Device Groups and Device Templates

Skylar One version 12.5.1

Table of Contents

Chapter 1

What is a Device Group?

Overview

A ***device group*** is a group of multiple devices in Skylar One (formerly SL1). 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 Skylar One 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' ". Skylar One 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.

NOTE: 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 Skylar One 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 in Skylar One (formerly SL1) 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:

- **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 Skylar One 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 Skylar One to monitor a website. Skylar One will periodically check the website for specified content. If the content cannot be found on the website, Skylar One 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; Skylar One 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 Skylar One 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; Skylar One 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 Skylar One to monitor the device and look for the specified service. You can define a service policy so that Skylar One 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; Skylar One 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 Skylar One to monitor the device and look for the process. You can define a process policy so that Skylar One 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; Skylar One 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. Skylar One 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 Skylar One 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, Skylar One 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 Skylar One.

Chapter

3

Creating and Editing Device Groups

Overview

This chapter describes how to create and edit device groups in Skylar One (formerly SL1).

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

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

This chapter covers the following topics:

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 (Devices > Device Groups).
2. The **Device Groups** page displays the following about each device group:
    - ***Plus-sign icon*** (+). Expands the device group and displays a list of member devices and the name, IP address, device category, device class, device Id, and organization for each member device.
    - ***Device Group Name***. Name of the device group.
    - ***ID***. Unique, numeric ID, assigned to the device group automatically by Skylar One.
    - ***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* ( ). Leads to the **Device Group Map** page, where you can view a hierarchical representation of the selected device group. For more information, see the section on *Using Device Group Maps and Views*.
- *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.

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.

Creating a Device Group

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

1. Go to the **Device Groups** page (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 Skylar One 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 Skylar One 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 "Scheduled 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 > Classic Discovery or System > Manage > Discovery in the classic user interface), 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 > Classic Discovery or System > Manage > Discovery in the classic user interface), you must explicitly set ***Visibility*** to *Discovery* for each child device group.

- ***Visibility***. Specifies where in Skylar One the device group will be visible. Choices are:
  - *Maps/Views.* If selected, the device group will appear in the **Device Group Map** page (Classic Maps > Device Maps > Device Groups), the **Custom Device Group Map** page (Classic Maps > My Customized Maps), and the **Device Group Views** page (Classic Maps > 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 > Classic Discovery or System > Manage > Discovery in the classic user interface). 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.
- *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 Skylar One. 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 Skylar One 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. Open a device group from the **Device Groups** page (Devices > Device Groups) and go to the **Static Devices and Groups** pane.
2. Click the **[Add]** button then select ***Add Devices***.
3. The **Device Alignment** modal appears and displays a list of all devices in Skylar One.
4. In the **Device Alignment** modal, 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. Open a device group from the **Device Groups** page (Devices > Device Groups) and 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.

NOTE: If you remove a static device from a device group while the device is in maintenance mode, the device will stay in maintenance mode until you disable it. You must disable the maintenance schedule on the device itself in the **Device Manager** (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface by clicking on its calendar ( ) icon. For more information, see the chapter on "Device Maintenance" in the ***Device Management*** manual.

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

1. Open a device group from the **Device Groups** page (Devices > Device Groups) and 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 Skylar One.
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. Open a device group from the **Device Groups** page (Devices > Device Groups) and 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'. Skylar One 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.

> **NOTE:** Starting with version 11.1.0, Skylar One reduced the amount of time it took to evaluate dynamic device group rules, which in previous versions of Skylar One caused Skylar One to refresh the membership of the device group too slowly, resulting in events not being suppressed for devices in the device group.

To add a dynamic rule:

1. Open a device group from the **Device Groups** page (Devices > Device Groups) and 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more organizations, Skylar One 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, Skylar One 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more device classes, Skylar One 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, Skylar One 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more device categories, Skylar One 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, Skylar One 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. Skylar One will use the string to search for devices with matching device names. If you do not use wildcard characters, Skylar One will return only devices with a device name that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any device name that begins with "term".
    - **term*. Skylar One searches for any device name that ends with "term".
    - *te?m*. Skylar One searches for any device name that contains the text "te[any single character]m".
    - *!term*. Skylar One searches for any device name that does not include the text "term".
    - *term1, term2*. Skylar One searches for any device name that contains either "term1" or "term2".

