



Device Groups and Device Templates

SL1 version 8.10.0

Table of Contents

| | |
|--|-----------|
| What is a Device Group? | 4 |
| What is a Device Template? | 6 |
| Creating and Editing Device Groups | 9 |
| Before You Start | 10 |
| Viewing the List of Device Groups | 10 |
| Filtering the List of Device Groups | 11 |
| Special Characters | 12 |
| Creating a Device Group | 16 |
| Adding and Removing Static Devices and Child Device Groups | 21 |
| Adding Dynamic Rules | 22 |
| The Relationship Selection Page | 31 |
| Editing and Deleting Dynamic Rules | 34 |
| Creating Device Groups From Views | 34 |
| Editing an Existing Device Group | 35 |
| Assigning Devices to a Device Group During Discovery | 36 |
| Controlling Access to a Device Group | 36 |
| Defining the Actions for a Device Group | 36 |
| Deleting a Device Group | 37 |
| Example of Creating a Device Group | 39 |
| Creating and Editing Device Templates | 40 |
| Before You Start | 41 |
| Viewing the List of Device Templates | 41 |
| Filtering the List of Device Templates | 42 |
| Special Characters | 44 |
| Creating a Device Template | 45 |
| Defining Device Properties and Device Thresholds in the Config Tab | 48 |
| Defining Interface Monitoring in the Interface Tab | 53 |
| Defining Web-Content Monitoring in the CV Policies Tab | 58 |
| Defining TCP/IP Port Monitoring in the Port Policies Tab | 61 |
| Defining Windows Services Monitoring in the Svc Policies Tab | 63 |
| Defining Process Monitoring in the Proc Policies Tab | 65 |
| Aligning Dynamic Applications and Defining Thresholds in the Dynamic Apps Tab | 67 |
| Aligning Log File Monitoring Policies in the Logs Tab | 71 |
| Creating a New Device Template Based on an Existing Device Template | 73 |
| Editing an Existing Device Template | 74 |
| Using Device Templates | 76 |
| Before You Start | 77 |
| Using a Device Template to Edit the Configuration of the Devices in a Device Group | 77 |
| Using a Configuration Template to Edit the Configuration of One or More Individual Devices | 80 |
| Using the Bulk Configuration Tool to Apply Ad Hoc Settings to a Device Group | 83 |
| Using the Bulk Configuration Tool to Apply Ad Hoc Settings to One or More Devices | 86 |
| Example Device Group and Device Template | 89 |
| Example Device Group | 90 |
| Example Configuration Template | 91 |
| Using Device Group Maps and Views | 93 |
| Viewing the Device Maps for a Device Group | 94 |
| Viewing the Device Group Map Page for a Single Device Group | 95 |
| Viewing the Classic Views of a Device Group | 96 |
| Viewing Custom Device Maps | 96 |
| Using the Interface for Device Group Views | 97 |

| | |
|---|------------|
| Drag-and-Drop Editing | 97 |
| Fields and Buttons | 97 |
| Creating a Device Group from an Existing Device Group in the Device Group Map | 98 |
| Creating a New Device Group From My Customized Maps | 99 |
| Creating a New Device Group From an Existing Device Group in My Customized Maps | 101 |
| Scheduling Downtime for a Device Group | 102 |
| Viewing the Schedule Manager | 103 |
| Defining a Scheduled or Recurring Device Group Maintenance Window | 104 |
| Enabling or Disabling One or More Scheduled Device Group Maintenance Windows | 107 |
| Deleting One or More Scheduled Device Group Maintenance Windows | 108 |
| Events and Device Groups | 109 |
| Searching Events by Device Group | 110 |
| Suppressing an Event for a Device Group | 111 |
| Automation Policies and Tickets | 113 |
| What is an Automation Policy? | 114 |
| Aligning an Automation Policy with a Device Group | 114 |
| What is an Action Policy? | 116 |
| Aligning a Ticket with a Device Group | 118 |
| Searching for a Ticket Aligned with a Device Group | 119 |
| Assigning Device Groups and Applying Device Templates During Discovery | 121 |
| What is Discovery? | 121 |
| Assigning Devices to a Device Group During Discovery | 122 |
| Applying a Device Template to Devices During Discovery | 124 |

Chapter

1

What is a Device Group?

Overview

A **device group** is a group of multiple devices. Device groups allow you to:

- Use device configuration templates to perform initial configuration for multiple devices simultaneously.
- Use device configuration templates to make changes to the configuration for multiple devices simultaneously.
- In the **[Views]** tab, view each device group and the sub-groups and devices within each device group.
- Schedule maintenance and downtime for multiple devices simultaneously.
- Suppress events on multiple devices simultaneously.
- Include the device group in an automation policy. An automation policy allows you to trigger an automatic action if specified criteria are met on all the devices in the device group.

A device can belong to multiple device groups. For example, suppose SL1 discovered a server. Suppose this server hosts a corporate website that you want to monitor with a web-content policy. Suppose this server also hosts a MySQL database that you want to monitor with a Dynamic Application for MySQL. You could make this server a member of two device groups, one device group for web servers and another device group for MySQL databases. You could then use a device configuration template to apply a web-content policy to all devices in the device group for web servers and another device configuration template to apply a Dynamic Application for MySQL to all devices in the device group for MySQL servers.

You can add devices to a device group either explicitly or dynamically.

- You can create **static device groups**, where you explicitly assign one or more devices to a device group.
- You can create **dynamic device groups**, where you define **rules** for the device group. Each device that meets the criteria in the rule is automatically included in the device group. For example, suppose that you define a rule that specifies "include all devices in the *System* organization, with an IP address that starts with '10.100.100' ". SL1 would automatically assign all devices from the *System* organization with an IP of "10.100.100.*" to the new device group. When a new device is added to the *System* organization with an IP that begins with "10.100.100.*", that device will also be included in the device group. If a device with an IP that starts with "10.100.100.*" is removed from the *System* organization, that device will also be removed from the device group.
- You can create a device group that includes both explicitly assigned devices and also includes a dynamic rule. This device group will include both the explicitly assigned devices and all devices that meet the criteria in the dynamic rule.

The IT Services feature in SL1 uses device groups to define an IT Service. An IT Service contains sets of rules that define the state of that IT Service based on the state of the devices within the device group. For example, if you created an IT Service that represents the state of your email service, the associated device group might contain your DNS Servers, Exchange Servers, and Virtual Devices that are associated with Email Round-Trip Policies. To learn more about IT Services, see the **IT Services** manual.

This manual describes how to define groups, device configuration templates, view device groups, manage device groups, and include device groups in event suppressions and automation policies.

Chapter 2

What is a Device Template?

Overview

Device templates allow you to save a device configuration, apply it to one or more devices, and reuse the same configuration over and over again. A device template contains the following tabs and settings:

The screenshot displays the 'Device Template Editor | Config Template Settings' interface. At the top, there are 'New' and 'Reset' buttons. Below them is a 'Template Name' field containing 'Support: Apply Applications'. The interface is divided into several tabs: 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', and 'Dyn Apps'. The 'Config' tab is active, showing two main sections: 'Access & Monitoring' and 'Device Preferences'. The 'Access & Monitoring' section includes fields for Device Organization (AWS), SNMP Read (c0sm0s), SNMP Write (None), Availability Protocol (TCP), Avail Port (ICMP), Latency Protocol (TCP), Latency Port (ICMP), Avail+Latency Alert (Disabled), Collection (Enabled), Collector Grp (CUG1), Coll. Type (Standard), Critical Ping (Disabled), and Event Mask (Disabled). The 'Device Preferences' section includes checkboxes for Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, Disable Asset Update, and Bypass Interface Inventory. Below these sections is the 'Device Retention & Basic Thresholds' section, which features sliders for System Latency (500 ms), Availability Packet Size (56 bytes), Availability Ping Count (1 pings), Daily Rollup Bandwidth Data (365 days), Frequent Rollup Bandwidth Data (60 days), Hourly Rollup Bandwidth Data (120 days), and Raw Performance Data (90 days). The 'Interface Inventory Settings' section at the bottom includes sliders for Interface Inventory Timeout (600000 ms) and Maximum Allowed Interfaces (10000). At the very bottom, there are 'Save' and 'Save As' buttons.

- **Config.** Contains all the fields in the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Device Properties** page or the **Device Thresholds** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.
- **Interface.** Contains all the fields in the **Interface Properties** page that define how SL1 will monitor one or more network interfaces, and the thresholds for those network interfaces. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Interface Properties** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.
- **CV Policies.** Specifies one or more web-content policies that can be applied to all devices that use the template. These web-content policies enable SL1 to monitor a website. SL1 will periodically check the website for specified content. If the content cannot be found on the website, SL1 will generate an event. When you apply a device template to a device, you do not have to manually define any web-content and availability policies in the **Monitoring Policies** page for the devices. All the devices that use the template will inherit the web-content policies from the device template; SL1 will automatically create these web-content policies for each device that uses the template.
- **Port Policies.** Specifies one or more TCP/IP Port policies that can be applied to all member devices. These TCP/IP Port policies tell SL1 to monitor a specified port for availability every five minutes. Availability refers to the port's ability to accept connections and data. When you apply a device template to a device group, you do not have to manually define any TCP/IP port policies in the **Monitoring Policies** page for the member devices. All the devices in the device group will inherit the TCP/IP port policies from the device template; SL1 will automatically create these port policies for each device that uses the template.
- **Svc Policies.** Specifies one or more Windows service policies that can be applied to devices that use the template. These Windows service policies tell SL1 to monitor the device and look for the specified service. You can define a service policy so that SL1 monitors whether or not the service is running and then performs an action (starts, pauses, or restarts the service, reboots or shuts down the device, triggers the execution of a remote script or program). When you apply a device template to devices, you do not have to manually define any Windows service policies in the **Monitoring Policies** page for those devices. All the devices that use the template will inherit the Windows service policies from the device template; SL1 will automatically create these Windows service policies for each device that uses the template.
- **Proc Policies.** Specifies one or more Process policies that can be applied to devices that use the template. These Process policies tell SL1 to monitor the device and look for the process. You can define a process policy so that SL1 monitors whether or not the process is running, and optionally, how much memory a process can use and how many instances of a process can run simultaneously. When you apply a device template to devices, you do not have to manually define any Process policies in the **Monitoring Policies** page for those devices. All the devices that use the device template will inherit the Process policies from the device template; SL1 will automatically create these process policies for each device that uses the template.
- **Dynamic Apps.** Specifies one or more Dynamic Applications that can be aligned with devices that use the template. SL1 will use the specified Dynamic Applications to retrieve data from the devices that use the template. (Note that each device that uses the template might also be aligned with additional Dynamic Applications that have been aligned with the device in other ways; for example, from the automatic alignment that occurs during discovery.) When you apply a device template to devices, you do not manually have to align Dynamic Applications in the **Dynamic Application Collections** page for those devices. All devices that use the device template will be aligned with the Dynamic Applications specified in the device template.

- If you select a Dynamic Application in a Device Template, and that Dynamic Application has associated thresholds, you can change one or more of those thresholds from the Device Template. The thresholds you specify in the Device Template will override the thresholds defined in the Dynamic Application. When you apply a device template to devices, you do not manually have to edit the Dynamic Application Thresholds in the **Device Thresholds** page for those devices. All devices that use the device template will inherit the Dynamic Application Thresholds specified in the device template.
- You can change the frequency at which SL1 will poll all devices that use a device template to retrieve the information specified in a Dynamic Application. This value will override the default value specified in the Dynamic Applications.

You can apply device templates to:

- One or more **device groups**.
- One or more devices, selected from the **Device Manager** page.

NOTE: You can add device templates to PowerPacks. To learn how to add device templates to PowerPacks, see the manual *Using PowerPacks*.

You can also apply device templates to automate the initial configuration of multiple devices. If you change a device template, you can use it to automate the editing of the configuration of multiple devices.

Device templates are not dynamic. That is, when you update or change a device template, no changes are made to any devices that have used the template in the past.

You can make temporary changes to a device template, apply the template to a devices, and then exit the device template without saving the temporary changes. In this way, you can apply settings to a device group but not permanently save the settings in the device template.

NOTE: If you make changes to a device template or simply apply the device template a second time, SL1 will not create duplicate policies on the member devices. However, if you edit a device template and make a change to a policy, the policy will be updated on the member devices.



The section on [using device templates](#) describes in detail all the ways you can use a device template in SL1.

Creating and Editing Device Groups

Overview

This chapter describes how to create and edit device 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 includes the following topics:

| | |
|---|-----------|
| Before You Start | 10 |
| Viewing the List of Device Groups | 10 |
| <i>Filtering the List of Device Groups</i> | 11 |
| <i>Special Characters</i> | 12 |
| Creating a Device Group | 16 |
| <i>Adding and Removing Static Devices and Child Device Groups</i> | 21 |
| <i>Adding Dynamic Rules</i> | 22 |
| <i>The Relationship Selection Page</i> | 31 |
| <i>Editing and Deleting Dynamic Rules</i> | 34 |
| <i>Creating Device Groups From Views</i> | 34 |
| Editing an Existing Device Group | 35 |
| <i>Assigning Devices to a Device Group During Discovery</i> | 36 |
| Controlling Access to a Device Group | 36 |
| <i>Defining the Actions for a Device Group</i> | 36 |

Before You Start

You might want to consider the following when planning your device groups:

- How do you configure your devices? Can you group devices by their configuration? If so, you might want to create device groups based on their configuration and then use configuration templates to manage the configuration for all devices in the device group.
- Remember that when you create a device group, you can control the actions that can be performed with the device group and control access to the device group. You should plan which users need access to the device group and what they will do with the device group.
- Device groups can be nested. Remember that child device groups are not required to inherit the same set of actions as the parent device group. This feature allows you to fine tune actions and access for device groups.

Viewing the List of Device Groups

From the **Device Groups** page, you can view the list of existing device groups and access tools to create, edit, and manage device groups.

To view a list of existing device groups:

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







The screenshot shows a web interface for 'Device Groups | Groups Found [4]'. It features a table with columns for Device Group Name, ID, Owner, Access, Dev. Count, Grp. Count, Bulk Count, Edited By, and Last Edited. Below this is a detailed view of device groups with columns for Device Name, IP Address, Category, Class | Sub-class, ID, and Organization.

| Device Group Name | ID | Owner | Access | Dev. Count | Grp. Count | Bulk Count | Edited By | Last Edited |
|---------------------------------|----|-----------|--------|------------|------------|------------|-------------|---------------------|
| SAC ITSM Test | 3 | em7admin | Shared | 1 | -- | -- | AutoRegUser | 2017-04-18 13:52:01 |
| SAC Scheduler Test | 5 | em7admin | Shared | 1 | -- | -- | AutoAdmin | 2017-04-18 15:21:33 |
| SAC Scheduler Test (IT Service) | 6 | AutoAdmin | Shared | -- | -- | -- | AutoAdmin | 2017-04-18 15:24:13 |
| Servers | 1 | em7admin | Shared | -- | -- | 1 | em7admin | 2017-04-17 19:49:51 |

| Device Name | IP Address | Category | Class Sub-class | ID | Organization |
|---------------------------------|---------------|----------|--|----|----------------------------------|
| 10-64-171-130_ISO_CDB | 10.64.171.130 | EM7 | ScienceLogic, Inc. EM7 Database | 25 | SAC_Sanity_Device_Templates_Test |
| 2012-sharepoint | 10.7.7.149 | Servers | Microsoft Windows Server 2012 R2 | 2 | System |
| huib | 10.72.48.28 | Servers | Linux CentOS 7 | 3 | System |
| lenny-test1-dist-ap-10-2-4-21 | 10.2.4.21 | EM7 | ScienceLogic, Inc. EM7 Admin Portal | 8 | System |
| lenny-test1-dist-cu1-10-2-4-23 | 10.2.4.23 | EM7 | ScienceLogic, Inc. EM7 Data Collector | 13 | System |
| lenny-test1-dist-cu2-10-2-4-24 | 10.2.4.24 | EM7 | ScienceLogic, Inc. EM7 Data Collector | 9 | System |
| lenny-test1-dist-mc-10-2-4-25 | 10.2.4.25 | EM7 | ScienceLogic, Inc. EM7 Message Collector | 10 | System |
| lenny-test2-alo-10-2-4-30 | 10.2.4.30 | EM7 | ScienceLogic, Inc. EM7 All-in-One | 11 | System |
| lenny-test2-dist-ap-10-2-4-31 | 10.2.4.31 | EM7 | ScienceLogic, Inc. EM7 Admin Portal | 12 | System |
| Mbl_CentralLicensingSystem_4_26 | 10.2.4.28 | EM7 | ScienceLogic, Inc. OEM | 6 | System |
| SAC-ISO-AIO-9-30 | 10.2.9.30 | EM7 | ScienceLogic, Inc. EM7 All-in-One | 27 | SAC_Scheduler_Test |
| SAC-ISO3-AP-9-55 | 10.2.9.55 | EM7 | ScienceLogic, Inc. EM7 Admin Portal | 36 | SAC_Sanity_IC_Test |
| SAC-ISO3-DB-9-56 | 10.2.9.56 | EM7 | ScienceLogic, Inc. EM7 Database | 28 | SAC_Sanity_IC_Test |
| SAC-PATCH-AIO-9-20 | 10.2.9.20 | EM7 | ScienceLogic, Inc. EM7 All-in-One | 31 | SAC_Sanity_IC_Test |
| SAC-PATCH-AP-9-25 | 10.2.9.25 | EM7 | ScienceLogic, Inc. EM7 Admin Portal | 17 | SAC_Sanity_Label_Test |
| SAC-PATCH-CU1-9-27 | 10.2.9.27 | EM7 | ScienceLogic, Inc. EM7 Data Collector | 18 | SAC_ITSM_Test |
| smmpSm_10-2-4-19 | 10.2.4.19 | EM7 | ScienceLogic, Inc. EM7 Database | 7 | System |

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

TIP: To sort the list of device groups, 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. The **Last Edited** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- **Device Group Name.** Name of the device group.
- **ID.** Unique, numeric ID, assigned to the device group automatically by SL1.
- **Owner.** User who created the device group.
- **Access.** Specifies whether users can view and use the device group. Shared device groups can be viewed by other users who belong to the same organization as the creator. Private device groups can be viewed only by the creator of the device group and administrators.
- **Dev Count.** Number of devices in the device group.
- **Grp Count.** Number of device groups included in this device group. If the number is greater than zero, the current group is a parent group and contains sub-groups or child groups.
- **Rule Count.** Specifies the number of dynamic rules included in the device group.
- **Edited By.** User who created or last edited the device group.
- **Last Edited.** Date and time the device group was created or last edited.
- **Tools.** For each device group, one or more of the following tools are available:
 - *Edit this app* (). Leads to the **Device Group Editor** page, where you can edit the parameters of the device group.
 - *View IT Service* (). Leads to the **IT Service Summary** page, where you can view the IT Service dashboards that have been configured for the IT Service that uses this device group. For details on the **IT Service Summary** page, see the manual on **IT Services**.
 - *Bulk configuration* (). Leads to the **Apply Device Configuration Template** page, where you can make one-time changes to a configuration template and apply a configuration template to the device group.
 - *Group Map View* (). Displays the **Device Group Views** page for the selected device group.
 - *Group Scheduling* (). Leads to the **Device Group Scheduling** page where you can schedule downtime for maintenance for all devices in the device group.
 - *List devices matching dynamic rules* (). Displays the **Matched Devices** modal page. This page displays a list of all devices that match all rules in the device group.

Filtering the List of Device Groups

The following describes each filter on the **Device Groups** page:

- **Device Group Name.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching name.
- **ID.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching ID. SL1 automatically assigns this unique, numeric ID to each device group.
- **Owner.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have the specified.
- **Access.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching access (Shared or Private).
- **Dev Count.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a number of devices.
- **Grp Count.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching number of child device groups.
- **Rule Count.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching number of dynamic rules.
- **Edited By.** You can enter text to match, including special characters, and the **Device Groups** page will display only device groups that have a matching user name in the **Edited By** field.
- **Last Edited.** Only those device groups that have the specified creation date or last-edited date will be displayed. The choices are:
 - *All.* Display all device groups that match the other filters.
 - *Last Minute.* Display only device groups that have been created within the last minute.
 - *Last Hour.* Display only device groups that have been created within the last hour.
 - *Last Day.* Display only device groups that have been created within the last day.
 - *Last Week.* Display only device groups that have been created within the last week.
 - *Last Month.* Display only device groups that have been created within the last month.
 - *Last Year.* Display only device groups that have been created within the last year.

Special Characters

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

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

String and Numeric

- **,** (comma). Specifies an "OR" operation. Works for string and numeric values. For example:
 "dell, micro" matches all values that contain the string "dell" OR the string "micro".

- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:
 "dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.
- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:
 "!dell" matches all values that do not contain the string "dell".
 "! ^ micro" would match all values that do not start with "micro".
 "!fer\$" would match all values that do not end with "fer".
 "! ^ \$" would match all values that are not null.
 "! ^ " would match null values.
 "!\$" would match null values.
 "!*" would match null values.
 "happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

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

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:
 "hel*er" would match "helpers" and "helicopter" but not "hello".
 "325*" would match "325", "32561", and "325000".
 "**000" would match "1000", "25000", and "10500000".
- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:
 "!?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 "scienceologic", but not "conscious".

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

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

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

`!^` would match null values.

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

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

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

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

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

`!$` would match null values.

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

Numeric

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

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

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

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

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

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

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

- < (less than). Matches numeric values only. Specifies any value "less than". For example:
 "<12" would match all values less than 12.
- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:
 "=>7" would match all values 7 and greater.
- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:
 "=<12" would match all values 12 and less.
- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:
 "=-5" would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio\$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo\$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contain the characters "silo".
- "!"^silo". Matches only text that does not start with "silo".
- "!0\$". Matches only text that does not end with "0".
- "!"^silo\$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!"^". Matches null values, typically represented as "--" in most pages.
- "!"\$". Matches null values, typically represented as "--" in most pages.
- "!"^\$". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*l*o\$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would match.
- "!"^s*i*l*o\$". Matches all text that does not contain the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".

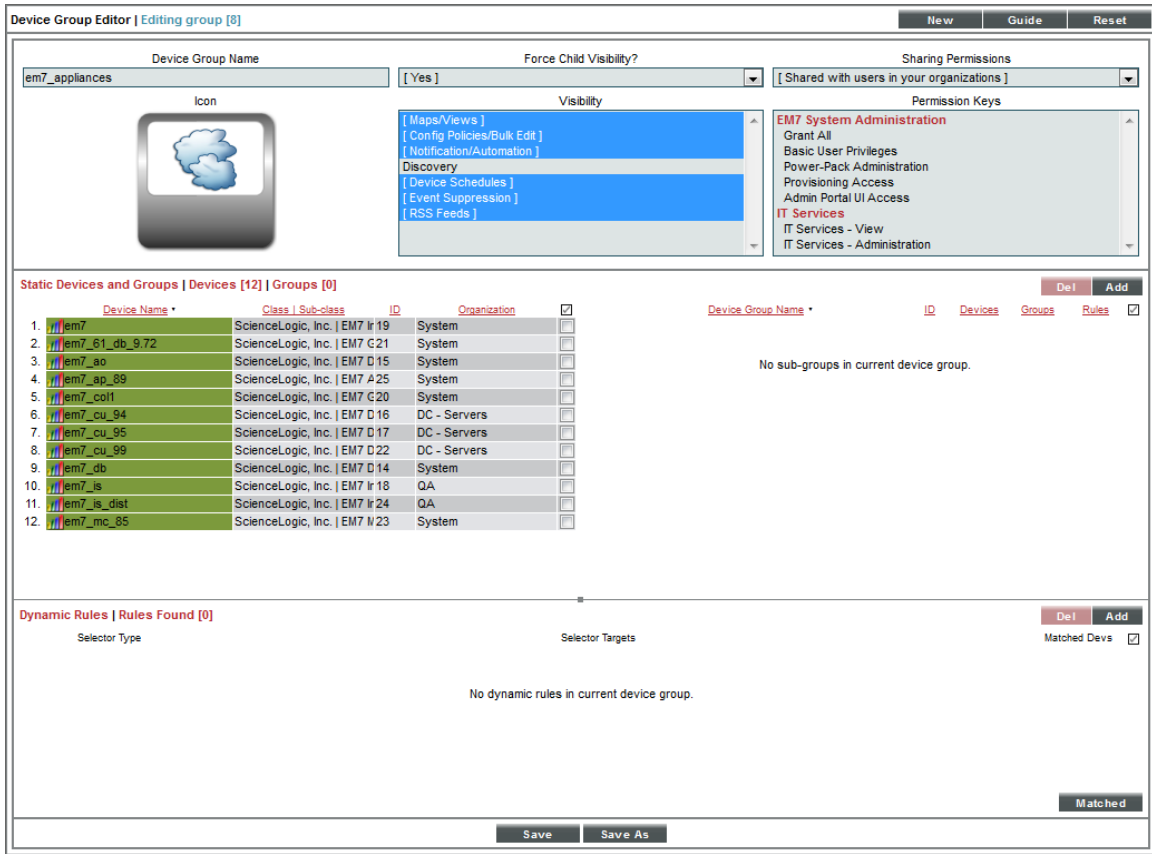
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol" and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- "!silo". Matches text that does not contain "silo".
- "!^silo\$". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.
- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "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 Device Group

To define a new device group, perform the following steps:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).
2. In the **Device Groups** page, click the **[Create]** button.

3. The **Device Group Editor** page appears.



4. In the **Device Group Editor** page, supply values in each field and select devices to include in the device group. You can also select other device groups to include in the new device group. The selected device groups will be children device groups to the new device group.

- **Device Group Name.** Specify the name of the new device group.
- **Icon.** Select an icon to represent the new device group. To add an icon to this list, go to the **Device Icon Browser** modal page (System > Customize > Device Classes, click the **[Icon]** button) and then select the **[Import]** button.
- **Force Child Visibility.** If the current device group includes another device group, that nested device group is considered a "child" device group. A device group can contain multiple children device groups. Those children device groups can also contain nested device groups. The **Force Child Visibility** feature specifies whether or not **all nested** device groups will inherit the **Visibility** settings of the parent device group. This field affects all **Visibility** settings except *Maps/Views* and *Discovery*. Choices are:
 - **No.** Child device groups will not inherit the **Visibility** settings of the parent device group. When SL1 performs actions on the parent device group, devices in the child device groups will be acted upon **only** if the child device groups have the appropriate **Visibility** setting.

For example, suppose a device group **parent_groupA** includes a nested device group called **child_groupB** and another nested device group called **child_groupC**.

Suppose **parent_groupA** has **Force Child Visibility** set to No.

Suppose **parent_groupA** has **Visibility** set to *Notification/Automation*.

Suppose **parent_groupA** is aligned with an Automation Policy.

All the devices in **parent_groupA** can be acted upon by that Automation Policy.

Suppose **child_groupB** has **Visibility** set to *Views/Maps* only.

The devices in **child_groupB** will not be acted upon by the Automation Policy, because **child_groupB** does not have the required **Visibility** setting and because **child_groupB** does not inherit the **Visibility** settings of **parent_groupA**.

Suppose **child_groupC** has **Visibility** set to *Notification/Automation*.

All the devices in **child_groupC** will be acted upon by the Automation Policy, because **child_groupC** has the required **Visibility** setting.

The value in **Force Child Visibility** for **parent_groupA** is recursive and affects all child, grandchild, great grandchild etc. device groups nested under the parent group

- Yes. Child device groups will inherit the **Visibility** settings of the parent device group, regardless of the **Visibility** settings for the child device group. When SL1 performs actions on the parent device groups, all devices in each child device group will also be acted upon, regardless of the **Visibility** settings for each child device group.

For example, suppose a device group **parent_groupX** includes a nested device group. called **child_groupY**.

Suppose **parent_groupX** has **Force Child Visibility** set to Yes.

Suppose **parent_groupX** has **Visibility** set to *Device Schedules*.

Suppose you define a maintenance schedule for **parent_groupX** that says "stop collection for **parent_groupX** on October 17, from 3:00 AM until 3:30 AM.

On October 17, from 3:00 AM until 3:30 AM, all the devices in **parent_groupX** will have a Collection State of "Maintenance".

Suppose **child_groupY** has **Visibility** set to *Maps/Views* only.


On October 17, from 3:00 AM until 3:30 AM, all the devices in **child_groupY** will have a collection status of "Maintenance", even though **child_groupY** does not have **Visibility** set to *Device Schedule*. This is because **child_groupY** inherited the **Visibility** of **parent_groupX**. However, because **child_group_Y** does not have **Visibility** set to *Device Schedule*, a user cannot explicitly schedule maintenance for **child_group_Y**.


