Device Management

Skylar One version 12.5.21

Table of Contents

Introduction **12**

What is a Device? 13

What is a Device Record? 13

What is a Device Class? 14

What is a Device Category? 14

How Does Skylar One Manage Devices? 15

What is Discovery? 16

What is a Credential? 16

Using Multiple Credentials 16

What is a Virtual Device? 17

What are Component Devices? 17

What is a Dynamic Application? 18

What is a Skylar One Agent? 18

What is Virtualization? 19

What is an Asset Record? 19

Using the Devices Page **21**

Viewing the List of All Devices 22

Viewing Additional Data about a Device 26

Adding Devices with Discovery 27

Creating a Physical Device without Running Discovery 27

Creating a Virtual Device 27

Installing an Agent 28

Merging and Unmerging Devices 28

Merging Devices from the Devices Page 29

Unmerging Devices from the Devices Page 31

Designating Favorite Devices 31

Aligning a Device with a Different Organization 32

Assigning a New Icon to a Device 32

Deleting a Device 33

Running a Device Report 33

Performing Bulk Actions on Multiple Devices 34

Using the Device Investigator **37**
What is the Device Investigator? 37
Using the Info Drawer on the Device Investigator Page 40
Running a Device Report 42
Using Device Tools in the Action Runner 43
Overview of the Device Investigator Tabs 45
The Investigator Tab 45
Customizing the Appearance of Widgets on the Investigator Tab 47
Adding and Removing Metrics on the Investigator Tab 48
Editing the Metric Panel Order on the Investigator Tab 48
Combining Charts on the Investigator Tab 49
Applying a Custom Device Investigator Layout to Other Devices 49
Creating a New Custom Investigator Layout 50
Selecting an Existing Custom Device Investigator Layout 51
Managing Custom Device Investigator Layouts 51
The Settings Tab 53
The Anomaly Detection Tab 60
The Attributes Tab 61
The Changes Tab 62
About the Changes Widget 62
Configuring and Enabling the Changes Widget 63
Creating a SOAP/XML Credential for Skylar Automation (PowerFlow) 64
Syncing Skylar One Devices with ServiceNow 64
Editing the Run Book Action (ServiceNow Integrations only) 65
Syncing Skylar One Devices with Skylar Compliance 65
Permanently Enabling the Widget 65
Temporarily Enabling the Widget 67
The Collections Tab 68
The Configs Tab 69
The Events Tab 70
The Interfaces Tab 71
The Journals Tab 71

The Logs Tab ... 71
The Map Tab ... 73
The Monitors Tab ... 73
The Notes Tab ... 74
The Performance Metrics Tab ... 75
The Ports Tab ... 76
The Processes Tab ... 76
The Redirects Tab ... 77
The Relationships Tab ... 78
The Schedules Tab ... 78
The Services Tab ... 78
The Software Tab ... 79
The Summary Tab ... 79
The Thresholds Tab ... 80
The Tickets Tab ... 81
Using the Device Manager Page ... 82
Viewing the List of All Devices ... 83
Device Manager Preferences ... 86
Using the Advanced Filter with the List of Devices ... 86
Generating a Report for Multiple Devices ... 87
Generating a Report for a Single Device ... 87
Viewing the List of Component Devices ... 88
Availability for Component Devices ... 91
Viewing Child Devices ... 91
Using the Advanced Filter with the List of Component Devices ... 92
Bulk Actions in the Device Management Page ... 92
Bulk Actions for Component Devices ... 94
Bulk Merging and Unmerging of Devices in the Classic User Interface ... 95
Performing a Bulk Device Merge in the Classic User Interface ... 96
Performing a Bulk Device Unmerge in the Classic User Interface ... 98
Managing a Single Device with the Device Administration Panel ... 99
What is the Device Administration Panel? ... 100

Actions Menu 101
Device Properties 104
Viewing Read-Only Information About the Device 105
Editing Device Settings 106
Identification 106
Monitoring & Management 106
Topology Settings 110
Preferences 115
Adding an IP Address to a Device 116
Removing an IP Address from a Device 117
Managing Device IPs 117
Clearing the Device Cache 119
Aligning a Secondary Credential 119
Adding the Device to a Device Group 120
Creating a Ticket About the Device 122
Adding a Note to a Device 122
Aligning Custom Attributes with a Device 123
Creating a New Extended Custom Attribute 124
Deleting an Extended Custom Attribute from a Device 125
Associating a Product SKU with the Device 125
Merging Devices 126
Merging and Unmerging Devices from the Devices Page 127
Merging Devices from the Devices Page 127
Unmerging Devices from the Devices Page 128
Merging Individual Devices in the Classic User Interface 129
Unmerging Individual Devices in the Classic User Interface 130
Performing Administrative Tasks for One or More Devices 130
Shortcut Keys for the Device Administration Panel 132
Device Toolbox 134
What is the Device Toolbox? 134
Accessing the Device Toolbox page 134
Viewing the Session Logs 136

Device Classes and Device Categories **138**
Device Classes 139
Generic | SNMP Device Class 139
Non-SNMP Device Classes 139
Component Device Classes 139
Agent-Only Device Classes 140
Legacy ICMP Device Classes 140
Viewing the List of Device Classes 141
Viewing the List of Device Classes in the Classic Skylar One User Interface 142
Creating Device Classes 143
Creating a New SNMP-Enabled Device Class 144
Editing an SNMP-Enabled Device Class 152
Creating a New Device Class for a Device with Device Class "Generic | SNMP" 152
Creating a New Device Class for Devices That Do Not Support SNMP 153
Applying the New Device Class 157
Maintaining the New Device Class During Auto-Discovery 158
Editing a Device Class That is Not SNMP-Enabled 158
Creating a New Component Device Class 159
Editing a Component Device Class 160
Managing Device Classes 160
Manually Assigning a Device Class to a Device 160
Changing the Icon for a Device Class 161
Managing Device Classes in the Classic Skylar One User Interface 162
Manually Changing the Device Class for a Device in the Classic Skylar One User Interface 163
Changing the Icon for a Device Class in the Classic Skylar One User Interface 163
Aligning One or More Device Classes with a Device Dashboard 164
Deleting One or More Device Classes 164
Device Categories 165
"Pingable" Device Category 165
Viewing the List of Device Categories 166
Creating a New Device Category 167
Editing a Device Category 168