- ***Device IP***. Displays a field in which you can enter a string. Skylar One will use the string to search for devices with matching IP addresses. If you do not use wildcard characters, Skylar One will return only devices with a device IP that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any device IP that begins with "term".
    - **term*. Skylar One searches for any device IP that ends with "term".
    - *te?m*. Skylar One searches for any device IP that contains the text "te[any single character]m".
    - */term*. Skylar One searches for any device IP that does not include the text "term".
    - *term1, term2*. Skylar One searches for any device IP that contains either "term1" or "term2".
    - If you select the ***Invert*** checkbox, Skylar One 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 Skylar One (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, Skylar One 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, Skylar One 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 Skylar One (Active, NOT Active, User-Disabled, NOT User-Disabled, Unavailable, NOT Unavailable, Scheduled Maintenance, NOT Scheduled Maintenance, System-Disabled, NOT System-Disabled, User-Initiated Maintenance, NOT User-Initiated Maintenance).
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more collection states, Skylar One 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more Collector Groups, Skylar One 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, Skylar One 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 Skylar One 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, Skylar One 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, Skylar One 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. Skylar One will use the string to search for devices that are running a matching system process. If you do not use wildcard characters, Skylar One will return only devices running a process that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any process name that begins with "term".
    - **term*. Skylar One searches for any process name that ends with "term".
    - *te?m*. Skylar One searches for any process name that contains the text "te[any single character]m".
    - *!term*. Skylar One searches for any process name that does not include the text "term".
    - *term1, term2*. Skylar One searches for any process name that contains either "term1" or "term2".
    - If you select the ***Invert*** checkbox, Skylar One 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. Skylar One will use the string to search for devices that are running a matching Windows service. If you do not use wildcard characters, Skylar One will return only devices running a Windows services that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any Windows Service name that begins with "term".
    - **term*. Skylar One searches for any Windows Service name that ends with "term".
    - *te?m*. Skylar One searches for any Windows Service name that contains the text "te[any single character]m".
    - */term*. Skylar One searches for any Windows Service name that does not include the text "term".
    - *term1, term2*. Skylar One searches for any Windows Service name that contains either "term1" or "term2".
    - If you select the ***Invert*** checkbox, Skylar One 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more SKUs, Skylar One 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, Skylar One 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 Skylar One.
    - To filter the list, you can enter a string in the field under the title.
    - If you select one or more active events, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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. Skylar One will use the string to search for devices that have a matching value in the ***Make*** field in their asset records (Skylar One automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, Skylar One will return only devices that have a ***Make*** field that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any asset make that begins with "term".
    - **term*. Skylar One searches for any asset make that ends with "term".
    - *te?m*. Skylar One searches for any asset make that contains the text "te[any single character]m".
    - *!term*. Skylar One searches for any asset make that does not include the text "term".
    - *term1, term2*. Skylar One searches for any asset make that contains either "term1" or "term2".
- ***Asset Model***. Displays a field in which you can enter a string. Skylar One will use the string to search for devices that have a matching value in the ***Model*** field in their asset records (Skylar One automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, Skylar One will return only devices that have a ***Model*** field that exactly matches the string. You can use the following syntax in the field:
    - *term**. Skylar One searches for any asset model that begins with "term".
    - **term*. Skylar One searches for any asset model that ends with "term".
    - *te?m*. Skylar One searches for any asset model that contains the text "te[any single character]m".
    - *!term*. Skylar One searches for any asset model that does not include the text "term".
    - *term1, term2*. Skylar One searches for any asset model that contains either "term1" or "term2".

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

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

- ***Asset Software Version***. Displays a field in which you can enter a string. Skylar One will use the string to search for devices that have a matching ***Software Version*** field in their asset records (Skylar One automatically creates an asset record for each device during nightly auto-discovery). If you do not use wildcard characters, Skylar One 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**. Skylar One searches for any software version that begins with "term".
    - **term*. Skylar One searches for any software version that ends with "term".
    - *te?m*. Skylar One searches for any software version that contains the text "te[any single character]m".
    - *!term*. Skylar One searches for any software version that does not include the text "term".
    - *term1, term2*. Skylar One searches for any software version that contains either "term1" or "term2".

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

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

NOTE: If you input *!** in to the Dynamic Rule Operator Selector Definition field, your search returns all devices that have an empty value for that attribute.

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.

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

- ***Relationship Selector***. You can choose to include child 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, descendents, 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 Skylar One discovers devices and component devices that meet the criteria for the dynamic device group, Skylar One 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 child 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 child 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 Skylar One.
- ***Organization***. The organization to which the device is assigned.
- ***Collection State***. The current condition of data collection for the device. The device can have one or more of the following Collection States:

- *Active*. Skylar One is collecting data from the device.
- *Unavailable*. Skylar One cannot connect to the device, and will not collect data from the device until the device becomes available. A physical device falls back to executing the availability ping every five minutes, unless you have critical ping enabled. Component devices get their availability calculated by the component discovery Dynamic Application of the parent device.
- *User-Disabled*. Skylar One is not currently collecting data from the device because the user has disabled collection.
- *System-Disabled*. Skylar One is not currently collecting data from the device because the system has disabled collection.
- *Scheduled Maintenance*. Skylar One is not currently collecting data from the device because it is currently in scheduled maintenance mode.
- *User-Initiated-Maintenance*. Skylar One is not currently collecting data from the device because it has manually been put into maintenance mode by a user.
- *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. Skylar One cannot collect data from the device at this time.

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

- ***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 Skylar One.
- ***Organization***. The organization to which the device is assigned.
- ***Collection State***. The current condition of data collection for the device. The device can have one or more of the following Collection States:
    - *Active*. Skylar One is collecting data from the device.
    - *Unavailable*. Skylar One cannot connect to the device, and will not collect data from the device until the device becomes available.
    - *User-Disabled*. Skylar One is not currently collecting data from the device because the user has disabled collection.
    - *System-Disabled*. Skylar One is not currently collecting data from the device because the system has disabled collection.
    - *Scheduled Maintenance*. Skylar One is not currently collecting data from the device because it is currently in scheduled maintenance mode.
    - *User-Initiated-Maintenance*. Skylar One is not currently collecting data from the device because it has manually been put into maintenance mode by a user.
    - *Component Vanished*. The component device has vanished, i.e. is not currently being reported by its root device. Skylar One cannot collect data from the device at this time.