Suppose **child_groupY** includes a nested device group, called **grandchild_groupZ**. Suppose **grandchild_groupZ** has **Visibility** set to *Discovery* only.

On October 17, from 3:00 AM until 3:30 AM, all the devices in **grandchild_groupZ** will have a collection status of "Maintenance", even though **grandchild_groupZ** does not have **Visibility** set to *Device Schedule*. This is because **grandchild_groupZ** inherited the **Visibility** of **parent_groupX**. However, because **grandchild_group_Z** does not have **Visibility** set to *Device Schedule*, a user cannot explicitly schedule maintenance for **grandchild_group_Z**.

The value in **Force Child Visibility** for **parent_groupX** is recursive and affects all child, grandchild, great grandchild etc. device groups nested under the parent group . However, inherited **Visibility** settings only apply to child, grandchild, great grandchild and so forth device groups if the action controlled by the **Visibility** setting is performed on the parent device group.

NOTE: The **Force Child Visibility** feature affects **only actions that expand a device group into a list of devices**. The **Force Child Visibility** feature does not affect the **Visibility** settings for *Maps/Views* and *Discovery*. Children device groups cannot inherit the **Visibility** settings for *Maps/Views* and *Discovery*, even if **Force Child Visibility** is set to Yes. If you want a parent device group to appear in the Views pages, set **Visibility** to *Maps/Views*. If you want children device groups to appear in the Views pages, you must explicitly set **Visibility** to *Maps/Views* for each child device group. If you want a parent device group to appear in the list of device groups in the **Discovery Control Panel** page (System > Manage > Discovery), set **Visibility** to *Discovery*. If you want children device groups to appear in the list of device groups in the **Discovery Control Panel** page (System > Manage > Discovery), you must explicitly set **Visibility** to *Discovery* for each child device group.

- **Visibility**. Specifies where in SL1 the device group will be visible. Choices are:
 - *Maps/Views*. If selected, the device group will appear in the **Device Group Map** page (Views > Device Maps > Device Groups), the **Custom Device Group Map** page (Views > My Customized Maps), and the **Device Group Views** page (Views > Classic Views > Device Groups).
 - *Config Policies/Bulk Edit*. If selected, the building blocks icon () is visible in the **Device Groups** page. This allows you to configure all the devices in the device group using a device template.
 - *Notification/Automation*. If selected, the device group will appear in the list of device groups in the **Automation Policy Editor** modal page (Registry > Run Book > Automation > Edit/Create). This page allows you to trigger an automatic action if specified criteria are met on all the devices in the device group.

- *Discovery*. If selected, the device group appears in the field **Auto-add Devices to Device Group** in the **Discovery Control Panel** page (System > Manage > Discovery). This allows you to automatically add newly discovered devices to a pre-existing device group during the discovery process.
- *Device Schedules*. If selected, the calendar icon () is visible in the **Device Groups** page. This allows you to schedule downtime for all the devices in the device group. The scheduled downtime will appear in the **Maintenance Schedule** page for each device in the device group.
- *Event Suppression*. If selected, the device group will appear in the **[Suppressions]** tab in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). In this page, you can suppress the event for all devices in the device group.
- *RSS Feeds*. If selected, the device group appears in the field **Device Group Filter** in the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds). This field allows you to filter events included in the RSS feed; only events that occur on devices in the selected device group(s) will appear in the custom RSS feed.
- *IT Services*. This is a view-only option. If this option is selected when the **Device Group Editor** is loaded, the device group is associated with an IT service and was created automatically by SL1. Do not select or deselect this option.
- **Sharing Permissions**. Specifies whether other users can view and use the device group, in both the **Device Groups** page and in the pages in SL1 where the device group is visible. Choices are:
 - *Shared with users in your organization*. The device group can be viewed and used by other users who belong to the same organization as the creator.
 - *Private (visible only to you)*. The device group can be viewed and used only by the creator of the device group and administrators.
- **Permission Keys**. If you selected *Shared with users in your organization* in the **Sharing Permissions** field, you can specify the Access Keys that a user of type "user" must have to view the device group. The **Permission Keys** field will display a list of all the Access Keys in the EM7 System Administration category and all the Access Keys in the Device Group category.
 - *If you select one or more Access Keys in the Permissions Keys field, each user must meet the following criteria to access the device group:*
 - The user must have at least one of the selected Access Keys to access the device group.
 - The user must be granted one or more Access Keys that contains the Access Hooks "Registry" and "Registry > Devices > Device Groups"
 - The user and creator of the device group must be members of a common organization.

NOTE: For both the user and the creator of the device group, the common organization can be either the primary organization or an additional organization membership. For example, the user could have a primary organization of "East Coast NOC" and an additional organization membership in the organization "Headquarters". The creator of the device group could have a primary organization of "West Coast NOC" and an additional organization membership in the organization "Headquarters". In this situation, the user and creator of the device group are both members of a common organization.

- If you do not select one or more Access Keys in the *Permissions Keys* field, any user meeting the following two requirements can access the device group:
 - The user must be granted one or more Access Keys that contains the Access Hooks "Registry" and "Registry > Devices > Groups".
 - The user and creator of the device group must be members of a common organization.

NOTE: Users of type "administrator" will be able to view and access all device groups, regardless of the settings in the **Shared** field and the **Permission Keys** field.

5. Optionally, [add static devices and child device groups to the new device group](#).
6. Optionally, [add dynamic rules to the new device group](#).
7. Click the **[Save]** button in the **Device Group Editor** page to save the device group. The new device group will appear in the **Device Group** page. You can now perform actions upon all the devices in the device group simultaneously.

Adding and Removing Static Devices and Child Device Groups

You can explicitly assign one or more devices or child device-groups to a device group. These devices and device groups are considered **static** because they will remain in the device group until you manually remove them.

To manually add a device to a device group:

1. Go to the **Static Devices and Groups** pane.
2. Click the **[Add]** button then select **Add Devices**.
3. The **Device Alignment** modal page appears and displays a list of all devices in SL1.
4. In the **Device Alignment** modal page, select the checkbox of each device you want to include in the device group. Click the **[Add/Remove]** button in the lower right.
5. The selected devices will appear in the **Static Devices and Groups** pane.

To remove one or more static devices from the device group:

1. Go to the **Static Devices and Groups** pane.
2. Select the checkbox for each device you want to remove.
3. Click the **[Del]** button (in the upper right).
4. The selected device(s) no longer appear in the **Static Devices and Groups** pane.

To manually add a child device-group to a device group:

1. Go to the **Static Devices and Groups** pane.
2. Click the **[Add]** button then select **Add Groups**.
3. The **Device Group Alignment** modal page appears and displays a list of all device groups in SL1.
4. In the **Device Group Alignment** modal page, select the checkbox of each device group you want to include in the device group. Click the **[Add/Remove]** button in the lower right.
5. The selected device groups will appear in the **Static Devices and Groups** pane.

To remove one or more static device-groups from the device group:

1. Go to the **Static Devices and Groups** pane.
2. Select the checkbox for each child device-group you want to remove.
3. Click the **[Del]** button (in the upper right).
4. The selected device group(s) no longer appear in the **Static Devices and Groups** pane.

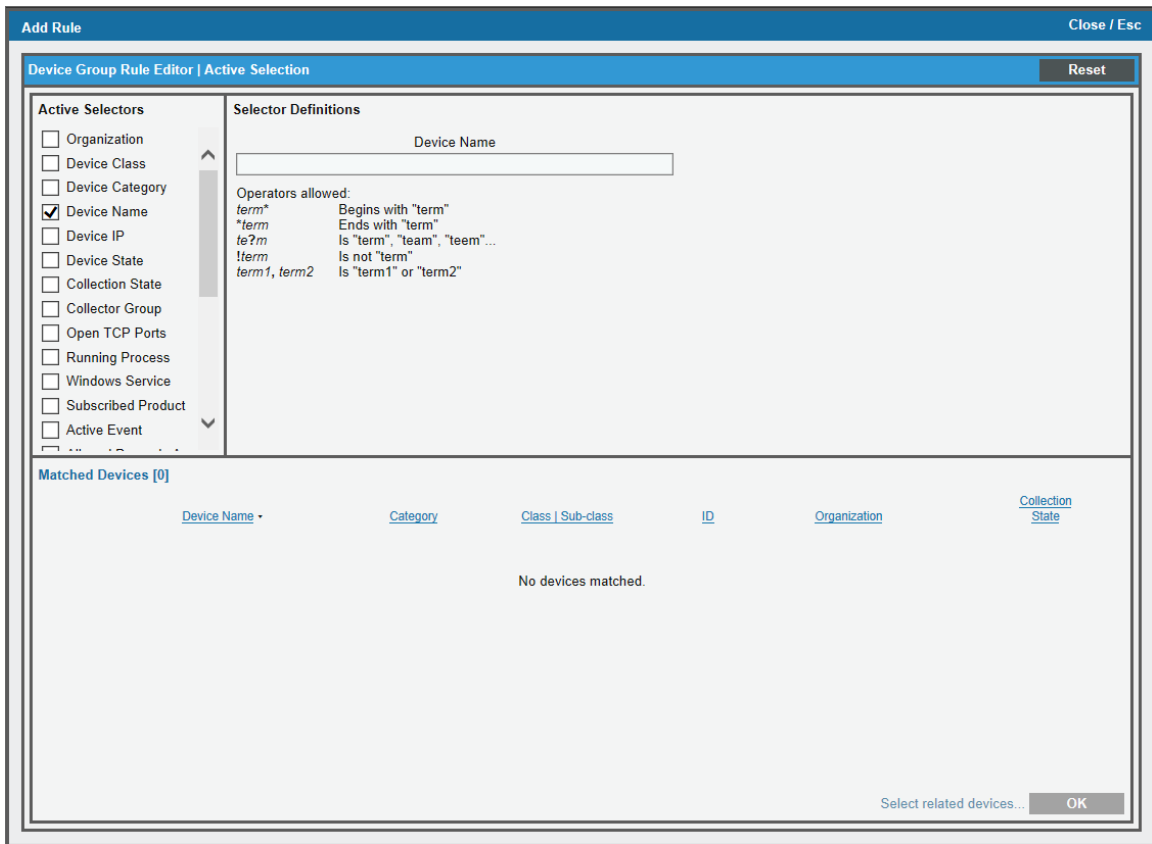
Adding Dynamic Rules

You can create **dynamic rules** for the device group. Each device that meets the criteria in the rule is automatically included in the device group.

For example, suppose that you define a rule that specifies "include all devices in the System organization, with an IP address that starts with '10.100.100'. SL1 would automatically assign all devices from the System organization with an IP of "10.100.100.*" to the new device group. When a new device is added to the System organization with an IP that begins with "10.100.100.*", that device will also be included in the device group. If a device with an IP that starts with "10.100.100.*" is removed from the System organization, that device will also be removed from the device group.

To add a dynamic rule:

1. Go to the **Dynamic Rules** pane.
2. Click the **[Add]** button (in the upper right of the pane). The **Device Group Rule Editor** modal page appears.



3. You can select one or more **Active Selectors**. To be included in the device group, a device must match all the **Selector Definitions**.
4. Depending upon your selection, you can enter the following options in the **Selector Definitions** pane.
 - **Organization**. Displays a list of all organizations in SL1.
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more organizations, SL1 will search for devices that are members of at least one the selected organization(s) and include those devices in the device group. For example, if you select two organizations, all devices from each organization will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** members of the selected organization(s) and include those devices in the device group.

- **Device Class.** Displays a list of all device classes in SL1 .
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more device classes, SL1 will search for devices that are members of the selected device class(es) and include those devices in the device group. For example, if you select two device classes, all devices from each device class will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** members of the selected device class(es) and include those devices in the device group.

- **Device Category.** Displays a list of all device categories in SL1 .
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more device categories, SL1 will search for devices that are members of the selected device categories and include those devices in the device group. For example, if you select two device categories, all devices from each device category will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** members of the selected device categories and include those devices in the device group.

- **Device Name.** Displays a field in which you can enter a string. SL1 will use the string to search for devices with matching device names. If you do not use wildcard characters, SL1 will return only devices with a device name that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any device name that begins with "term".
 - **term*. SL1 searches for any device name that ends with "term".
 - *te?**m*. SL1 searches for any device name that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any device name that does not include the text "term".
 - *term1*, *term2*. SL1 searches for any device name that contains either "term1" or "term2".

- **Device IP.** Displays a field in which you can enter a string. SL1 will use the string to search for devices with matching IP addresses. If you do not use wildcard characters, SL1 will return only devices with a device IP that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any device IP that begins with "term".
 - **term*. SL1 searches for any device IP that ends with "term".
 - *te?**m*. SL1 searches for any device IP that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any device IP that does not include the text "term".
 - *term1*, *term2*. SL1 searches for any device IP that contains either "term1" or "term2".
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** have a matching IP address and include those devices in the device group.

- **Device State.** Displays a list of all device states in SL1 (Notice, Healthy, Minor, Major, Critical). Each device's state is the same as the highest severity event associated with the device..
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more device states, SL1 will search for devices that are members of the selected device states and include those devices in the device group. For example, if you select two device states, all devices from each device state will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** have the selected device state and include those devices in the device group.

- **Collection State.** Displays a list of all collection states in SL1 (Active, NOT Active, User-Disabled, NOT User-Disabled, Unavailable, NOT Unavailable, Maintenance, NOT Maintenance, System-Disabled, NOT System-Disabled)..
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more collection states, SL1 will search for devices that are members of the selected device states and include those devices in the device group. For example, if you select two collection states, all devices with the first collection state and all devices with the second collection state will be included in the device group.

- **Collector Group.** Displays a list of all Collector Groups in SL1 .
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more Collector Groups, SL1 will search for devices that are members of the selected Collector Groups and include those devices in the device group. For example, if you select two Collector Groups, all devices from each Collector Group will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** members of the select Collector Group(s) and include those devices in the device group.

- **Open TCP Ports.** Displays a list of all open TCP ports that SL1 has discovered on at least one device.
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more ports, SL1 will search for devices have that have those ports open and include those devices in the device group. For example, if you select two collection ports, all devices where the first port is open and all devices where the second port is open will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** have the selected port(s) open and include those devices in the device group.

- **Running Process.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that are running a matching system process. If you do not use wildcard characters, SL1 will return only devices running a process that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any process name that begins with "term".
 - **term*. SL1 searches for any process name that ends with "term".
 - *te?m*. SL1 searches for any process name that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any process name that does not include the text "term".
 - *term1, term2*. SL1 searches for any process name that contains either "term1" or "term2".
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** running the selected processes open and include those devices in the device group.

- **Windows Service.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that are running a matching Windows service. If you do not use wildcard characters, SL1 will return only devices running a Windows services that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any Windows Service name that begins with "term".
 - **term*. SL1 searches for any Windows Service name that ends with "term".
 - *te?m*. SL1 searches for any Windows Service name that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any Windows Service name that does not include the text "term".
 - *term1, term2*. SL1 searches for any Windows Service name that contains either "term1" or "term2".
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** running a matching Windows service and include those devices in the device group.

- **Subscribed Product.** Displays a list of all product SKUs in SL1.
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more SKUs, SL1 will search for devices that subscribe to at least one the selected SKU(s) and include those devices in the device group. For example, if you select two SKUs, all devices that subscribe to one of the two SKUs will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** subscribe to the selected SKU(s) and include those devices in the device group.

- **Active Event.** Displays a list of all active events in SL1.
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more active events, SL1 will search for devices for which that event is currently active and include those devices in the device group. For example, if you select two events, all devices for which one of the two events is active will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices for which the event is **not** currently active and include those devices in the device group.

- **Aligned Dynamic App.** Displays a list of all Dynamic Applications that are currently aligned with one or more devices.
 - To filter the list, you can enter a string in the field under the title.
 - If you select one or more aligned Dynamic Applications, SL1 will search for devices that are aligned with those Dynamic Applications and include those devices in the device group. For example, if you select two Dynamic Applications, all devices that are aligned with each of the Dynamic Applications will be included in the device group.
 - If you select the **Invert** checkbox, SL1 will search for devices that are **not** aligned with the selected Dynamic Application(s).

- **Asset Make.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Make** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Make** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset make that begins with "term".
 - **term*. SL1 searches for any asset make that ends with "term".
 - *te?**m*. SL1 searches for any asset make that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset make that does not include the text "term".
 - *term1*, *term2*. SL1 searches for any asset make that contains either "term1" or "term2".

- **Asset Model.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Model** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Model** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset model that begins with "term".
 - **term*. SL1 searches for any asset model that ends with "term".
 - *te?**m*. SL1 searches for any asset model that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset model that does not include the text "term".
 - *term1*, *term2*. SL1 searches for any asset model that contains either "term1" or "term2".

- **Asset Function.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Function** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Function** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset function that begins with "term".
 - **term*. SL1 searches for any asset function that ends with "term".
 - *te?m*. SL1 searches for any asset function that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset function that does not include the text "term".
 - *term1, term2*. SL1 searches for any asset function that contains either "term1" or "term2".

- **Asset Owner.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Management Type** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Management Type** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset owner that begins with "term".
 - **term*. SL1 searches for any asset owner that ends with "term".
 - *te?m*. SL1 searches for any asset owner that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset owner that does not include the text "term".
 - *term1, term2*. SL1 searches for any asset owner that contains either "term1" or "term2".

- **Asset Location.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Facility/Data Center** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Facility/Data Center** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset location that begins with "term".
 - **term*. SL1 searches for any asset location that ends with "term".
 - *te?m*. SL1 searches for any asset location that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset location that does not include the text "term".
 - *term1, term2*. SL1 searches for any asset location that contains either "term1" or "term2".

- **Asset Serial.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Serial** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have a **Serial** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset serial that begins with "term".
 - **term*. SL1 searches for any asset serial that ends with "term".
 - *te?m*. SL1 searches for any asset serial that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset serial that does not include the text "term".
 - *term1, term2*. SL1 searches for any asset serial that contains either "term1" or "term2".

- **Asset Tag.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value in the **Asset Tag** field in their asset records (SL1 automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, SL1 will return only devices that have an **Asset Tag** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any asset tag that begins with "term".
 - **term*. SL1 searches for any asset tag that ends with "term".
 - *te?m*. SL1 searches for any asset tag that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any asset tag that does not include the text "term".
 - *term1, term2*. SL1 searches for any asset tag that contains either "term1" or "term2".

- **Software Title.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching title in the list of software defined in the **Licenses** tab in the asset record for the device. If you do not use wildcard characters, SL1 will return only devices that have a **Software Title** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any software title that begins with "term".
 - **term*. SL1 searches for any software title that ends with "term".
 - *te?m*. SL1 searches for any software title that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any software title that does not include the text "term".
 - *term1, term2*. SL1 searches for any software title that contains either "term1" or "term2".
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** have a matching software title in the list of software and include those devices in the device group.

- **Software Version.** Displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching version number in the list of software defined in the **Licenses** tab in the asset record for the device. If you do not use wildcard characters, SL1 will return only devices that have a **Software Version** field that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any software version that begins with "term".
 - **term*. SL1 searches for any software version that ends with "term".
 - *te?m*. SL1 searches for any software version that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any software version that does not include the text "term".
 - *term1, term2*. SL1 searches for any software version that contains either "term1" or "term2".
 - If you select the **Invert** checkbox, SL1 will search for devices that do **not** have a matching version number in the list of software and include those devices in the device group.
 - **Custom Attribute.** The Active Selectors field includes an entry for each custom attribute defined in your SL1 system. When you select a custom attribute, the Selector Definitions pane displays a field in which you can enter a string. SL1 will use the string to search for devices that have a matching value for this custom attribute. If you do not use wildcard characters, SL1 will return only devices with a custom attribute that exactly matches the string. You can use the following syntax in the field:
 - *term**. SL1 searches for any attribute value that begins with "term".
 - **term*. SL1 searches for any attribute value that ends with "term".
 - *te?m*. SL1 searches for any attribute value that contains the text "te[any single character]m".
 - *!term*. SL1 searches for any attribute value that does not include the text "term".
 - *term1, term2*. SL1 searches for any attribute value that contains either "term1" or "term2".
5. After you have selected an Active Selector and the Selector Definitions, you can specify that you want to **include children devices, all descendent devices, parent devices, or all ancestor devices**. To do this **do not click the [OK] button**. Instead, click the **Select related devices** link next to the **[OK]** button. If you do not want to include related devices, click the **[OK]** button to add the new rule.
 6. If you clicked the **Select related devices** link, the **Relationship Selection** modal page appears. In this modal page, you can select devices by relationship. The **Matched Devices** pane displays all the devices that match all the criteria in the rule. The list of devices changes as you add and remove criteria.
 7. Click the **[OK]** button to add the new rule.

NOTE: If a single dynamic rule includes multiple criteria, a device must match **all** the criteria to be included in the device group (like the SQL AND operator). If a single device group includes multiple dynamic rules, a device must match only a single rule to be included in the device group (like the SQL OR operator). To view a list of devices that are currently included in the device group based on the dynamic rules defined in the device group, click the **[Matched]** button.

The Relationship Selection Page

If you click the **Select related device link** in the **Device Group Rule Editor** page, the **Relationship Selection** page appears:

| Device Name | Category | Class Sub-class | ID | Organization | Collection State |
|-------------------------|----------|------------------------|------|--------------|------------------|
| 1. //vol/EM7 | NAS | NFS Export | 969 | Intel | Unavailable |
| 2. //vol/NetAppOSS | NAS | NFS Export | 970 | Intel | Unavailable |
| 3. //vol/NetAppOSS/home | NAS | NFS Export | 967 | Intel | Unavailable |
| 4. //vol/vol1 | NAS | NFS Export | 966 | Intel | Unavailable |
| 5. //vol/vol2 | NAS | NFS Export | 968 | Intel | Unavailable |
| 6. 10.0.0.1 | Pingable | Ping ICMP | 924 | Intel | Active |
| 7. 10.0.0.101 | Switches | Cisco Systems Cataly | 1766 | Intel | Active |
| 8. 10.100.100.30 | Pingable | Linux ICMP | 1511 | Intel | Unavailable |
| 9. 10.100.100.31 | Pingable | Linux ICMP | 1512 | Intel | Unavailable |
| 10. 10.100.100.32 | Pingable | Linux ICMP | 935 | Intel | Unavailable |
| 11. 10.100.100.33 | Pingable | Linux ICMP | 934 | Intel | Unavailable |
| 12. 10.100.100.34 | Pingable | Linux ICMP | 933 | Intel | Unavailable |
| 13. 10.100.100.35 | Pingable | Linux ICMP | 929 | Intel | Active |

The **Relationship Selection** page includes the following panes:

- **Relationship Selector.** You can choose to include children devices, all descendent devices (children, grandchildren, great grandchildren, etc), parent devices, or all ancestor devices (parents, grandparents, great grandparents, etc). You can also choose to further filter by including only the children, descendants, parents, and ancestors devices that are related to the "Seed Devices" through one or more selected Dynamic Applications.

NOTE: For details on building relationships with Dynamic Applications, see the *Dynamic Application Development* manual.

- **Seed Devices.** This is the list of devices you defined in the **Device Group Rule Editor** page. You can include these devices in the device group or include only the children, descendants, parents, ancestors.

- **Matched Devices.** This is the list of devices that will be included in the device group when you click the [OK] button.

NOTE: As SL1 discovers devices and component devices that meet the criteria for the dynamic device group, SL1 will automatically add those devices and component devices to the device group.

Relationship Selectors

In this pane, you can specify devices to include in the device group based on their relationships to the Seed Devices:


- **Children of.** If you select this checkbox, all children devices of the Seed Devices are included in the device group.
- **Descendents of.** This checkbox is enabled only if you select the **Children of** checkbox. If you select this checkbox, all children devices, grandchildren devices, great grandchildren devices, etc of the Seed Devices are included in the device group.
- **Parents of.** If you select this checkbox, all parent devices of the Seed Devices are included in the device group.
- **Ancestors of.** This checkbox is enabled only if you select the **Parents of** checkbox. If you select this checkbox, all parent devices, grandparent devices, great grandparent devices, etc of the Seed Devices are included in the device group.
- **Related by.** This checkbox is enabled only if you select the **Children of** checkbox or the **Parents of** checkbox. You can further filter the devices in the device group by including only the children, descendents, parents, and ancestors devices that are related to the Seed Devices through one or more selected Dynamic Applications. If you select this checkbox, you can select one or more Dynamic Applications from the list of Dynamic Applications that can create relationships. Only those devices that meet all the criteria will be included in the device group.
- **Include seed devices.** This checkbox is enabled only if you select the **Children of** checkbox or the **Parents of** checkbox. If you select this checkbox, the related Seed Devices are included in the device group. Seed Devices with no relationships are not included in the group.

Seed Devices

This is the list of devices you defined in the **Device Group Rule Editor** page. You can include these devices in the device group or include only the children, descendants, parents, and ancestors of these devices.

For each Seed Device, the **Relationship Selection** page displays.

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

- **Device Name.** Name of the device. For devices running SNMP or with DNS entries, the name is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- **Category.** The ScienceLogic category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the Device-Class/Sub-Class.
- **Class / Sub-class.** The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during discovery, at the same time as the Category.
- **ID.** Device ID. This is a unique number automatically assigned to the device by SL1.
- **Organization.** The organization to which the device is assigned.
- **Collection State.** Collection state can be one of the following:
 - *Active.* SL1 is currently collecting data from the device.
 - *Disabled.* SL1 is not currently collecting data from the device.
 - *Unavailable.* The device is currently unavailable, so SL1 cannot collect data from the device at this time.
 - *Component Vanished.* The component device has vanished, i.e. is not currently being reported by its root device. SL1 cannot collect data from the device at this time.
- **Tools.** Displays icons for managing devices. The choices are:
 - *Device Management* . Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the Device Management tools.


Matched Devices

This is the list of devices that match all the criteria in the **Relationship Selection** page.

For each Matched Device, the **Relationship Selection** page displays:

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


- **Device Name.** Name of the device. For devices running SNMP or with DNS entries, the name is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- **Category.** The ScienceLogic category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the Device-Class/Sub-Class.
- **Class / Sub-class.** The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during discovery, at the same time as the Category.
- **ID.** Device ID. This is a unique number automatically assigned to the device by SL1.
- **Organization.** The organization to which the device is assigned.

- **Collection State.** Collection state can be one of the following:
 - *Active.* SL1 is currently collecting data from the device.
 - *Disabled.* SL1 is not currently collecting data from the device.
 - *Unavailable.* The device is currently unavailable, so SL1 cannot collect data from the device at this time.
 - *Component Vanished.* The component device has vanished, i.e. is not currently being reported by its root device. SL1 cannot collect data from the device at this time.
- **Tools.** Displays icons for managing devices. The choices are:
 - *Device Management* (). Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the Device Management tools.

Click the [OK] button to accept all changes and exit the Relationship Selection page.

Editing and Deleting Dynamic Rules

To edit a dynamic rule:

1. Go to the **Dynamic Rules** pane.
2. Find the dynamic rule you want to edit. Click its wrench icon (.
3. The **Device Group Rule Editor** modal page appears.
4. In the **Device Group Rule Editor** modal page, you can edit existing criteria, delete existing criteria, or add new criteria.

To delete one or more dynamic rules:

1. Go to the **Dynamic Rules** pane.
2. For each dynamic rule you want to delete, select its checkbox.
3. Click the [Del] button.
4. Each selected dynamic rule is no longer displayed in the **Dynamic Rules** pane. The device group will no longer include devices that matched the deleted dynamic rule(s).

Creating Device Groups From Views

You can also create a new device group from an existing device group in the **Device Group Map** page. To learn more about creating a device group from an existing device group, see the section **Creating a Device Group from an Existing Map** in the section on [Using Device Group Views](#).

You can also create a view in Views > My Customized Maps. That new view will be saved as a device group.

A Customized Map allows you to view the devices and links that are most important to you.


When you create a Customized Map, you are also creating a new device group (which appears in the **Device Group** page). You can add devices and other sub-device groups to the new map, just as you would to a standard device group.

To learn more about how to use Customized Maps, see the manual **Views**.

Editing an Existing Device Group

You can edit the properties of an existing device group, including adding or deleting devices from the device group and adding or deleting other (child) device groups from the device group.

To edit an existing device group:


1. Go to the **Device Group** page (Registry > Devices > Device Groups).
2. In the **Device Group** page, find the device you want to edit. Click its wrench icon (.
3. The **Device Group Editor** page appears, populated with values from the selected device group.