Duplicating a Device Category ... 168
Assigning an Icon to a Device Category ... 168
Managing Device Categories in the Classic Skylar One User Interface ... 169
Viewing the List of Device Categories in the Classic Skylar One User Interface ... 169
Creating a New Device Category in the Classic Skylar One User Interface ... 170
Editing a Device Category in the Classic Skylar One User Interface ... 171
Deleting a Device Category ... 171
Aligning One or More Device Categories with a Device Dashboard ... 171
Device Relationships ... **173**
What are Device Relationships? ... 174
Viewing the List of Device Relationships ... 175
Viewing Relationships for a Single Device ... 176
Viewing Device Topology Maps ... 178
Defining Device Relationships ... 179
Event Correlation ... 179
Events that Might Appear on the Events Page ... 180
Defining Event Correlation ... 180
Example: Child Event Suppression ... 181
Layer-2 Topology Collection and Processing ... 182
Layer-2 Topology Processing ... 183
CDP Topology Collection ... 183
CDP Topology Processing ... 185
LLDP Topology Collection ... 185
LLDP Topology Processing ... 186
Layer-3 Topology Collection ... 187
Layer-3 Topology Processing ... 187
ARP Topology Collection ... 188
ARP Topology Processing ... 188
Device Maintenance ... **189**
What is Scheduled Maintenance? ... 189
What is User Maintenance? ... 191
The Maintenance Minimum Severity Setting ... 191

Enabling and Disabling User Maintenance for a Single Device 191
Enabling and Disabling User Maintenance for One or More Devices 192
Scheduling Maintenance for a Single Device 193
Viewing the Schedule Manager 193
Defining a Scheduled or Recurring Device Maintenance Window for a Single Device 194
Scheduling Maintenance for One or More Devices 197
Enabling or Disabling Scheduled Maintenance for One or More Devices 197
Deleting Scheduled Maintenance for One or More Devices 198
Managing Dynamic Applications 199
Viewing the List of All Dynamic Applications in Skylar One 199
Managing the Dynamic Applications Aligned to a Device 203
Viewing the List of Dynamic Applications Aligned to a Device 204
Viewing Information about a Dynamic Application Aligned to a Device 205
Changing the Credential for a Dynamic Application Aligned to a Device 206
Updating the Poll Frequency for a Dynamic Application Aligned to a Device 207
Manually Aligning a Dynamic Application to a Device 207
Viewing the Status of a Dynamic Application Aligned to a Device 208
Understanding the Found Status 209
Understanding the Collecting Status 209
Enabling and Disabling Dynamic Application Data Collection for a Device 210
Enabling and Disabling Collection for Specific Collection Objects 210
Running a Dynamic Application on a Device 210
Managing the Dynamic Applications Associated with a Device in the Classic Skylar One User Interface 211
Viewing the Dynamic Applications Associated with a Device in the Classic Skylar One User Interface 211
Manually Associating a Dynamic Application with a Device in the Classic Skylar One User Interface 213
Editing the Credential Associated with a Dynamic Application in the Classic Skylar One User Interface 214
Viewing the Status of a Dynamic Application Associated with a Device in the Classic Skylar One User Interface 215
Found 215
Collect 215

Performing Other Administrative Tasks for an Aligned Dynamic Application in the Classic Skylar One User Interface ... 216
Enabling or Disabling Objects ... 216
Restarting Automatic Maintenance of Collection Objects ... 217
Editing the Poll Frequency for a Dynamic Application on the Current Device ... 217
Stopping Data Collection for a Dynamic Application ... 218
Resetting Statistical Data for a Dynamic Application ... 218
Resetting Persistent Session Objects for a Dynamic Application ... 219
Testing Data Collection for a Dynamic Application ... 220
Removing Data Collected by a Dynamic Application ... 220
How Skylar One Manages the Collection Status for Dynamic Applications ... 221
Stopping Collection ... 221
Starting Collection ... 222
Collection Objects that are Excluded from Maintenance ... 222
Status of Objects for Deviation ... 222
Bulk Un-Aligning Dynamic Applications ... 223
Setting Thresholds for Dynamic Applications ... 223
Dynamic Applications and Discovery ... 224
How Does Skylar One Align Dynamic Applications During Discovery? ... 224
Queuing Discovery from the Dynamic Applications Manager Page ... 225
Device Thresholds and Data Retention ... 226
Global Settings for Thresholds ... 227
Device Thresholds ... 232
Defining Device Thresholds in the Classic Skylar One User Interface ... 239
Bulk Management with Device Groups and Device Templates ... 241
What is a Device Group? ... 241
What is a Device Template? ... 242
Creating a Physical Device without Running Discovery ... 245
Requirements ... 246
Using the User Interface to Create a Physical Device ... 246
Creating a Physical Device from the Devices Page ... 246
Creating a Physical Device from the Device Manager Page ... 246

Managing Physical Devices Created in the User Interface 247
Using a CSV File to Create Multiple Physical Devices 247
Creating Multiple Physical Devices Using a CSV File from the Devices Page 249
Creating Multiple Physical Devices Using a CSV File from the Device Manager Page 249
Managing Physical Devices Created Using a CSV File 250
Using the API to Create a Physical Device 250
Creating a Physical Device with the API 250
Example 251
Managing Physical Devices Created with the API 253
Available Actions for the Device Resource 253
Virtual Devices 256
What is a Virtual Device? 256
Defining a Virtual Device 257
Creating a Virtual Device from the Devices Page 257
Creating a Virtual Device from the Device Manager Page 257
Directing Data to a Virtual Device 258
Redirecting Log Data to a Virtual Device 258
Aligning a Dynamic Application with a Virtual Device 259
Aligning a Dynamic Application with a Virtual Device from the Device Investigator 259
Aligning a Dynamic Application with a Virtual Device from the Device Administration Panel 260
Customizing the User Interface for a Device 262
Custom Navigation in the Classic User Interface 262
Editing a Custom Navigation tab 263
Vanishing & Purging Devices 265
Setting Vanish and Purge Thresholds 266
Viewing the List of Vanished Devices 267
Using the Advanced Filters 269
Unmerging Vanished Devices 269
Manually Purging Selected Devices 270
Setting One or More Devices to Never Purge 270
Device Dashboards 271
Viewing the List of Device Dashboards 272

Creating a Device Dashboard ... 273
Aligning Device Dashboards ... 273
Aligning a Device Dashboard with a Device ... 274
Aligning a Device Dashboard with a Device Class ... 274
Aligning a Device Dashboard with a Device Category ... 275
Aligning a Device Dashboard with a Dynamic Application ... 275
Editing a Device Dashboard ... 276
Deleting a Device Dashboard ... 276
Copying a Device Dashboard ... 277
Defining the Global Default for Device Dashboards ... 277
Unaligning a Device Dashboard ... 278
Moving Alignment for Device Dashboards ... 278
Using Custom Attributes ... **279**
Custom Attributes ... 279
Viewing the List of Custom Attributes ... 280
Viewing the List of Subscribers for a Custom Attribute ... 282
Creating Custom Attributes ... 284
Deleting One or More Custom Attributes ... 285
Adding Custom Attributes for a Device ... 285
Adding Custom Attributes for a Device in the Classic Skylar One User Interface ... 287
Custom Attributes in the ScienceLogic API ... 287
Using the ScienceLogic API to View, Create, and Edit Custom Attributes ... 288
Using a Dynamic Application to Create and/or Populate Custom Attributes ... 288
Using Custom Attributes to Define Device Groups ... 290
Viewing Custom Attributes in the Custom Table Widget ... 291

Chapter 1

Introduction

Overview

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

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

This chapter covers the following topics:

What is a Device? 13
What is a Device Record? 13
What is a Device Class? 14
What is a Device Category? 14
How Does Skylar One Manage Devices? 15
What is Discovery? 16
What is a Credential? 16
What is a Virtual Device? 17
What are Component Devices? 17
What is a Dynamic Application? 18

What is a Skylar One Agent? *18*
What is Virtualization? *19*
What is an Asset Record? *19*

What is a Device?