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

- ***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 Classic Maps > 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 (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.
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 (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
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** (Classic Maps > Classic Views > Device Groups), and the **Custom Device Group Map** (Classic Maps > 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 Skylar One the device group will be visible. Choices are:
  - *Maps/Views*. If selected, the device group will appear in the **Device Group Map** page (Classic Maps > 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 > Classic Discovery or System > Manage > Discovery in the classic user interface). 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.
- *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 Skylar One. 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 (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, select the checkbox at the top of the page.
3. In the ***Select Action*** drop-down in the bottom right of the page, select *DELETE Device Groups*.
4. 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 Skylar One.
- ***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 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.

Chapter 4

Creating and Editing Device Templates

Overview

Device templates in Skylar One (formerly SL1) 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 *Creating 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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), 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 (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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), you can use the bulk **Actions** menu or 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 Skylar One user interface:

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

This chapter covers the following topics:

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 (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
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 Skylar One.
    - ***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 ion 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*.

Creating a Device Template

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

1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. Click the **[Create]** button. The **Device Template Editor** page appears.
3. In the ***Template Name*** field, supply a name for the template.
4. 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 Skylar One 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 Skylar One to monitor a website. Skylar One will periodically check the website for specified content. If the content cannot be found on the website, Skylar One 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; Skylar One 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 Skylar One 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; Skylar One 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 Skylar One to monitor the device and look for the specified service. You can define a service policy so that Skylar One 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; Skylar One 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 Skylar One to monitor the device and look for the process. You can define a process policy so that Skylar One 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; Skylar One 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. Skylar One 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 Skylar One 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 Skylar One agent will monitor on a device and the logs that the Skylar One agent will send to Skylar One. When the Skylar One agent sends a log to Skylar One, Skylar Onedisplays the log entry in the Device Logs for the associated device. Skylar One 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; Skylar One 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.

Access & Monitoring

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

> **NOTE**: If you include a device template in a PowerPack and then install the PowerPack on a different Skylar One system, the ***Device Organization*** field will be cleared and disabled on the Skylar One 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 Skylar One to gather information from the device. This community string is defined on the **Credentials** page (Manage > Credentials) or 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 Skylar One to send information to the device. This community string is defined on the **Credentials** page (Manage > Credentials) or the **Credential Management** page (System > Manage > Credentials).

NOTE: SNMP credentials that are deleted from Skylar One will also be removed from device templates.

- ***Availability Protocol***. Protocol that Skylar One will use to communicate with the device to determine the device's availability. Choices are *TCP*, *UDP*, or *ICMP*.
- ***Avail Port***. Port that Skylar One will use to communicate with the device to determine the device's availability.
- ***Latency Protocol***. Protocol that Skylar One will use to communicate with the device to determine the device's latency. Choices are *TCP*, *UDP*, or *ICMP*.
- ***Latency Port***. Port that Skylar One will use to communicate with the device to determine the device's latency.
- ***Avail + Latency Alert***. Specifies how Skylar One 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*. Skylar One 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*. Skylar One 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 Skylar One will collect data from the device . Choices are "enabled" or "disabled".
- ***Collector Grp***. Specifies the collector group that Skylar One will use to collect data from the device. You can select from a list of existing collector groups.
- ***Coll. Type***. Specifies how Skylar One should perform discovery. The choices are:
    - *Standard*. Skylar One will perform discovery of each device based on the device's IP address. This method is appropriate for devices using standard DNS.
    - *DHCP*. Skylar One 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 Skylar One should "ping" the device. If the device does not respond, Skylar One creates an event. The choices are *disabled*, *every 5 seconds*, *every 15 seconds*, *every 30 seconds*, *every 60 seconds*, and *every 120 seconds*.

NOTE: Skylar One does not use data from the critical ping to create device availability reports. Skylar One 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.

Device Preferences

- ***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 Skylar One to perform a daily scan of the device for open ports.

- ***Auto-Update***. This checkbox specifies whether or not you want Skylar One to perform a nightly discovery of the device and update records with changes to the device. If this field is unchecked, Skylar One will not perform nightly discovery; changes to the device, including newly opened ports, will not be recorded by Skylar One.
- ***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 magnifying glass icon (🔍) in the **Device Properties** page) and during *nightly auto-discovery* (run automatically by Skylar One 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, Skylar One will scan all IP addresses on a device when looking for open ports. If the device uses multiple IP Addresses, Skylar One will scan for open ports on all IPs during initial dynamic-discovery and nightly dynamic-discovery.
- ***Dynamic Discovery***. If selected, Skylar One will automatically assign the appropriate Dynamic Applications to the device during discovery.
- ***Preserve Hostname***. If selected, the name of the device in Skylar One will remain the same, even if the name of the actual device is changed. If unselected, the Skylar One name for the device will be updated if the name of the actual device is changed.
- ***Disable Asset Update***. If selected, during nightly discovery, Skylar One 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).

Device Retention & Basic Thresholds

- ***System Latency***. During polling, Skylar One initially pings monitored devices. The value in this field is the maximum number of milliseconds for the device to respond to Skylar One's ping (round-trip time divided by 2). When the latency threshold is exceeded, Skylar One 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, Skylar One 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 Skylar One 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).
- ***SSL Certificate Purge Timeout***. Specifies the number of days after which SSL certificate data will be purged. The default value is 0 days.

NOTE: In Skylar One, 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.