Device Group Editor | Editing group [8] New Guide Reset

Device Group Name: em7_appliances

Force Child Visibility?: [Yes]

Sharing Permissions: [Shared with users in your organizations]

Icon: 

Visibility:

- [Maps/Views]
- [Config Policies/Bulk Edit]
- [Notification/Automation]

Discovery:

- [Device Schedules]
- [Event Suppression]
- [RSS Feeds]

Permission Keys:

- EM7 System Administration
- Grant All
- Basic User Privileges
- Power-Pack Administration
- Provisioning Access
- Admin Portal UI Access
- IT Services
- IT Services - View
- IT Services - Administration

Static Devices and Groups | Devices [12] | Groups [0] Del Add

| Device Name | Class Sub-class | ID | Organization | |
|---------------|--------------------------------|--------------|--------------|--------------------------|
| em7 | ScienceLogic, Inc. EM7 Ir 19 | System | | <input type="checkbox"/> |
| em7_61_db_972 | ScienceLogic, Inc. EM7 G21 | System | | <input type="checkbox"/> |
| em7_ao | ScienceLogic, Inc. EM7 D 15 | System | | <input type="checkbox"/> |
| em7_ap_89 | ScienceLogic, Inc. EM7 A25 | System | | <input type="checkbox"/> |
| em7_coi1 | ScienceLogic, Inc. EM7 G20 | System | | <input type="checkbox"/> |
| em7_cu_94 | ScienceLogic, Inc. EM7 D 16 | DC - Servers | | <input type="checkbox"/> |
| em7_cu_95 | ScienceLogic, Inc. EM7 D 17 | DC - Servers | | <input type="checkbox"/> |
| em7_cu_99 | ScienceLogic, Inc. EM7 D 22 | DC - Servers | | <input type="checkbox"/> |
| em7_db | ScienceLogic, Inc. EM7 D 14 | System | | <input type="checkbox"/> |
| em7_is | ScienceLogic, Inc. EM7 Ir 18 | QA | | <input type="checkbox"/> |
| em7_is_dist | ScienceLogic, Inc. EM7 Ir 24 | QA | | <input type="checkbox"/> |
| em7_mc_85 | ScienceLogic, Inc. EM7 Ir 23 | System | | <input type="checkbox"/> |

No sub-groups in current device group.

Dynamic Rules | Rules Found [0] Del Add

Selector Type: Selector Targets

Matched Devs:

No dynamic rules in current device group.

Matched

Save Save As

4. You can edit the values in one or more of the fields in this page. For details on each field, see the section on [Creating a Device Group](#).

5. Click the **[Save]** button to save your changes to the device group.

You can also add devices to a device group from the **Device Manager** page. To add devices to an existing device group from the **Device Manager** page:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox for each device you want to add to an existing device group.
3. In the **Select Action** drop-down list, the *Add to Device Group* list shows each device group the device(s) can be added to.
4. Select the device group you want to add the device(s) to. To add the device(s), click the **[Go]** button. Depending on the Visibility setting for the device group, the selected device(s) will then appear in the **Device Group Editor**, the **Group Maps View**, the **Device Group Views** (Views > Classic Views > Device Groups), and the **Custom Device Group Map** (Views > My Customized Maps) and will inherit the properties of the device group, including scheduling, event suppression, and automation policy membership.

Assigning Devices to a Device Group During Discovery

You can add devices to a device group during discovery. To learn more about assigning devices to a device group during discovery, see the section [Assigning Device Groups and Applying Device Templates During Discovery](#).


Controlling Access to a Device Group


When creating or editing a device group, you can define the actions that can be performed with the device group and also determine which users will be allowed to access the device group. These sections will describe how to control access to a device group.

Defining the Actions for a Device Group

The **Visibility** field in the **Device Group Editor** page defines which actions can be performed with the device group.

NOTE: Users who are allowed to view the device group will automatically be allowed to perform the selected actions on the device group.

- **Visibility.** Specifies where in SL1 the device group will be visible. Choices are:
 - *Maps/Views.* If selected, the device group will appear in the **Device Group Map** page (Views > Device Maps > Device Groups).
 - *Config Policies/Bulk Edit.* If selected, the building blocks icon () is visible in the **Device Group** page. This allows you to configure all the devices in the device group using a device template.


- *Notification/Automation*. If selected, the device group will appear in the list of device groups in the **Automation Policy Editor** modal page (Registry > Run Book > Automation > Edit/Create). This page allows you to trigger an automatic action if specified criteria are met on all the devices in the device group.
- *Discovery*. If selected, the device group appears in the field **Auto-add Devices to Device Group** in the **Discovery Control Panel** page (System > Manage > Discovery). This allows you to automatically add newly discovered devices to a pre-existing device group during the discovery process.
- *Device Schedules*. If selected, the calendar icon () is visible in the **Device Group** page. This allows you to schedule downtime for all the devices in the device group. The scheduled downtime will appear in the **Maintenance Schedule** page for each device in the device group.
- *Event Suppression*. If selected, the device group will appear in the **Suppressions** tab in the **Event Policy Editor** page. In this page, you can suppress the event for all devices in the device group.
- *RSS Feeds*. If selected, the device group appears in the field **Device Group Filter** in the **Custom RSS Feeds** page (Preferences > Desktop Tools > RSS Feeds). This field allows you to filter events included in the RSS feed; only events that occur on devices in the selected device group(s) will appear in the custom RSS feed.
- *IT Services*. This is a view-only option. If this option is selected when the Device Group Editor is loaded, the device group is associated with an IT service and was created automatically by SL1. Do not select or deselect this option.

Deleting a Device Group

You can delete a device group. Deleting a device group does not delete its member devices or affect the configuration of the member devices. When you delete a device group, you can no longer manage the member devices as a group.

NOTE: When you delete a parent device-group, the child groups are **not** deleted.

To delete a device group:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).
2. In the **Device Groups** page, find the device group you want to delete. Select its checkbox. To select all device groups, click the gray checkmark ()

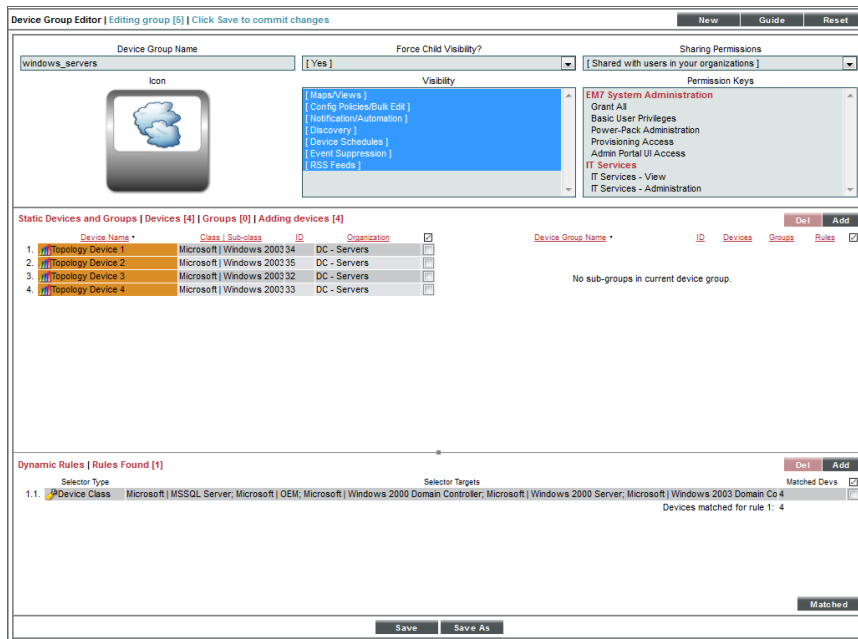
- In the **Select Action** drop-down in the bottom right of the page, select **DELETE Device Groups**.

The screenshot displays a web application interface for managing device groups. At the top, there's a header 'Device Groups | Groups Found [4]' with buttons for 'Create', 'Reset', and 'Go to'. Below this is a table with columns: Device Group Name, ID, Owner, Access, Dev Count, Grp Count, Rule Count, Edited By, and Last Edited. The table lists four groups: 'SAC ITSM Test', 'SAC Scheduler Test', 'SAC Scheduler Test (IT Service)', and 'Servers'. The 'Servers' group is selected, indicated by a minus sign and a blue background. Below the main table, there's a detailed view of the selected group, showing columns for Device Name, IP Address, Category, Class | Sub-class, ID, and Organization. This view lists 17 devices, including various database and server instances. In the bottom right corner, a 'Select Action' dropdown menu is open, showing options: 'Administrations', 'DELETE Device Groups' (which is highlighted in blue), and another 'Select Action' option. A 'Go' button is visible next to the dropdown.

- The device group is deleted and no longer appears in the list of device groups.

Example of Creating a Device Group

Here is our example device group:



- **Title.** We named our device group "windows_servers".
- **Icon.** We chose the Microsoft Windows icon.
- **Force Child Visibility.** We selected "Yes", so that the settings for the device group will apply to any future child device groups.
- **Visibility.** We selected all options, so our new device group is visible in all areas of SL1.
- **Sharing Permissions.** We selected "Shared with users in your organizations", so other users of type "user" can view the use the device group.
- **Permission Keys.** We did not select any permission keys for the device group. This means that any user who has permission to view the Registry > Devices > Device Groups page and is a member of our organization can view the device group.
- **Add Remove Devices.** We selected four Windows servers to be members of this device group.

Creating and Editing Device Templates

Overview

Device templates allow you to save a device configuration, apply it to one or more devices, and reuse the same configuration over and over again. A device template contains multiple tabs. For a list of the tabs and their descriptions, see the [What is a Device Template?](#) section.

When you apply a device template to a device group or to selected devices, all the devices that use the device template will inherit the field values from the device template. Therefore, you will not need to manually define settings for each device in the affected pages.

You can use a device template in multiple ways:

- You can apply a device template to a **device group** to automate the configuration of all devices in the device group.
- From the **Device Manager** page (Registry > Devices > Device Manager), you can apply a device template to one or more selected devices to automate the configuration of the selected devices.
- From the **Device Groups** page (Registry > Devices > Device Groups), you can use the bulk configuration tool to apply configuration settings to all the devices in a device group. These configuration settings do not have to be defined or saved in a device template.
- From the **Device Manager** page (Registry > Devices > Device Manager), you can use the bulk configuration tool to apply configuration settings to one or more selected devices. These configuration settings do not have to be defined or saved in a device template.

All the ways to use a device template are described in the section on [using device templates](#).

This chapter describes how to create a device template and how to edit a device template.

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

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

This chapter includes the following topics:

| | |
|--|-----------|
| Before You Start | 41 |
| Viewing the List of Device Templates | 41 |
| Filtering the List of Device Templates | 42 |
| <i>Special Characters</i> | 44 |
| Creating a Device Template | 45 |
| <i>Defining Device Properties and Device Thresholds in the Config Tab</i> | 48 |
| <i>Defining Interface Monitoring in the Interface Tab</i> | 53 |
| <i>Defining Web-Content Monitoring in the CV Policies Tab</i> | 58 |
| <i>Defining TCP/IP Port Monitoring in the Port Policies Tab</i> | 61 |
| <i>Defining Windows Services Monitoring in the Svc Policies Tab</i> | 63 |
| <i>Defining Process Monitoring in the Proc Policies Tab</i> | 65 |
| <i>Aligning Dynamic Applications and Defining Thresholds in the Dynamic Apps Tab</i> | 67 |
| <i>Aligning Log File Monitoring Policies in the Logs Tab</i> | 71 |
| Creating a New Device Template Based on an Existing Device Template | 73 |
| Editing an Existing Device Template | 74 |

Before You Start

Before you start creating and working with device templates, consider the following:

- How have you defined device groups? Can you apply a uniform set of configuration settings to all the devices in a device group?
- Are there multiple devices that require the same set of configuration settings? Could you create a device template to configure these devices?
- Do most of the devices in a device group require a uniform set of configuration settings, yet there are a few devices that require a different set of configuration settings? If so, you could create a child device group for the few devices that require a different set of configuration settings. You could apply one device template to the parent device group and another device template to the child device group.


Viewing the List of Device Templates

To view a list of existing device templates:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).

| Configuration Templates Templates Found [5] | | | | | | | Create | Reset | Guide |
|---|----|------------|---------------------|----------------|---------------------|--|--------|-------|-------|
| Template Name | ID | Created By | Created On | Last Edited By | Edited On | | | | |
| 1. Support: Apply Applications | 3 | em7admin | 2014-01-02 14:57:28 | em7admin | 2015-05-14 11:26:32 | | | | |
| 2. Support: Discovery Template | 2 | em7admin | 2014-01-02 14:57:28 | em7admin | 2015-05-14 11:26:32 | | | | |
| 3. UCS Template | 1 | em7admin | 2013-03-04 12:03:24 | em7admin | 2015-05-14 11:26:30 | | | | |
| 4. VMware vSphere Template | 5 | em7admin | 2013-03-06 16:44:24 | em7admin | 2015-05-14 11:26:44 | | | | |
| 5. VMware vCloud Template | 4 | em7admin | 2013-02-05 14:25:10 | em7admin | 2015-05-14 11:26:41 | | | | |

2. The **Configuration Templates** page displays the following about each device template:

- **Template Name.** Name of the configuration template.
- **ID.** Unique, numeric ID, assigned to the device template automatically by SL1.
- **Created By.** Username of the user who created the device template.
- **Created On.** Date the device template was created.
- **Last Edited By.** Username of the user who created or last edited the device template.
- **Edited On.** Date and time the device group was created or last edited.
- **Tools.** For each device template, one or more of the following tools may be available:
 - *Edit this template* (). Leads to the **Device Template Editor** page, where you can view the details of a device template and edit one or more values on a configuration template.
 - *Checkbox* (). To delete a device template, select this checkbox, select the **Select Actions** drop-down (in the lower right) and then select *Delete Template*.

Filtering the List of Device Templates

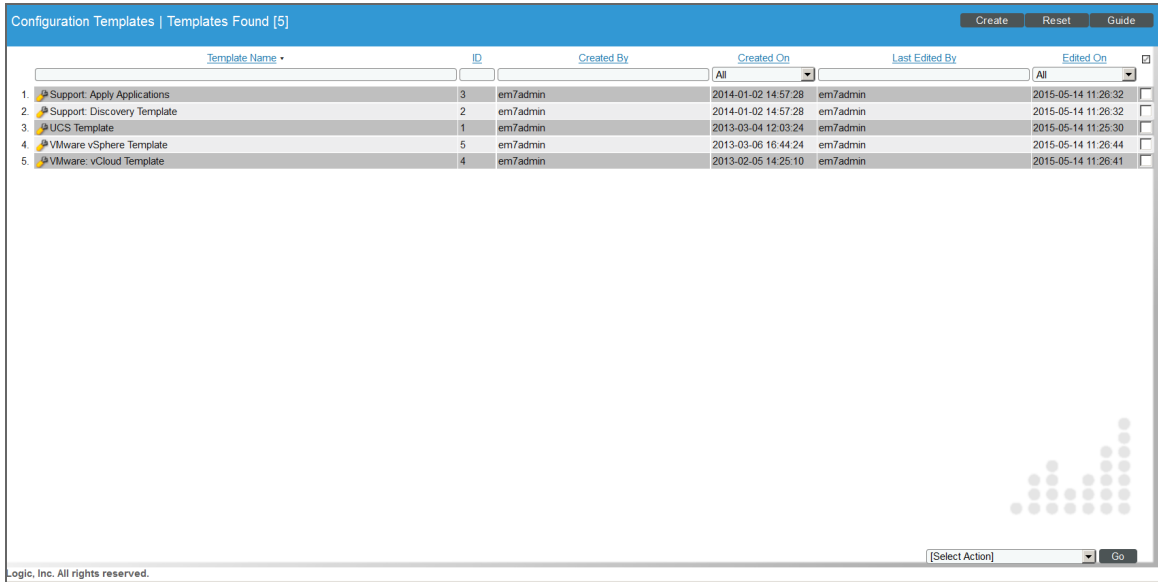
The **Configuration Templates** page includes six filters. You can filter the list of device templates by one or more of the following parameters: **Template Name**, **ID**, **Created By**, **Created On**, **Last Edited By**, and **Edited On**. You can specify one or more parameter to filter the display of device templates. Only device templates that meet all of the filter criteria will be displayed in the **Configuration Templates** page.

You can filter by one or more parameters. The list of device templates is dynamically updated as you select each filter. For each filter except **Created On** and **Edited On**, you must enter text to match against. SL1 will search for device templates that match the text, including partial matches. Text matches are not case-sensitive.

You can use *special characters* in each filter.

To filter the list of device templates:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).



Configuration Templates | Templates Found [5]

| | Template Name | ID | Created By | Created On | Last Edited By | Edited On | |
|----|-----------------------------|----|------------|---------------------|----------------|---------------------|--------------------------|
| 1. | Support: Apply Applications | 3 | em7admin | 2014-01-02 14:57:28 | em7admin | 2015-05-14 11:26:32 | <input type="checkbox"/> |
| 2. | Support: Discovery Template | 2 | em7admin | 2014-01-02 14:57:28 | em7admin | 2015-05-14 11:26:32 | <input type="checkbox"/> |
| 3. | UCS Template | 1 | em7admin | 2013-03-04 12:03:24 | em7admin | 2015-05-14 11:26:30 | <input type="checkbox"/> |
| 4. | VMware vSphere Template | 5 | em7admin | 2013-03-06 16:44:24 | em7admin | 2015-05-14 11:26:44 | <input type="checkbox"/> |
| 5. | VMware: vCloud Template | 4 | em7admin | 2013-02-05 14:25:10 | em7admin | 2015-05-14 11:26:41 | <input type="checkbox"/> |

Logic, Inc. All rights reserved. [Select Action] Go

2. The **Configuration Templates** page displays a list of device templates. To sort the list, you can enter a value in one or more of the following headings:
 - **Template Name.** Name of the device template. You can enter text to match, including special characters, and the **Configuration Templates** page will display only device templates that have a matching template name.
 - **ID.** Unique, numeric ID, assigned to the device template automatically by SL1. You can enter numbers to match, including special characters, and the **Configuration Templates** page will display only device templates that have a matching template ID.
 - **Created By.** ScienceLogic user who created the device template. You can enter text to match, including special characters, and the **Configuration Templates** page will display only device templates that were created by a matching username.
 - **Created On.** Date and time the device template was created. You can select from a list of time periods. The **Configuration Templates** page will display only device templates that were created within that time period.
 - **Last Edited By.** ScienceLogic user who last edited the device template. You can enter text to match, including special characters, and the **Configuration Templates** page will display only device templates that were edited by a matching username.
 - **Last Edited.** Date and time the device template was last edited. You can select from a list of time periods. The **Configuration Templates** page will display only device templates that were last edited within that time period.

Special Characters

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Creating a Device Template

To define a new device template, perform the following steps:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).

- Click the **[Create]** button. The **Device Template Editor** page appears:

The screenshot shows the 'Device Template Editor | Config Template Settings' page. At the top, there is a 'Template Name' input field and 'New' and 'Reset' buttons. Below this is a navigation bar with tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, displaying several sections:

- Access & Monitoring:** Includes dropdown menus for Device Organization (AWs), SNMP Read (c0sm0s (Longer Timeout)), Availability Protocol (TCP), Latency Protocol (TCP), Avail+Latency Alert (Disabled), Collection (Enabled), Coll. Type (Standard), Critical Ping (Disabled), Event Mask (Disabled), SNMP Write (None), Avail Port (ICMP), Latency Port (ICMP), and Collector Grp (CUG-Core1-COS5-mysql56-phc).
- Device Preferences:** Includes checkboxes for Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, and Disable Asset Update, along with a Bypass Interface Inventory checkbox.
- Device Retention & Basic Thresholds:** Features sliders for System Latency (100 ms), Availability Packet Size (56 bytes), Availability Ping Count (1 pings), Daily Rollup Bandwidth Data (730 days), Hourly Rollup Bandwidth Data (120 days), Raw Performance Data (7 days), and Daily Rollup Performance Data (730 days).
- Interface Inventory Settings:** Includes sliders for Interface Inventory Timeout (600000 ms) and Maximum Allowed Interfaces (10000 interfaces).

At the bottom of the form are 'Save' and 'Save As' buttons.

- In the **Template Name** field, supply a name for the template.
- You can then supply values in one or more of the following tabs:

NOTE: In each tab, all of the fields are disabled (grayed-out) by default. To enable a field and change its value, click on the field name.

- Config.** Contains all the fields in the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Device Properties** page or the **Device Thresholds** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.
- Interface.** Contains all the fields in the **Interface Properties** page that define how SL1 will monitor one or more network interfaces and the thresholds for those network interfaces. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Interface Properties** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.

- **CV Policies.** Specifies one or more web-content policies that can be applied to all devices that use the template. These web-content policies enable SL1 to monitor a website. SL1 will periodically check the website for specified content. If the content cannot be found on the website, SL1 will generate an event. When you apply a device template to a devices, you do not have to manually define any web-content and availability policies in the **Monitoring Policies** page for the devices. All the devices that use the template will inherit the web-content policies from the device template; SL1 will automatically create these web-content policies for each device that uses the template.
- **Port Policies.** Specifies one or more TCP/IP Port policies that can be applied to all member devices. These TCP/IP Port policies tell SL1 to monitor a specified port for availability every five minutes. Availability refers to the port's ability to accept connections and data. When you apply a device template to a device group, you do not have to manually define any TCP/IP port policies in the **Monitoring Policies** page for the member devices. All the devices in the device group will inherit the TCP/IP port policies from the device template; SL1 will automatically create these port policies for each device that uses the template.
- **Svc Policies.** Specifies one or more Windows service policies that can be applied to devices that use the template. These Windows service policies tell SL1 to monitor the device and look for the specified service. You can define a service policy so that SL1 monitors whether or not the service is running and then performs an action (starts, pauses, or restarts the service, reboots or shuts down the device, triggers the execution of a remote script or program). When you apply a device template to devices, you do not have to manually define any Windows service policies in the **Monitoring Policies** page for those devices. All the devices that use the template will inherit the Windows service policies from the device template; SL1 will automatically create these Windows service policies for each device that uses the template.
- **Proc Policies.** Specifies one or more Process policies that can be applied to devices that use the template. These Process policies tell SL1 to monitor the device and look for the process. You can define a process policy so that SL1 monitors whether or not the process is running and optionally, how much memory a process can use and how many instances of a process can run simultaneously. When you apply a device template to devices, you do not have to manually define any Process policies in the **Monitoring Policies** page for those devices. All the devices that use the device template will inherit the Process policies from the device template; SL1 will automatically create these process policies for each device that uses the template.

- **Dynamic Apps.** Specifies one or more Dynamic Applications that can be aligned with devices that use the template. SL1 will use the specified Dynamic Applications to retrieve data from the devices that use the template. (Note that each device that uses the template might also be aligned with additional Dynamic Applications that have been aligned with the device in other ways; for example, from the automatic alignment that occurs during discovery.) When you apply a device template to devices, you do not manually have to align Dynamic Applications in the **Dynamic Application Collections** page for those devices. All devices that use the device template will be aligned with the Dynamic Applications specified in the device template.
 - If you select a Dynamic Application in a Device Template, and that Dynamic Application has associated thresholds, you can change one or more of those thresholds from the Device Template. The thresholds you specify in the Device Template will override the thresholds defined in the Dynamic Application. When you apply a device template to devices, you do not manually have to edit the Dynamic Application Thresholds in the **Device Thresholds** page for those devices. All devices that use the device template will inherit the Dynamic Application Thresholds specified in the device template.
 - You can change the frequency at which SL1 will poll all devices that use a device template to retrieve the information specified in a Dynamic Application. This value will override the default value specified in the Dynamic Applications.
 - **Logs.** Specifies one or more Log File Monitoring Policies to apply to all devices that use the template. A Log File Monitoring Policy specifies a log file or Windows log that the SL1 agent will monitor on a device and the logs that the SL1 agent will send to SL1. When the SL1 agent sends a log to SL1, SL1 displays the log entry in the Device Logs for the associated device. SL1 can then use that log entry to trigger events. When you apply a device template to devices, you do not have to manually define any log monitoring policies in the Log File Monitoring page for those devices. All of the devices that use the device template will inherit the log monitoring policies from the device template; SL1 will automatically align the log monitoring policy with each device that uses the template.
5. In each tab in a device template, you can choose to define all the fields or you can choose to define only one or more fields. When you apply the configuration template to devices, only those fields you defined in the template will be applied to the devices. For the remaining fields, the devices will retain their previous values or use the default values.
 6. If you see a grayed-out field in a device template, this means that the template will not change the current value for that field; the devices that use this template will retain their previous values or use the default values for that field. To change the value of a grayed-out field, simply click on the field and edit the value.

Defining Device Properties and Device Thresholds in the Config Tab

The **[Config]** tab allows you to define the configuration settings from the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page.

In the **[Config]** tab, you can define one or more of the following fields:

NOTE: In the **[Config]** tab, you can choose to define all the fields from the **Device Properties** page and the **Device Thresholds** page or you can choose to define only one or more fields. When you apply the device template to devices, only those fields you defined in the template will be applied to the devices. For the remaining fields, the devices will retain their previous values or use the default values. When you have disabled a field, it appears grayed-out in the device template.

- **Device Organization.** Organization that will become the parent organization for the device. You can select from a list of all organizations in SL1.

NOTE: If you include a device template in a PowerPack and then install the PowerPack on a different SL1 system, the **Device Organization** field will be cleared and disabled on the SL1 system where the PowerPack is installed. For details, see the manual on **PowerPacks**.

- **SNMP Read.** The community string for read-only access to SNMP information on the device. The community string is a password that allows SL1 to gather information from the device. This community string is defined in the **Credential Management** page (System > Manage > Credentials).


- **SNMP Write.** The community string for write access to SNMP information on the device. The community string is a password that allows SL1 to send information to the device. This community string is defined in the **Credential Management** page (System > Manage > Credentials).
- **Availability Protocol.** Protocol that SL1 will use to communicate with the device to determine the device's availability. Choices are *TCP, UDP, or ICMP*.
- **Avail Port.** Port that SL1 will use to communicate with the device to determine the device's availability.
- **Latency Protocol.** Protocol that SL1 will use to communicate with the device to determine the device's latency. Choices are *TCP, UDP, or ICMP*.
- **Latency Port.** Port that SL1 will use to communicate with the device to determine 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.
- **Collection.** Specifies whether SL1 will collect data from the device . Choices are "enabled" or "disabled".
- **Collector Grp.** Specifies the collector group that SL1 will use to collect data from the device. You can select from a list of existing collector groups.
- **Coll. Type.** Specifies how SL1 should perform discovery. The choices are:
 - *Standard.* SL1 will perform discovery of each device based on the device's IP address. This method is appropriate for devices using standard DNS.
 - *DHCP.* SL1 will perform discovery of each device based on the device's MAC address. This method is appropriate for devices using DHCP.

- **Critical Ping.** Frequency with which SL1 should "ping" the device. If the device does not respond, SL1 creates an event. The choices are *disabled*, *every 5 seconds*, *every 15 seconds*, *every 30 seconds*, *every 60 seconds*, and *every 120 seconds*.

NOTE: SL1 does not use data from the critical ping to create device availability reports. SL1 will continue to collect device availability data only every five minutes.

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

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

- **Event Mask.** Events that occur on a single device within the selected time interval are grouped together. This allows related events to be rolled-up and posted together, under one event description. Select a time span from the drop-down list. Values range from 30 seconds to 1 month.
- **Auto-Clear Events.** Auto Clear automatically removes an event from the **Event Console** if a specified succeeding event occurs. For example, suppose the event "Device not responding to ping" occurs. If the next polling session produces the event "Device now responding normally to ping", the Auto Clear feature could clear the event. If you do not want events to be cleared automatically, uncheck this field. For the selected device, this field overrides the global auto-clear settings in the **Event Policy Editor** page.
- **Accept All Logs.** This checkbox specifies whether or not you want to keep and save all logs for this device. If you want to retain only logs associated with events, uncheck this field.
- **Daily Port Scans.** This checkbox specifies whether or not you want SL1 to perform a daily scan of the device for open ports.
- **Auto-Update.** This checkbox specifies whether or not you want SL1 to perform a nightly discovery of the device and update records with changes to the device. If this field is unchecked, SL1 will not perform nightly discovery; changes to the device, including newly opened ports, will not be recorded by SL1.
- **Bypass Interface Inventory.** This checkbox specifies whether or not the discovery processes should discover network interfaces. This value is used during *re-discovery* (clicking the binoculars icon ()) in the **Device Properties** page) and during *nightly auto-discovery* (run automatically by SL1 every night to update device information).
 - If selected, discovery processes will not attempt to discover interfaces for each device aligned with this template.
 - If not selected, discovery processes will attempt to discover network interfaces for each device aligned with this template using the **Interface Inventory Timeout** value and **Maximum Allowed Interfaces** value for the device.
- **Scan All IPs.** If selected, SL1 will scan all IP addresses on a device when looking for open ports. If the device uses multiple IP Addresses, SL1 will scan for open ports on all IPs during initial dynamic-discovery and nightly



dynamic-discovery.