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

Some of the devices that Skylar One can monitor are:

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

In Skylar One, devices also include component devices and virtual devices.

What is a Device Record?

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

- Physical network hardware, such as servers, switches, routers, or printers.
- A component of a larger system, such as a data store in a hypervisor system or a blade server.

- Any other entity about which you want to collect data, but want or need to associate that data with a container that does not correspond directly to a physical device or a component. For example, you might configure a device record that represents a web site or a cloud service.

What is a Device Class?

Device classes determine:

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

Administrators can define new or legacy device classes and customize properties of existing device classes on the **Device Classes** page (Devices > Device Classes), or on the **Device Class Editor** page (System > Customize > Device Classes) in the classic Skylar One user interface.

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

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

The following sections describe the types of device classes used in Skylar One.

What is a Device Category?

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

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

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

How Does Skylar One Manage Devices?

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

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

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

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

What is Discovery?

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

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

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

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

What is a Credential?

Credentials are access profiles that allow Skylar One to retrieve information from devices and from software applications on devices. Credentials typically include information such as a username and password, as well as any additional information required for accessing and monitoring devices. Dynamic Applications in Skylar One use credentials to retrieve SNMP information, database information, SOAP information, XML information, XSLT information, and WMI information.

Using Multiple Credentials

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

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

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

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

What is a Virtual Device?

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

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

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

What are Component Devices?

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

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

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

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

Depending on your Key Privileges, you can access the Device Management tools, the Device Administration tools, view details about each device's interfaces, generate and print a report about a device, file a ticket about a device, view an asset record for a device, and perform bulk administrative tasks from this page.

What is a Dynamic Application?

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

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

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

- SNMP
- SQL
- XML
- SOAP
- XSLT (uses SOAP and XSLT to convert XML data to a new format)
- WMI (Windows Management Instrumentation), including WMI and WBEM
- Windows PowerShell
- Custom Python applications (called "snippets") for proprietary or more complex data retrieval

What is a Skylar One Agent?

The ***Skylar One agent*** is a program that you can install on a device monitored by Skylar One. There is a Windows agent, an AIX agent, a Solaris agent, and a Linux agent. The agent collects data from the device and pushes that data back to Skylar One.

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

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

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

What is Virtualization?

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

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

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

Virtual machines are frequently used to:

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

What is an Asset Record?

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

In Skylar One, asset records can contain information about:

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

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

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

Chapter 2

Using the Devices Page

Overview

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

> **NOTE:** The list of devices on the **Devices** page matches the list of devices on *the Device Manager page* (Devices > Classic Devices) in the classic Skylar One user interface.

This chapter covers the following topics:

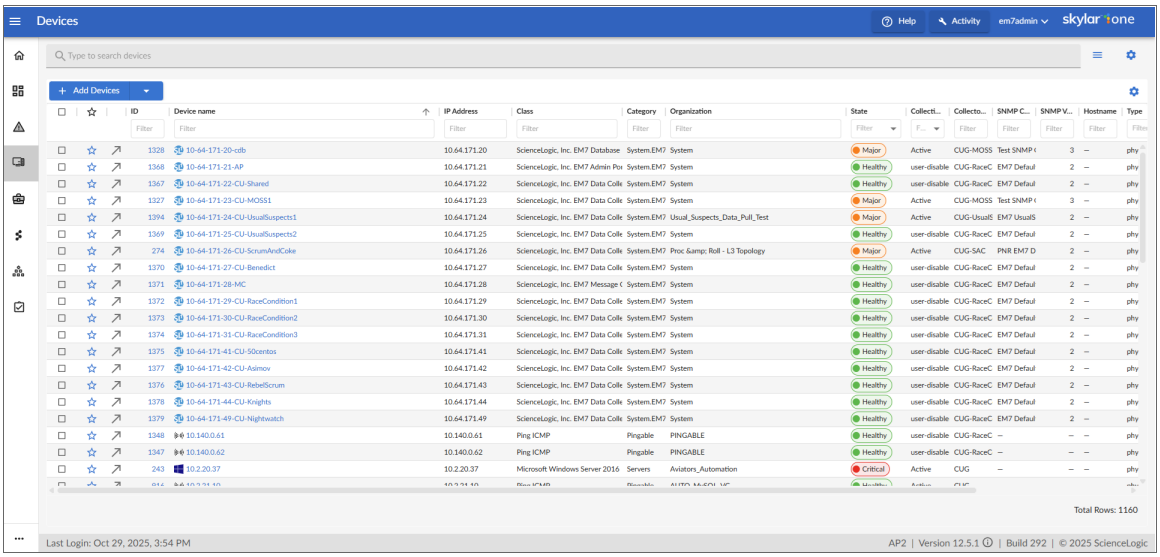
Viewing the List of All Devices 22
Viewing Additional Data about a Device 26
Adding Devices with Discovery 27
Creating a Physical Device without Running Discovery 27
Creating a Virtual Device 27
Installing an Agent 28
Merging and Unmerging Devices 28
Designating Favorite Devices 31
Aligning a Device with a Different Organization 32
Assigning a New Icon to a Device 32

Deleting a Device 33
Running a Device Report 33
Performing Bulk Actions on Multiple Devices 34

Viewing the List of All Devices

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

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



TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

TIP: You can use the ***Search*** field to look for specific items in the list. For more information, see *Using Basic Search* in the ***Introduction to Skylar One*** manual. If you are looking for a very specific set of device classes, click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. In this mode, you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see *Performing an Advanced Search* in the ***Introduction to Skylar One*** manual.