Topology Settings

- ***L2 Topology*** . Select from the following Layer-2 topology options for the device:
    - *Disabled*. Disables Layer-2 topology collection and processing for the device.
    - *Processing Enabled*. Enables Layer-2 topology processing for the device using the "Enterprise Database: Topology Crunch" process to determine Layer-2 topology relationships based on device category, with the purpose of connecting network devices to each other, but uses methods other than the standard SNMP for collection.
    - *Collection and Processing Enabled*. Enables Layer-2 topology collection and processing for the device using the standard SNMP collection methods and the "Enterprise Database: Topology Crunch" process to determine Layer-2 topology relationships based on device category, with the purpose of connecting network devices to each other.
    - *Enhanced Processing Enabled*. Enables more robust Layer-2 topology processing for the device, but using methods other than the standard SNMP for collection. This enhanced processing can form Layer-2 relationships between any devices that match a MAC address from the BRIDGE-MIB or sourced from Dynamic Applications, regardless of device category.
    - *Collection and Enhanced Processing Enabled*. Enables more robust Layer-2 topology processing and collection for the device, using the standard SNMP collection methods. This enhanced processing can form Layer-2 relationships between any devices that match a MAC address from the BRIDGE-MIB or sourced from Dynamic Applications, regardless of device category.
    - *Clear Override*. If selected, the device inherits the Layer-2 topology collection and processing settings assigned to its device class.

- ***L3 Topology***. Select from the following Layer-3 topology options for the device:
    - *Disabled*. Disables Layer-3 topology collection and processing for the device.
    - *Processing Enabled*. Enables Layer-3 topology processing for the device using the "Enterprise Database: Topology Crunch" process to determine Layer-3 topology relationships, but requires all the hops in a traceroute to respond and match devices within Skylar One in order to form the relationship.
    - *Collection and Processing Enabled*. Enables Layer-3 topology collection and processing for the device using the "Enterprise Database: Topology Crunch" process to determine Layer-3 topology relationships, but requires all the hops in a traceroute to respond and match devices within Skylar One in order to form the relationship.
    - *Enhanced Processing Enabled*. Enables more robust Layer-3 topology processing for the device, where the system will form relationships between any two hops that respond and match devices in Skylar One rather than discarding incomplete traceroutes or results that include unmatched hops.
    - *Collection and Enhanced Processing Enabled*. Enables more robust Layer-3 topology processing and collection for the device, where the system will form relationships between any two hops that respond and match devices in Skylar One rather than discarding incomplete traceroutes or results that include unmatched hops.
    - *Clear Override*. If selected, the device inherits the Layer-3 topology collection and processing settings assigned to its device class. .

- ***CDP Topology***. Select from the following Cisco Discovery Protocol (CDP) topology options for the device:

    - *Disabled*. Disables CDP topology collection and processing for the device.

    - *Processing Enabled*. Enables CDP topology processing for the device using the "Enterprise Database: Topology Crunch" process to determine CDP topology relationships between two devices that both respond with CDP neighbor data, show each other as a neighbor, and are managed devices in Skylar One, but uses methods other than standard SNMP for collection.

    - *Collection and Processing Enabled*. Enables CDP topology collection and processing for the device using standard SNMP collection methods and the "Enterprise Database: Topology Crunch" process to determine CDP topology relationships between two devices that both respond with CDP neighbor data, show each other as a neighbor, and are managed devices in Skylar One.

    - *Enhanced Processing Enabled*. Enables more robust CDP topology processing for the device, but using methods other than standard SNMP for collection. This enhanced processing can form CDP relationships between two devices so long as at least one of those devices responds with CDP neighbor data and is a manged device in Skylar One.

    - *Collection and Enhanced Processing Enabled*. Enables more robust CDP topology processing and collection for the device, using the standard SNMP collection methods. This enhanced processing can form CDP relationships between two devices so long as at least one of those devices responds with CDP neighbor data and is a manged device in Skylar One.

    - *Clear Override*. If selected, the device inherits the CDP topology collection and processing settings assigned to its device class. .

- ***LLDP Topology***. Select from the following Link Layer Discovery Protocol (LLDP) topology options for the device:
    - *Disabled*. Disables LLDP topology collection and processing for the device.
    - *Processing Enabled*. Enables LLDP topology processing for the device using the "Enterprise Database: Topology Crunch" process to determine LLDP topology relationships between two devices that both respond with LLDP neighbor data, show each other as a neighbor, and are managed devices in Skylar One, but uses methods other than standard SNMP for collection.
    - *Collection and Processing Enabled*. Enables LLDP topology collection and processing for the device using standard SNMP collection methods and the "Enterprise Database: Topology Crunch" process to determine LLDP topology relationships between two devices that both respond with LLDP neighbor data, show each other as a neighbor, and are managed devices in Skylar One.
    - *Enhanced Processing Enabled*. Enables more robust LLDP topology processing for the device, but using methods other than standard SNMP for collection. This enhanced processing can form LLDP relationships between two devices so long as at least one of those devices responds with LLDP neighbor data and is a manged device in Skylar One.
    - *Collection and Enhanced Processing Enabled*. Enables more robust LLDP topology processing and collection for the device, using the standard SNMP collection methods. This enhanced processing can form LLDP relationships between two devices so long as at least one of those devices responds with LLDP neighbor data and is a manged device in Skylar One.
    - *Clear Override*. If selected, the device inherits the LLDP topology collection and processing settings assigned to its device class. .