- **Dynamic Discovery.** If selected, SL1 will automatically assign the appropriate Dynamic Applications to the device during discovery.
- **Preserve Hostname.** If selected, the name of the device in SL1 will remain the same, even if the name of the actual device is changed. If unselected, the SL1 name for the device will be updated if the name of the actual device is changed.
- **Disable Asset Update.** If selected, during nightly discovery, SL1 will not update the asset record associated with the device. For the selected device, this checkbox over-rides any settings defined in the **Asset Automation** page (System > Settings > Assets).
- **System Latency.** During polling, SL1 initially pings monitored devices. The value in this field is the maximum number of milliseconds for the device to respond to SL1's ping (round-trip time divided by 2). When the latency threshold is exceeded, SL1 generates an event for that device. The default value is 1500 ms. **To disable this threshold** for the current device, set the threshold to 0 (zero) milliseconds. When you disable a threshold, SL1 does not generate an event for the threshold.
- **Availability Ping Count.** If the **Availability Protocol** for a device is set to *ICMP*, this field specifies the number of packets that should be sent during each availability check. The default value is 1.
- **Availability Packet Size.** If the **Availability Protocol** for a device is set to *ICMP*, this field specifies the size of each packet, in bytes, that is sent during each availability check. The default value is 56 bytes.
- **Availability Required Ping Percentage.** If the **Availability Protocol** for a device is set to *ICMP*, this field specifies the percentage of packets that must be returned during an availability check for SL1 to consider the device available. The default value is 100%.
- **Device Logs Max.** Maximum number of records to store in the device log. When a log file reaches its maximum size, the oldest records will be deleted. The default value is 495,000 records.
- **Device Logs Age.** Maximum number of days to store each record in the device log. Records that are older than the specified number of days are automatically deleted. The default value is 546 days.
- **Bandwidth Data.** Number of days to retain bandwidth usage data and CBQoS bandwidth data collected from each interface on a device. This data is collected as frequently as every minute (depending upon the user-defined monitoring policy). Bandwidth data that is older than the specified number of days is automatically deleted. The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Daily Rollup Bandwidth Data.** Number of days to retain daily normalized data and daily normalized CBQoS data for each interface on a device. Daily normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Hourly Rollup Bandwidth Data.** Number of days to retain hourly normalized data and hourly normalized CBQoS data for each interface on a device. Hourly normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Raw Performance Data.** Number of days to store raw performance data (usually data collected by Dynamic Applications).

- **Daily Rollup Performance Data**. Number of days to retain daily normalized performance data for the device. This setting applies to daily normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific **Daily Rollup Retention** setting has not been defined. Daily normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Hourly Rollup Performance Data**. Number of days to retain hourly normalized performance data for the device. This setting applies to hourly normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific **Hourly Rollup Retention** setting has not been defined. Hourly normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Journal Data**. Number of days to retain raw collected data from Dynamic Applications of type "journal." The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).
- **Configuration Data**. Number of days to retain data from Dynamic Applications of type "configuration." The default value is defined in the Data Retention Settings page (System > Settings > Data Retention).

NOTE: In SL1, normalized data does not include polling sessions that were missed or skipped. So for normalized data, null values are not included when calculating maximum values, minimum values, or average values.

TIP: You might want to retain normalized data for longer periods of time and non-normalized data for shorter periods of time. This allows you to save space and still create historical reports.

- **Interface Inventory Timeout**. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop scanning the device, will not update the device, and will continue with discovery. When a value for this setting is specified for a device in the Device Thresholds page or applied to a device using a device template, this setting is used during *re-discovery* (clicking the binoculars icon ()) in the Device Properties page) and during *nightly auto-discovery* (run automatically by SL1 every night, to update device information). The default value is 600,000 ms (10 minutes).
- **Maximum Allowed Interfaces**. Maximum number of interfaces per device. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not update the device, and will continue with discovery. When a value for this setting is specified for a device in the Device Thresholds page or applied to a device using a device template, this setting is used during *re-discovery* (clicking the binoculars icon ()) in the Device Properties page) and during *nightly auto-discovery* (run automatically by SL1 every night, to update device information). The default value is 10,000.

Defining Interface Monitoring in the Interface Tab

The **[Interface]** tab allows you to define one or more fields from the **Interface Properties** page; these fields define how SL1 will monitor one or more network interfaces and the thresholds for those network interfaces. Each field that you define will be applied to all the devices that use the template.

In the **[Interface]** tab, you can define one or more of the following fields:

- **Apply Settings To.** Specifies which interfaces should use the settings defined in this tab. The choices are:
 - *All Interfaces on device.* Applies the settings to all discovered network interfaces on each member device.
 - *Management interface only.* Applies the settings only to the interface that SL1 uses to communicate with each member devices.
- **Collection State.** This field can have one of two values:
 - *Enabled:* SL1 monitors the network interface and collects data on the network interface for reports.
 - *Disabled:* SL1 does not monitor the network interface or collect data on the network interface for reports.

- **Collection 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 selected intervals.

- **Interface Alerting.** Alerting for this interface can be enabled or disabled. When disabled, the interface is monitored, but events are not generated for the interface.
- **Rollover Alerting.** 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 rollover frequently.
- **Collect Errors.** Specifies whether or not SL1 will collect data on packet errors on the interface. Packet errors occur when packets are lost due to hardware problems such as breaks in the network or faulty adapter hardware.
- **Collect Discards.** Specifies whether or not SL1 will collect data on interface discards. Discards occur when an interface receives more traffic than it can handle (either 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.
- **Measurement Scale.** Unit of measurement for bandwidth reports for the interface. The choices are:
 - Mega
 - Giga
 - Kilo
 - Tera
 - Peta

- **Percentile Calculation.** 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 interfaces. Billing is at the specified percentile point.

- **Counter Type.** Specifies whether the interface uses a 32-bit counter or a 64-bit counter to measure bandwidth on the interface. During 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 1.85×10^{16} 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.
 - *Counter 32.* Specify that the interface uses a 32-bit counter.
 - *Counter 64.* Specify that the interface uses a 64-bit counter.

- **Percentile Factor.** Many service providers use a percentile bandwidth measure when billing customers for bandwidth usage. In this field, you can select the percentile factor, and SL1 will perform the calculations for you at billing time. For example, if a provider chose the percentile factor "95", SL1 would collect bandwidth data every five 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. The choices for percentile factor are:
 - 100% - 1%, in increments of 1%.

- **Auto Name Update.** Specifies whether SL1 should update or overwrite the interface name during nightly discovery.

- **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}. You can use a combination of string text and the following tokens to define the interface name format for events, such as string_{name}, string_{alias}, {name} {alias}, or {ifdesc}:
 - {alias}
 - {name}
 - {state}
 - {ifdescr}
 - {if_id}

- {did}
- {ifindex}
- {ifphysaddress}
- {iftype}
- {ifspeed}
- {ifhighspeed}
- {ifoperstatus}
- {ifadminstatus}

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*.

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 threshold or the custom threshold you define in this pane.

- **Inbound %.** If the rate of inbound transfer on the interface is greater than the value selected in this field, SL1 will generate an event. Possible choices are 0% through 100%. The value can include up to three digits after the decimal point. The percentage is in relation to all traffic on the interface. So if inbound transfer on this interface exceeds the selected percentage of all traffic, SL1 will generate an event. The default value is 65%.
- **Outbound %.** If the rate of outbound transfer on the interface is greater than the value selected in this field, SL1 will generate an event. Possible choices are 0% through 100%, in increments of 1%. The percentage is in relation to all traffic on the interface. So if outbound transfer on this interface exceeds the selected percentage of all traffic, SL1 will generate an event. The default value is 65%. The value can include up to three digits after the decimal point.
- **Inbound Bandwidth.** If the rate of inbound transfer on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 Mbps (no alerting). The value can include up to three digits after the decimal point.
- **Outbound Bandwidth.** If the rate of outbound transfer on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 Mbps (no alerting). The value can include up to three digits after the decimal point.
- **Inbound Errors.** If the number of inbound packet errors on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 packets (no alerting). The value can include up to three digits after the decimal point.

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

- **Outbound Errors.** If the number of outbound packet errors on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 packets (no alerting). The value can include up to three digits after the decimal point.
- **Inbound Discards.** If the number of inbound discards on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 packets (no alerting). The value can include up to three digits after the decimal point.

NOTE: Packet discards occur when an interface receives more traffic than it can handle (either very large message or many messages simultaneously). Discards can also occur when an interface has been specifically configured to discard. For example, a user might configure a router's interface to discard packets from a non-authorized IP.

- **Outbound Discards.** If the number of outbound discards on the interface is greater than the value selected in this field, SL1 will generate an event. The default value is 0 packets (no alerting). The value can include up to three digits after the decimal point.
- **Inbound Error %.** If the percentage of inbound errors (that is, the percentage of all inbound traffic during a single polling session that results in an error) on this interface is greater than the value selected in this field, SL1 will generate an event. The value can include up to three digits after the decimal point.
- **Outbound Error %.** If the percentage of outbound errors (that is, the percentage of all outbound traffic during a single polling session that results in an error) on this interface is greater than the value selected in this field, SL1 will generate an event. The value can include up to three digits after the decimal point.
- **Inbound Discard %.** If the percentage of inbound discards (that is, the percentage of all inbound traffic during a single polling session that results in a discard) on this interface is greater than the value selected in this field, SL1 will generate an event. The value can include up to three digits after the decimal point.
- **Outbound Discard %.** If the percentage of outbound discards (that is, the percentage of all outbound traffic during a single polling session that results in a discard) on this interface is greater than the value selected in this field, SL1 will generate an event. The value can include up to three digits after the decimal point.

Defining Web-Content Monitoring in the CV Policies Tab

The **[CV Policies]** tab allows you to define one or more web-content and availability policies. These policies enable SL1 to monitor a website. SL1 will periodically check the website for specified content. If the content cannot be found on the website, SL1 will generate an event.

In the [CV Policies] tab, you can define one or more of the following fields:

- **Subtemplate Selection.** In this pane, you can choose to add a new Web Content Monitoring policy to the configuration template or edit an existing Web Content Monitoring policy in the configuration template.
 - **To add a new Web Content Monitoring policy to the configuration template,** select *Add New CV Sub-template*.
 - **To edit an existing Web Content Monitoring policy,** highlight it. The remaining panes will be populated with values from the selected policy.
- **Policy Name.** Name of the new policy. Can be any combination of letters and numbers.
- **State.** Specifies whether or not the policy is active. You can select one of the following:
 - *Enabled.* Policy is active. SL1 will query the specified website every five minutes.
 - *Disabled.* Policy is not active.
- **Port.** Port on web-server to which SL1 will send queries. This is usually port 80 (the HTTP port) or port 443 (the HTTPS port).
- **Timeout.** After specified number of seconds, SL1 should stop trying to connect to the website, or if already connected, stop searching for content. If the timeout period elapses before SL1 can connect or find the content, an event is generated.

- **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 following variable in this field:
 - **%D**. SL1 replaces this variable with the IP address of the currently aligned device.
 - **%N**. SL1 replaces this variable with the hostname of the currently aligned device.
- **Post String**. If the URL is very long or requires data that cannot be transferred with a standard "GET" request (that is, data that cannot be included in the URL), you can enter a POST string in this field. The data will be sent with the cURL equivalent of an HTTP POST command. Data should be formatted as follows:
 - variable=value
 - If you are going to include more than one variable/value pair, separate each pair with an ampersand.
 - For example, suppose you want to send values for the following fields:
 - Birthyear
 - Value
 - You could enter the following in the Post String field:
 - Birthyear=1980%Value=OK

NOTE: If you want to include non-alphanumeric characters in the **Post String** field, make sure you encode the characters using appropriate URL encoding.

- **Cookie Value**. For pages that require a cookie value to be set, enter the cookie value in this field.
- **Browser Emulation**. Specifies how to format the query. Select the agent that is compatible with the web server.
- **HTTP Auth Username:Password**. For websites that pop-up a dialog box asking for username and password, use this field. Enter the user name and password in this field. Use the format "username:password".
- **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**. Regular expression to search for.
- **Expression Check #2**. Another regular expression to search for.
- **Error Codes**. Specifies the HTTP status code you expect to receive in the response. If any other status code is returned, SL1 will generate an event.
- **Referer String**. URL of the website. Some load-balanced configurations will not allow a request for a specific IP address. If you entered a specific IP address in the URL field, you can spoof a URL in this field.

- **Host Resolution**. Host name of the website. Some load-balanced configurations will not allow a request for a specific IP address. If you entered a specific IP address in the URL field, you can spoof a fully-qualified host name in this field. You can include the following variable in this field:
 - `%N`. SL1 replaces this variable with hostname of the currently aligned device.
- **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 "username:password".
- **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 exceeded 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."

Defining TCP/IP Port Monitoring in the Port Policies Tab

The **[Port Policies]** tab allows you to define one or more TCP/IP Port policies (otherwise defined in the **Monitoring Policies** page for a device). These TCP/IP Port policies tell SL1 to monitor a specified port for availability every five minutes. Availability refers to the port's ability to accept connections and data.

In the **[Port Policies]** tab, you can define one or more of the following fields:

- **Subtemplate Selection.** In this pane, you can choose to add a new TCP/IP Port Monitoring policy to the configuration template or edit an existing TCP/IP Port Monitoring policy in the configuration template.
 - **To add a new Port Monitoring policy to the configuration template,** click *Add New Port Sub-template*.
 - **To edit an existing Port Content Monitoring policy,** highlight it. The remaining panes will be populated with values from the selected policy.
- **Add Policy To.** Specifies how the template should apply the TCP/IP Port Monitoring policy. Choices are:
 - *All devices.* SL1 will apply the TCP/IP Port Monitoring policy to each device aligned with this configuration template.
 - *Only devices whose IP(s) have a matching port.* SL1 will apply the TCP/IP Port Monitoring policy only to those devices where the port is available.

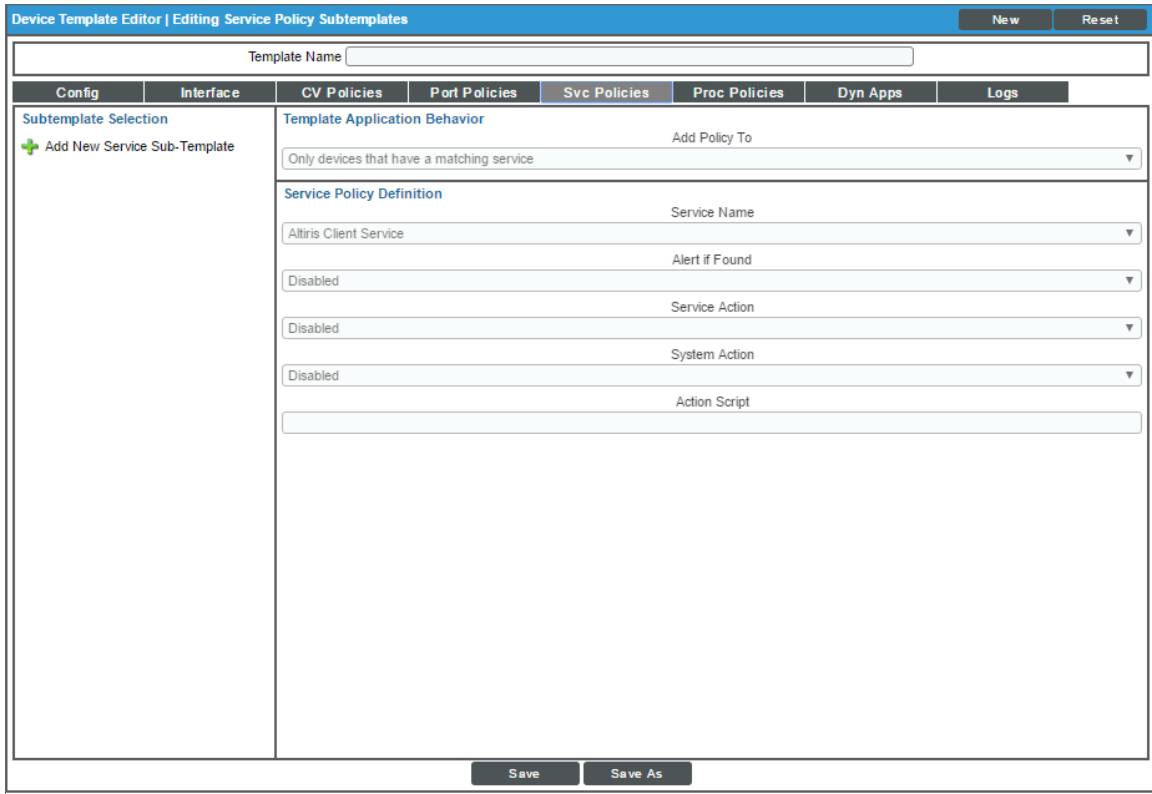
- **Per-IP Policy Creation.** Specifies whether SL1 should apply the TCP/IP Port Monitoring policy to all IP addresses on each member device or only to the Admin Primary IP address. Choices are:
 - *All Device IPs.* SL1 will apply the TCP/IP Port Monitoring policy to all IP addresses on each member device.
 - *Management IP Only.* SL1 will apply the TCP/IP Port Monitoring policy only to IP address each member device uses to communicate with SL1.
- **Port/Service.** Port number and the corresponding service running on the port.
- **State.** Can be one of the following:
 - *Enabled.* Port is being monitored by ScienceLogic port Policy.
 - *Disabled.* Port is not being monitored by ScienceLogic port Policy.
- **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 60 seconds.

NOTE: SL1 does not use this ping data to create device availability reports. SL1 will continue to collect device availability at the interval specified during discovery.

Defining Windows Services Monitoring in the Svc Policies Tab

The **[Svc Policies]** tab allows you to define one or more Windows service policies (otherwise defined in the **Monitoring Policies** page for a device). These Windows service policies tell SL1 to monitor the device and look for the specified service. You can define a service policy so that SL1 monitors whether or not the service is running and then performs an action (starts, pauses, or restarts the service, reboots or shuts down the device, triggers the execution of a remote script or program).

In the [Svc Policies] tab, you can define one or more of the following fields:



- **Subtemplate Selection.** In this pane, you can choose to add a new Windows Service Monitoring policy to the configuration template or edit an existing Windows Service Monitoring policy in the configuration template.
 - **To add a new Windows Service Monitoring policy to the configuration template,** select *Add New Service Sub-template*.
 - **To edit an existing Windows Service Monitoring policy,** highlight it. The remaining panes will be populated with values from the selected policy.
- **Add Policy To.** Specifies how SL1 should apply the template to member devices. Choices are:
 - *All devices.* SL1 will apply the Windows Service Monitoring policy to each device aligned with this configuration template, even if the specified Windows service is not available on each device.
 - *Only devices that have a matching service.* SL1 will apply the Windows Service Monitoring policy only to those member devices where the service is available.
- **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.** Condition under which SL1 should create an event about the service. Choices are:
 - *Disabled.* SL1 will create an event if the service is disabled.
 - *Enabled.* SL1 will create an event if the service is enabled.
- **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 the service has the condition specified in the **Alert if Found** field, stop the service.
 - *Start Service.* If the service has the condition specified in the **Alert if Found** field, start the service.
 - *Pause Service.* If the service has the condition specified in the **Alert if Found** field, pause the service.
 - *Restart Service.* If the service has 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 the service has the condition specified in the **Alert if Found** field, reboot the computer.
 - *Shutdown System.* If the service has the condition specified in the **Alert if Found** field, shutdown the computer.
- **Action Script.** If the device is a Windows computer running a WMI agent, you can execute a script on the computer, based on the condition specified in the **Alert if Found** field. 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`.

Defining Process Monitoring in the Proc Policies Tab

The **[Proc Policies]** tab allows you to define one or more Process policies (otherwise defined in the **Monitoring Policies** page for a device). These Process policies tell SL1 to monitor the device and look for the process. You can define a process policy so that SL1 monitors whether or not the process is running and optionally, how much memory a process can use and how many instances of a process can run simultaneously.

In the **[Proc Policies]** tab, you can define one or more of the following fields:

- **Subtemplate Selection.** In this pane, you can choose to add a new Process Monitoring policy to the configuration template or edit an existing process Monitoring policy in the configuration template.
 - **To add a new Process Monitoring policy to the configuration template,** click *Add New Service Sub-template*.
 - **To edit an existing Process Monitoring policy,** highlight it. The remaining panes will be populated with values from the selected policy.
- **Add Policy To.** Specifies how SL1 should apply the template to member devices. Choices are:
 - *All devices.* SL1 will apply the Process policy to each device aligned with this configuration template, even if the specified process is not available on each device.
 - *Only devices that have a matching service.* SL1 will apply the Process Monitoring policy only to those member devices where the process is available.
- **Process Name.** The name of the process. Select from a list of all processes running on this device.
- **Process Argument.** The arguments with which the process is invoked.
- **Memory Limit.** The amount of memory each instance of the process is allowed to use. If an instance of this process exceeds this memory limit, SL1 will generate an event. The event will have a severity of "Major" and will say "process using too much memory". This is an optional field.

- **Minimum 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."
- **Maximum 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."
- **Process User.** Search for the following process user or process owner when the process is running. This field is helpful for finding processes running as root or su which should not be.

NOTE: Some hardware includes information about a process user or owner for each process in the SNMP data; some do 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.

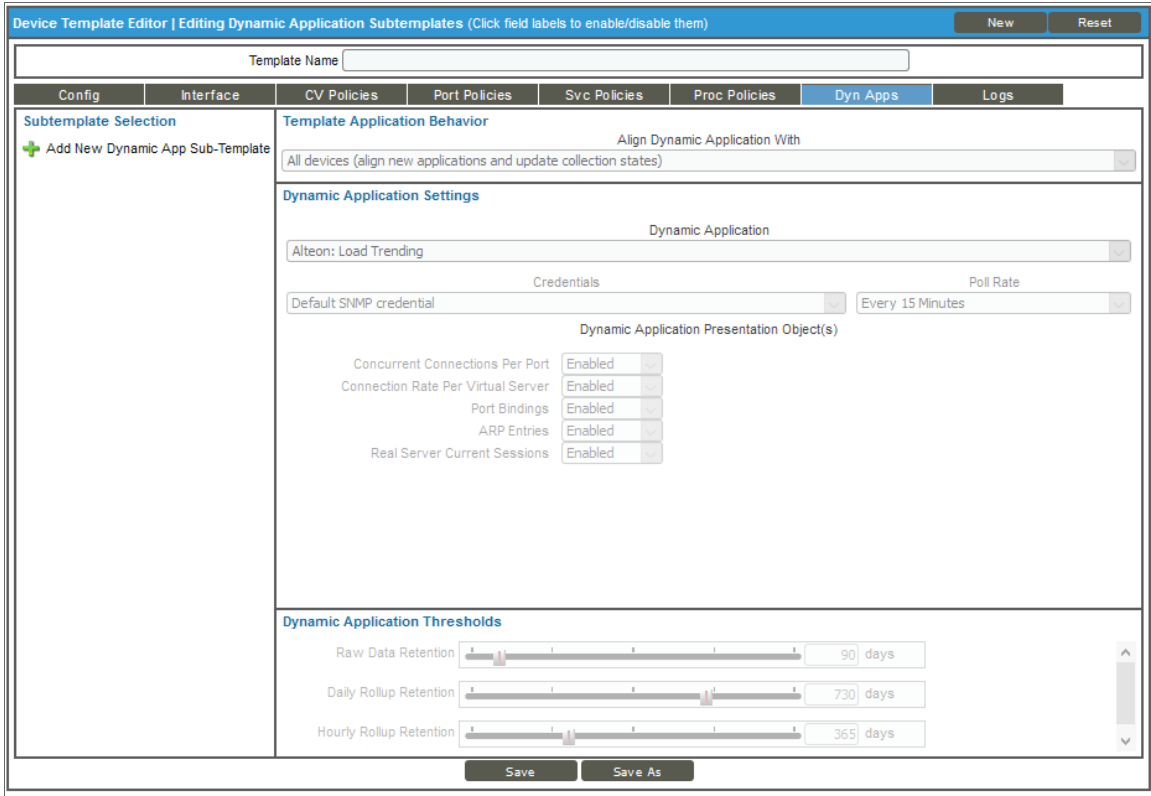
- **Alert if Found.** If you enable this option, SL1 generates an event when this process runs. The event will be of severity "major" and will say "Illicit process running."


Aligning Dynamic Applications and Defining Thresholds in the Dynamic Apps Tab

The **[Dynamic Apps]** tab allows you to select one or more Dynamic Applications to align with devices that use the device template. Dynamic Applications define which data will be collected from a device, the frequency of collection, and how the data will be displayed. When you apply a device template to a device group or selected devices, you do not have to manually align the Dynamic Applications with the devices that use the template. All devices that use the template will be aligned with the Dynamic Applications specified in the device template.

If you select a Dynamic Application in a Device Template, and that Dynamic Application has associated thresholds, you can change one or more of those thresholds in the Device Template. The thresholds in the Device Template will override the thresholds defined in the Dynamic Application. When you apply a device template to devices, you do not manually have to edit the Dynamic Application Thresholds in the **Device Thresholds** page for the devices that use the template. All devices that use the template will inherit the Dynamic Application Thresholds specified in the device template.

In the **[Dynamic Apps]** tab, you can define one or more of the following fields:



- **Subtemplate Selection.** In this pane, you can choose to add one or more existing Dynamic Application to the configuration template.
 - **To select the Dynamic Application,** click on the green plus-sign () and then select the Dynamic Application in the **Dynamic Application** field.
- **Align Dynamic Application With.** Specifies how SL1 should apply the template to member devices. Choices are:
 - *All devices (align new applications and update collection states).* SL1 will align the Dynamic Application with each device that uses the template, even if the SL1 cannot use the Dynamic Application to retrieve data from one or more of those devices.
 - *Only devices that are already aligned to this application (update collection states only).* SL1 will apply the settings for this Dynamic Application only to each device that both uses this template and is already aligned with the specified Dynamic Application.
- **Dynamic Application.** Select the Dynamic Application to include in the device template. You can select from a list of all Dynamic Applications.

- **Credentials.** Select a credential for the selected Dynamic Application. You can select from a list of credentials that are appropriate for the Dynamic Application. For example, if you select a Dynamic Application of type "SNMP Performance", the **Credentials** field will allow you to select from a list of SNMP credentials.
- **Poll Rate.** Frequency, in minutes, at which SL1 will poll all devices that use this device template and retrieve the information specified in this Dynamic Application. You can use this field to set a custom polling frequency for one or more devices. This value over-rides the default value for the Dynamic Application (defined in the **Dynamic Applications Properties Editor** page). The default value is "1". Select from the pull-down menu. The choices range from 1 minute to 24 hours.
- **Dynamic Application Presentation Object(s).** This pane displays a list of presentation objects (for Dynamic Applications of type "Performance") or collection objects (for Dynamic Applications of type "Configuration").

- A **collection object** is a data point that is monitored by the Dynamic Application. At the polling frequency specified in the Dynamic Application, SL1 will retrieve a value for that data point.

For example, suppose you have a Dynamic Application named "Cisco: Environmental Status".

- This Dynamic Application contains a collection object named "fan_state". The collection object will contain the current status of a fan.
- This Dynamic Application is aligned with the device "cisco_catalyst".
- The Dynamic Application will retrieve data from member devices every 30 minutes. This means that every 30 minutes SL1 will connect to the device "cisco_catalyst" and retrieve the value for fan status; possible values could be normal, warning, critical, and shutdown. This value will be stored in the collection object "fan_state".

For each aligned device, SL1 displays the latest value for each collection object in the **Configuration Report** page.

- You can enable or disable each collection object that appears in the **Dynamic Object Collection** pane.
 - **Enabled.** SL1 will try to collect data for this collection object at the frequency specified in the Dynamic Application. SL1 will try to collect data for this collection object from each device that uses the device template.
 - **Disabled.** SL1 will not try to collect data for this collection object.
- A **presentation object** is a definition of a report. The definition is stored in an object (a presentation object). The definition of the report is based on data retrieved with the Dynamic Application and stored in collection objects. These reports appear in the **Performance** page for each aligned device.

For example, suppose you have a Dynamic Application named "Cisco: Summary Statistics". Suppose this Dynamic Application includes the presentation object "% I/O Memory Used".

Suppose that the definition of this presentation object is "(number of broadcast packets/number of multicast packets) / 100", where "number of broadcast packets" is a collection object and "number of multicast packets" is a collection object.