TIP: If you do not see one of these columns, click the gear icon (⚙) and then select *Column Preferences* to add or remove columns. You can also drag columns to different locations on the page or click on a column heading to sort the list by the values in that column. Skylar One retains any changes you make to the columns that appear on the page and will automatically recall those changes the next time you visit the page. For more information, see the section on *Editing the Settings for an Inventory Page* in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

NOTE: By default, the **Devices** page footer displays the total number of devices discovered. If you apply a filter, the footer will display the total number of search returns that satisfy your filter and the total number of devices available on your machine.

For each device, the **Devices** page can display the following information:

- ***ID***. The Device ID. This is a unique number that Skylar One automatically assigns to the device during discovery.
- ***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.
- ***IP Address***. The device's IP address.
- ***Class***. The manufacturer and type of device. The device class is automatically assigned during discovery, at the same time as the category.
- ***Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, and printers, among others. The category is automatically assigned during discovery, at the same time as the as device class. For more information about device categories, see the chapter on "Managing Device Classes and Device Categories" in the ***Device Management*** manual.
- ***Organization***. The organization to which the device is assigned.
- ***State***. The current condition of the device, based upon events generated by the device. The device can have one of the following States:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.
    - *Notice*. Device has an informational event associated with it.
    - *Healthy*. Device is running with no problems.

- ***Collection 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*.

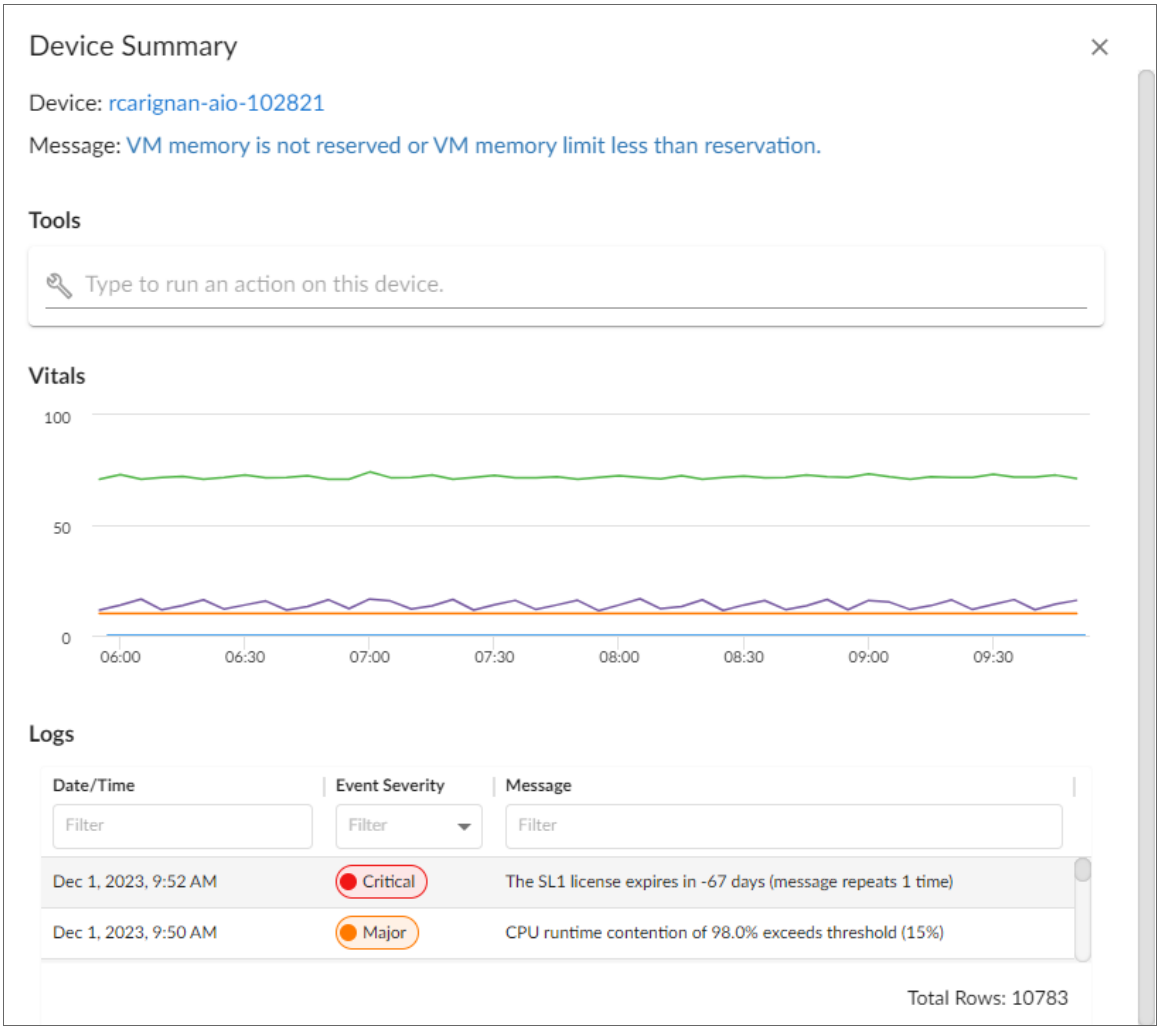
- ***Collector Group***. The collector group to which the device belongs. Collector groups are groups of Skylar One Data Collectors, which are defined on the **Collector Groups** page (Manage > Collector Groups).
- ***SNMP Credential***. The name of the SNMP credential used to monitor the device.
- ***SNMP Version***. The version of SNMP used to monitor the device.
- ***Hostname***. The fully qualified hostname for the device, for devices that are discovered and managed by hostname (instead of IP address). This column does not appear by default, but you can add it by clicking **Grid Settings** > *Column Preferences*.
- ***Date Created***. The date and time on which the device was created.
- ***Organization ID***. The unique numeric identifier of the organization to which the device is assigned.
- ***Class ID***. The unique numeric identifier of the device class.
- ***Category ID***. The unique numeric identifier of the device category assigned to the device.

- ***Type***. The type of device. Options include:
  - *Physical*. A hardware-based device with an IP address.
  - *Component*. An entity that runs under the control of a management device.
  - *Virtual*. A container for collected data.
- ***Collector Group ID***. The unique numeric identifier of the collector group to which the device belongs.
- ***Asset ID***. The ID of any asset associated with the device. The asset ID displays as a hyperlink that you can click to view the asset's properties. For more information about assets, see the ***Asset Management*** manual.
- ***Last Poll***. The date and time at which Skylar One last polled the device.
- ***Uptime***. The amount of time since the device was last initialized.
- ***SL Agent***. Indicates whether an Skylar One agent is installed on the device. If so, you can click the ***Yes*** hyperlink to display a modal where you can update the agent's configuration.
- Location-based columns. The following columns display information about the device's assigned location:
  - ***ID (Location)***. The unique ID of the device's location.
  - ***Name (Location)***. The name of the device's location.
  - ***Latitude (Location)***. The geographic latitude of the device's location.
  - ***Longitude (Location)***. The geographic longitude of the device's location.
  - ***Street (Location)***. The street address of the device's location.
  - ***City (Location)***. The city where the device's location is located.
  - ***State (Location)***. The state where the device's location is located.
  - ***Zipcode (Location)***. The ZIP or postal code for the device's location.
  - ***Country (Location)***. The country where the device is located.
  - ***Domestic Region (Location)***. The regional area with the country where the device is located.
  - ***Global Region (Location)***. The broader geographic region where the device is located.
  - ***Notes (Location)***. Additional information related to the device's location.
  - ***Description (Location)***. A brief description of the device's location.
  - ***Organizations (Location)***. The organizations aligned with the device's location.

