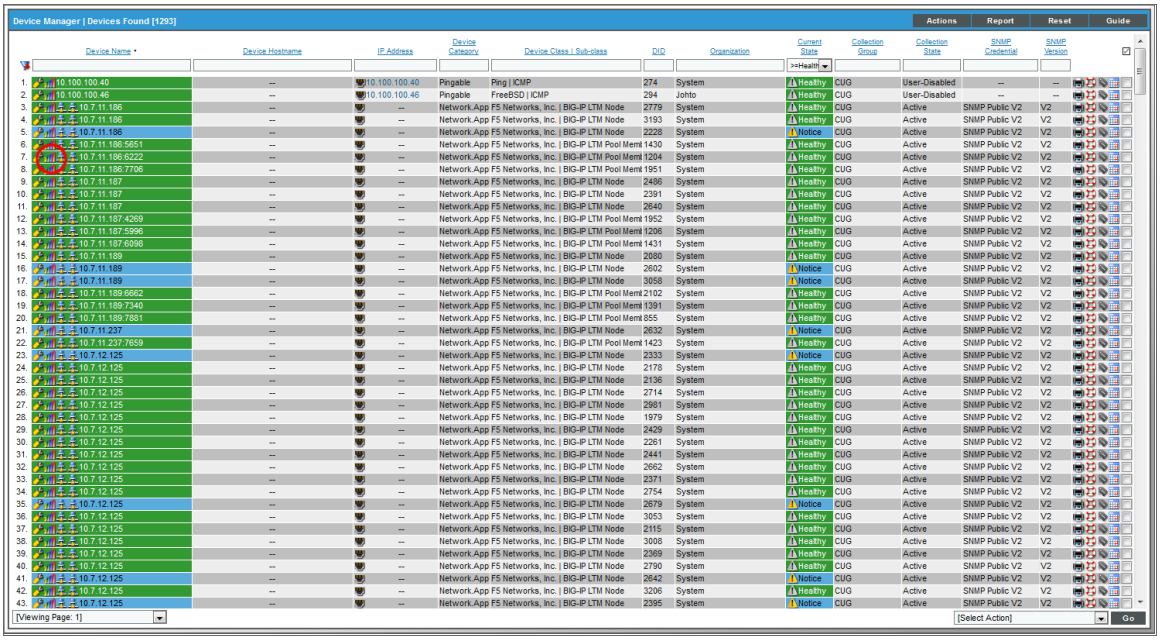
- ***Monitored***. Specifies whether or not SL1 is monitoring this Windows service.

Viewing a List of Windows Services on a Single Device in the Classic SL1 User Interface

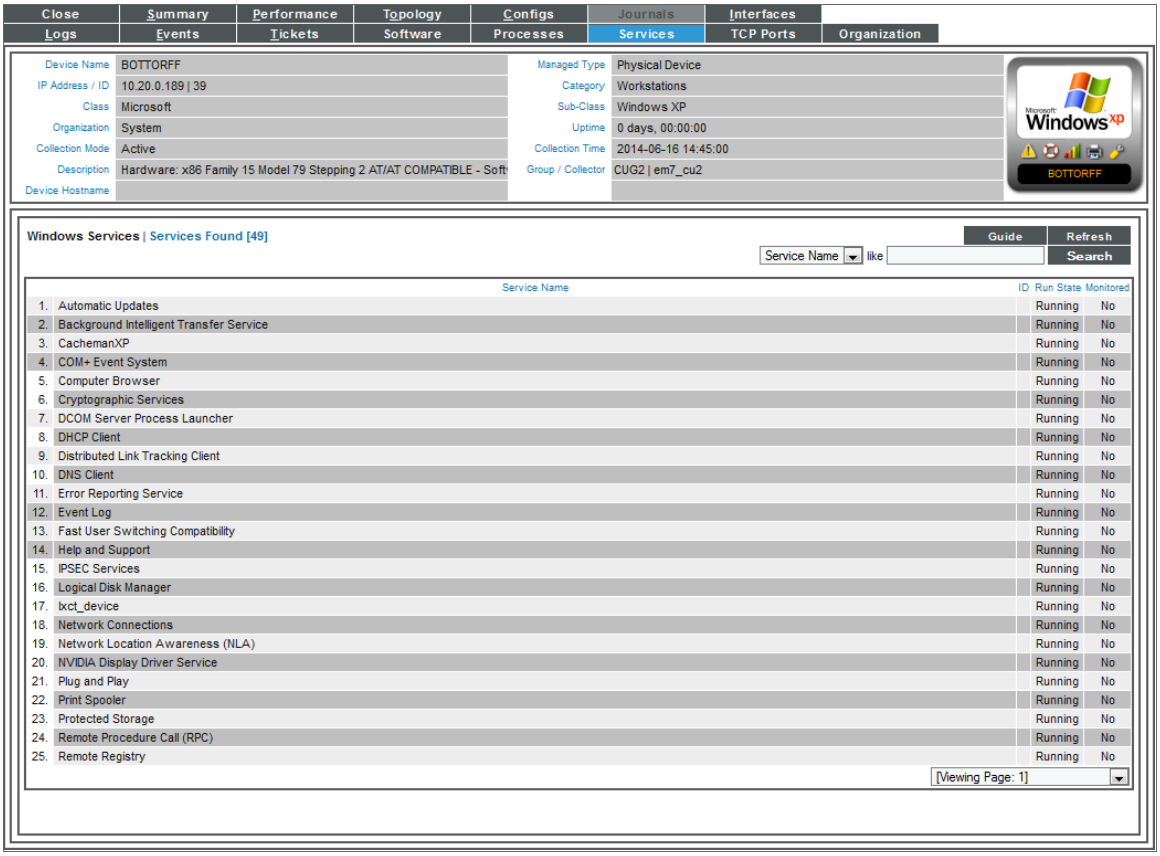
The **Windows Services** page displays a list of all of the Windows services that are running on a single device.

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.



3. In the **Device Reports** panel, select the Services tab. The **Windows Services** page appears.



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 and Viewing Reports about Windows Services

This section describes how to generate and view reports about Windows services.

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).
2. On the **Windows Services** page, click the **[Report]** button. The **Export current view as a report** modal appears.

> **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.

3. In the **Export current view as a report** modal, 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)
4. Click 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.

EM7™ Management Systems

Windows Service Exclusion Report
April 17, 2015, 3:56 am

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.lo	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).
2. In the **Windows Services** page, find an instance of the Windows service you want to generate an exclusion report for.
3. Click its printer icon ( ). You will be prompted to save or view the generated report.

Viewing Reports about Windows Services

See the section on *Viewing Performance Graphs* for information and examples of reports for Windows services.

Chapter 19

Grouping Dynamic Application Data Using Collection Labels

Overview

This chapter describes Collection Labels and Collection Groups.