Suppose that this Dynamic Application has a polling frequency of every 30 minutes and is aligned with the device "cisco_router". This means that every 30 minutes, SL1 will connect to the device "cisco_router" and retrieve the collection objects for the Dynamic Application.

SL1 will then use the values from the collection objects "number of broadcast packets" and "number of multicast packets" to calculate the value of the presentation object and then graph that value. SL1 will graph the value that results from each polling session in the **Performance** page for the aligned device.

- You can enable or disable each presentation object.
 - *Enabled*. This is the default value. For each device that uses the device template, SL1 will try to generate the report defined by the presentation object. If SL1 can successfully retrieve the data (from the collection objects specified by the presentation object) from the device, the report will appear in the **Performance** page.
 - *Disabled*. SL1 will not try to generate the report defined by the presentation object.

NOTE: As you disable a presentation object, SL1 checks the collection objects associated with the presentation object. If a collection object is used in only one presentation object, and that presentation object is disabled, SL1 will no longer collect data for the associated collection object. If a collection object is used in multiple presentation objects, and one or more of those presentation objects is still enabled, SL1 will continue to collect data for the associated collection object. If a collection object is used in multiple presentation objects, and all those presentation objects are disabled, SL1 will no longer collect data for that collection object.

- **Dynamic Application Thresholds.** This pane displays a list of *threshold objects* associated with the Dynamic Application. You can accept the default value as defined in the Dynamic Application, or you can manually change the value within this template.
 - A *threshold object* is a variable that contains a threshold value. SL1 can use this threshold value when defining alerts and presentation objects.

For example, suppose we have a Dynamic Application named "Cisco:Swap". Suppose this Dynamic Application includes two collection objects: "Free Swap", and "Used Swap". Suppose this Dynamic Application also includes a threshold object called "high_swap" with a value of "80".

We could then create an alert that uses the collection objects to specify "when swap usage exceeds the value of the threshold object (80%), trigger an alert".

We could define an event policy, based on this alert.

For each aligned device, this swap threshold will also appear in the **Device Thresholds** page.
 - **To change the value of a threshold object**, click on the name of the threshold and then move the slider. The new threshold value will be used for each device that uses the device template.
- **Raw Data Retention.** Number of days to retain raw data collected from the device using this Dynamic Application. Raw data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.

- **Crunched Data Retention**. Appears only for Journal Dynamic Applications. Number of days to retain data that has been processed using the presentation objects in this Dynamic Application. The default value is defined in the **Data Retention Settings** page.
- **Hourly Rollup Retention**. Appears only for performance Dynamic Applications. Number of days to retain hourly normalized data for this Dynamic Application. Hourly normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- **Daily Rollup Retention**. Appears only for performance Dynamic Applications. Number of days to retain daily normalized data for this Dynamic Application. Daily normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.

Aligning Log File Monitoring Policies in the Logs Tab

Log File Monitoring policies can be aligned to devices using a Device Template.


The **Logs** tab allows you to align one or more Log File Monitoring Policies with the devices that use the device template. A Log File Monitoring Policy specifies a log file or Windows log that the SL1 agent will monitor on a device and the logs that the agent will send to SL1. When the SL1 agent sends a log to SL1, SL1 displays the log entry in the **Device Logs & Messages** page for the associated device. SL1 can then use that log entry to trigger events.

In the **Logs** tab, you can:

- Apply an existing Log File Monitoring Policy to each device that uses the device template.
- Override one or more of the parameters of the selected Log File Monitoring Policy. These overrides will apply only to the devices that use this device template.

In the **Logs** tab, you can define one or more of the following fields:

The screenshot shows the 'Device Template Editor' window with the 'Logs' tab selected. The window title is 'Device Template Editor | Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)'. At the top right are 'New' and 'Reset' buttons. Below the title bar is a 'Template Name' input field. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Logs' tab is active. The interface is split into two panes. The left pane, 'Subtemplate Selection', contains a green plus icon and the text 'Add New Log Policy Sub-Template'. The right pane, 'Template Application Behavior', has a dropdown menu 'Align Log Monitoring Policy With' set to 'All compatible devices'. Below this is the 'Log Monitoring Settings' section with a dropdown 'Log Monitoring Policy' set to 'server1_logs', and three input fields for 'File Path', 'Limit', and 'Filter'. At the bottom are 'Save' and 'Save As' buttons.

- **Subtemplate Selection.** In this pane, you can choose to add one or more existing Dynamic Application to the configuration template.
 - **To align an existing Log File Monitoring Policy with the device template,** click the plus icon () in the Subtemplate pane and then supply values in one or more of the fields.
 - **To edit a Log File Monitoring Policy in device template,** go to the Subtemplate Selection pane and select the Log File Monitoring Policy you want to edit. The field in the right pane will be populated with values from the selected policy. You can then edit one or more values for the policy.

The **Logs** tab includes the following fields in the right pane:


- **Align Log Monitoring Policy With.** Select how to align the Log File Monitoring Policy. Choices are:
 - *All compatible devices.* Apply the Log File Monitoring Policy to all devices that include the SL1 agent and use an operating system supported by the type of Log File Monitoring Policy.
 - *Only devices that are already aligned to this log policy.* Apply the edited Log File Monitoring Policy only to devices that are already aligned with the Log File Monitoring Policy.
- **Log Monitoring Policy.** Select from a list of existing Log File Monitoring policies. Select the Log File Monitoring Policy you want to align with devices to which the template is applied.

The following fields allow you to override one or more settings in the Log File Monitoring Policy you selected in the **Log Monitoring Policy** field. These overrides apply only to devices that use the device template:

- **File Path**. If you selected *File* in the **Type** field, this field is displayed. Enter the full path of the file to monitor.
- **Source**. If you selected *Event Log* in the **Type** field, this field is displayed. Select the Windows log to monitor. Choices are:
 - *application*
 - *system*
 - *security*
- **Limit**. The maximum log messages the agent sends to SL1 per minute. If the number of matching logs exceeds this value, the agent will stop sending logs to the platform for the remainder of the minute. The limit resets at the beginning of the next minute. For example, suppose you set this field to *10,000*. Suppose the agent monitors a device that has 30,000 log messages. The agent will retrieve 10,000 logs and then wait until the beginning of the next minute. The agent will then retrieve the next 10,000 logs and then wait until the beginning of the next minute. The agent will continue to retrieve 10,000 logs per minute until it has retrieved all the logs from the device.
- **Filter**. Specify a regular expression that will be used to evaluate the log messages in the specified file or Windows log. If a log message matches this regular expression, the SL1 agent will send that log message to SL1. If a log message does not match this regular expression, the SL1 agent will not send that log message to SL1.

Creating a New Device Template Based on an Existing Device Template

To define a new device template based on an existing template, perform the following steps:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
2. In the **Configuration Templates** page, find the device template you want to use as a template to create a new device template. Click its wrench icon ().
3. In the **Device Template Editor** page, supply a new value in the **Name** field.

CAUTION: If you do not enter a new value in the **Name** field, SL1 will save the new device template under the same name as the existing device template, but with a different ID number. In some cases, this could make management of device templates difficult. Best practice is to supply a new name for the new device template.


4. Edit one or more fields, if desired.
5. Click the **[Save As]** button.
6. The new device template will appear in the **Configuration Templates** page.

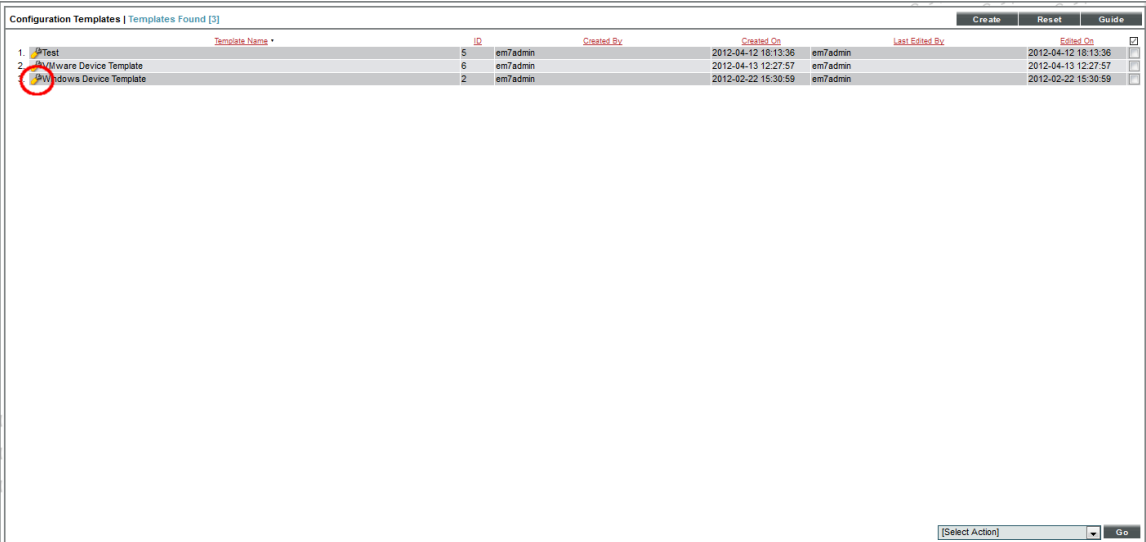
Editing an Existing Device Template


You can edit an existing device template and change one or more of its parameters.

NOTE: Device templates are not dynamic. That is, when you update or change a device template, no changes are made to any devices that have used the template in the past.

To edit a device template:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
2. In the **Configuration Templates** page, find the device template you want to edit. Click its wrench () icon.



| | Template Name | ID | Created By | Created On | Last Edited By | Edited On | |
|----|-------------------------|----|------------|---------------------|----------------|---------------------|---|
| 1. | Test | 5 | em7admin | 2012-04-12 18:13:36 | em7admin | 2012-04-12 18:13:36 |  |
| 2. | VMware Device Template | 6 | em7admin | 2012-04-13 12:27:57 | em7admin | 2012-04-13 12:27:57 |  |
| | Windows Device Template | 2 | em7admin | 2012-02-22 15:30:59 | em7admin | 2012-02-22 15:30:59 |  |

3. The **Device Template Editor** page appears, populated with values from the selected device template.

The screenshot displays the 'Device Template Editor | Config Template Settings' interface. At the top, there are 'New' and 'Reset' buttons. Below is a 'Template Name' input field. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, showing three main sections:

- Access & Monitoring:** Includes dropdowns for Device Organization (AWs), SNMP Read (c0sm0s (Longer Timeout)), Availability Protocol (TCP), Latency Protocol (TCP), Avail+Latency Alert (Disabled), Collection (Enabled), Coll. Type (Standard), Critical Ping (Disabled), and Event Mask (Disabled). It also has fields for SNMP Write (None), Avail Port (ICMP), Latency Port (ICMP), and Collector Grp (CUG-Core1-COS5-mysql56-phc).
- Device Retention & Basic Thresholds:** Features sliders for System Latency (100 ms), Availability Packet Size (56 bytes), Availability Ping Count (1 pings), Daily Rollup Bandwidth Data (730 days), Hourly Rollup Bandwidth Data (120 days), Raw Performance Data (7 days), and Daily Rollup Performance Data (730 days).
- Interface Inventory Settings:** Includes sliders for Interface Inventory Timeout (600000 ms) and Maximum Allowed Interfaces (10000 interfaces).

At the bottom, there are 'Save' and 'Save As' buttons. A 'Device Preferences' section on the right contains several checkboxes: Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, Disable Asset Update, and Bypass Interface Inventory.

4. If you see a grayed-out field in a device template, this means that when the template is applied to a device, the value for that field will not be changed. The device will either retain its current value for that field or will use the default value for that field. To change the value of a grayed-out field, simply click on the name of the field and edit the value.
5. In each tab, you can change one or more parameters. For a description of each field, see the previous sections in this chapter.
6. Click the **[Save]** button to save your changes to the device template.

Chapter

5

Using Device Templates

Overview

This chapter describes how to use a device template.

Device templates allow you to save a device configuration, apply it to one or more devices, and reuse the same configuration over and over again.

When you apply a device template to a device group or to selected devices, all the devices in the device group or all the selected devices will inherit the field values from the device template. Therefore, you will not need to manually define settings for each device in the affected pages.

You can use a device template in multiple ways:

- You can apply a device template to a **device group** to automate the configuration of all devices in the device group.
- From the **Device Manager** page (Registry > Devices > Device Manager), you can apply a device template to one or more selected devices to automate the configuration of the selected devices.
- From the **Device Groups** page (Registry > Devices > Device Groups), you can use the bulk configuration tool to apply configuration settings to all the devices in a device group. These configuration settings do not have to be defined or saved in a device template.
- From the **Device Manager** page (Registry > Devices > Device Manager), you can use the bulk configuration tool to apply configuration settings to one or more selected devices. These configuration settings do not have to be defined or saved in a device template.

NOTE: Any policies configured with a device template cannot be removed. The only action available after a policy is added to a template is editing the policy with the same device template. There is no bulk action option to add or edit policies, and no way to remove policies using a device template.

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

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

This chapter includes the following topics:

| | |
|---|----|
| <i>Before You Start</i> | 77 |
| <i>Using a Device Template to Edit the Configuration of the Devices in a Device Group</i> | 77 |
| <i>Using a Configuration Template to Edit the Configuration of One or More Individual Devices</i> | 80 |
| <i>Using the Bulk Configuration Tool to Apply Ad Hoc Settings to a Device Group</i> | 83 |
| <i>Using the Bulk Configuration Tool to Apply Ad Hoc Settings to One or More Devices</i> | 86 |
| <i>Example Device Group and Device Template</i> | 89 |
| <i>Example Device Group</i> | 90 |
| <i>Example Configuration Template</i> | 91 |

Before You Start

Before you start creating and working with device templates, consider the following:

- How have you defined device groups? Can you apply a uniform set of configuration settings to all the devices in a device group?
- Are there multiple devices that require the same set of configuration settings? Could you create a device template to configure these devices?
- Do most of the devices in a device group require a uniform set of configuration settings, yet there are a few devices that require a different set of configuration settings? If so, you could create a child device group for the few devices that require a different set of configuration settings. You could apply one device template to the parent device group and another device template to the child device group.

Using a Device Template to Edit the Configuration of the Devices in a Device Group

When you define a device group, you can select one or more devices to include in the device group. These devices have already been discovered by SL1 and include the default configuration that is applied to a device when it is initially discovered.

Device groups can also include *devices that are automatically added to the device group upon discovery*. These devices also include the default configuration that is applied to a device when it is initially discovered.

You can use a device template to change the configuration of all devices in a device group.

When you apply a device template to a device group, you can avoid manually defining the following for the member devices:

- Settings in the **Device Properties** page or the **Device Thresholds** page.
- Interface monitoring policies.
- Web-content monitoring policies.
- Port monitoring policies.
- Windows service monitoring policies.
- Process monitoring policies.
- Aligning Dynamic Applications, enabling and disabling object collection, and changing thresholds associated with Dynamic Applications.

All the devices in the device group will inherit the field values from the device template.

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Config Policies/Bulk Edit* in the **Visibility** field, you cannot apply a device template to the device group.

To use a device template to change the configuration of all devices in a device group:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).
2. In the **Device Groups** page, find the device group to which you want to apply a device template. Click its building blocks icon (🧱).

| | Device Group Name * | ID | Owner | Access | Dev_Count | Grp_Count | Rule_Count | Edited By | Last Edited | |
|-------|---|----|----------|---------|-----------|-----------|------------|-----------|---------------------|---|
| 1. + | Acme: IIS SQL database servers (IT Service) | 4 | em7admin | Shared | 1 | -- | -- | em7admin | 2012-02-27 14:03:51 | 🧱 |
| 2. + | Pcisco_switches | 6 | em7admin | Private | -- | -- | 1 | em7admin | 2012-03-05 10:50:30 | 🧱 |
| 3. + | Pdb_servers | 7 | em7admin | Private | -- | -- | 1 | em7admin | 2012-03-05 15:41:20 | 🧱 |
| 4. + | Device Group Test | 12 | em7admin | Private | -- | -- | -- | em7admin | 2012-03-05 15:07:53 | 🧱 |
| 5. + | em7_appliances | 8 | em7admin | Shared | 12 | -- | -- | em7admin | 2012-03-19 18:04:31 | 🧱 |
| 6. + | Simple Availability Service (IT Service) | 1 | em7admin | Private | 3 | -- | -- | em7admin | 2012-02-25 13:06:10 | 🧱 |
| 7. + | Test Group | 13 | em7admin | Private | 6 | -- | -- | em7admin | 2012-03-23 11:15:44 | 🧱 |
| 8. + | Testing_export | 9 | em7admin | Private | 2 | -- | -- | em7admin | 2012-03-05 11:25:46 | 🧱 |
| 9. + | WAN_circuit_1 (IT Service) | 3 | em7admin | Shared | 2 | -- | -- | em7admin | 2012-02-27 12:33:05 | 🧱 |
| 10. + | windows_servers | 5 | em7admin | Shared | 4 | -- | 1 | em7admin | 2012-05-21 17:59:08 | 🧱 |
| 11. + | Workspace_Map | 10 | em7admin | Private | -- | -- | -- | em7admin | 2012-03-05 12:21:23 | 🧱 |
| 12. + | Workspace_Map | 11 | em7admin | Private | 3 | -- | -- | em7admin | 2012-03-05 12:23:06 | 🧱 |

3. The **Bulk Device Configuration** page appears.

The screenshot displays the 'Bulk Device Configuration' window. At the top, it shows the title 'Bulk Device Configuration' and a 'Reset' button. Below this is a header bar with the text 'Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)'. The main area is divided into several sections:

- Template Selection:** A dropdown menu for 'Template' (set to 'New / One-off Template'), a checkbox for 'Save When Applied & Confirmed', and a text field for 'Template Name'.
- Navigation Tabs:** A row of tabs including 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is currently selected.
- Access & Monitoring:** A section with various settings such as 'Device Organization' (air), 'SNMP Read' (Automation Test Credential), 'SNMP Write' (None), 'Availability Protocol' (TCP), 'Latency Protocol' (TCP), 'Avail+Latency Alert' (Disabled), 'Collection' (Enabled), 'Coll. Type' (Standard), 'Critical Ping' (Disabled), and 'Event Mask' (Disabled).
- Device Preferences:** A section with checkboxes for 'Auto-Clear Events', 'Scan All IPs', 'Accept All Logs', 'Dynamic Discovery', 'Daily Port Scans', 'Preserve Hostname', 'Auto-Update', 'Disable Asset Update', and 'Bypass Interface Inventory'.
- Device Retention & Basic Thresholds:** A section with sliders for 'System Latency' (462 ms), 'Daily Rollup Bandwidth Data' (60 days), 'Availability Packet Size' (56 bytes), 'Frequent Rollup Bandwidth Data' (31 days), 'Availability Ping Count' (1 pings), 'Hourly Rollup Bandwidth Data' (48 days), and 'Raw Performance Data' (7 days).
- Interface Inventory Settings:** A section with a slider for 'Interface Inventory' (600000 ms) and a dropdown for 'Maximum Allowed' (10000 interfaces).

An 'Apply' button is located at the bottom center of the configuration area.

- In the **Template** field, select an existing device template.
- **Save When Applied & Confirmed.** From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template.
 - *If you select this field, any changes you make to fields in the **Bulk Device Configuration** page will be saved to the template.*
 - *If you don't select this field, you can edit the values in any of the fields, and the edited values won't be saved in the device template, but will be applied to the selected devices.*

4. Click the **[Apply]** button to apply the device template and any changed field values to the device group.

5. The **Device Setting Confirmation** page appears.

Bulk Device Configuration Close / Esc

Device Template Editor | Applying Template to Devices | Click [Save] to commit changes | Config Template Settings (Click field labels to edit) Reset

Setting Confirmation | The following settings will be applied

Organization: DC - Servers Dynamic Applications: 8

Device Selection Confirmation | The following devices will be altered

| | Device Name | IP Address | DID |
|----|-------------------|------------|-----|
| 1. | 10.2.2.31 | 10.2.2.31 | 29 |
| 2. | Topology Switch A | 10.40.40.2 | 36 |
| 3. | Topology Switch B | 10.40.40.3 | 37 |

Back Confirm

- In this page you can view any settings in the device template that are different from SL1 default settings.
 - You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group or selected devices.
 - You can also view a list of devices to which the device template will be applied.
6. To approve the changes and the device list, click the **[Confirm]** button in the **Device Setting Confirmation** page.
 7. The settings in the device template will be applied to the selected devices in the device group.

Using a Configuration Template to Edit the Configuration of One or More Individual Devices

You can apply a device template to one or more devices individually, rather than as part of a device group.

When SL1 discovers a device, SL1 applies some default configuration settings to that device. You can edit these settings or use a device template to edit the settings for one or more devices.

You can use a device template to change the configuration of one or more selected devices.

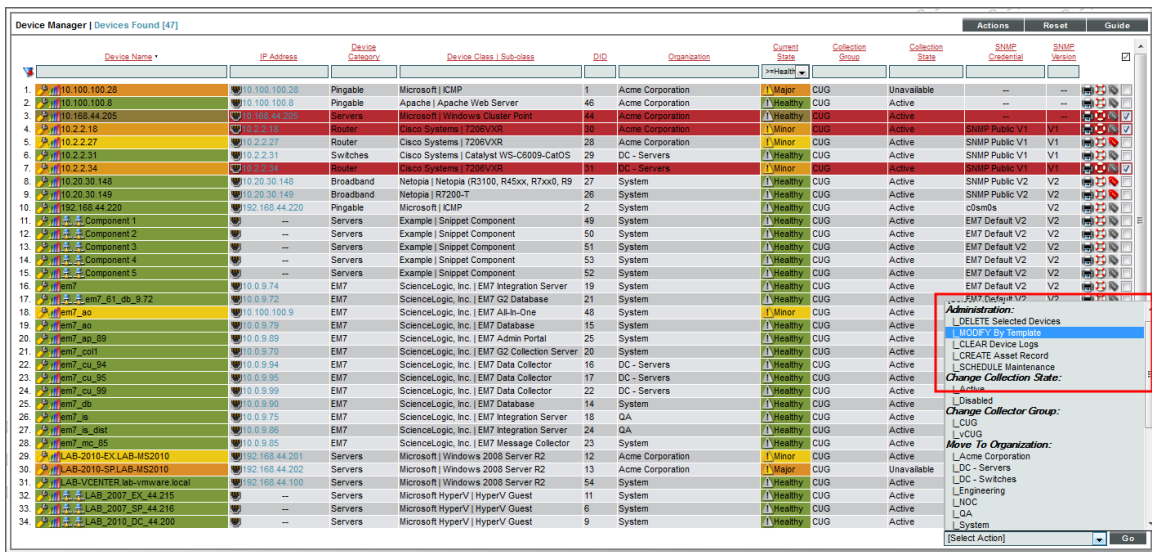
When you apply a device template to one or more devices, you can avoid manually defining the following for the devices:

- Settings in the **Device Properties** page or the **Device Thresholds** page.
- Interface monitoring policies.
- Web-content monitoring policies.
- Port monitoring policies.
- Windows service monitoring policies.
- Process monitoring policies.
- Aligning Dynamic Applications, enabling and disabling object collection, and changing thresholds associated with Dynamic Applications.

All the selected devices will inherit the field values from the device template.

To use a device template to change the configuration of one or more devices:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox for each device you want to apply a device template to.



3. In the **Select Actions** field, in the lower right, select the option **Modify by Template**. Click the **[Go]** button.

4. The **Bulk Device Configuration** page appears.

The screenshot displays the 'Bulk Device Configuration' window. At the top, there's a title bar and a sub-header 'Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)'. Below this, there are fields for 'Template' (set to 'New / One-off Template'), 'Save When Applied & Confirmed' (checkbox), and 'Template Name'. A navigation bar contains tabs: 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, showing sections: 'Access & Monitoring' (with fields for Device Organization, SNMP Read/Write, Availability/Latency Protocols, Alert, Collection, Coll. Type, Critical Ping, Event Mask), 'Device Preferences' (with checkboxes for Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, Disable Asset Update, Bypass Interface Inventory), 'Device Retention & Basic Thresholds' (with sliders for System Latency, Availability Packet Size, Availability Ping Count, and rollup bandwidth data), and 'Interface Inventory Settings' (with fields for Interface Inventory and Maximum Allowed). An 'Apply' button is at the bottom center.

- In the **Template** field, select an existing device template.
- **Save When Applied & Confirmed**. From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template.
 - If you select this field, any changes you make to fields in the **Bulk Device Configuration** page will be saved to the template.
 - If you don't select this field, you can edit the values in any of the fields, and the edited values won't be saved in the device template, but will be applied to the device group.

5. Click the **[Apply]** button to apply the device template and any changed field values to the selected devices.

6. The **Device Setting Confirmation** page appears.

Bulk Device Configuration Close / Esc

Device Template Editor | Applying Template to Devices | Click [Save] to commit changes | Config Template Settings (Click field labels to edit) Reset

Setting Confirmation | The following settings will be applied

| | |
|----------------------------|-------------------------|
| Organization: DC - Servers | Dynamic Applications: 8 |
|----------------------------|-------------------------|

Device Selection Confirmation | The following devices will be altered

| | Device Name | IP Address | DID |
|----|-------------------|------------|-----|
| 1. | 10.2.2.31 | 10.2.2.31 | 29 |
| 2. | Topology Switch A | 10.40.40.2 | 36 |
| 3. | Topology Switch B | 10.40.40.3 | 37 |


Back Confirm

- In this page, you can view any settings in the device template that are different from SL1 default settings.
- You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group or selected devices.
- You can also view a list of devices to which the device template will be applied.

7. To approve the changes and the device list, click the **[Confirm]** button in the **Device Setting Confirmation** page.


8. The device template will be applied to the selected devices.

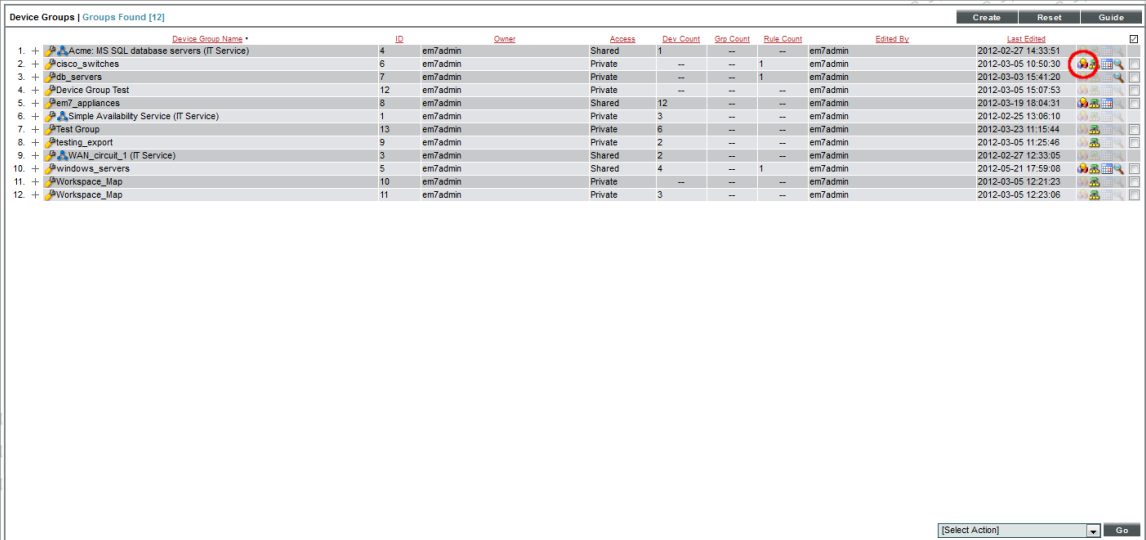
Using the Bulk Configuration Tool to Apply Ad Hoc Settings to a Device Group













You can use the bulk configuration tool () in the **Device Groups** page to apply one or more settings that are usually defined in a device template to a device group. You can apply settings that are not currently saved in a device template and then exit the bulk configuration tool without saving the settings as a device template. In effect, you can manually apply configuration settings to one or more devices, without creating or saving a device template.

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Config Policies/Bulk Edit* in the **Visibility** field, you cannot perform bulk configuration to the device group.