NOTE: If you have defined any *custom attributes* for your devices, you can also add those custom attributes as columns that appear on the **Devices** page.

Viewing Additional Data about a Device

On the **Events** page and the **Devices** page, you can click the **Open** icon ( ) next to an event or device to open a **Device Summary** modal:



NOTE: On the **Events** page, the **Device Summary** modal displays only for events that are aligned with devices.

The detail window for that device contains the **Tools** pane, the **Vitals** graphs, and the **Logs** pane:

- The **Tools** pane enables you to run a set of diagnostic tools or user-initiated actions in the **Activity Center**, or to click on custom links that will open in a separate browser window. Click the search bar to search for tools, actions, or custom links that are available for the device.

- The **Vitals** pane displays graph data for the past four hours of CPU usage, memory usage, and latency for that device, where relevant. You can zoom in on a shorter time frame in the **Vitals** graph by clicking and dragging, and you can go back to the original time span by clicking the **[Reset zoom]** button.
- The **Logs** pane displays a list of events associated with that device.

TIP: To open the detail or Investigator page for an item, click the link for the item name at the top of the detail window.

Adding Devices with Discovery

On the **Devices** page, you can click the **[Add Devices]** button to run a guided or unguided network ***discovery*** session, a process that searches for and adds more devices to Skylar One for monitoring.

For more information about adding devices using guided or unguided discovery, see the ***Discovery & Credentials*** manual.

Creating a Physical Device without Running Discovery

Skylar One allows you to manually create physical devices without running discovery. When you do so, a device record exists in Skylar One before Skylar One can communicate with the device.

In some cases, service providers find it useful to pre-populate a Skylar One system with device records but set the status of the manually created devices to *Disabled*. When network and firewall work are completed, the provider can then enable the devices and use discovery to keep the device data up-to-date.

You can manually create a physical device in three ways:

- In the user interface
- By uploading device data via a CSV file
- With the ScienceLogic API

In the user interface, one of the places you can create a physical device without running discovery is on the **Devices** page. To do so, click the down arrow icon ( ) next to the **[Add Devices]** button and then select *Create Physical Device* or *Create Physical Device from File*.

For more information, see the section *Creating a Physical Device from the Devices Page*.

Creating a Virtual Device

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

- Monitor a device or application that doesn't support TCP/IP, SNMP, or both. The device's data can be pushed to Skylar One via another method (for example, email) and stored in a virtual device.

- Monitor multiple SNMP agents on a single device. In such a case, one of the SNMP agents (for example, a hardware agent) can be associated with the device and another SNMP agent (for example, an agent that monitors a software application) can be associated with a virtual device.
- Isolate and monitor specific parameters separately from their originating device. For example, you might want to monitor a database and keep its data separate from the hardware data you are collecting from the host device.

You can create a virtual device on the **Devices** page. To do so, click the down arrow icon ( ) next to the **[Add Devices]** button and then select *Create Virtual Device*.

For more information, see the section *Creating a Virtual Device from the Devices Page*.

Installing an Agent

If you are using a distributed Skylar One system *without* the Skylar One Extended Architecture (which includes Compute Nodes, Storage Nodes, and a Management Node), you can install a Skylar One agent from the **Devices** page. To do so, click the down arrow next to the **[Add Devices]** button and then select *Download/Install Agent*.

For more information, see the chapter on "Installing the Skylar One Agent" in the ***Monitoring with the Skylar One Agent*** manual.

Merging and Unmerging Devices

If your Skylar One system includes a physical device and a component device that both represent the same device, you can merge those device records into a single record for easier monitoring. Merging does not remove, replace, or add any data; merging simply groups data together.

There are several benefits to merging physical and component devices:

- Merging consolidates the devices and their data–device fields, values, graphs, behaviors, and other user interface elements–providing you with a single set of data for the device.
- Merging reduces the number of duplicated events and administrative tasks.
- Merged devices consume only a single device license.

For example, you might discover a virtual machine device component representing a server, and then later discover an IP-based device from the same server. To prevent duplicate events from occurring for the same server, minimize administrative tasks, and prevent a negative impact on your licensing by inflating the number of devices being monitored by Skylar One, you could merge the virtual machine component and the corresponding IP-based device into a single device record.

> **NOTE:** You ***cannot*** merge a component device with a physical device that acts as the root device for a dynamic component map (DCM) tree.

When you merge a physical device and a component device, the device record for the component device no longer displays in the user interface, while the device record for the physical device displays in user

interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the record for the physical device.

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

> **NOTE:** You can merge only two individual devices together into a single merged device. To do so, you must have user permissions that allow merging and unmerging on both devices. For more information about user access permissions, see the ***Access Permissions*** manual.

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

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

> **TIP:** Use consistent device hostnames to make device merging easier.

Skylar One enables you to merge and unmerge devices from the **Devices** page using a single workflow that supports both individual and bulk operations. For the current workflow, see *Merging and Unmerging Devices from the Devices Page*.

For legacy workflows in the classic Skylar One user interface, see *Merging Individual Devices in the Classic User Interface* to merge individual devices and *Unmerging Individual Devices in the Classic User Interface* to unmerge them. To merge or unmerge multiple devices at once in the classic Skylar One user interface, refer to *Bulk Merging and Unmerging of Devices in the Classic User Interface*.

You can merge or unmerge physical and component device records that represent the same device directly from the **Devices** page. This workflow supports both single and multiple device selections, allowing you to merge or unmerge one device pair or multiple device pairs.

Merging Devices from the Devices Page

You can merge physical and component device records that represent the same device on the **Merge Devices** modal from the **Devices** page.

To open the **Merge Devices** modal:

1. Go the **Devices** page.
2. Click the drop-down arrow button next to the **[Add Devices]** button and select *Merge Devices*. The **Merge Devices** modal appears.

The **Merge Devices** modal displays two tables: **Physical Device** and **Component Device**. Each table includes columns such as ***Device Name***, ***IP Address***, ***Device Category***, ***Device Class***, ***Device ID***, and ***Organization***, along with column filters to help you locate devices.