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

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

This chapter covers the following topics:

What are Collection Labels and Collection Groups? *329*
Viewing the List of Collection Labels *329*
Creating a Collection Group *335*
Creating a Collection Label *335*
What are Duplicates and How Does SL1 Manage Them? *338*
What is Precedence? *339*
Aligning a Presentation Object with a Collection Label *339*
Viewing and Managing the List of Presentation Objects Aligned with a Collection Label *341*
Viewing and Editing Duplicate Presentation Objects by Collection Label *345*
Viewing and Managing the List of Devices Aligned with a Collection Label *347*
Editing Duplicate Presentation Objects by Device *349*
Editing Duplicate Presentation Objects for a Single Device *351*

Editing a Collection Label *352*
Deleting a Collection Label *353*
Viewing Reports About Collection Labels on a Single Device *353*
Viewing Dashboards About Collection Labels *354*

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:

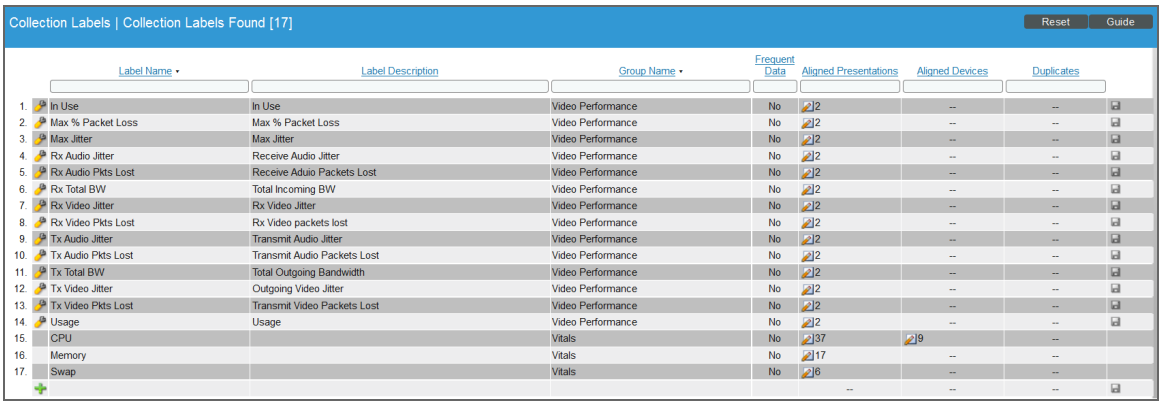
- Suppose you monitor phone systems from multiple vendors.
- Suppose you want to create a dashboard that displays the ten phone systems that drop the most calls.
- You could create a Collection Group called "Dropped Calls".
- You could create two Collection Labels: "Average Dropped Calls", and "Raw Dropped 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:



	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	--	--
					--	--	--

- ***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 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:

> **NOTE**: You can also use the "!" character in combination with the arithmetical 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.

Examples

- "!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".
- "aio$". Matches only text that ends with "aio".

- " ^ shu". Matches only text that begins with "shu".
- " ^ silo$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contains the characters "silo".
- "! ^ silo". Matches only text that does not start with "silo".
- "!0$". Matches only text that does not end with "0".
- "! ^ silo$". Matches only text that is not the exact text "silo", with no characters before or after.
- "! ^ ". Matches null values, typically represented as "--" in most pages.
- "!$". Matches null values, typically represented as "--" in most pages.
- "! ^ $". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- " ^ s*i*l*o$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- "! ^ s*i*l*o$". Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol' and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- " !silo ". Matches text that does not contain "silo".
- " ! ^ silo$ ". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.
- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".

- "^?n*SAN$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

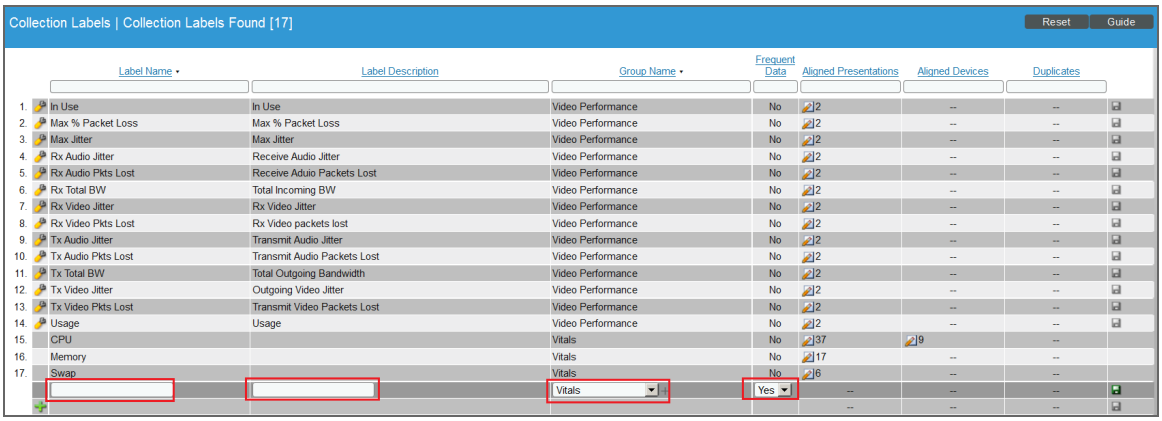
Creating a Collection Group

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.



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).

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
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, SL1 ***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
- calulcates 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
4. 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).
5. 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 SL1 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.

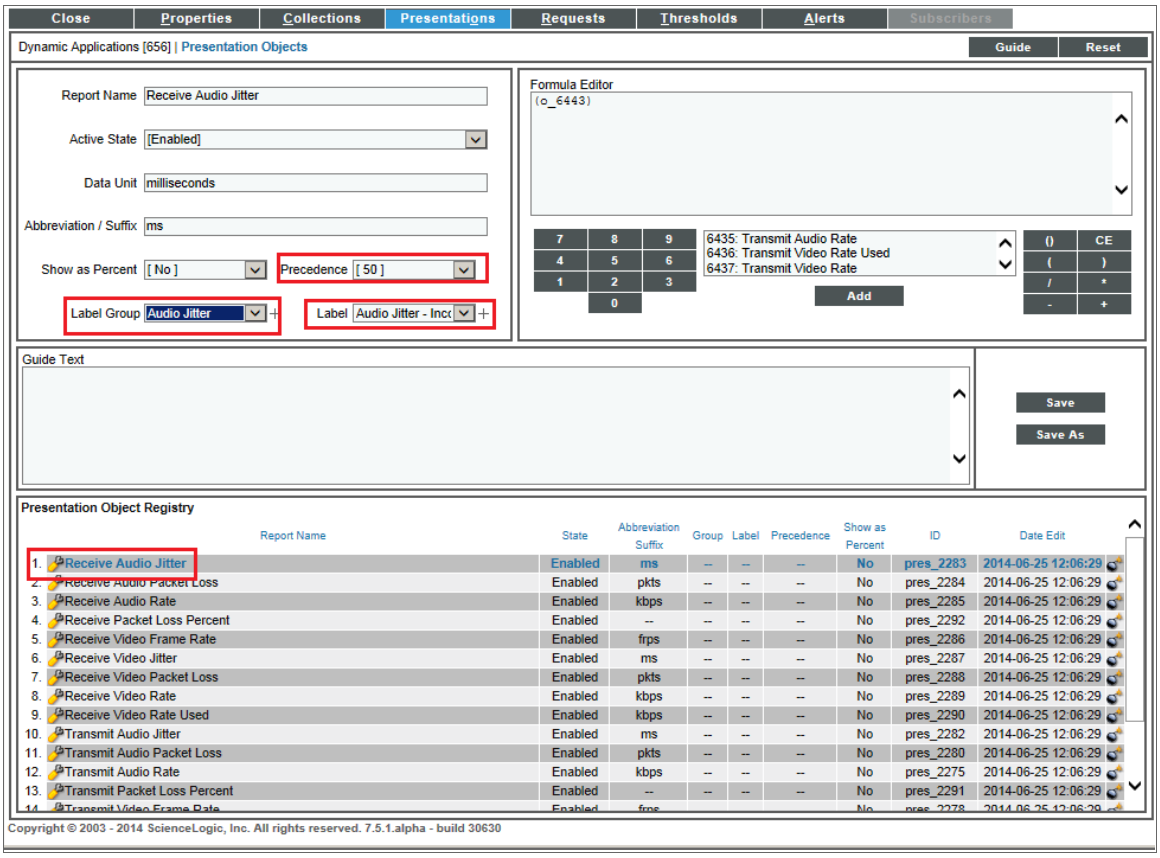
- When a Dynamic Application is manually aligned with a device in the **Dynamic Application Collections** page
- When devices are manually merged.