To use the bulk configuration tool to apply settings to a device group:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).
2. In the **Device Groups** page, find the device group to which you want to apply configuration settings. Click its building blocks icon ()



| | Device Group Name | ID | Owner | Access | Dev. Count | Grp. Count | Bulk Count | Edited By | Last Edited | |
|-------|--|----|----------|---------|------------|------------|------------|-----------|---------------------|---|
| 1. + | Acme: MS SQL database servers (IT Service) | 4 | em7admin | Shared | 1 | -- | -- | em7admin | 2012-02-27 14:33:51 |  |
| 2. + | Cisco_switches | 6 | em7admin | Private | -- | -- | 1 | em7admin | 2012-03-05 10:50:30 |  |
| 3. + | db_servers | 7 | em7admin | Private | -- | -- | 1 | em7admin | 2012-03-03 15:41:20 |  |
| 4. + | Device Group Test | 12 | em7admin | Private | -- | -- | -- | em7admin | 2012-03-05 15:07:53 |  |
| 5. + | em7_appliances | 8 | em7admin | Shared | 12 | -- | -- | em7admin | 2012-03-19 18:04:21 |  |
| 6. + | Simple Availability Service (IT Service) | 1 | em7admin | Private | 3 | -- | -- | em7admin | 2012-02-25 13:06:10 |  |
| 7. + | Test Group | 13 | em7admin | Private | 6 | -- | -- | em7admin | 2012-03-23 11:15:44 |  |
| 8. + | Testing_export | 9 | em7admin | Private | 2 | -- | -- | em7admin | 2012-03-05 11:25:46 |  |
| 9. + | WAN_circuit_1 (IT Service) | 3 | em7admin | Shared | 2 | -- | -- | em7admin | 2012-02-27 12:33:05 |  |
| 10. + | windows_servers | 5 | em7admin | Shared | 4 | -- | 1 | em7admin | 2012-05-21 17:59:08 |  |
| 11. + | Workspace_Map | 10 | em7admin | Private | -- | -- | -- | em7admin | 2012-03-05 12:21:23 |  |
| 12. + | Workspace_Map | 11 | em7admin | Private | 3 | -- | -- | em7admin | 2012-03-05 12:23:06 |  |

3. The **Bulk Device Configuration** page appears.

The screenshot displays the 'Bulk Device Configuration' window. At the top, it shows the title 'Bulk Device Configuration' and a 'Reset' button. Below this is a header bar with the text 'Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)'. The main area is divided into several sections:

- Template Selection:** A dropdown menu set to 'New / One-off Template', a checkbox for 'Save When Applied & Confirmed', and a 'Template Name' input field.
- Navigation Tabs:** A row of tabs including 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is currently selected.
- Access & Monitoring:** A section with various dropdown menus and checkboxes, including 'Device Organization' (air), 'SNMP Read' (Automation Test Credential), 'SNMP Write' (None), 'Availability Protocol' (TCP), 'Latency Protocol' (TCP), 'Avail+Latency Alert' (Disabled), 'Collection' (Enabled), 'Coll. Type' (Standard), 'Critical Ping' (Disabled), and 'Event Mask' (Disabled).
- Device Preferences:** A section with checkboxes for 'Auto-Clear Events', 'Scan All IPs', 'Accept All Logs', 'Dynamic Discovery', 'Daily Port Scans', 'Preserve Hostname', 'Auto-Update', 'Disable Asset Update', and 'Bypass Interface Inventory'.
- Device Retention & Basic Thresholds:** A section with sliders and input fields for 'System Latency' (462 ms), 'Daily Rollup Bandwidth Data' (60 days), 'Availability Packet Size' (56 bytes), 'Frequent Rollup Bandwidth Data' (31 days), 'Availability Ping Count' (1 pings), 'Hourly Rollup Bandwidth Data' (48 days), and 'Raw Performance Data' (7 days).
- Interface Inventory Settings:** A section with a slider for 'Interface Inventory' (600000 ms) and a dropdown for 'Maximum Allowed' (10000 interfaces).

An 'Apply' button is located at the bottom center of the configuration area.

- In the **Template** field, select *New/One-Off Template*
- **Save When Applied & Confirmed.** From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template. The edited values will be applied to the selected device group. You do not have to save the edited values in a device template; they can be for one-time only use.
 - *If you select this field*, any changes you make to fields in the **Bulk Device Configuration** page will be saved to a new template.
 - *If you don't select this field*, you can edit the values in any of the fields, and the edited values won't be saved in the device template, but will be applied to the device group.

4. Click the **[Apply]** button to apply the settings to the device group.

5. The **Device Setting Confirmation** page appears.

Bulk Device Configuration Close / Esc

Device Template Editor | Applying Template to Devices | Click [Save] to commit changes | Config Template Settings (Click field labels to enable) | **Reset**

Setting Confirmation | The following settings will be applied

Organization: DC - Servers Dynamic Applications: 8

Device Selection Confirmation | The following devices will be altered

| | Device Name | IP Address | DID |
|----|-------------------|------------|-----|
| 1. | 10.2.2.31 | 10.2.2.31 | 29 |
| 2. | Topology Switch A | 10.40.40.2 | 36 |
| 3. | Topology Switch B | 10.40.40.3 | 37 |

Back **Confirm**

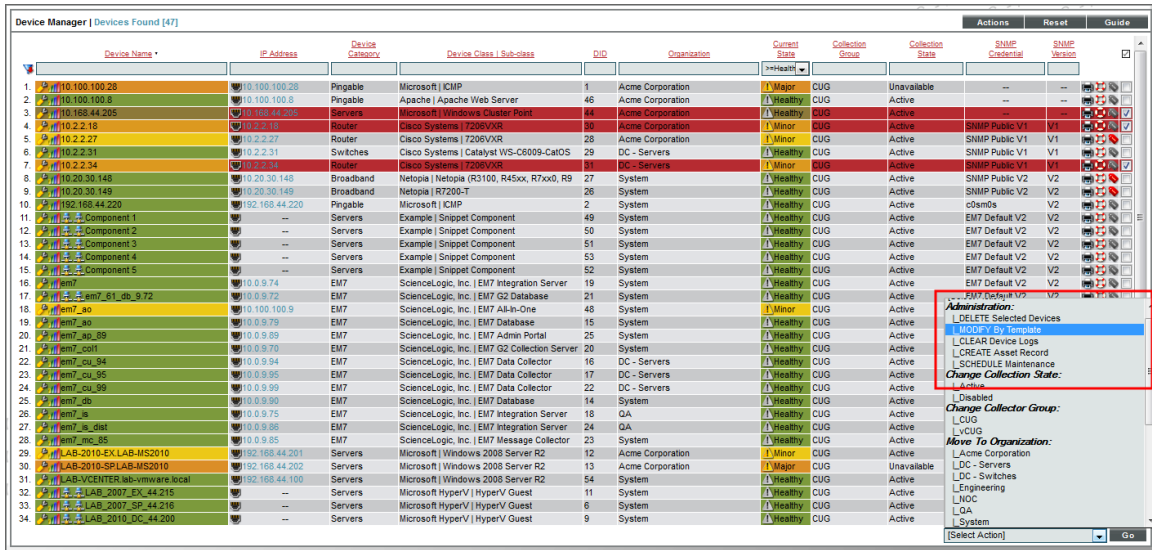
- In this page, you can view any settings in the device template that are different from SL1 default settings.
 - You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group.
 - You can also view a list of devices to which the device template will be applied.
6. To approve the changes and the device list, click the **[Confirm]** button in the **Device Setting Confirmation** page.
 7. The settings from the **Bulk Device Configuration** page will be applied to the selected devices in the device group.

Using the Bulk Configuration Tool to Apply Ad Hoc Settings to One or More Devices

You can use the *Modify by Template* action in the **Device Manager** page to apply one or more settings that are usually defined in a device template to one or more devices. You can apply settings that are not currently saved in a device template and then exit the bulk configuration tool without saving the settings as a device template.

To use the *Modify by Template* action to apply settings to one or more devices:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox for each device you want to apply configuration settings to.



3. In the **Select Actions** field, in the lower right, select the option *Modify by Template*.

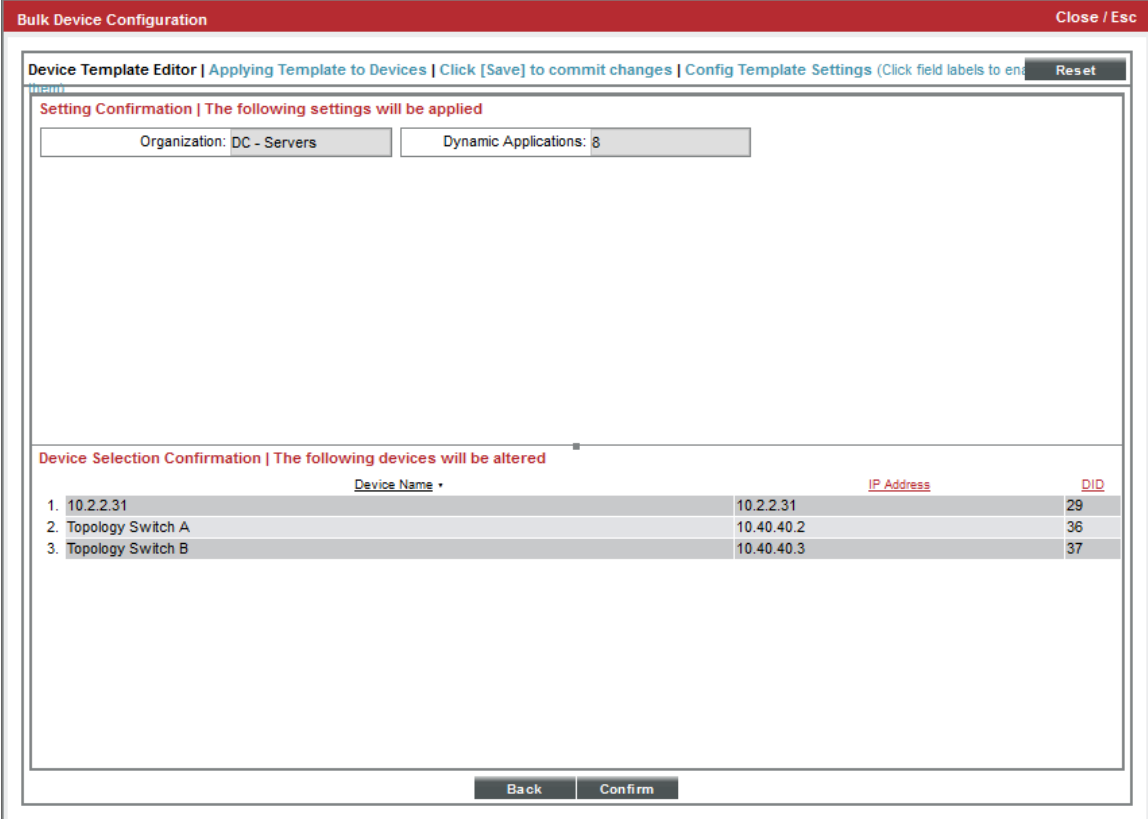
4. The **Bulk Device Configuration** page appears.

The screenshot displays the 'Bulk Device Configuration' window. At the top, it shows the title 'Bulk Device Configuration' and a 'Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)' header. Below this, there are fields for 'Template' (set to 'New / One-off Template'), 'Save When Applied & Confirmed' (checkbox), and 'Template Name'. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, showing sections for 'Access & Monitoring', 'Device Preferences', 'Device Retention & Basic Thresholds', and 'Interface Inventory Settings'. The 'Access & Monitoring' section includes fields for Device Organization, SNMP Read/Write, Availability/Latency Protocols, and Alerts. 'Device Preferences' includes checkboxes for Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, and Disable Asset Update. 'Device Retention & Basic Thresholds' features sliders for System Latency (462 ms), Availability Packet Size (56 bytes), Availability Ping Count (1 pings), and bandwidth data rollup periods (Daily: 60 days, Frequent: 31 days, Hourly: 48 days, Raw Performance: 7 days). 'Interface Inventory Settings' includes 'Interface Inventory' (600000 ms) and 'Maximum Allowed' (10000 interfaces). An 'Apply' button is located at the bottom center.

- In the **Template** field, select *New/One-Off Template*
- **Save When Applied & Confirmed**. From the **Bulk Device Configuration** page, you can edit the value in any of the fields in any of the tabs of the device template. The edited values will be applied to the selected devices. You do not have to save the edited values in a device template; they can be for one-time only use.
 - *If you select this field*, any changes you make to fields in the **Bulk Device Configuration** page will be saved to a new template.
 - *If you don't select this field*, you can edit the values in any of the fields, and the edited values won't be saved, but will be applied to the selected devices.

5. Click the **[Apply]** button to apply the field values to the selected device(s).

6. The **Device Setting Confirmation** page appears.



Bulk Device Configuration Close / Esc

Device Template Editor | Applying Template to Devices | Click [Save] to commit changes | Config Template Settings (Click field labels to enable) Reset

Setting Confirmation | The following settings will be applied

Organization: DC - Servers Dynamic Applications: 8

Device Selection Confirmation | The following devices will be altered

| | Device Name | IP Address | IID |
|----|-------------------|------------|-----|
| 1. | 10.2.2.31 | 10.2.2.31 | 29 |
| 2. | Topology Switch A | 10.40.40.2 | 36 |
| 3. | Topology Switch B | 10.40.40.3 | 37 |

Back Confirm

- In this page, you can view any settings in the device template that are different from SL1 default settings.
- You can click a field to disable it. When you disabled a field, its value will not be applied to the selected device group or selected devices.
- You can also view a list of devices to which the device template will be applied.

7. To approve the changes and the device list, click the **[Apply]** button in the **Device Setting Confirmation** page.

8. The settings from the **Bulk Device Configuration** page will be applied to each selected device.

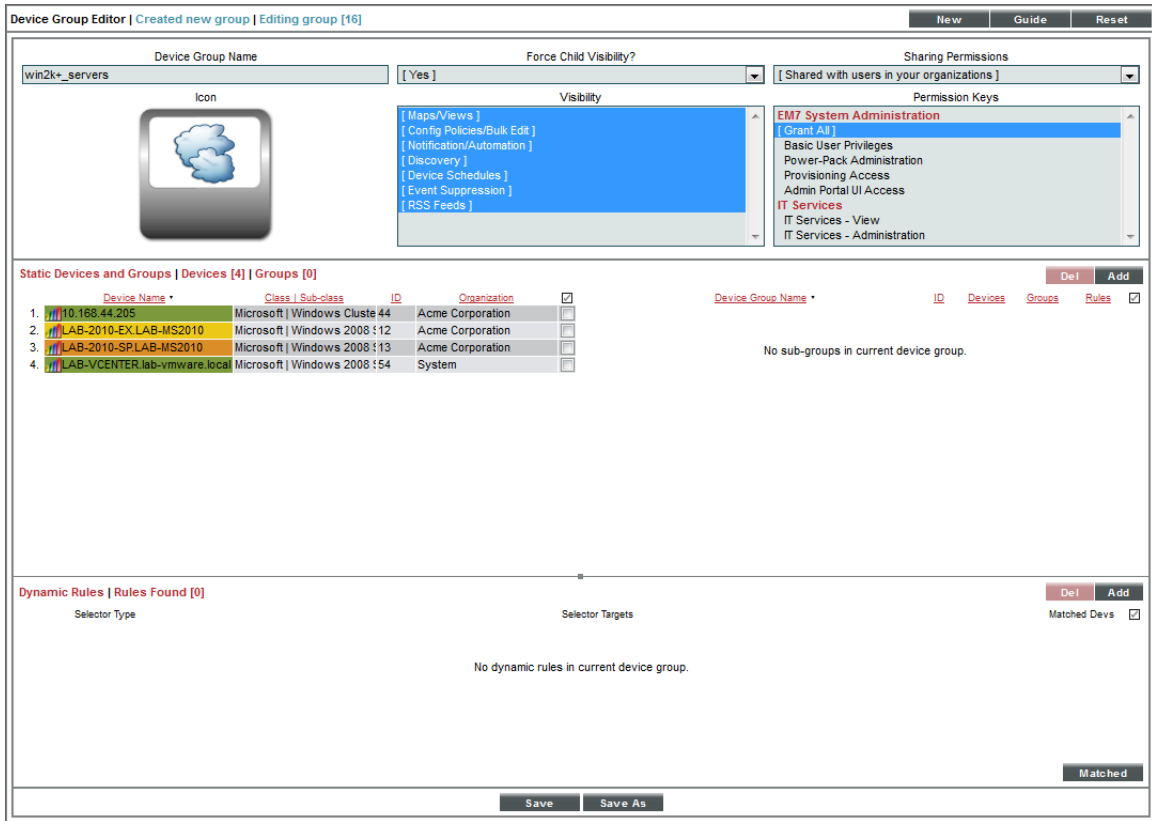
Example Device Group and Device Template

In this section, we'll create an example device group and an example device template. We'll then apply the device template to the device group.

Suppose we want to manage all Windows servers running Windows 2000 or later. We will create a device group that contains those servers.

Suppose we want to create a device template for all Windows servers running Windows 2000 or later. We want to use a single credential for each Windows server and apply consistent ScienceLogic settings to each server. We will create a device template for those servers.

Example Device Group



Here is our example device group:

- **Title.** We named our device group "win2k+_servers".
- **Icon.** We accepted the default icon.
- **Force Child Visibility.** We selected "Yes", so that the settings for the device group will apply to any future child device groups.
- **Visibility.** We selected all options, so our new device group is visible in all areas of SL1.
- **Sharing Permissions.** We selected "Shared with users in your organization", so other users can view the use the device group.
- **Permission Keys.** We did not select any permission keys for the device group. This means that any user who has permission to view the **Device Groups** page and is a member of the same organization as the creator of the device group can view the device group.
- **Add/Remove Devices.** We selected four Windows servers to be members of this device group.

Example Configuration Template

The screenshot shows the 'Device Template Editor' interface. At the top, there's a title bar with 'Device Template Editor | Click [Save] to commit changes | Config Template Settings (Click field labels to enable/disable them)' and buttons for 'New' and 'Reset'. Below the title bar, the 'Template Name' is set to 'win2k+_server_settings'. The interface is divided into several tabs: 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, showing two main sections: 'Access & Monitoring' and 'Device Preferences'. The 'Access & Monitoring' section includes fields for 'Device Organization' (NOC), 'SNMP Read' (EM7 Default V2), 'Availability Protocol' (ICMP), 'Latency Protocol' (ICMP), 'Avail+Latency Alert' (Disabled), 'Collection' (Enabled), 'Coll. Type' (Standard), 'Critical Ping' (Disabled), and 'Event Mask' (Group in blocks every 30 seconds). The 'Device Preferences' section includes 'Auto-Clear Events' (checked), 'Scan All IPs' (unchecked), 'Accept All Logs' (checked), 'Dynamic Discovery' (checked), 'Daily Port Scans' (checked), 'Preserve Hostname' (checked), 'Auto-Update' (checked), and 'Disable Asset Update' (unchecked). Below these sections are 'Device Retention & Basic Thresholds' and 'Interface Inventory Settings'. 'Device Retention & Basic Thresholds' includes sliders for 'System Latency' (462 ms), 'Daily Rollup Bandwidth Data' (60 days), 'Availability Packet Size' (56 bytes), 'Frequent Rollup Bandwidth Data' (31 days), 'Availability Ping Count' (1 pings), 'Hourly Rollup Bandwidth Data' (48 days), and 'Raw Performance Data' (7 days). 'Interface Inventory Settings' includes 'Interface Inventory Timeout' (600000 ms) and 'Maximum Allowed Interfaces' (10000 interfaces). At the bottom, there are 'Save' and 'Save As' buttons.

Here is our example device template. We defined fields only in the **Config** tab:

- **Template Name.** We named our template "win2k+_server_settings".
- **Device Organization.** We selected the organization "NOC". Each device to which we apply this template will become a member of that organization.
- **SNMP Read.** We selected the credential named "EM7 Default V2" as our SNMP Read credential.
- **SNMP Write.** We did not select a write credential, because we do not need SL1 to write to the devices.
- **Availability Protocol.** We selected ICMP (ping) as our availability protocol. This means that SL1 will ping a device to determine its availability.
- **Latency Protocol.** We selected ICMP (ping) as our latency protocol. This means that SL1 will ping a device to determine its latency.
- **Collection.** We selected *Enabled*, so that SL1 will collect data from the devices that use this template.
- **Collector Group.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Coll. Type.** We selected *Standard* because our network does not use DHCP.
- **Critical Ping.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.

- **Event Mask.** We selected *Group in blocks every 1 minute*. This means that events that occur on a single device within a single minute are grouped together under a single description.
- **Auto-Clear Events.** We enabled this option. Auto Clear automatically removes an event from the **Event Console** if a specified succeeding event occurs. For example, suppose the event "Device not responding to ping" occurs. If the next polling session produces the event "Device now responding normally to ping", the Auto Clear feature could clear the event.
- **Scan All IPs.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Accept All Logs.** We enabled this option. For each member device, all logs will be saved, not just event logs.
- **Dynamic Discovery.** We enabled this option. During discovery, SL1 will automatically assign the appropriate Dynamic Applications to each device that uses this template.
- **Daily Port Scans.** We enabled this option. SL1 will perform a daily scan of each member device for open ports.
- **Preserve Hostname.** We enabled this option. For each member device, the name of the device will **not** be updated in SL1 if the name of the device is changed on the device.
- **Auto-Update.** We enabled this option. SL1 will perform a nightly discovery of the device and update records with changes to the device.
- **Disable Asset Update.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **System Latency.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Device Logs Max.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Log Age Max.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Bandwidth Data.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Normalized BW Data.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Performance Data.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.
- **Normalized Perf Data.** We did not enable this field. When this template is applied, the devices that use this template will use the existing value for this field or the default value for this field.

Using Device Group Maps and Views

Overview



This chapter describes views and maps for device groups.

There are three types of views and maps for each device group:

- From the **Device Groups** page (Registry > Devices > Device Groups), you can view a hierarchical report on each device group. The **Device Group Map** page allows you to view devices by device group and also view the relationships between device groups and child-groups. This makes it easy to visualize and manage device groups.
- From the **[Views]** tab you can view an icon-based view of a device group. This page allows you to easily identify the devices in a device group, sort that list of devices, and quickly determine the status of each device.
- From the **[Views]** tab, you can also view a topology-based view of a device group. This view includes all layer-2, layer-3, CDP, LLDP, and event correlation relationships.

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Maps/Views* in the **Visibility** field, SL1 will not create a device group View for the device group.

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

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

This chapter includes the following topics:

[Viewing the Device Maps for a Device Group](#) 94

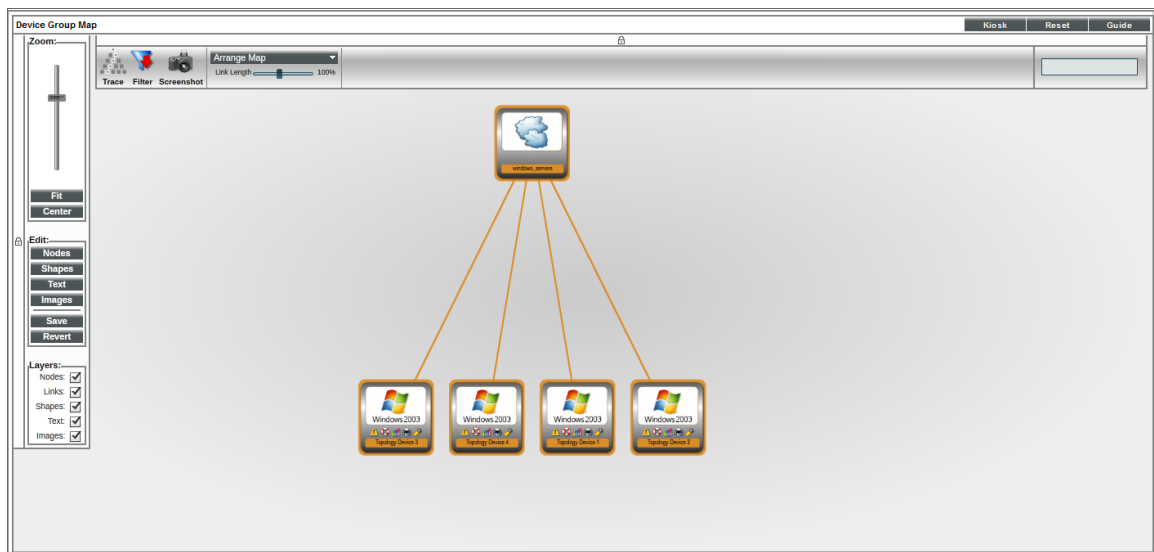
| | |
|---|---------------------|
| Viewing the Device Group Map Page for a Single Device Group | 95 |
| Viewing the Classic Views of a Device Group | 96 |
| Viewing Custom Device Maps | 96 |
| Using the Interface for Device Group Views | 97 |
| Drag-and-Drop Editing | 97 |
| Fields and Buttons | 97 |
| Creating a Device Group from an Existing Device Group in the Device Group Map | 98 |
| Creating a New Device Group From My Customized Maps | 99 |
| Creating a New Device Group From an Existing Device Group in My Customized Maps | 101 |

Viewing the Device Maps for a Device Group

In the **Device Group Map** page, you can select from a list of device groups and then view a graphical representation of the selected device group.

To access the **Device Group Map** page and view a map for any device group:


1. Go to the **Device Group Map** page (Views > Device Maps > Device Groups).
2. From the NavBar, select the device group you want to view.

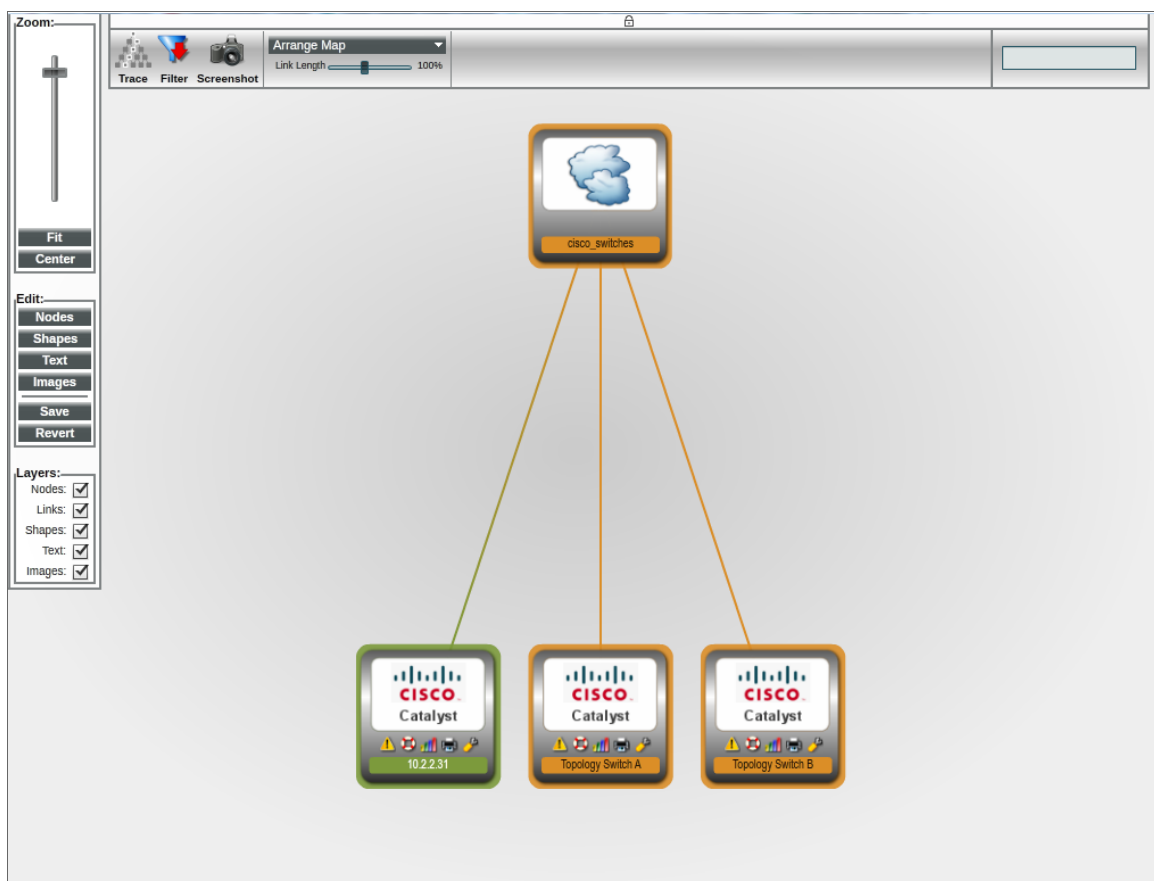


3. The **Device Group Map** page displays the selected device group. For details on this page, see the section on [Using the Interface for Device Group Views](#).

Viewing the Device Group Map Page for a Single Device Group

In the **Device Groups** page, you can view a hierarchical representation of a selected device group. To access the **Device Group Views** page and view a map for a single device group:

1. Go to the **Device Groups** page (Registry > Devices > Device Groups).
2. In the **Device Groups** page, find the device group for which you want to view a map. Click its map icon ().