Interface Inventory Settings

- ***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, Skylar One 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 magnifying glass icon (🔍) on the **Device Properties** page) and during *nightly auto-discovery* (run automatically by Skylar One 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, Skylar One 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 magnifying glass icon (🔍) on the **Device Properties** page) and during *nightly auto-discovery* (run automatically by Skylar One 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 Skylar One 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 Skylar One uses to communicate with each member devices.
- ***Collection State***. This field can have one of two values:
    - *Enabled*: Skylar One monitors the network interface and collects data on the network interface for reports.
    - *Disabled*: Skylar One 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 Skylar One 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 Skylar One 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 Skylar One 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 Skylar One 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, Skylar One automatically discovers which type of counter is associated with each interface. A 32-bit counter will roll-over (restart at 0) after about four billion octets (bytes) have passed through the interface. A 64-bit counter will roll-over after 1.85 x 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, Skylar One 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 Skylar One will perform the calculations for you at billing time. For example, if a provider chose the percentile factor "95", Skylar One 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 Skylar One 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 Skylar One, 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 Skylar One, 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, Skylar One 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 Skylar One should monitor an interface, Skylar One will collect data about the interface and also monitor performance thresholds for the interface. Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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 that the value selected in this field, Skylar One 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 that the value selected in this field, Skylar One 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 that the value selected in this field, Skylar One 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 that the value selected in this field, Skylar One 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 Skylar One to monitor a website. Skylar One will periodically check the website for specified content. If the content cannot be found on the website, Skylar One 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. Skylar One will query the specified website every five minutes.
    - *Disabled*. Policy is not active.
- ***Port***. Port on web-server to which Skylar One will send queries. This is usually port 80 (the HTTP port) or port 443 (the HTTPS port).
- **Timeout**. After specified number of seconds, Skylar One should stop trying to connect to the website, or if already connected, stop searching for content. If the timeout period elapses before Skylar One 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*. Skylar One replaces this variable with the IP address of the currently aligned device.
    - *%N*. Skylar One 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 Skylar One 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, Skylar One 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*. Skylar One 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, Skylar One 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, Skylar One 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 Skylar One. If the download speed is not at least the speed specified in this field, Skylar One 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, Skylar One 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 Skylar One 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, Skylar One 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, Skylar One 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 Skylar One 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*. Skylar One 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*. Skylar One will apply the TCP/IP Port Monitoring policy only to those devices where the port is available.

- ***Per-IP Policy Creation***. Specifies whether Skylar One 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*. Skylar One will apply the TCP/IP Port Monitoring policy to all IP addresses on each member device.
  - *Management IP Only*. Skylar One will apply the TCP/IP Port Monitoring policy only to IP address each member device uses to communicate with Skylar One.
- ***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 Skylar One should "ping" the device. If the device does not respond, Skylar One creates an event. The choices are:
  - *Disabled*. Skylar One will not ping the device.
  - *Enabled*. Skylar One will ping the device every 60 seconds.

NOTE: Skylar One does not use this ping data to create device availability reports. Skylar One 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 Skylar One to monitor the device and look for the specified service. You can define a service policy so that Skylar One 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 Skylar One should apply the template to member devices. Choices are:
    - *All devices*. Skylar One 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*. Skylar One 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 Skylar One.
- ***Alert if Found***. Condition under which Skylar One should create an event about the service. Choices are:
    - *Disabled*. Skylar One will create an event if the service is disabled.
    - *Enabled*. Skylar One 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 Skylar One to monitor the device and look for the process. You can define a process policy so that Skylar One 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 Skylar One should apply the template to member devices. Choices are:
    - *All devices*. Skylar One 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*. Skylar One 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.
- ***Ignore Case***. Select this checkbox if you want Skylar One to ignore case-sensitivity in the process name when determining whether to run this process policy.
- ***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, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One will not generate an alert, even if it finds this process running.

- ***Alert if Found***. If you enable this option, Skylar One 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 **[Dyn Apps]** tab of the **Device Template Editor** 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 **[Dyn 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 a Dynamic Application, click on the plus-sign (+) and then select the Dynamic Application in the ***Dynamic Application*** field.
    - To edit a Dynamic Application in device template, go to the **Subtemplate Selection** pane and select the Dynamic Application you want to edit. The fields in the right pane will be populated with values from the selected Dynamic Application. You can then edit one or more values for the Dynamic Application.
    - To delete a Dynamic Application, click the delete icon (🗑) next to its name.
- ***Align Dynamic Application With***. Specifies how Skylar One should apply the template to member devices. Choices are:
    - *All devices (align new applications and update collection states*). Skylar One will align the Dynamic Application with each device that uses the template, even if the Skylar One 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)*. Skylar One 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 Skylar One 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, Skylar One 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 Skylar One 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, Skylar One 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*. Skylar One will try to collect data for this collection object at the frequency specified in the Dynamic Application. Skylar One will try to collect data for this collection object from each device that uses the device template.
    - *Disabled*. Skylar One 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, Skylar One will connect to the device "cisco_router" and retrieve the collection objects for the Dynamic Application.

Skylar One 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. Skylar One 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, Skylar One will try to generate the report defined by the presentation object. If Skylar One 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*. Skylar One will not try to generate the report defined by the presentation object.