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.



5. The top pane is populated with values from the selected presentation object. Select values for the following fields:

1. ***Precedence***. Set the global precedence for this Collection Label-presentation object pair. For more information, see the section on *Precedence*.

2. ***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.

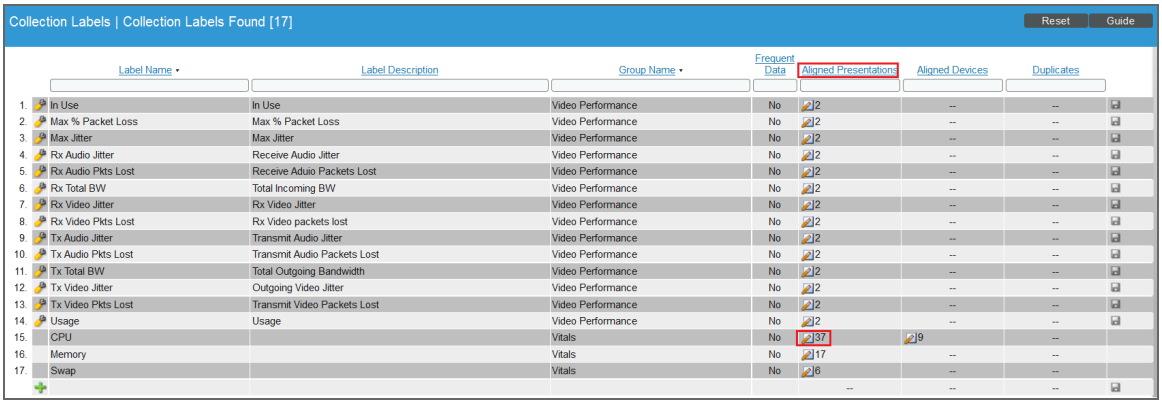
3. ***Label***. Select from a list of existing Collection Labels or click on the plus-sign icon ( ) and enter the value for a new Collection Label. The current presentation object will be aligned with the specified Collection Label.

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

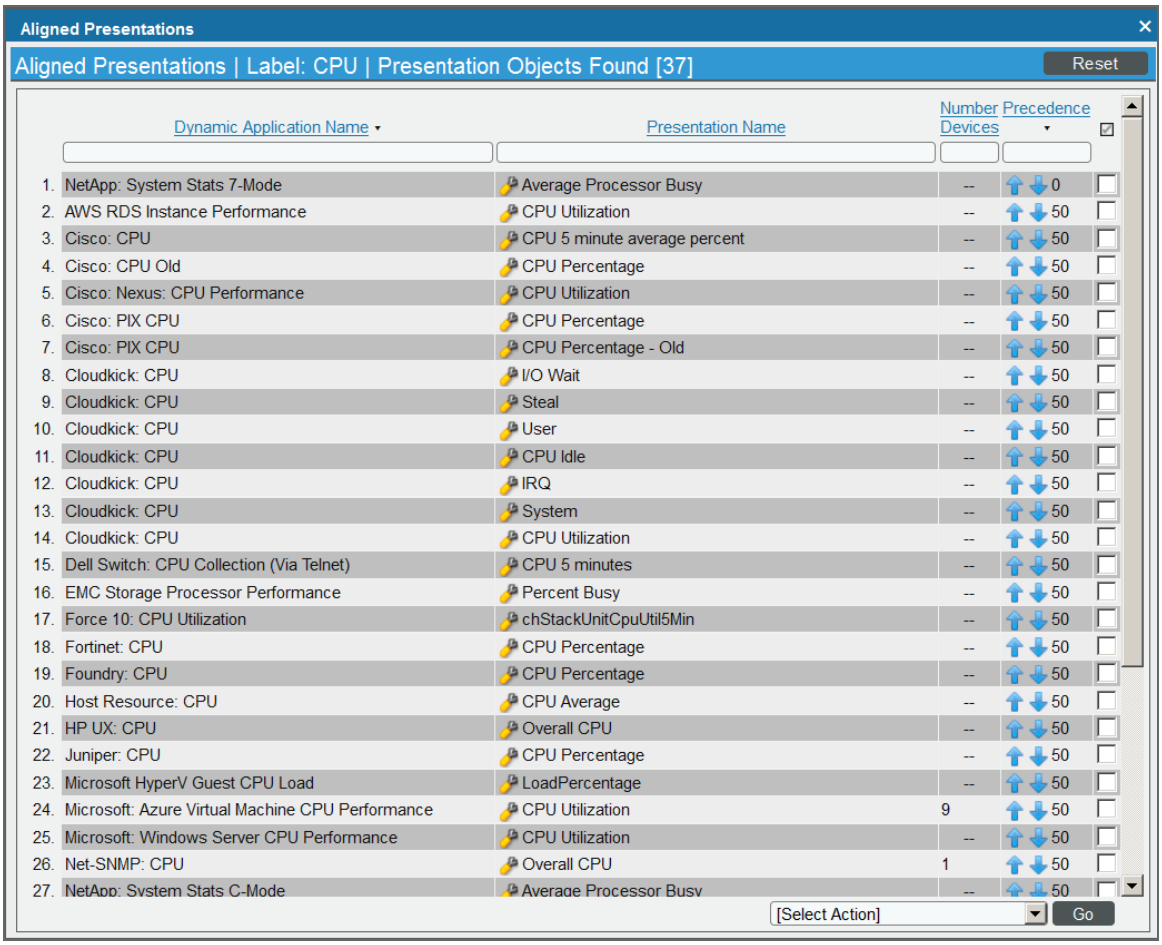
From the **Collection Labels** page, you can view information about each Collection Label. For each Collection Label, you can view a list of presentation objects aligned with that Collection Label. To view this information:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).