3. The **Device Group Views** page displays the selected device group. For details on this page, see the section on [Using the Interface for Device Group Views](#).

Viewing the Classic Views of a Device Group

From the **[Views]** tab you can view an icon-based view of a device group. This page allows you to easily identify the devices in a device group, sort that list of devices, and quickly determine the status of each device. To view an icon-based view of a device group:

1. Go to the **Device Group Map** page (Views > Classic Views > Device Groups).
2. The **Device Group Views** page appears. In the drop-down list in the upper left, select a device group view to view.



Viewing Custom Device Maps

From the **[Views]** tab, you can also view a topology-based view of a device group. This view includes all layer-2, layer-3, CDP, LLDP, and event correlation relationships.

To view a topology map of a device group:

1. Go to Views > My Customized Maps.
2. In the NavBar, select the name of the device group you want to view.
3. The **Custom Device Group Map** page appears, where you can view the devices and network relationships in the device group.

Customized maps appear in the following sections in the left NavBar:

- **Views > My Customized Maps.** Personalized maps that you create.

- **Views > User Customized Maps.** If you are a user of type "administrator", you can navigate to the maps in this section to view and edit all customized maps in SL1, even if the device group associated with the map was defined with the field **Shared** (visible to all users) set to *no*.
- **Views > Shared Customized Maps.** If a customized map or device group is defined as "shared", you can view the maps in this section. The maps in Shared Customized Maps require the same Access Hooks and Access Keys as device groups. Depending upon the Access Keys assigned to your account, you might be able to edit Shared Customized Maps created by other users. To learn more about Access Hooks and Access Keys, see the manual **Access Permissions**.

NOTE: If you create a device group from the **Device Groups** page and set the **Visibility** field to include *Maps/Views*, the device group will appear as a map in **Custom Device Group Map** page (Views > My Customized Maps). If you set the **Shared** field to *yes*, the device group will appear for other users as a map in the **Shared Customized Maps** page (Views > Shared Customized Maps).

Using the Interface for Device Group Views

When viewing a map of a device group, you can edit the display by using the drag-and-drop editing features and using the fields in the page. The following sections describe how to use the tools available in the map page.

Drag-and-Drop Editing

A node is a connection point—either a redistribution point or communication endpoint. Each device in the maps page is an individual node that can be placed in different areas of the map while retaining its link to other devices. You can drag-and-drop nodes to reposition them on the map to make viewing and managing devices easier. You can use drag-and-drop editing in the following ways:

- You can move the entire map around the pane by clicking in any spot in the background, holding down the left-mouse key and dragging the mouse. The map will be dragged around by the spot you initially clicked on.
- You can use your mouse to select and move nodes within a map. To edit and move nodes around the map, first enter Nodes mode by clicking the **[Edit: Nodes]** button.

Fields and Buttons

Each view page includes multiple fields and buttons for editing the display of a view.

- **Kiosk.** Spawns a new page, where the map appears in full-screen. This display model is helpful in NOC environments.
- **Reset.** Resets the default display. Any unsaved changes are removed.
- **Lock Icon.** Toggles on and off the display of the menu at the left of the pane and the menu at the top of the pane. When the lock icon appears in white, the menu is "locked" and will continue to be displayed in the pane. When the lock icon appears in gray, the menu is displayed only when you are working in the menu. To make the hidden menu appear again, mouse over the border where the menu resides.

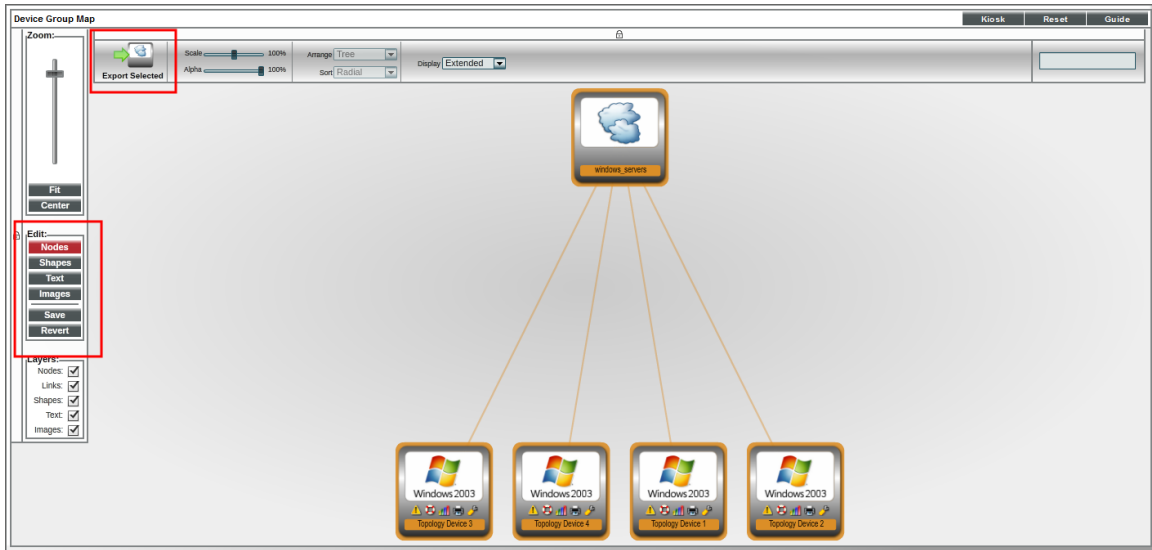
- **Trace + fields.** Displays two fields in the upper right of the page that allow you to search for and highlight one or two devices in the device group/organization/category, depending on the Device Map selected.
- **Take Screenshot.** Saves the current display as a .png file to the local computer.
- **Filter.** Toggles on and off the display of the **Node Filters** checkboxes. These checkboxes allow you to filter the nodes included in a map based on whether a device or connection is managed or unmanaged in SL1, whether the node is part of a device group, the status of the device (healthy, notice, minor, major, critical), or the device category assigned to the device.
- **Arrange Map.** Specifies that SL1 should automatically rearrange the map nodes in the selected pattern. Choices are: *Tree, Radical Tree, Grid, and Random.*
- **Zoom bar.** Magnifies and contracts the map.
- **Fit.** Adjusts the zoom to fit the entire map within the pane.
- **Center.** Centers the map in the middle of the pane without changing the zoom.
- **Edit: Nodes.** Displays a menu at the top of the pane that allows you to edit the display of nodes in the map.
- **Edit: Shapes.** Displays a menu at the top of the pane that allows you to add hand-drawn shapes on the map. The menu allows you to select shapes, drag-and-drop points, line thickness, fills, transparency, and colors. You can also delete shapes that were previously added to the map.
- **Edit: Text.** Displays a menu at the top of the pane that allows you to add text to the map and format the text. You can also delete text that was previously added to the map.
- **Edit: Images.** Displays a menu at the top of the pane that allows you to import and format an image. You can include the image in the map or use the image as the background of the map. You can also delete an image that was previously added to the map.
- **Edit: Save.** Saves changes to the map.
- **Edit: Revert.** Ignores all changes and returns to the last saved version of the map.
- **Layers: Nodes.** Toggles the display of devices in the map.
- **Layers: Links.** Toggles the display of links in the map.
- **Layers: Shapes.** Toggles the display of hand-drawn shapes in the map.
- **Layers: Text.** Toggles the display of manually entered text in the map.
- **Layers: Images.** Toggles the display of imported images in the map.

Creating a Device Group from an Existing Device Group in the Device Group Map

You can create a device group from the **Device Group Map** page. You can export the device group to a Customized Map, and the device group will be added to the **Device Groups** page (Registry > Devices > Device Groups). To create a device group from the **Device Group Map** page:

1. Go to the **Device Group Map** page (Views > Device Maps > Device Groups).
2. Select a device group from the NavBar.

- When the **Device Group Map** page appears with the selected device group, click the **[Edit: Nodes]** button. To create the new device group, hold the **<Shift>** key and select the devices you want to add to the new device group.



- After you have selected the devices for the device group, click the **[Export Selected]** button.
- Provide a name for the device group and click **[OK]**. The device group will be added to the **Device Groups** page (Registry > Devices > Device Groups) and can be exported into a Customized Map.

To read more about Device Groups maps, see the manual [Views](#).

Creating a New Device Group From My Customized Maps

When you initially create a Customized Map and add devices and device groups to the Customized Map, you are actually defining a Device Group; however, you are using the maps interface instead of the **Device Groups** page to do so.

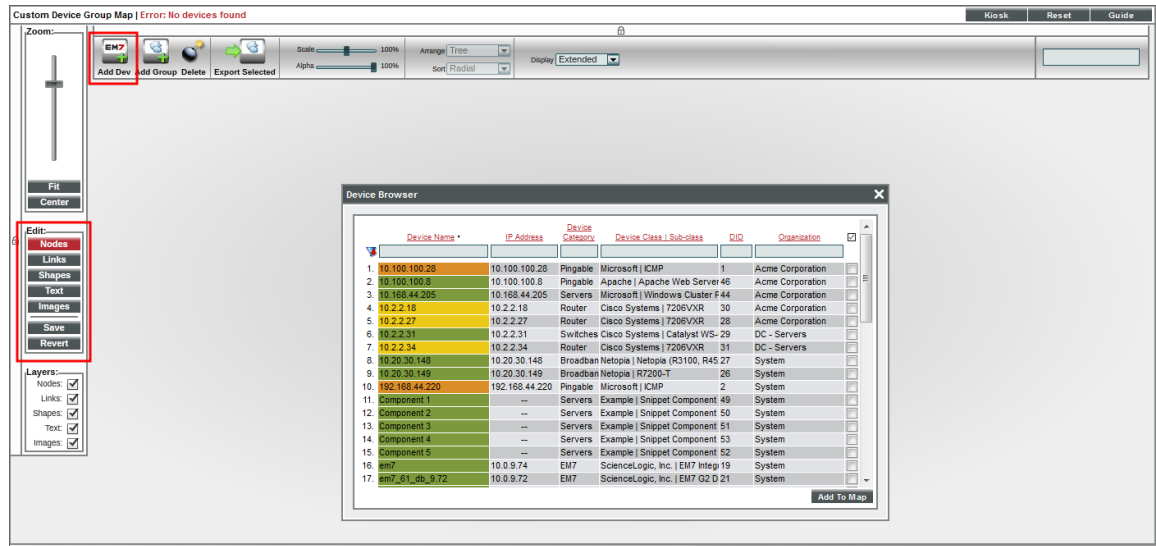
NOTE: You can also create a Device Group from the **Device Groups** page. If you select **Maps** in the **Visibility** field, the Device Group will appear as a map in Views > My Customized Maps. If you set the **Shared** field to yes, the device group will appear as a map in Views > Shared Customized Maps.

NOTE: By default, device groups created in the **Custom Device Group Map** page include only **Maps/Views** under **Visibility** and have **Shared** set to no. However, you can change these default settings by editing the device group from the **Device Groups** page (Registry > Devices > Device Groups).

To create a new Customized Map and add device groups:

- Go to the **Custom Device Group Map** page (Views > My Customized Maps).

2. In the NavBar, select **New Group/Map**.
3. In the map pane, click the **Edit:[Nodes]** button to add devices and optionally device groups to your Customized Map.



4. **To add a device to the Customized Map**, in the Nodes menu at the top of the pane, click the **Add Dev** icon. When the **Device Browser** modal appears, search for the device(s) you want to add to the Customized Map. Select the checkbox for one or more devices you want to add to the Customized Map.
5. **To add a device group to the Customized Map**, in the Nodes menu at the top of the pane, click the **Add Group** icon. When the **Device Browser** modal page appears, search for the device group(s) you want to add to the Customized Map. Select the checkbox for one or more device groups you want to include in the Customized Map.
6. **To delete a device from the Customized Map**, click the device's icon, click the **Edit:[Nodes]** button to make the Nodes menu appear at the top of the pane, and then click the **Delete** icon (🗑️).
7. **To delete a device group from the Customized Map**, click the device group's icon, click the **Edit:[Nodes]** button to make the Nodes menu appear at the top of the pane, and then click the **Delete** icon (🗑️).

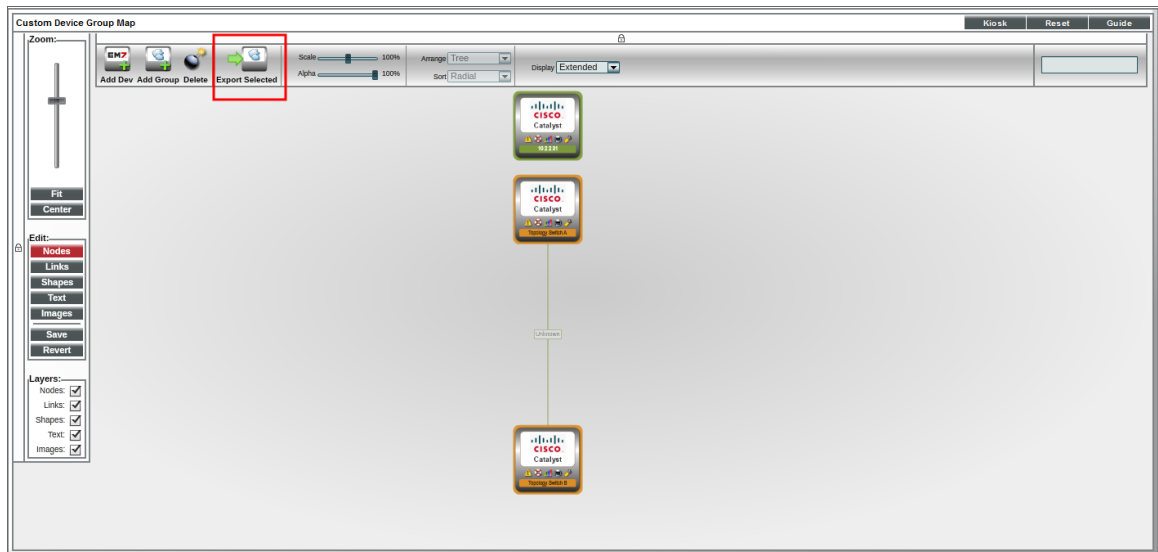
NOTE: If a device group includes a dynamic rule, SL1 will examine the rule and automatically add devices that match the rule's criteria to the device group. If you delete a device that SL1 has automatically added to the device group, the device will reappear the next time you view the device group map.

8. If SL1 detects Layer 2, Layer 3, CDP, LLDP, or VMware relationships between the devices, SL1 automatically includes the appropriate links in the Customized Map.
9. After you add devices and device groups to the map, you can manually create and edit existing links.
10. Clicking on an icon for a device group displays the Customized Map for that device group.
11. When you click the **Edit:[Save]** button, SL1 prompts you to provide a name for the new Customized Map.

To read more about Device Groups maps, see the manual [Views](#).

Creating a New Device Group From an Existing Device Group in My Customized Maps

1. Go to the **Custom Device Group Map** page (Views > My Customized Maps).
2. In the NavBar, select the device group you want to use as the basis for the new device group.
3. In the map pane, click the **Edit:[Nodes]** button to expose the **[Export Selected]** button.



4. To create the new device group, hold the **<Shift>** key and click the devices you want to add to the new device group.
5. After you have selected the devices for the device group, click the **[Export Selected]** button.
6. Provide a name for the device group and click **[OK]**. The device group will be added to the **Device Groups** page (Registry > Devices > Device Groups) and can be exported into a Customized Map.
7. If SL1 detects Layer 2, Layer 3, CDP, LLDP, or VMware relationships between the devices, SL1 automatically includes the appropriate links in the Customized Map.
8. After you add devices and device groups to the map, you can manually create and edit existing links.
9. Clicking on an icon for a device group displays the Customized Map for that device group.

To read more about Device Groups maps, see the manual [Views](#).

Scheduling Downtime for a Device Group

Overview

This chapter describes how to schedule maintenance times for device groups.



You can use the **Schedule Manager** page to schedule downtime for an entire device group. This allows you to schedule maintenance and update tasks for all the devices in the device group and also inform other users of the scheduled downtime.

When the scheduled downtime occurs, each device in the device group will have a collection status of "maintenance".

You can specify whether or not you want SL1 to collect data from the devices in the device group during the scheduled maintenance. During scheduled maintenance, no events will be triggered for the devices in the device group.

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Device Schedules* in the **Visibility** field, you will not be able to schedule downtime and maintenance for the device group.

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

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

This chapter includes the following topics:

| | |
|---|-----|
| Viewing the Schedule Manager | 103 |
| Defining a Scheduled or Recurring Device Group Maintenance Window | 104 |

| | |
|--|---------------------|
| Enabling or Disabling One or More Scheduled Device Group Maintenance Windows | 107 |
| Deleting One or More Scheduled Device Group Maintenance Windows | 108 |

Viewing the Schedule Manager


The **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon) displays the following information about each scheduled or recurring device group maintenance window:

The screenshot shows a web interface titled "Schedule Manager | Schedules Found [2]". It contains a table with the following columns: Schedule Summary, Schedule Description, Event ID, sch_id, Context, Timezone, Start Time, Duration, Recurrence Interval, End Date, Last Run, Owner, Organization, Visibility, and Enabled. Two rows of data are visible:

| | Schedule Summary | Schedule Description | Event ID | sch_id | Context | Timezone | Start Time | Duration | Recurrence Interval | End Date | Last Run | Owner | Organization | Visibility | Enabled |
|----|---------------------|----------------------|----------|--------|---------------|---------------|---------------------|----------|---------------------|----------|----------|-----------|--------------|------------|---------|
| 1. | Nightly Maintenance | Nightly Maintenance | 183 | 10 | Device Groups | America/New_Y | 2017-01-20 03:00:00 | 30 minu | Every 1 Day | -- | -- | banderton | System | World | Yes |
| 2. | Weekly Patching | Weekly Patching | 184 | 11 | Device Groups | America/New_Y | 2017-01-20 03:30:00 | 30 minu | Every 1 Week | -- | -- | banderton | System | World | Yes |

At the bottom right of the table, there is a "(Select Action)" dropdown menu and a "Go" button.

- **Schedule Summary.** Displays the name assigned to the scheduled process.
- **Schedule Description.** Displays a description of the scheduled process.
- **Event ID.** Displays a unique, numeric ID for the scheduled process. SL1 automatically created this ID for each scheduled process.
- **sch id.** Displays a unique, numeric ID for the schedule. SL1 automatically created this ID for each schedule.
- **Context.** Displays the area of SL1 upon which the schedule works.
- **Timezone.** Displays the time zone associated with the scheduled process.
- **Start Time.** Displays the date and time at which the scheduled process will begin.
- **Duration.** Displays the duration, in minutes, which the scheduled process occurs.
- **Recurrence Interval.** If applicable, displays the interval at which the scheduled process recurs.
- **End Date.** If applicable, displays the date and time on which the scheduled process will recur.
- **Last Run.** If applicable, displays the date and time the scheduled process most recently ran.
- **Owner.** Displays the username of the owner of the scheduled process.
- **Organization.** Displays the organization to which the scheduled process is assigned.
- **Visibility.** Displays the visibility level for the scheduled process. Possible values are "Private", "Organization", or "World".
- **Enabled.** Specifies if the scheduled process is enabled. Possible values are "Yes" or "No".

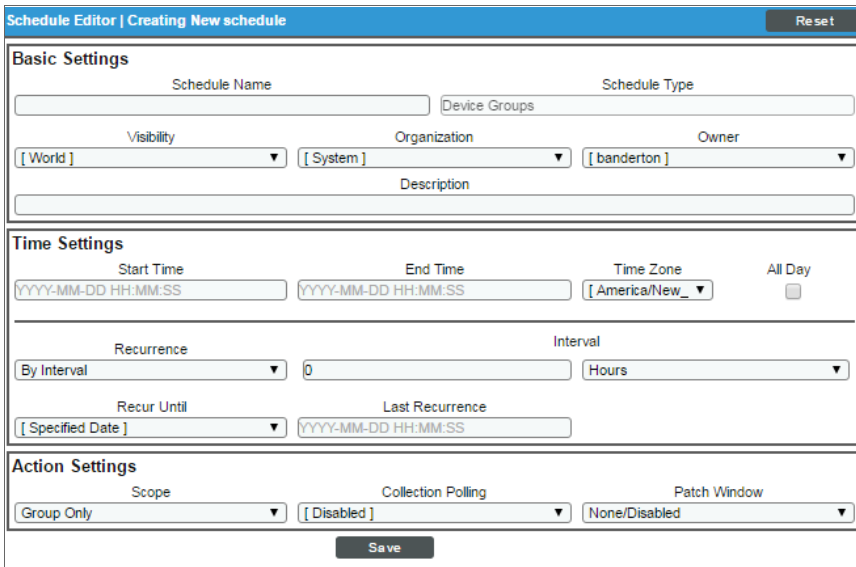
To edit a scheduled or recurring device group maintenance window, click its wrench icon () and update the settings as needed on the **Schedule Editor** modal page. (For more information, see the section [Defining a Scheduled or Recurring Device Group Maintenance Window.](#))

Defining a Scheduled or Recurring Device Group Maintenance Window

You can schedule a device group maintenance window in SL1 from the **Schedule Manager** page. SL1 will automatically set the status of each device in the device group to "maintenance" at the scheduled time.

To define a scheduled or recurring device group maintenance window:

1. Go to the **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon).
2. Click **[Create]**. The **Schedule Editor** modal page appears.
3. On the **Schedule Editor** modal page, make entries in the following fields:



The screenshot shows the 'Schedule Editor | Creating New schedule' modal page. It is divided into three main sections: Basic Settings, Time Settings, and Action Settings. The Basic Settings section includes fields for Schedule Name, Schedule Type, Device Groups, Visibility (set to [World]), Organization (set to [System]), Owner (set to [banderton]), and a Description field. The Time Settings section includes Start Time, End Time, Time Zone (set to [America/New_]), and an All Day checkbox. It also has Recurrence (set to By Interval), Interval (set to 0 Hours), Recur Until (set to [Specified Date]), and Last Recurrence (set to YYYY-MM-DD HH:MM:SS). The Action Settings section includes Scope (set to Group Only), Collection Polling (set to [Disabled]), and Patch Window (set to None/Disabled). A Save button is located at the bottom of the form.

Basic Settings

- **Schedule Name.** Type a name for the scheduled process.
- **Schedule Type.** Indicates the scheduled process type (such as Tickets, Reports, or Devices).
- **Visibility.** Select the visibility for the scheduled process. You can select one of the following:
 - *Private.* The scheduled process is visible only to the owner selected in the **Owner** field.
 - *Organization.* The scheduled process is visible only to the organization selected in the **Organization** field.

- *World*. The scheduled process is visible to all users.
- **Organization**. Select the organization to which you want to assign the scheduled process.
- **Owner**. Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
- **Description**. Type a description of the scheduled process.

Time Settings

- **Start Time**. Click in the field and select the date and time you want the scheduled process to start.
- **End Time**. Click in the field and select the date and time you want the scheduled process to end.
- **Time Zone**. Select the region or time zone for the scheduled start time.

NOTE: If you want SL1 to automatically adjust for daylight savings time (if applicable), then you must select a named region (such as *America/New York*) in the **Time Zone** field. If you select a specific time zone (such as *EST*) or a specific time offset (such as *GMT-5*), then SL1 will not automatically adjust for daylight savings time.

- **All Day**. Select this checkbox if the scheduled process occurs all day rather than during a specific period of time. If you do so, the **End Time** field becomes disabled.
- **Recurrence**. Select whether you want the scheduled process to occur once or on a recurring basis. You can select one of the following:
 - *None*. The scheduled process occurs only once.
 - *By Interval*. The scheduled process recurs at a specific interval.

If you select *By Interval*, the following additional fields appear:

- **Interval**. In the first field, enter a number representing the frequency of the scheduled process, then select the time interval in the second field. Choices are *Minutes*, *Hours*, *Days*, *Weeks*, or *Months*. For example:
 - If you specify "6 Hours", then the scheduled process recurs every six hours from the time listed in the **Start Time** field.
 - If you specify "10 Days", then the scheduled process recurs every 10 days from the date listed in the **Start Time** field.
 - If you specify "2 Weeks", then the scheduled process recurs every two weeks, on the same day of the week as the **Start Time**.
 - If you specify "3 Months" the ticket recurs every three months, on the same day of the month as the **Start Time**.

- **Recur Until.** Specifies when the scheduled process stops recurring. You can select one of the following:
 - *No Limit.* The scheduled process recurs indefinitely until it is disabled.
 - *Specified Date.* The scheduled process recurs until a specific date and time. If you select *Specified Date*, you must select a date and time in the **Last Recurrence** field.
- **Last Recurrence.** Click in the field and select the date and time you want the scheduled process to stop recurring.

Action Settings

- **Scope.** Select if the scheduled maintenance will affect only the group or both the group and children devices.
- **Collection Polling.** Specifies whether SL1 should perform collection on the device during the scheduled maintenance. Choices are:
 - *Enabled.* During scheduled maintenance, SL1 will collect data from the device, but no events will be triggered for the device.
 - *Disabled.* During scheduled maintenance, SL1 will not collect data from the device.
- **Patch Window.** You can specify a "patch window" within the larger maintenance period. The "patch window" allows SL1 to limit the suppression of events to a small time-frame within the larger maintenance window. Your choices are:
 - *None*
 - *Between 5 minutes and 60 minutes*, in five-minute intervals.

For example:

Suppose you have to patch a server that is monitored by SL1. Suppose you know you will perform this task sometime between midnight and 6:00 AM. Suppose you know that the actual patch process requires only 15 minutes of downtime for the server. In SL1, you would define a maintenance window of 24:00 - 6:00 and a patch window of 15 minutes. In this scenario:

1. At 24:00, SL1 generates an event saying that the server is going into maintenance mode. Because you have defined a patch window, SL1 continues to monitor this server as normal.
2. At 3:00, you apply the patch to the server. The server reboots, and SL1 generates an event saying that the server is offline. The first event that both matches or exceeds the **Patch Maintenance Minimum Severity** in the **Behavior Settings** page (System > Settings > Behavior) and occurs within the larger maintenance window triggers the start of the patch window.
3. SL1 suppresses the event that triggered the patch maintenance window and instead generates an event "Patch Maintenance Window Opened".
4. For the next 15 minutes, SL1 will suppress all events for the device.
5. At 3:15, SL1 will generate an event for "Patch Maintenance Window Closed". This event clears the previous event "Patch Maintenance Window Opened".

6. SL1 will now generate events for the device, even though the maintenance window extends until 6:00.

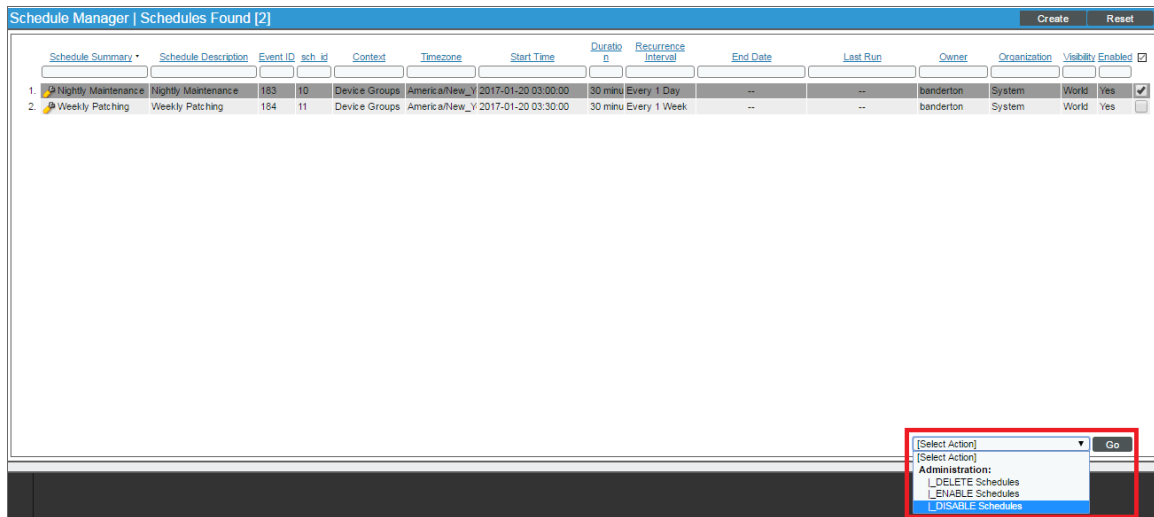
NOTE: If the patch was applied at 5:50, the server was rebooted, and SL1 generated an event saying that the server is offline, events would be suppressed only until the end of the maintenance window, 6:00, even though the patch window is 15 minutes.