NOTE: As you disable a presentation object, Skylar One 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, Skylar One 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, Skylar One 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, Skylar One 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. Skylar One 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 Skylar One agent will monitor on a device and the logs that the agent will send to Skylar One. When the Skylar One agent sends a log to Skylar One, Skylar One displays the log entry in the **Device Logs & Messages** page for the associated device. Skylar One 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:

- ***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 (+) 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.
- To delete a Log File Monitoring Policy, click the delete icon ( ) next to its name.

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 Skylar One 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.
- ***Limit***. The maximum log messages the agent sends to Skylar One 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 Skylar One agent will send that log message to Skylar One. If a log message does not match this regular expression, the Skylar One agent will not send that log message to Skylar One.

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 (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. 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, Skylar One 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 (Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface).
2. Find the device template you want to edit. Click its wrench () icon.
3. The **Device Template Editor** page appears, populated with values from the selected device template.
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 in Skylar One (formerly SL1).

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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), 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 (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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), you can use the bulk **Actions** menu or 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 Skylar One user interface:

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

This chapter covers the following topics:

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 Skylar One 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 (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 ( ).
3. The **Bulk Device Configuration** page appears.
    - 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.
    - In this page you can view any settings in the device template that are different from Skylar One 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 Skylar One discovers a device, Skylar One 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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Depending on which page you are on, do one of the following:
   - On the **Devices** page, select the checkbox for each device you want to apply a device template to. Then click the **[Actions]** menu and select *Modify by Template*. The **Modify by Template** page appears.
   - On the **Device Manager** page, select the checkbox for each device you want to apply a device template to. Then click the ***Select Actions*** menu, select *Modify by Template*, and click the **[Go]** button. The **Bulk Device Configuration** page appears.
3. Do the following:

- In the ***Template*** field, select an existing device template.
- ***Save When Applied & Confirmed***. From this page, you can edit the value of any of the fields in any of the tabs of the device template.
    - *If you select this checkbox*, any changes you make to the template's fields will be saved to the template.
    - *If you don't select this checkbox*, 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 device template and any changed field values to the selected devices.
5. The **Device Setting Confirmation** page appears.
    - In this page, you can view any settings in the device template that are different from Skylar One 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 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 (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 ( ).

3. The **Bulk Device Configuration** page appears.
    - 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.
    - In this page, you can view any settings in the device template that are different from Skylar One 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 **Devices** page or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Depending on which page you are on, do one of the following:
    - On the **Devices** page, select the checkbox for each device you want to apply configuration settings to. Then click the **[Actions]** menu and select *Modify by Template*. The **Modify by Template** page appears.

- On the **Device Manager** page, select the checkbox for each device you want to apply configuration settings to. Then click the ***Select Actions*** menu, select *Modify by Template*, and click the **[Go]** button. The **Bulk Device Configuration** page appears.

3. Do the following:
   - In the ***Template*** field, select *New/One-Off Template*.
   - ***Save When Applied & Confirmed***. From this 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 checkbox*, any changes you make to any of the fields on any of the tabs will be saved to a new template.
     - *If you don't select this checkbox*, 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.
4. Click the **[Apply]** button to apply the changed field values to the selected devices.
5. The **Device Setting Confirmation** page appears.
   - In this page, you can view any settings in the device template that are different from Skylar One 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 **[Apply]** button in the **Device Setting Confirmation** page.
7. The changed settings will be applied to the selected devices.

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 Skylar One.
- ***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

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 Skylar One to write to the devices.
- ***Availability Protocol***. We selected ICMP (ping) as our availability protocol. This means that Skylar One will ping a device to determine its availability.
- ***Latency Protocol***. We selected ICMP (ping) as our latency protocol. This means that Skylar One will ping a device to determine its latency.
- ***Collection***. We selected *Enabled*, so that Skylar One 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, Skylar One will automatically assign the appropriate Dynamic Applications to each device that uses this template.
- ***Daily Port Scans***. We enabled this option. Skylar One 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 Skylar One if the name of the device is changed on the device.
- ***Auto-Update***. We enabled this option. Skylar One 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.

Chapter 6

Using Device Group Maps and Views

Overview

This chapter describes views and maps for device groups in Skylar One (formerly SL1).

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

- From the **Device Groups** page (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 **Classic Maps** (Maps > Classic Maps or the **[Views]** tab in the classic user interface) you can view an icon-based view of a device group from the Device Maps > Device Groups view. 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 **Classic Maps** (Maps > Classic Maps or the **[Views]** tab in the classic user interface), you can also view a topology-based view of a device group from the Topology Maps view. 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, Skylar One will not create a device group View for the device group.

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

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

This chapter covers the following topics:

Viewing the 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 (Classic Maps > 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 (Devices > Device Groups).
2. In the **Device Groups** page, find the device group for which you want to view a map and click its group map view icon ( ). The map opens in a new window.
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 (Classic Maps > 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 Classic Maps > My Customized Maps and click the name of the device group you want to view.
2. 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:

- ***My Customized Maps***. Personalized maps that you create.
- ***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 Skylar One, even if the device group associated with the map was defined with the field ***Shared*** (visible to all users) set to *no*.
- ***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 (Classic Maps > 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 (Classic Maps > 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

The blue navigation bar at the top of a map on the **Classic Maps** page includes the following:

- ***Search***. Type some or all of a node name in this field to search for specific nodes on the current map. Nodes that match the search criteria are highlighted in the map. Delete the search text to clear the search.
- **[Selections]** button(). After you select one or more nodes, you can click this button to show the details of that node or nodes in a **Details** pane to the right of the map. If you have more than one node selected, click the down arrow icon to select the node for which you want to view the **Details** pane. You can view the status for that node and the events associated with that node on the **Details** pane.