	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	--	--
					--	--	--

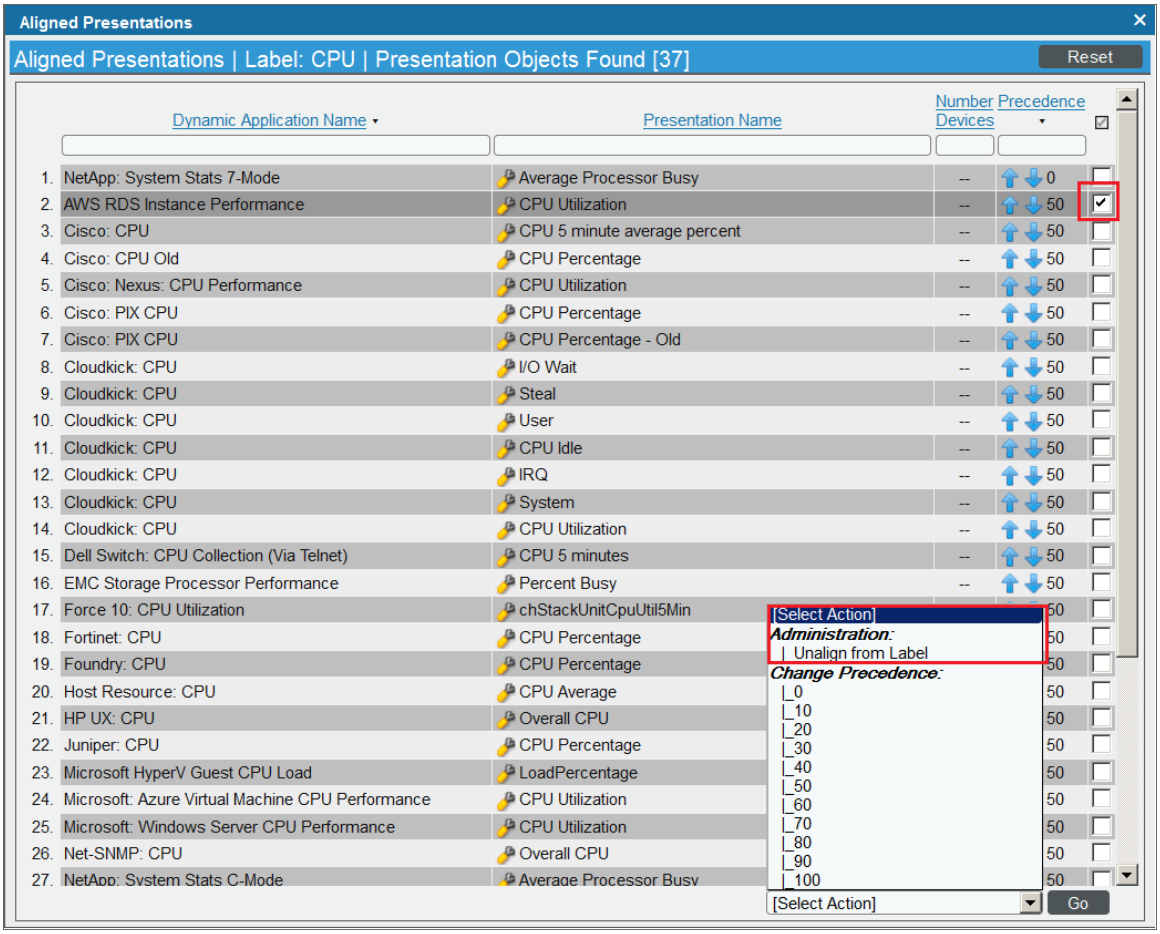
2. Find the Collection Label you are interested in. In the ***Aligned Presentations*** column, select the pencil icon ( ). The **Aligned Presentations** modal page appears:



3. 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.



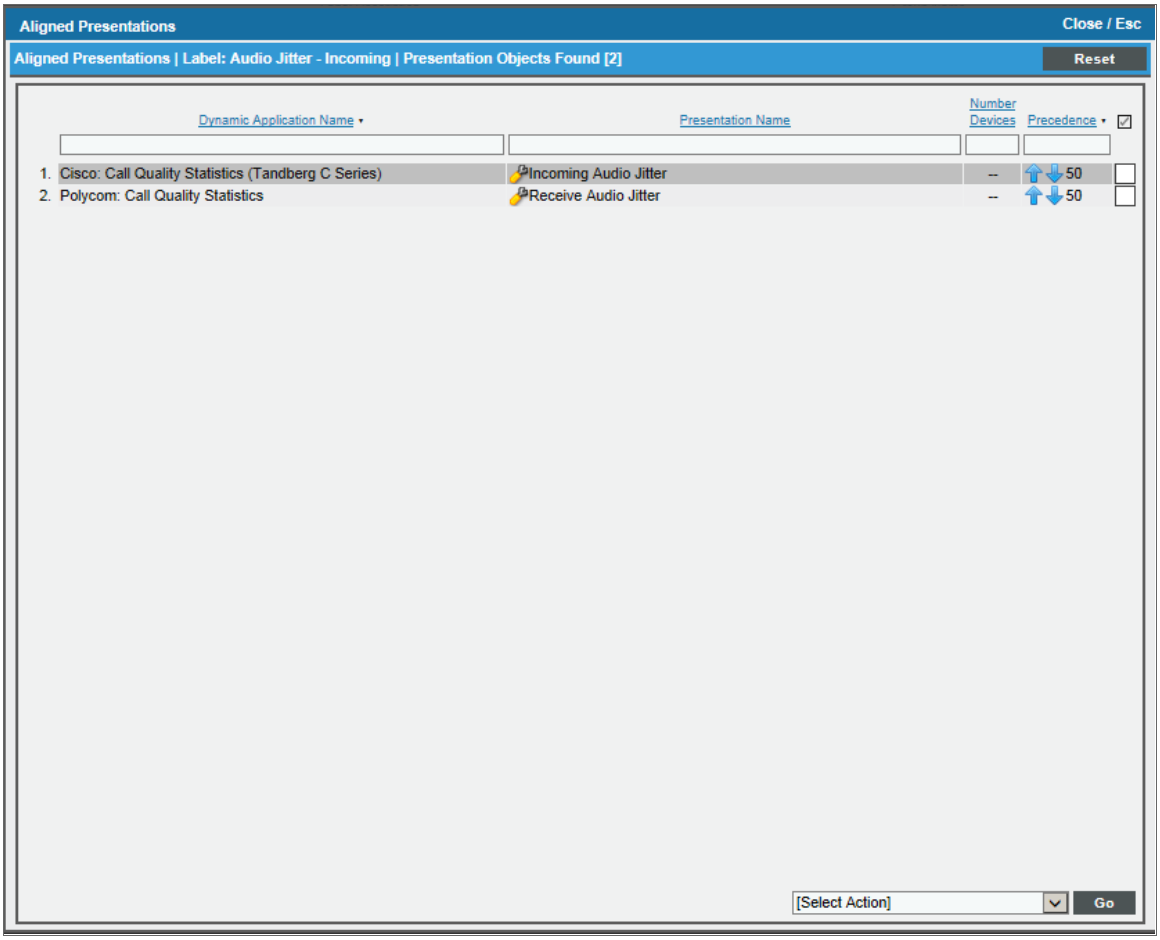
2. From the ***Select Action*** field in the lower right, select *Unalign from Label*. Select the **[Go]** button.
3. The selected presentation object will no longer be associated with the Collection Label.