At the top of the **Merge Devices** modal, you can control how devices are matched using the fields displayed above the device tables. By default, the **Merge Devices** modal allows you to manually select physical and component devices to merge. In this mode, Skylar One does not apply any matching logic, and no comparison criteria are displayed.

Optionally, you can enable ***Suggested Device Matches*** to allow Skylar One to automatically generate device merge suggestions based on selected matching criteria.

When **Suggested Device Matches** is not enabled, the modal displays the following matching fields:

- ***Name***
- ***IP Address***
- ***Organization***
- ***Device Class***

For each field, you can manually review and select one of the following options to define how the physical device and component device values are compared:

- *Ignore*. Skylar One does not evaluate this criterion when generating suggested matches.
- *Match*. Skylar One suggests device pairs only when the selected values on the physical device and component device are the same.
- *Does Not Match*. Skylar One suggests device pairs only when the selected values on the physical device and component device are different.

When you enable ***Suggested Device Matches***, the **Merge Devices** modal switches to an assisted matching mode and displays additional options for defining how Skylar One should generate merge suggestions. In this mode, Skylar One compares physical and component devices based on selected criteria and suggests device pairs that meet those conditions. In this view, additional matching fields become available:

- ***Collection State***
- ***Collection Group***

> **NOTE:** When ***Suggested Device Matches*** is enabled, the **Merge Devices** modal automatically preselects the suggested physical-component device pairs. You can review these selections and remove individual pairs before clicking **[Merge]**.

Skylar One uses the selected fields to automatically generate suggested physical-component device pairs. Fields set to *Ignore* are excluded from matching. Fields set to *Match* or *Does Not Match* determine how suggested matches are generated.

To merge one device pair or multiple device pairs:

1. From the **Merge Devices** modal, select one or more physical-component device pairs.
2. Review the selected pairs, then click **[Merge]**.

You can merge a single device pair or multiple device pairs in the same operation. To review previous merge activity, click **[View Merge Device Logs]**.

Unmerging Devices from the Devices Page

You can unmerge previously merged physical and component device records on the **Unmerge Devices** modal from **Devices** page.

To open the **Unmerge Devices** modal:

1. Go the **Devices** page.
2. Click the drop-down arrow button next to the **[Add Devices]** button and select *Unmerge Devices*. The **Unmerge Devices** modal appears.

The **Unmerge Devices** modal displays two tables: **Physical Device** and **Component Device**.

- The **Physical Device** table includes columns such as ***Device Name***, ***IP Address***, ***Device Category***, ***Device Class***, and ***Device ID***.
- The **Component Device** table includes columns such as ***Device Name***, ***Device Category***, ***Device Class***, ***Device ID***, ***Merged Date***, and ***Merged By***. These columns indicate when the device was merged and the user who performed the merge.

To unmerge one device pair or multiple device pairs:

1. From the **Unmerge Devices** modal, select one or more merged device pairs.
2. Review the selected pairs, then click **[Unmerge]**.

You can unmerge a single device pair or multiple device pairs in the same operation. To review previous merge and unmerge activity, click **[View Merge Device Logs]**.

> **NOTE:** You can click the**[Merge Devices]** button to open the **Merge Devices** modal.

Designating Favorite Devices

In Skylar One, you can select one or more devices to always display at the top of the **Devices** page. This process is called ***favoriting*** devices.

To make a device a favorite, click the ***Favorite Device*** star icon (☆) to add the device to your favorites list. Click the icon (★) again to remove the favorite status.

With favorite devices, you can:

- View your favorite devices at the top of the **Devices** page by default.
- Include favorites in the multi-sort function.
- Filter devices by favorite.

Aligning a Device with a Different Organization

To align a single device with a different organization:

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

> **TIP:** You can also bulk-align multiple devices with an organization. For more information, see the section on *Performing Bulk Actions on One or More Devices*.

Assigning a New Icon to a Device

You can customize the look and feel of the devices that appear on the **Devices** page by assigning an icon a device, device class, or device category.

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

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

> **TIP:** To assign an icon to more than one device, device class, or device category, select the checkboxes to the left of those items and click the **[Assign Icon]** button.

3. In the **Select an Icon** window, do one of the following:
   - To use an existing icon, proceed to step 7.
   - To upload a new icon from your local drive, make sure that the image file meets the following criteria, then proceed to step 4:
     - The image file should be in .SVG format.
     - The file should not be larger than 40 KB.
     - The file should not be animated.
     - The file should not contain bitmaps.

4. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears.
5. Complete the following fields in the **Add an Icon** window:
    - In the ***Icon name*** field, type a name for the icon you want to upload.
    - In the ***Add Tags*** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
    - You can click the ***Browse or Drop*** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
6. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
7. Select the icon from the list of icons and click the **[Select Icon]** button. The icon is assigned to the device, device class, or device category.

> **TIP:** You can use the ***Search*** field to search for a specific icon or narrow down the list of icons.

Deleting a Device

To delete a single device on the **Devices** page:

1. On the **Devices** page, click the **Actions** button (⋮) for the device and select *Delete Device*.
2. A dialog appears asking you to confirm that you want to permanently delete the device(s). To confirm, click **[Delete]**.

> **NOTE:** If you attempt to delete one or more devices that have associated asset records, you are given the option to delete those associated assets at the same time.

> **TIP:** You can also bulk-delete multiple devices. For more information, see the section on *Performing Bulk Actions on One or More Devices*.

Running a Device Report

From the **Devices** page or from the **Device Investigator** page for a specific device, you can generate a detailed report for a single device. You can specify the information to include in the report and the format that Skylar One will use to generate the report, including HTML, PDF, XLS, and more.

To run a device report:

1. Do one of the following:
    - On the **Devices** page, click the **Actions** button (⋮) for a specific device and select *Device Report*.

- On the **Device Investigator** page for a specific device, click the **[Report]** button in the top navigation bar.

The **Device Report** modal page appears.

2. In the ***Type*** drop-down, select the type of report you want to generate. Your options include:
   - **[Full Report]**. Includes information about device status, status of all device policies, status of all monitors, status of hardware components, status of all thresholds defined for the device, a list of all active events associated with the device, and information about the last collection time and last entry to the device log.
   - **[Status]**. Includes information about device status, status of all monitors, status of hardware components, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
   - **[Config]**. Includes status of all monitors, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
   - **[Contact]**. Includes contact information for the device's organization and contact information for all vendors and warranty or support accounts.
   - **[Hardware]**. Includes overview of hardware components for the device.
   - **[Notes]**. Includes all notes created in the **Notepad Editor** page.
   - **[Software]**. Displays a list of software installed on the device.
   - **[Processes]**. Displays a list of all processes running on the device.
   - **[Network]**. Includes information about network ports and network configuration.
   - **[Events]**. Includes a list of all active events associated with the device.
   - **[Health]**. Includes information about device status, status of all monitors, status of all Dynamic Applications associated with the device, status of all thresholds defined for the device, and a list of all active events associated with the device.
3. In the ***Format*** drop-down, select the format for the report. Your options include:
   - ***HTML***. Create the report as an HTML document.
   - ***PDF***. Create the report as a PDF document.
   - ***DOC***. Create the report as a Microsoft Word document.
   - ***XLS***. Create the report as Microsoft Excel spreadsheet.
   - ***CSV***. Create the report using comma-separated values.
4. Click **[Create Report]** to generate the report.