> **NOTE:** The number in the red circle on **Selections** () shows how many items are currently selected. If you selected more than one node, use the **[Previous]** and **[Next]** buttons at the bottom of the **Details** pane to view properties for the other nodes.

> **NOTE:** If you select two device nodes, you can click **[Selections]** () and select *Create Relationship* to create a relationship between those two device nodes in the map.

- **[Settings]** button (). This drop-down contains tabs for nodes, links, map settings, and edit shapes.
- **[Reset]** button (). Click to revert any unsaved changes you have made to your map.
- **[Save]** button (). Click to save any changes you have made to your map.

Chapter 7

Scheduling Downtime for a Device Group

Overview

This chapter describes how to schedule maintenance times for device groups in Skylar One (formerly SL1).

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 Skylar One 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 Skylar One user interface:

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

This chapter covers the following topics:

Viewing the Schedule Manager

You can view, create, edit, or delete scheduled or recurring maintenance windows for specific device groups from the **Schedule Manager** page (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface).

The **Schedule Manager** displays the following information about each scheduled or recurring device group maintenance window:

- ***Schedule Summary***. Displays the name assigned to the scheduled process.
- ***Schedule Description***. Displays a description of the scheduled process.
- ***Event ID***. Displays a unique, numeric ID for the scheduled process. Skylar One automatically creates this ID for each scheduled process.
- ***sch id***. Displays a unique, numeric ID for the schedule. Skylar One automatically creates this ID for each schedule.
- ***Context***. Displays the area of Skylar One 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 Skylar One from the **Schedule Manager** page. Skylar One 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 (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface).
2. Click **[Create]**. The **Schedule Editor** modal appears.
3. On the **Schedule Editor** modal, make entries in the following fields:

   Basic Settings

   - ***Schedule Name***. Type a name for the scheduled process.
   - ***Schedule Type***. Indicates the scheduled process type (such as Tickets, Reports, or Devices).
   - ***Visibility***. Select the visibility for the scheduled process. You can select one of the following:
     - *Private*. The scheduled process is visible only to the owner selected in the ***Owner*** field.
     - *Organization*. The scheduled process is visible only to the organization selected in the ***Organization*** field.
     - *World*. The scheduled process is visible to all users.
   - ***Organization***. Select the organization to which you want to assign the scheduled process.
   - ***Owner***. Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
   - ***Preserve Schedule***. Select this checkbox to exclude this schedule from being pruned after expiration.
   - ***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 Skylar One 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 Skylar One will not automatically adjust for daylight savings time. In addition, if you select a specific time zone, such as *EST*, that does not exist during daylight savings time observance, your schedules will be saved and execute at unexpected times.

- ***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.
    - *Every Xth day of the Week*. The scheduled process occurs at a monthly interval based on a day of the week. The day of the week displayed in this option matched the day selected in the ***Start Time*** field. For example, if you set the ***Start Time*** to Thursday, August 5th and that day is the first Thursday of the month, then the recurrence option will be *Every 1st Thursday*, and the scheduled process will occur monthly on the first Thursday of the month.

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 Skylar One should perform collection on the device during the scheduled maintenance. Choices are:
    - *Enabled*. During scheduled maintenance, Skylar One will collect data from the device, but no events will be triggered for the device.
    - *Disabled*. During scheduled maintenance, Skylar One will not collect data from the device. No events will be triggered for the device.

    NOTE: If a patch window is set, data collection will continue when a maintenance window opens and stop only during the patch window instead.

- ***Patch Window***. You can specify a "patch window" within the larger maintenance period. The "patch window" allows Skylar One 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 Skylar One. 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 Skylar One, 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, Skylar One generates an event saying that the server is going into maintenance mode. Because you have defined a patch window, Skylar One continues to monitor this server as normal.
  2. At 3:00, you apply the patch to the server. The server reboots, and Skylar One 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. Skylar One suppresses the event that triggered the patch maintenance window and instead generates an event "Patch Maintenance Window Opened".
  4. For the next 15 minutes, Skylar One will suppress all events for the device.
  5. At 3:15, Skylar One will generate an event for "Patch Maintenance Window Closed". This event clears the previous event "Patch Maintenance Window Opened".
  6. Skylar One 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 Skylar One 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 (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface).

NOTE: If you remove a static device from a device group while the device is in maintenance mode, the device will stay in maintenance mode until you disable it. You must disable the maintenance schedule on the device itself in the **Device Manager** (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface by clicking on its calendar ( ) icon. For more information, see the chapter on "Device Maintenance" in the ***Device Management*** manual.

To enable or disable one or more scheduled or recurring device group maintenance windows:

1. Go to the **Schedule Manager** page (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface).
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 (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface). To do this:

1. Go to the **Schedule Manager** page (Devices > Device Groups > calendar icon, or Registry > Devices > Device Groups > calendar icon in the classic SL1 user interface).

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 in Skylar One (formerly SL1).