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.

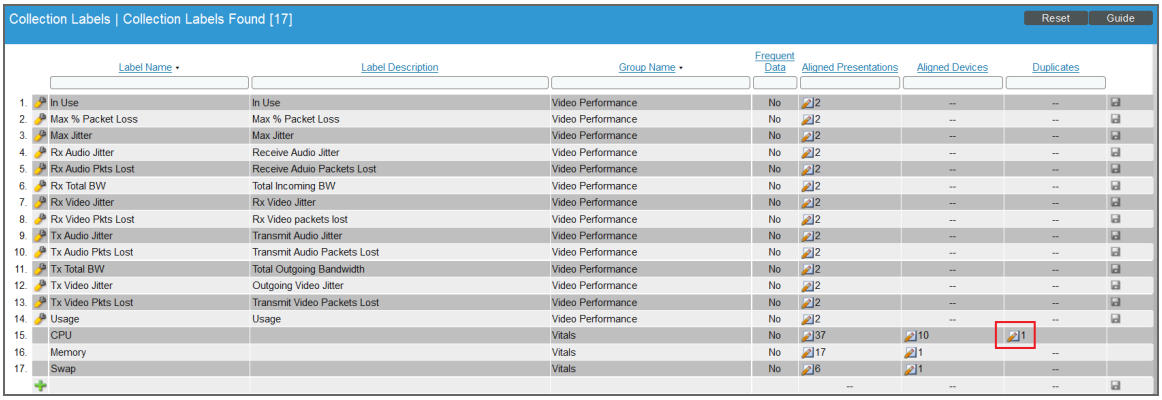
3. Repeat steps 2–4 for each Presentation Object for which you want to edit the precedence value.

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

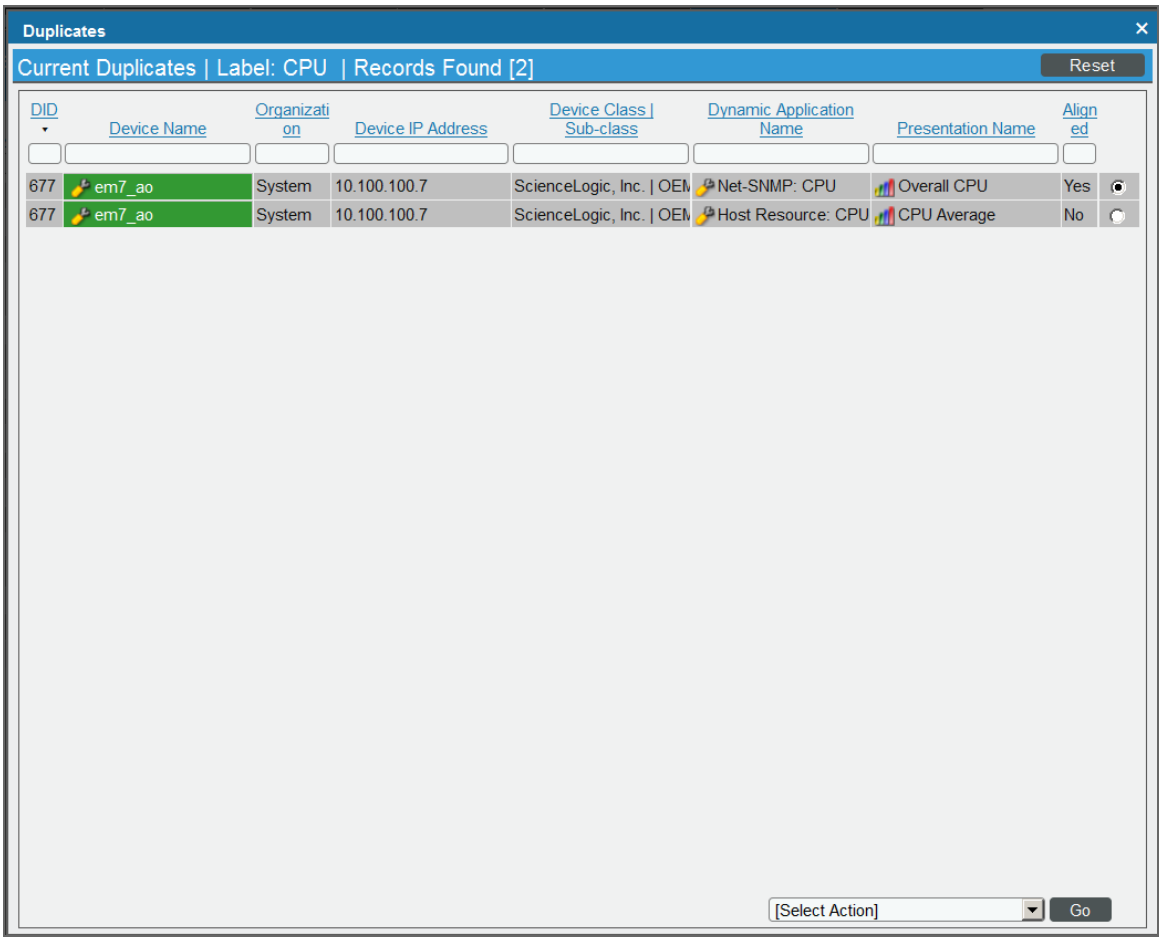
You can view a list of devices where duplicates occur, view how SL1 assigned the Collection Label-presentation object pair, and edit the Collection Label-presentation object pair for one or more devices. When you manually define a Collection Label-presentation object pair for a device, SL1 will not edit or change that pair.

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).



	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	--
					--	--	--

2. Find the Collection Label you are interested in. In the ***Duplicates*** column, select the pencil icon ( ). The **Duplicates** modal page appears.

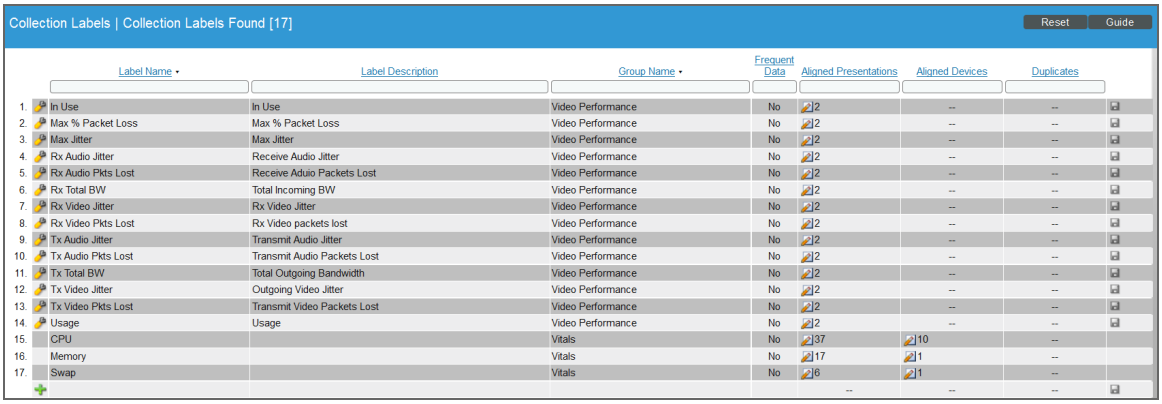


3. In the **Duplicates** modal page, you can view a list of devices for which there are multiple possible Collection Label-presentation object pairs. You can view which pair is currently assigned to the device.
4. To change the pair for a device, click on the pair's radio button.
5. Repeat step #4 for each device on which you want to edit the duplicate.
6. In the ***Select Action*** field (in the lower right), select *Align Presentation for Device*. Select the **[Go]** button.
7. 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