Performing Bulk Actions on Multiple Devices

On the **Devices** page, you can select the checkboxes for one or more devices in the list and then click the **[Actions]** button to perform certain tasks on the selected devices. The following options are available when you click the **[Actions]** button:

- *Add To Device Group*. Select the device groups you want to add the selected devices to and then click **[Add]**. For more information about device groups, see the manual ***Device Groups and Device Templates***.
- *Align Device Investigator Layout*. Select a device **[Investigator]** tab layout you want to apply to the selected devices and then click **[Next]**. For more information about device **[Investigator]** tab layouts, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

> **NOTE:** When bulk-aligning a device **[Investigator]** tab layout to one or more devices, you can apply the layout to all users only if you have the permissions to do so. Otherwise, the layout change will be applied only for you.

- *Align Organization*. Select an organization from the drop-down field and then click **[Align Organization]**. For more information about organizations, see the manual ***Organizations and Users***.
- *Align SNMP Read Credential*. Select an SNMP read-only credential from the list and then click **[Align]**. For more information on SNMP credentials, see the ***Discovery and Credentials*** manual.
- *Assign Icon*. Select an icon from the list and then click **[Select Icon]**. You can also add a new icon for selection. For more information, see the section on *Assigning a New Icon to a Device*.
- *Change Collection State*. Enables you to change the data collection status of the device in Skylar One. Your options are:
    - *Disable* (toggled off), in which Skylar One does not poll the device. If selected, the data displayed about the device in Skylar One is not updated.
    - *Enable* (toggle on), in which Skylar One actively polls the device on a regular basis and updates the data displayed about the device.
- *Change Collector Group*. Select a collector group from the list and then click **[Change]**. For more information about collector groups, see the chapter on "Collector Groups" in the ***System Administration*** manual.
- *Change User Maintenance Mode*. To enable or disable user maintenance mode for the selected device(s), select one of the following maintenance mode options and then click **[Change]**:
    - *Enabled without Collections*. This option puts the selected devices into user maintenance mode with collection disabled. The devices will remain in this state until you or another user disables user maintenance mode.
    - *Enabled with Collections*. This option puts the selected devices into user maintenance mode with collection enabled. The devices will remain in this state until you or another user disables user maintenance mode.
    - *Disable*. This option disables user maintenance mode for the selected devices.

  For more information about user maintenance mode, see the section on *Device Maintenance*.

- *Create Asset Record*. Creates an asset record for each selected device. Skylar One automatically populates as many fields as possible, using retrieved data. For more information about asset records, see the ***Asset Management*** manual.
- *Delete Devices*. A dialog appears asking you to confirm that you want to permanently delete the device(s). To confirm, click **[Delete]**.

> **NOTE:** If you attempt to delete one or more devices that have associated asset records, you are given the option to delete those associated assets at the same time.

- *Find Collection Label Duplicates*. Displays a list of currently duplicated collection labels for the selected devices. From this modal, you can edit the presentation object that is aligned with a collection label.
    - To select a collection label, use the drop-down list in the upper left.
    - To change the aligned presentation object for one or more devices:
        - Click on the radio button for the desired presentation object for the device.
        - For each additional device you want to edit, click on the radio button for the desired presentation object.
        - In the ***Select Action*** menu (lower right), select *Align Presentation for Device* and then click the **[Go]** button.

    For more information about collection labels, see the chapter on "Grouping Dynamic Application Data Using Collection Labels" in the ***Monitoring Device Infrastructure Health*** manual.
- *Modify By Template*. Displays the **Modify by Template** modal, which allows you to select a device template to change the configuration of the selected device(s). For more information, see the section on "Using a Configuration Template to Edit the Configuration of One or More Individual Devices" in the ***Device Groups and Device Templates*** manual.
- *Schedule Maintenance*. Displays the **Schedule Editor** modal, which allows you to schedule maintenance for the selected device(s). For more information, see the section on *Defining a Scheduled or Recurring Device Maintenance Window for a Single Device*.

Chapter 3

Using the Device Investigator

Overview

The **Device Investigator** page provides a view of detailed data for a specific device in Skylar One. This chapter describes the data that can be viewed on the **Device Investigator** page and its various tabs.

This chapter covers the following topics:

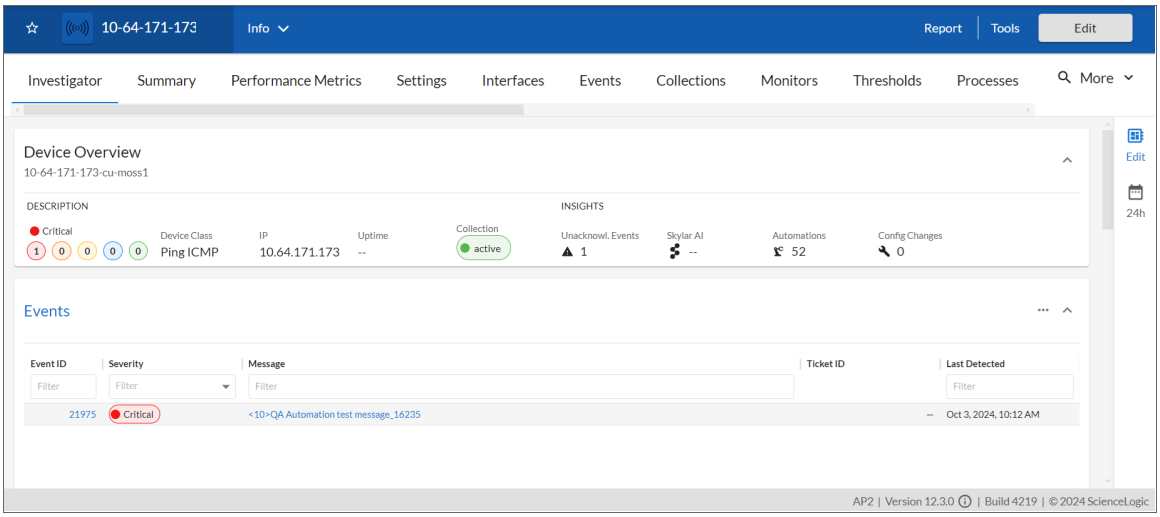
What is the Device Investigator? *37*

Overview of the Device Investigator Tabs *45*

What is the Device Investigator?