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 on the **Events** page or on the **Event Console** page (Events > Classic Events, or the Events tab in the classic SL1 user interface). 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 on the **Events** page or on 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 Skylar One user interface:

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

This chapter covers the following topics:

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 on the **Events** page or on the **Event Console** page (Events > Classic Events, or the Events tab in the classic SL1 user interface). On either of these pages, 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 search fields on the page allow you to filter the entire list of displayed events by a single parameter. Skylar One will update the page and display only events that have a matching parameter.

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

- ***Search***. You can select from a number of parameters, including:
    - *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. Skylar One 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.

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**: To be able to suppress an event for a device group, the **Device Group Editor** page for that device group must include *Event Suppression* in the ***Visibility*** field.

To suppress an event for a device group:

1. Go to the **Event Policies** page (Events > Event Policies, or Registry > Events > Event Manager in the classic SL1 user interface).
2. Click the Actions icon (⋮) for the event policy you want to edit and select *Edit*.
3. When the **Event Policy Editor** page appears, select the **[Suppressions]** tab.
4. In the **[Suppression]** tab, you can define or edit the following:
   - ***Device Groups***. Specifies the device groups on which you can suppress the event. To suppress the event on all devices in a device group, click the **[Select Device Groups]** button and select one or more device groups from the **Available Device Groups** window. The device group(s) will then appear in the list under ***Device Groups***. To remove a device group from the list, click the Close icon (✕) next to the device group in the list.

     > **NOTE:** You can use the box at the top of the ***Available Device Groups*** field to filter the list of device groups. You can enter an alpha-numeric string in the box, and the ***Available Device Groups*** field will include only device groups that match the string.

     > **NOTE:** Only device groups that have *Event/View Suppression* enabled will appear in this field.

5. Click **[Save]** to save your changes to the event policy.

Suppressing an Event for a Device Group in the Classic Skylar One User Interface

To suppress an event for a device group in the classic Skylar One user interface:

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.

Chapter 9

Automation Policies and Tickets

Overview

This chapter describes how to use run book automation and action policies with device groups in Skylar One (formerly SL1).

Skylar One includes automation features that allow you define specific conditions and the actions you want Skylar One 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***.)

Skylar One 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 Skylar One user interface:

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

This chapter covers the following topics:

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

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 > Classic Tickets, or the **[Tickets]** tab in the classic Skylar One user interface).
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 magnifying glass icon ( ) 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 > Classic Tickets, or the **[Tickets]** tab in the classic Skylar One user interface). 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.
3. 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***.

Chapter

10

Assigning Device Groups and Applying Device Templates During Discovery

Overview

This chapter describes how to assign device groups and apply device templates during discovery in Skylar One (formerly SL1).

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

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

This chapter covers the following topics:

What is Discovery?

Discovery is the process by which Skylar One retrieves data from the devices and applications in the network. Skylar One 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.

Skylar One'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 Skylar One then finds all the devices and components in the IP range. For each discovered device or component, Skylar One gathers detailed data. This data is used throughout Skylar One.

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

- During the initial identification step, Skylar One 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 beings. During the modeling phase, Skylar One 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***. Skylar One 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. Skylar One then uses the appropriate Dynamic Applications to retrieve detailed configuration and performance data from the device.

During discovery, Skylar One 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 classic 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.

NOTE: You can assign a device to a device group only during a classic discovery session. If you are using a guided or unguided discovery workflow from the **Devices** page, you can assign devices to a device group after they have been discovered.

To automatically assign devices to a device group during a classic discovery session:

1. Go to the **Discovery Control Panel** (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
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 Skylar One 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 Skylar One 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.

Assigning Devices to a Device Group After Discovery

In addition to assigning devices to a device class during classic discovery, you can also assign devices to a device group after the devices have already been discovered, regardless of the discovery type.

The steps for doing so vary based on whether you are adding devices to a device group from the **Devices** page or from the **Device Manager** page.

To assign devices to a device group from the **Devices** page:

1. Go to the **Devices** page.
2. Select the checkbox for each device you want to add to a device group, then click the **[Actions]** menu and select *Add to Device Group*. The **Add to Device Group** modal appears.
3. Select one or more device groups from the list, and then click **[Add]**.
4. On the confirmation modal that displays, click **[Proceed]**.

To assign devices to a device group from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Select the checkbox for each device you want to apply a device template to.
3. Click the ***Select Actions*** menu, select a device group from the **Add to Device Group** section, and then click the **[Go]** button.

> **NOTE:** If there are a large number of device groups and the device group you want to select does not appear in the list, select the *more device groups...* option from the **Add to Device Group** section of the ***Select Actions*** menu and then click the **[Go]** button. When the **Add Devices to Group** modal appears, select a device group from the list and then click **[Save]**.

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.

The steps for applying a device template during discovery vary based on whether you are using an unguided network discovery workflow or a classic discovery session.

To automatically apply a device template to devices during an unguided network discovery workflow:

1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** wizard appears.
4. Complete the fields on the **Add Devices** wizard. For more information on these fields, see the manual on ***Discovery and Credentials***.
5. To apply a device template to all devices from this discovery session, on the **Discovery Session Details** page of the **Add Devices** wizard, click the down arrow icon ( ) next to the ***Advanced options*** field to access additional discovery options, then use the following drop-down list:
   - ***Select Device Template***. As Skylar One 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 Skylar One.
6. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session. If you selected the **Run after save** option on the **Discovery Session Details** page, the discovery session runs automatically upon saving.

To automatically apply a device template to devices during classic discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
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 Skylar One 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 Skylar One.
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.

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

International: +1-703-354-1010