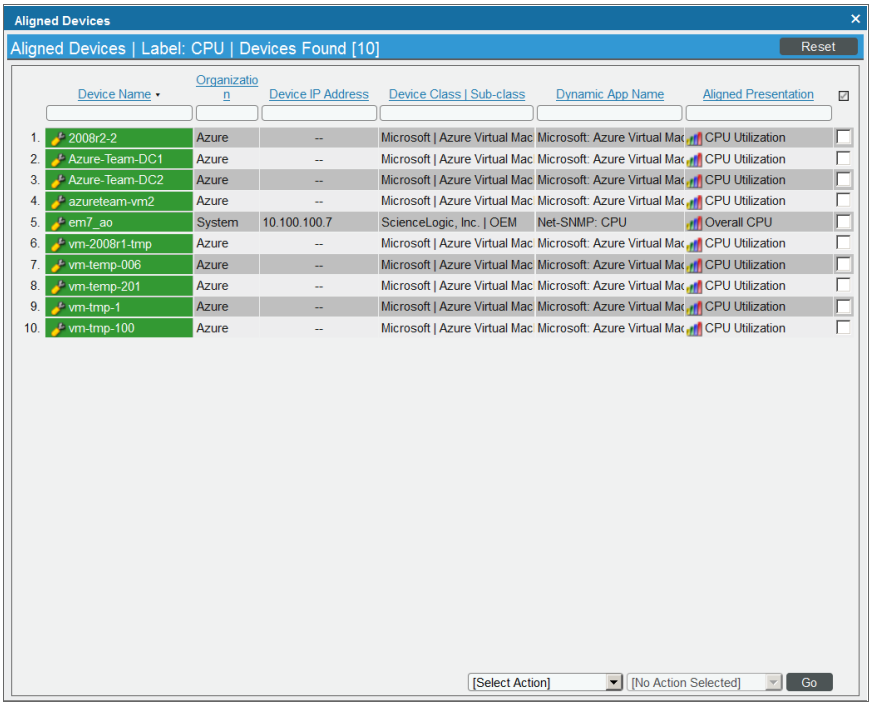
From the **Collection Labels** page, you can view information about each Collection Label. For each Collection Label, you can view a list of devices from which SL1 is collecting values. To view this information:

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 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	--
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 ( ).

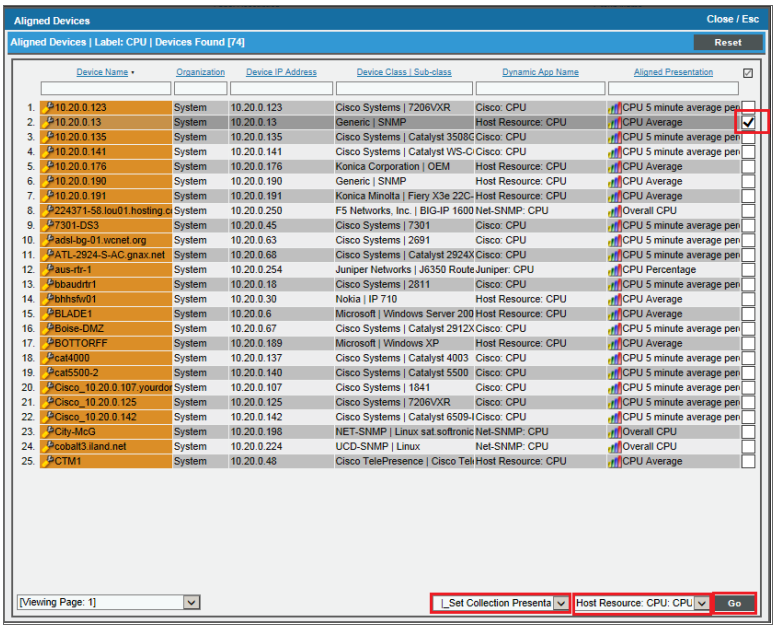


	Device Name	Organization	Device IP Address	Device Class | Sub-class	Dynamic App Name	Aligned Presentation
1.	2008r2-2	Azure	--	Microsoft | Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
2.	Azure-Team-DC1	Azure	--	Microsoft | Azure Virtual Mac	Microsoft: Azure Virtual Mac	CPU Utilization
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.

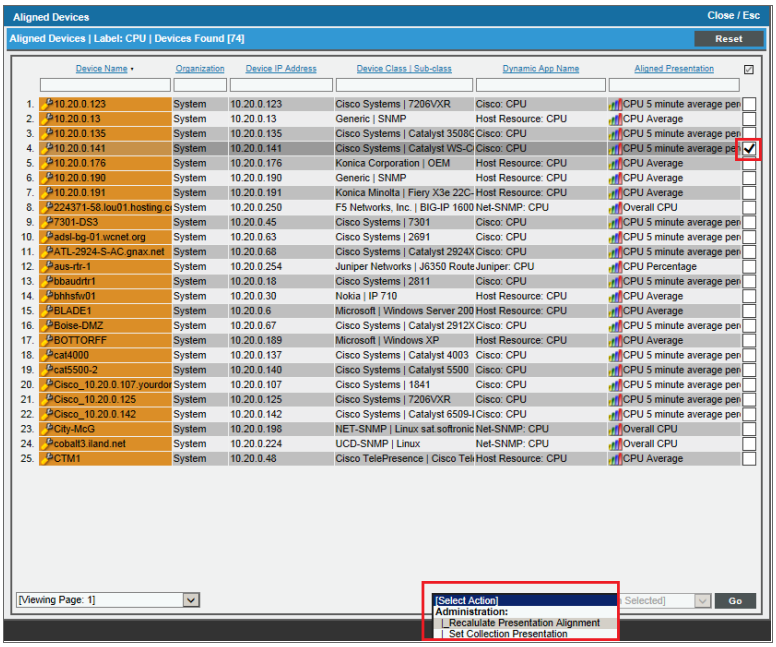


2. In the menus in the lower right, select ***Set Collection Presentation*** and then select the presentation object. Select the **[Go]** button.

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.