4. Click **[Save]**.

Enabling or Disabling One or More Scheduled Device Group Maintenance Windows

You can enable or disable one or more scheduled or recurring device group maintenance windows from the **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon). To do this:

1. Go to the **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon).

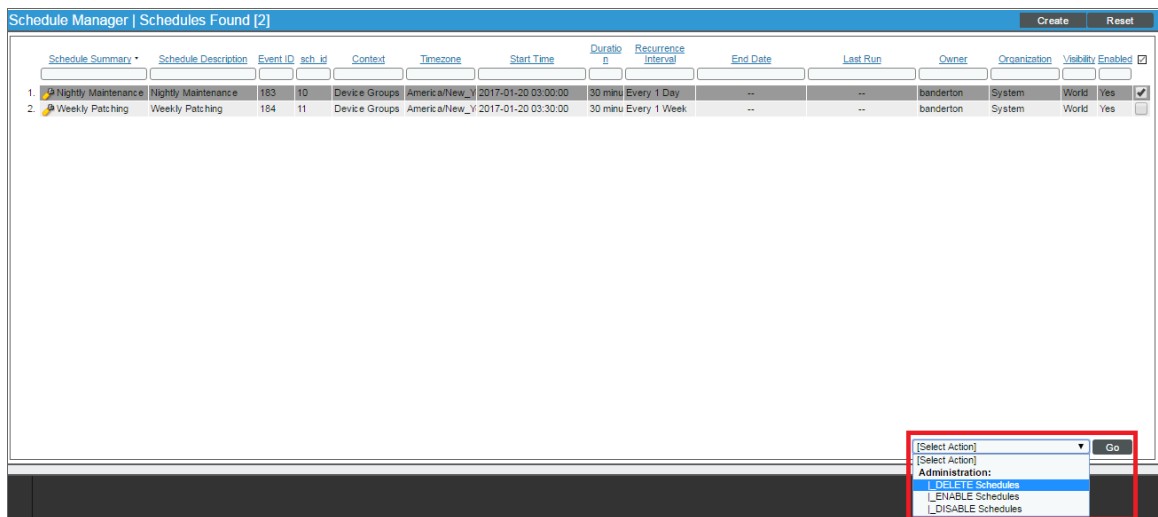


2. Select the checkbox icon for each scheduled process you want to enable or disable.
3. Click the **Select Action** menu and choose *Enable Schedules* or *Disable Schedules*.
4. Click the **[Go]** button.

Deleting One or More Scheduled Device Group Maintenance Windows

You can delete one or more scheduled or recurring device group maintenance windows from the **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon). To do this:

1. Go to the **Schedule Manager** page (Registry > Devices > Device Groups > calendar icon).



2. Select the checkbox icon for each scheduled process you want to delete.
3. Click the **Select Action** menu and choose *Delete Schedules*.
4. Click the **[Go]** button.

Chapter

8

Events and Device Groups

Overview

This chapter describes how to suppress an event for a device group.

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



Events are displayed in the **[Events]** tab in SL1, in the **Event Console** page. When you suppress an event, you are specifying that in the future, if this event occurs again on the same device, the event will not appear in the **Event Console** page. Basically, you are saying that if the event occurs again on the same device, you do not want to be notified.

If a suppressed event occurs on a different device, it will appear in the **Event Console** page.

You can suppress an event for a device group. The event will then be suppressed for all devices in the device group. The event will also be suppressed for all child device groups and their devices.

NOTE: For general details on events, see the manual *Events*.

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

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

This chapter includes the following topics:

[Searching Events by Device Group](#)110

Searching Events by Device Group

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

Events are displayed in the **[Events]** tab in SL1, in the **Event Console** page. In the **Event Console** page you can search for Device Group Names and Device Group IDs to find events that occurred on devices that are members of the specified Device Group.

The **Global Search** field in the upper left of the page allows you to filter the entire list of displayed events by a single parameter. SL1 will update the **Event Console** and display only events that have a matching parameter.

To use the **Global Search** field, enter values in the **Search** drop-down list and the **Text** field:

- **Search.** You can select from a number of parameters, that include:
 - *Device Group ID.* Unique ID for the device group associated with the event.
 - *Device Group Name.* Name of the device group associated with the event.
- **Text.** For each search parameter, you must enter text to match against. SL1 will search for events that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
 - *,* (comma). Specifies an "or" operation. For example:
"dell, micro" would match all values that contain the string "dell" OR the string "micro".
 - *&* (ampersand). Specifies an "and" operation. For example:
"dell & micro" would match all values that contain the string "dell" AND the string "micro".
 - *!* (exclamation mark). Specifies a "not" operation. For example:
"!dell" would match all values that do not contain the string "dell".

To perform another search on the results of the previous search:

1. Click the plus sign ($+$) to the left of the **Refresh Timer**.
2. This adds another **Search** field and **Text** field to the top of the page. This second search will search only the results from the first search.
3. You can add as many **Search** and **Text** fields as you need.

NOTE: You can save the results of a Global Search as a Custom View.

| Organization | Name | Type | Event Message | Severity | Acknowledged | Note | Token | External Ticket | Age / Elapsed | Last Detected | EID | Source | Count | Notify |
|----------------|---------------------------------|--|---|----------|--------------|------|-------|-----------------|---------------|---------------------|-------|----------|-------|--------|
| System | Simple Availability I/T Service | IT Service State Critical: Simple Availability Service | Critical | | | | | | 3 hrs 20 mins | 2012-05-23 16:56:06 | 24097 | Internal | 201 | |
| Acme Corporate | 10.100.100.20 | Device | Device Failed Availability Check: ICMP Ping | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23742 | Internal | 327 | 1 |
| Acme Corporate | 10.148-2010-EX-LAB | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 3 hrs 25 mins | 2012-05-23 16:57:45 | 24092 | Internal | 42 | 1 |
| Acme Corporate | 10.148-2010-SP-LAB-Device | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23744 | Internal | 327 | 1 |
| DC - Servers | Topology Device 1 | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23749 | Internal | 327 | 1 |
| DC - Servers | Topology Device 2 | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23751 | Internal | 327 | 1 |
| DC - Servers | Topology Device 3 | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23745 | Internal | 327 | 1 |
| DC - Servers | Topology Device 4 | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23747 | Internal | 327 | 1 |
| System | 192.168.44.220 | Device | Device Failed Availability Check: ICMP Ping | Major | | | | | 3 hrs 20 mins | 2012-05-23 16:57:45 | 24095 | Internal | 41 | 1 |
| System | Topology Switch A | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23753 | Internal | 327 | 1 |
| System | Topology Switch B | Device | Device Failed Availability Check: UDP - SNMP | Major | | | | | 1 day 3 hrs | 2012-05-23 16:57:45 | 23755 | Internal | 327 | 1 |
| Acme Corporate | 10.2.2.10 | Device | System or agent has recently restarted | Minor | | | | | 4 hrs 3 mins | 2012-05-23 16:55:21 | 24077 | Internal | 41 | 2 |
| Acme Corporate | 10.2.2.27 | Device | System or agent has recently restarted | Minor | | | | | 4 hrs 3 mins | 2012-05-23 16:55:21 | 24078 | Internal | 41 | 2 |
| Acme Corporate | 10.148-2010-EX-LAB | Network | Mailbox: Total Average Delivery Time has exceeded threshold | Minor | | | | | 1 wk 22 hrs | 2012-05-23 13:30:44 | 22143 | Dynamic | 2,014 | 2 |
| Acme Corporate | 10.148-2010-SP-LAB-Device | Device | Network latency exceeded threshold: No Response | Minor | | | | | 3 hrs 25 mins | 2012-05-23 16:57:45 | 24084 | Internal | 42 | 2 |
| DC - Servers | 10.2.2.34 | Device | System or agent has recently restarted | Minor | | | | | 4 hrs 3 mins | 2012-05-23 16:55:21 | 24078 | Internal | 41 | 2 |
| System | agent_26 | Device | App: 447: Snapshot: 372: threw exception (Traceback: Traceback in | Minor | | | | | 4 hrs 5 mins | 2012-05-23 16:36:06 | 24075 | Internal | 12 | 2 |
| System | System | Organization | EM7 minor event: Automation action %D Test for SNMP Set ip %D | Minor | | | | | 2 days 17 hrs | 2012-05-23 16:13:13 | 23406 | Internal | 629 | |

Suppressing an Event for a Device Group

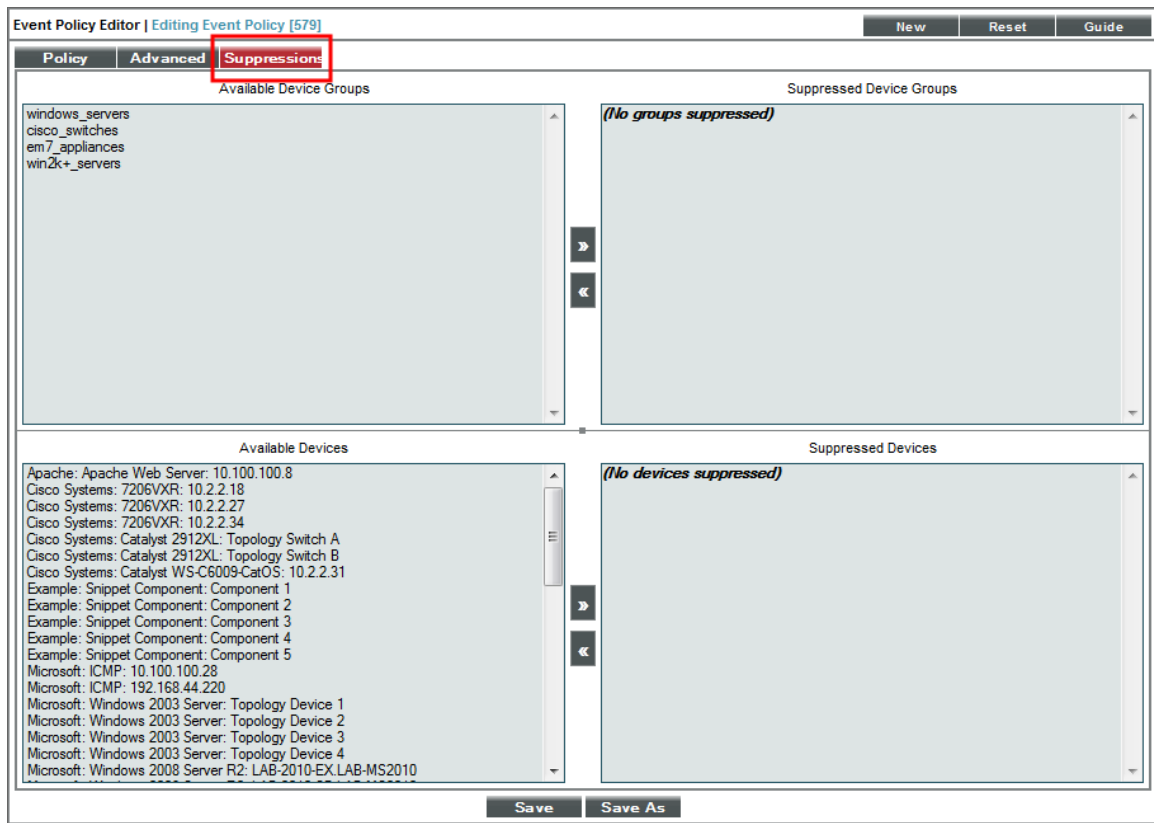
You can suppress an event for a device group. When you do so, you are suppressing the event for all devices in the device group (and optionally, any child device groups).

NOTE: If the definition for a device group, in the **Device Group Editor** page, does not include *Event Suppression* in the **Visibility** field, you will not be able to suppress an event for the device group.

To suppress an event for a device group:

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).

2. In the **Event Policy Manager** page, find the event you want to suppress. Click its wrench icon (🔧).



3. When the **Event Policy Editor** page appears, select the **[Suppressions]** tab.
4. In the **[Suppressions]** tab, you can define or edit the following:
 - **Available Device Groups.** Device groups for which you can suppress the event.
 - **Suppressed Device Groups.** Device groups for which the event is already suppressed.
5. You can use the arrow buttons (**[<<]** and **[>>]**) to move device groups from the Available and Suppressed lists.
6. Click the **[Save]** button to save your suppressions.

Automation Policies and Tickets



Overview

This chapter describes how to use run book automation and action policies with device groups in SL1.

SL1 includes automation features that allow you define specific conditions and the actions you want SL1 to execute when those conditions are met. These features can be found in the Registry > Run Book pages. (For more details on automation policies and action policies, see the manual *Run Book Automation*.)

SL1 also allows you to align a ticket with a device group when creating a ticket. You can align a ticket with a device group from the **Ticket Console** page.

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

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

This chapter includes the following topics:

| | |
|---|-----|
| <i>What is an Automation Policy?</i> | 114 |
| <i>Aligning an Automation Policy with a Device Group</i> | 114 |
| <i>What is an Action Policy?</i> | 116 |
| <i>Aligning a Ticket with a Device Group</i> | 118 |
| <i>Searching for a Ticket Aligned with a Device Group</i> | 119 |

What is an Automation Policy?

An **automation policy** allows you to define automatic actions that should be executed in response to events. The automation policy defines the conditions under which an automatic action should be executed.

When the criteria in an automation policy is met, an action is executed. This action is defined in an **action policy**. To view a list of action policies or edit or create an action policy, go to the **Action Policy Manager** page (Registry > Run Book > Actions).

For example, an automation policy might specify: If the event "illicit process" occurs on all the devices in device group "mailservers", and the event is not cleared within five minutes, execute the action policy "email NOC". The action policy "email NOC" could email all NOC staff about the "illicit process" event.

Automation policies can describe the criteria described below. One or more of these criteria must be met before an action is executed:

- One or more specified events must have occurred.
- Events must have occurred on one or more specified devices or **all devices in one or more specified device groups**.
- Event(s) must have specified severity (critical, major, minor, notice, or healthy).
- Events must have specified status (event is not cleared, event is now acknowledged, ticket is not created for event).
- Specific amount of time that must elapse while severity and status do not change.

When the criteria are met, the automation policy triggers the execution of one or more specified action policies.


Aligning an Automation Policy with a Device Group

When you align an automation policy with a device group, you specify that all the conditions in the automation policy must occur on at least one device in that device group before an action policy is executed. This is quicker and easier than manually selecting individual devices.

When you align a device group with an automation policy, all the devices in the device group and all child device groups and their devices are included in the automation policy.

To align an automation policy with a device group, perform the following:

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Notification/Automation* in the **Visibility** field, you will not be able to align an automation policy with the device group. Instead, you will have to manually select each device in the device group.

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. In the **Automation Policy Manager** page, you can:
 - Edit an existing automation policy. To do so, find the policy you want to edit and click its wrench icon ().
 - Create a new automation policy. To do so, click the **[Create]** button.

- When the **Automation Policy Editor** page appears, you can use the following fields to align the automation policy with a device group:

The screenshot shows the 'Automation Policy Editor' interface. At the top, there's a title bar with 'Automation Policy Editor | Editing Automation Policy [3]' and a 'Reset' button. The main form is divided into several sections:

- Policy Information:** Policy Name (PP Automation), Policy Type (Active), Policy State (Disabled), and Organization (Acme Corporation).
- Criteria Logic:** [Severity >=] [Minor,] [and 5 minutes has elapsed,] [and event is NOT cleared]
- Match Logic:** [Text search]
- Match Syntax:** (empty field)
- Repeat Time:** [Only once]
- Align With:** [Device Groups] (highlighted with a red box)
- Include events for entities other than devices (organizations, assets, etc.):**
- Available Device Groups:** A list of device groups including 'Acme: MS SQL database servers (IT Service)', 'cisco_switches', 'db_servers', 'Device Group Test', and 'em7_appliances'.
- Aligned Device Groups:** A list containing '(All devices)'.
- Available Events:** A list of events including 'Critical: AKCP: AC Voltage sensor detects no current', 'Critical: AKCP: DC Voltage sensor High Critical', 'Critical: AKCP: DC Voltage sensor Low Critical', 'Critical: AKCP: Dry Contact Sensor Low Critical', and 'Critical: AKCP: Smoke Detector Alert!'.
- Aligned Events:** A list containing 'Critical: Critical API'.
- Available Actions:** A list of actions including 'Send Email: event_escalation_Dir_of_Ops', 'SNMP Trap: EM7 Event Trap', 'SNMP Trap: PP RBA', 'Create Ticket: Create a Ticket', and 'SNMP Set: %D Test for SNMP Set'.
- Aligned Actions:** A list containing '1. SNMP Trap: PP RBA'.
- Buttons:** A 'Save' button is located at the bottom center.

- **Align With.** Specifies whether to align this automation policy with one or more devices or one or more device groups.
- **Available Device Groups.** If you selected *Device Groups* in the **Align With** field, this field displays a list of all device groups in SL1. You can select one or more device groups in this field. The selected event(s) and event criteria must occur on each selected device in each selected device group before the automation policy will be executed. To select a device group, highlight it and click the right-arrow button (>>).
- **Aligned Device Groups.** This pane displays a list of all device groups aligned with this automation policy. To deselect a device group, highlight it and click the left-arrow button (<<).

What is an Action Policy?

An **action policy** is an action that can be automatically triggered in SL1 when certain criteria are met. The triggers are defined in an **automation policy** in the **Automation Policy Manager** page (Registry > Run Book > Automation).

An action policy can perform one of the following tasks:

- Send an email message to a pre-defined list of users.
- Send an SNMP trap from SL1 to an external device.
- Create a new ticket (using ticket templates defined in **Ticket Templates** page [Registry > Ticketing > Templates])
- Update an existing ticket. An action policy can change the status and/or severity of an existing ticket and/or add a note to an existing ticket. For this action policy to trigger successfully, a ticket must be associated with the event that triggered the action.
- Write an SNMP value to an existing SNMP object on an external device.
- Query a database.
- Run a custom python script, called a snippet.
- Write an SNMP value to an existing SNMP object on an external device.

To create an action policy, go to the **Action Policy Manager** page (Registry > Run Book > Actions) and click the **[Create]** button.


The screenshot shows the 'Action Editor' window with a red title bar containing 'Close / Esc'. The main content area is titled 'Policy Editor | Creating New Action' and includes a 'Reset' button. The form contains the following fields and controls:

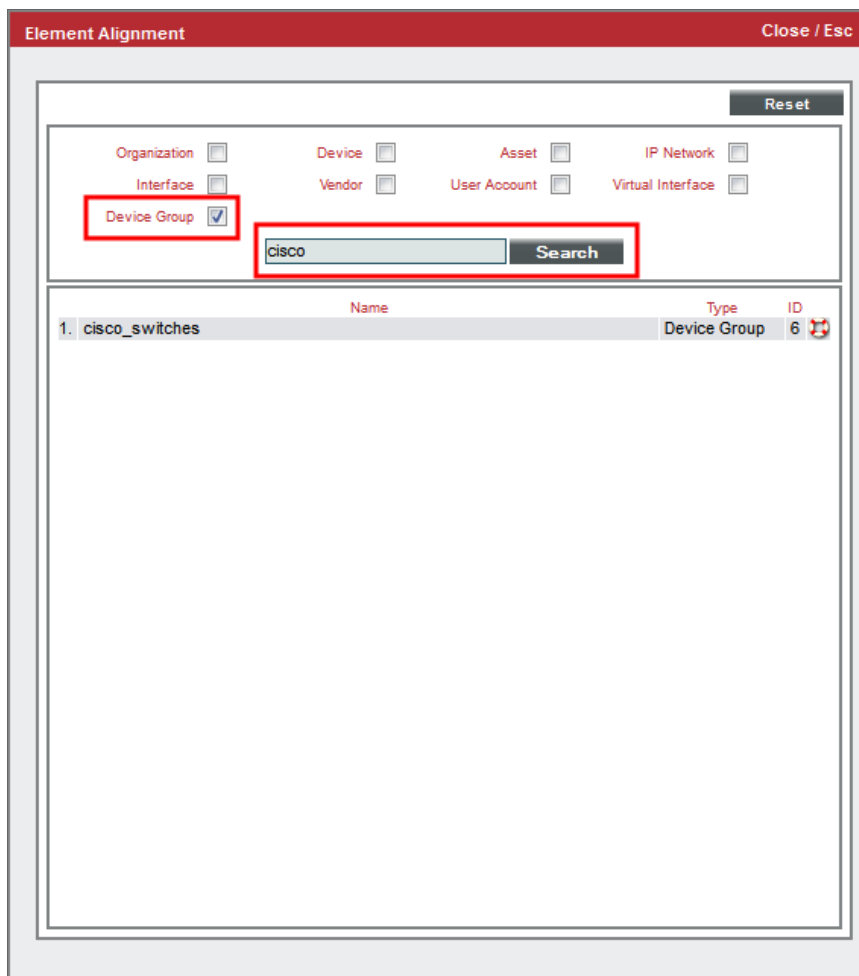
- Action Name:** A text input field.
- Action State:** A dropdown menu currently set to '[Enabled]'.
- Description:** A large text area.
- Organization:** A dropdown menu currently set to '[System]'.
- Action Type:** A dropdown menu currently set to 'Send an Email Notification'.
- Email Subject:** A text input field containing the placeholder '%S Event: %M'.
- Email Priority:** A dropdown menu currently set to '[Normal]'.
- Send as Plain Text:** A checkbox that is currently unchecked.
- Email Body:** A large text area containing the following text:

```
Severity: %S
First Occurred: %D
Last Occurred: %d
Occurrences: %c
Source: %Z
Organization: %O
Device: %X
```
- Available Emails:** A list of email addresses in a scrollable box:
 - bcorgan: bcorgan@company.com
 - dkahane: dkahane@super.com
 - em7admin: bleyland@sciencelogic.com
 - external contact: cbingley@netherfield.com
 - mantone: mantone@sciencelogic.com
 - prevere: prevere@company.com
 - samadams: samadams@company.com
 - sjohnson: sjohnson@company.com
- Assigned Emails:** An empty scrollable box.
- Navigation:** Two arrow buttons (right and left) between the 'Available Emails' and 'Assigned Emails' boxes.
- Save:** A button at the bottom center of the form.

Aligning a Ticket with a Device Group

A ticket is a request for work. This request can be in response to a problem that needs to be fixed, for routine maintenance, or for any type of work required by your enterprise. When creating a ticket you can align that ticket with a device group. To align a ticket with a device group:

1. Go to the **Ticket Console** page ([**Tickets**] tab).
2. In the **Ticket Console** page, click the [**Create**] button.
3. The **Ticket Editor** page appears. In the **Ticket Editor** page, the **Element** field allows you to select the element where the problem occurred. To select a device group, click the binoculars () to the right of the field.
4. The **Finder** page appears, where you can select the device group to align with the ticket.
5. To search for a device group, select the **Device Group** checkbox. To exclude an element from the search, unselect its checkbox.
6. In the *Search* field you can also enter a whole or partial string of text for the device group you want to find.
7. Click the [**Search**] button.






8. Click on the device group to align the device group to the ticket.

Searching for a Ticket Aligned with a Device Group

In the **Ticket Console** page you can search for existing tickets aligned with a device group. The **Ticket Console** page contains "filter-while-you-type" fields at the top of the page that allow you to filter the list of tickets by one more parameters. To search for a ticket aligned with a device group:

1. Go to the **Ticket Console** page ([**Tickets**] tab). In the **Ticket Console** page, the *Element Name* field allows you to search for device groups aligned with a ticket.
2. Enter a full or partial search string in the *Element Name* field. The list of tickets will be filtered to display the element(s) that meet your search criteria.

| Organization | Description | Severity | Queue | TID | State | Ticket Att. | Element Name | Element Type | Status | Category | Assigned To | Source | Created By |
|--------------|-------------|---------------|---------------|-----|-------|-----------------|---|--------------|--------|----------|-------------|-----------|------------|
| System | Test ticket | Sev 2 / Minor | documentation | 21 | foo | 1 mon 4 8:00 AM |  cisco <small>(3)</small>  cisco_switches | Device Group | Open | Abuse | em7admin | Automated | em7admin |

- You can access the **Device Group Editor** page for each ticket aligned with a device group by selecting its device icon () in the **Element** field. For more information on device groups, see the section on [Creating and Editing Device Groups](#).



For more information on tickets, see the manual *Ticketing*.

Assigning Device Groups and Applying Device Templates During Discovery

Overview

This chapter describes how to assign device groups and apply device templates during discovery.

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

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

This chapter includes the following topics:

| | |
|---|-----|
| <i>What is Discovery?</i> | 121 |
| <i>Assigning Devices to a Device Group During Discovery</i> | 122 |
| <i>Applying a Device Template to Devices During Discovery</i> | 124 |

What is Discovery?

Discovery is the process by which SL1 retrieves data from the devices and applications in the network. SL1 runs discovery to perform the initial discovery of your network and then nightly to collect and update information about your network. You can also manually initiate discovery for a single device, one or more device groups, or for the whole network, at any time.

SL1's Discovery tool automatically finds all the devices and components in your network. You must provide the Discovery tool with one or more IP addresses, and SL1 then finds all the devices and components in the IP range. For each discovered device or component, SL1 gathers detailed data. This data is used throughout SL1.

In SL1, discovery includes two steps: **Identification** followed by **Modeling**.

- During the initial identification step, SL1 divides and distributes the list of IPs among the collection processes running on the Data Collectors in a collector group. Each collection process works independently to discover each device and determine the device name, hostname, MAC address, and IP address of each discovered device.
- After each device has been discovered, the modeling phase begins. During the modeling phase, SL1 generates a unique identifier for each new device, assigns the device to a Device Class and a Device Category, and **optionally can assign each device to a specific Device Group and optionally can apply a device template to each device**. SL1 then reexamines each device in-depth, to align monitoring and collection tasks that correlate to the device type and the applications running on the device. SL1 then uses the appropriate Dynamic Applications to retrieve detailed configuration and performance data from the device.

During discovery, SL1 can gather the following types of information:

- For each device, performs detailed modeling of hardware, operating systems, applications, process, and services.
- Detects open network ports and generates alerts when illicit ports are found open.
- Recognizes and classifies all IANA interface types.
- Detects and models layer-2 and layer-3 networks.
- Maps and models virtual infrastructure, including VMware ESX servers and their guest operating systems.
- Automatically catalogs all discovered IP addresses, and categorizes IP networks and subnets.

Assigning Devices to a Device Group During Discovery

During discovery, you can specify that each device discovered during the discovery session be assigned to a selected device group. You can then configure and manage the devices as a device group, as described in the previous chapters of this manual.

NOTE: If the definition for a device group in the **Device Group Editor** page does not include *Discovery* in the **Visibility** field, you will not be able to automatically add all discovered devices to the device group. The device group will not appear in the list of device groups in the **Discovery Control Panel** page.

To automatically assign devices to a device group during discovery:

1. Go to the **Discovery Control Panel** (System > Manage > Discovery).
2. The **Discovery Control Panel** page appears.

3. Click the **[Create]** button to bring up the **Discovery Session Editor** modal page.

4. In the editor pane, enter values in each field. For more information on discovery, see the manual on **Discovery and Credentials**.
5. To assign devices from this discovery session to a selected device group, use the following field:
 - **Add Devices to Device Group(s)**. As SL1 discovers a device in the IP discovery list, that device is added to each selected device group. You can select one or more device groups from a list of device groups in SL1 that have "Discovery" selected in the **Visibility** field.

NOTE: A single device can be a member of multiple device groups.

6. Click the **[Save]** button to save your discovery settings. If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, this session will be queued.

Applying a Device Template to Devices During Discovery

During discovery, you can specify that a device template be applied to each device discovered during the discovery session. Normally, these devices would be automatically configured with ScienceLogic's default settings. When you specify a device template, these devices are automatically configured with the settings specified in the device template.

To automatically apply a device template to devices during discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. Click the **[Create]** button to bring up the **Discovery Session Editor** modal page.
3. In the editor pane, enter values in each field. For more information on discovery, see the manual on **Discovery and Credentials**.
4. To apply a device template to all devices from this discovery session, use the following drop-down list:
 - **Apply Device Template.** As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1.

The screenshot shows the 'Discovery Session Editor | Create New' modal window. It is divided into three main sections: 'IP and Credentials', 'Detection and Scanning', and 'Basic Settings'. The 'Apply Device Template' dropdown menu is highlighted with a red box. The dropdown menu is currently set to '[Choose a Template]'. The 'Basic Settings' section includes options for 'Discover Non-SNMP', 'Model Devices', 'Duplication Protection', 'Collection Server PID', 'Organization', and 'Add Devices to Device Group(s)'. The 'Save' button is located at the bottom center, and the 'Log All' button is at the bottom right.

5. Click the **[Save]** button to save your discovery settings. If no other discovery sessions are currently running, the session is executed immediately. If another discovery session is currently running, this session is queued.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010