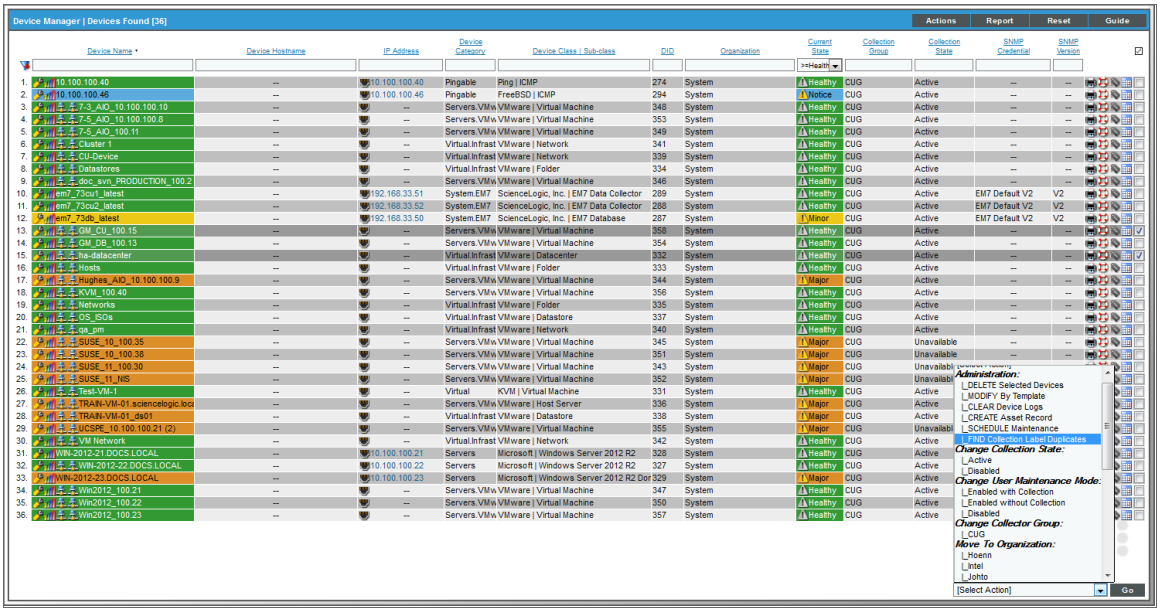
2. In the menus in the lower right, select ***Recalculate Presentation Alignment***. Select the **[Go]** button.
3. SL1 will evaluate the precedence of each possible presentation object and assign the presentation object with the lowest precedence.

Editing Duplicate Presentation Objects by Device

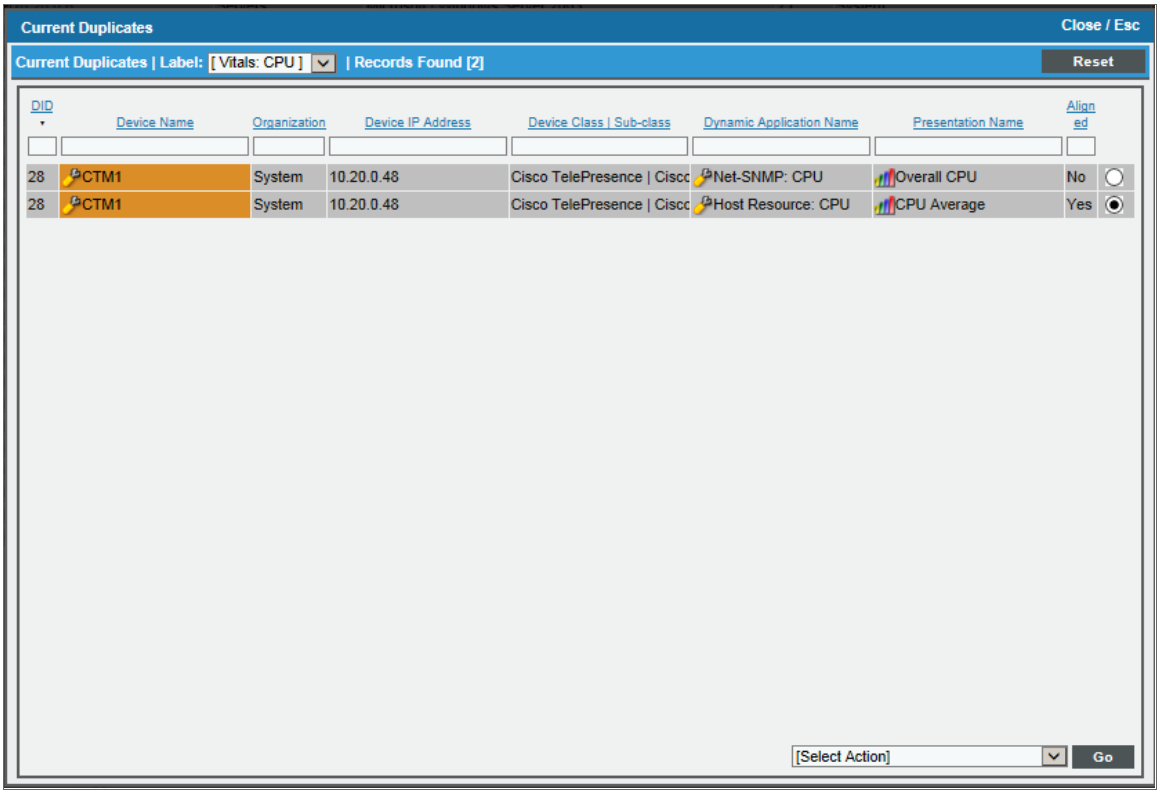
You can view a list of devices where duplicates occur, view how SL1 assigned the Collection Label-presentation object pair, and edit the Collection Label-presentation object pair for one or more selected devices. When you manually define a Collection Label-presentation object pair for a device, SL1 will not edit or change that pair:

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

2. Select the checkbox for each device you are interested in.



3. 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.
4. In the ***Select Action*** field (lower right), select **FIND Collection Label Duplicates**. Select the **[Go]** button.



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:

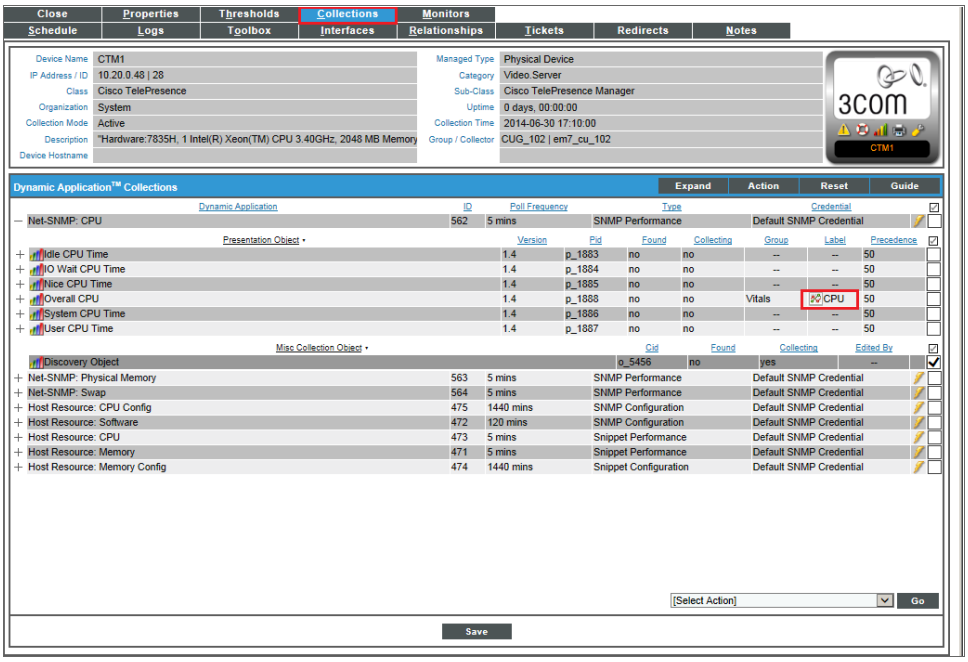
        - Click on the radio button for the desired presentation object for the device.
        - For each additional device you want to edit, click on the radio button for the desired presentation object.
        - In the ***Select Action*** menu (lower right), select *Align Presentation for Device*. Select 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.

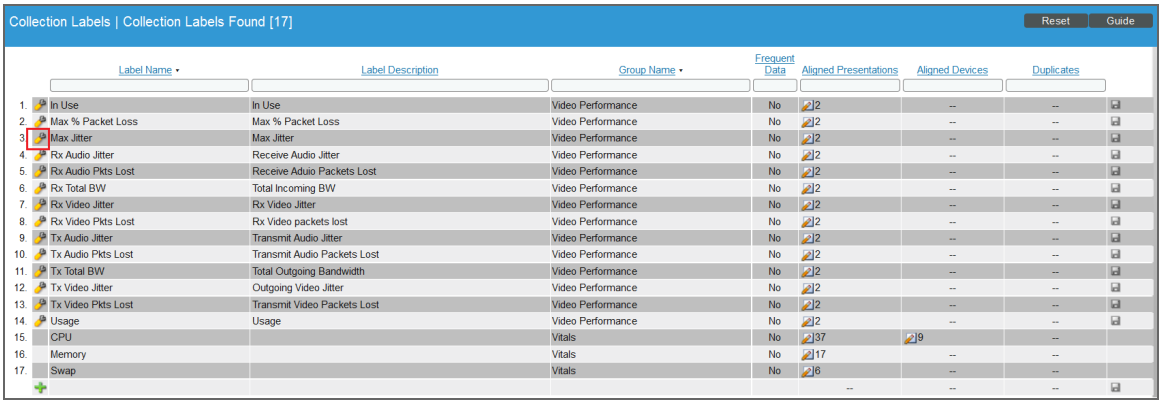


4. You will notice that some presentation objects include the chart icon in the ***Label*** column. These presentation objects are duplicates that are not currently aligned with a Collection Label. If you want to align one of these presentation objects with the Collection Label (instead of the current alignment), click on the chart icon.
5. 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:

1. Go to the **Collection Labels** page (System > Manage > Collection Labels).



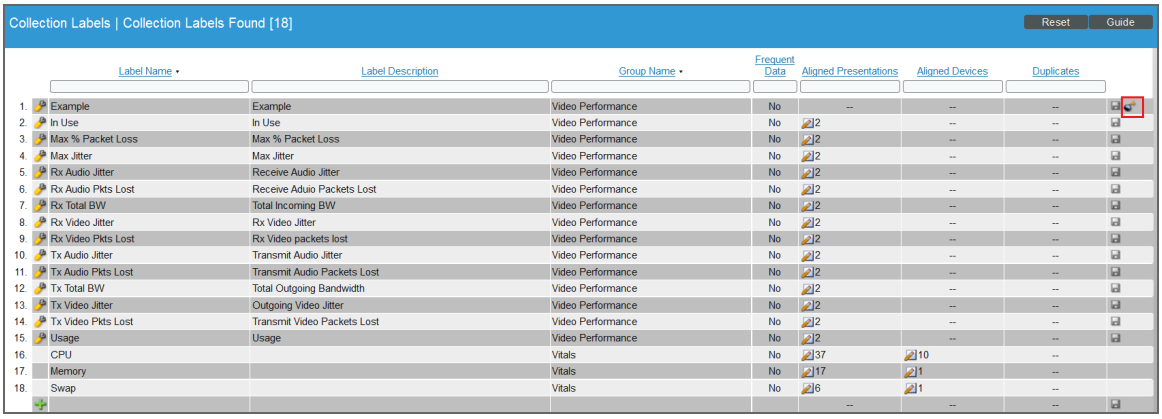
2. Find the Collection Label you want to edit. Select its wrench icon ( ).
3. You can edit one or more of the following:
   - ***Label Name***. Name of the Collection Label. This field is required.
   - ***Label Description***. Description of the Collection Label. This field is optional.
   - ***Group 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).



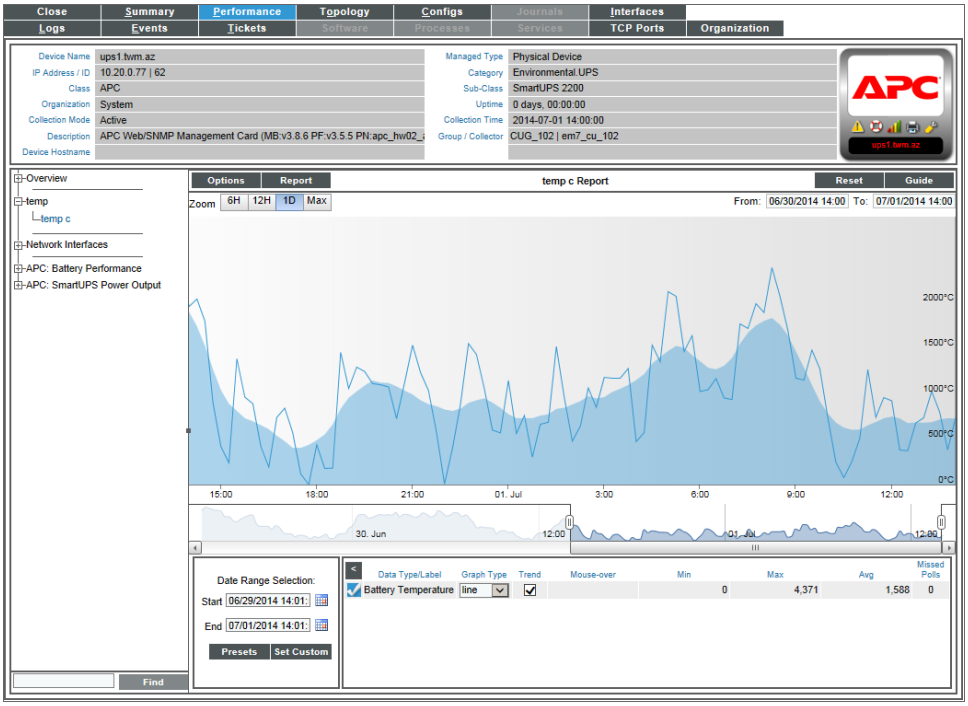
	Label Name	Label Description	Group Name	Frequent Data	Aligned Presentations	Aligned Devices	Duplicates
1.	Example	Example	Video Performance	No	--	--	--
2.	In Use	In Use	Video Performance	No	2	--	--
3.	Max % Packet Loss	Max % Packet Loss	Video Performance	No	2	--	--
4.	Max Jitter	Max Jitter	Video Performance	No	2	--	--
5.	Rx Audio Jitter	Receive Audio Jitter	Video Performance	No	2	--	--
6.	Rx Audio Pkts Lost	Receive Aduio 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.

© 2003 - 2023, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010