The **Device Investigator** displays a customizable, detailed set of data about a specific device.

From the **Devices** page, click the name of a particular device to open the **Device Investigator** page for that device.



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

Only tabs relevant to the selected device are available on the **Device Investigator** page. For example, the **[Agent]** and **[Machine Learning]** tabs do not display if the selected device does not use agents or machine learning-based anomaly detection.

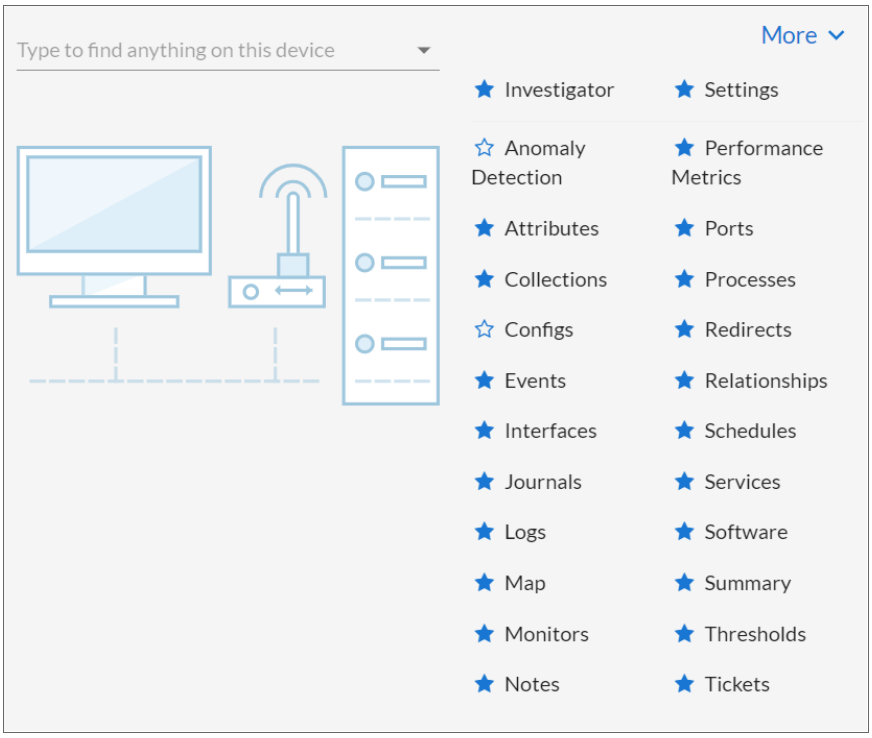
The **Device Investigator** page can include the following menus and buttons:

- *Info.* This drawer on the **[Investigator]** tab displays additional information about the device, along with the most recently updated values for uptime and collection time.
- *Report.* This button lets you generate a detailed report on the device.
- *Tools.* This button opens the **Activity Center**, where you can run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open in a separate browser window.

The **Device Investigator** page contains the following tabs:

- *Investigator*. Displays panels that provide basic information and metric data about a device. For most devices, the default panels include a Device Overview panel, Events, Logs, Availability, and combined charts for metrics such as utilization, discards, and errors. You can customize the panel layout on this page to meet your specific business needs, including select additional metrics to display.
- *Settings*. Lets you manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more. You can also set user maintenance preferences and disable or enable collection on that device.
- *Anomaly Detection*. Displays a list of anomaly detection metrics that are enabled for the device.
- *Attributes*. Lists the custom descriptive fields that are currently aligned with this device. On this tab, you can add and remove extended custom attributes to this device.
- *Changes*. Displays active and cleared Change Events for a device.

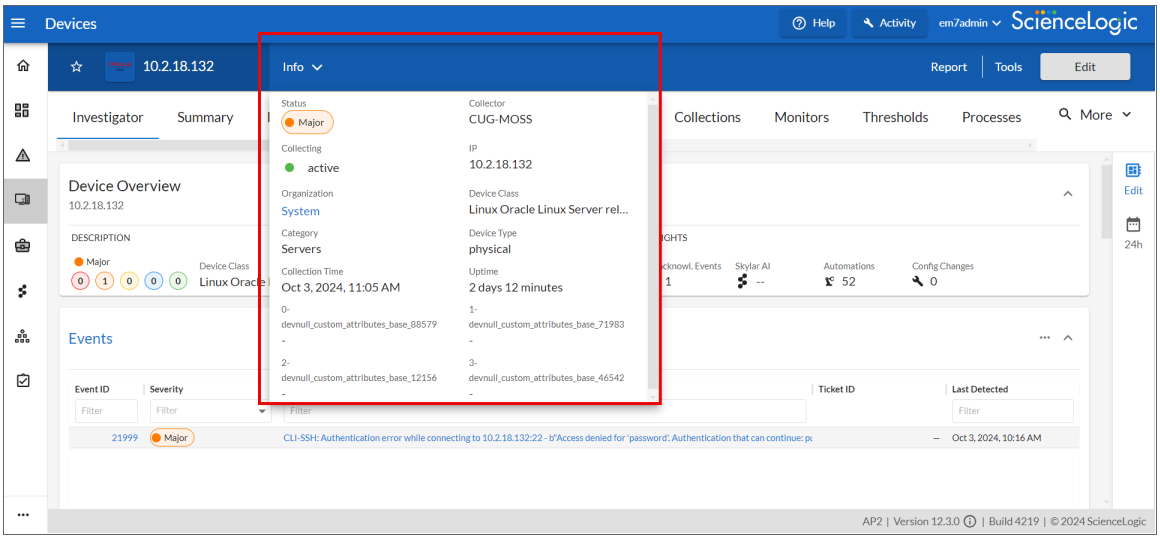
- *Collections*. Lets you align or un-align Dynamic Applications with this device, enable or disable collection for the Dynamic Applications, and run a Dynamic Application. You can also change credentials and update the poll frequency for a Dynamic Application.
- *Configs*. Displays configuration information collected from the device by Dynamic Applications. If this device does not have any configuration data, this tab does not appear.
- *Events*. Displays a list of active and cleared events for the device. You can acknowledge events from this tab and add event notes.
- *Interfaces*. Displays information about the interfaces used by the device. If this device does not use interfaces, this tab does not appear.
- *Journals*. Displays journal entry information collected from the device by Dynamic Applications.
- *Logs*. Displays all of the messages Skylar One and the Skylar One agent, if applicable, have collected from the device.
- *Map*. Opens a map of that device and the devices it is related to (for systems that have the **Maps** page enabled).
- *Monitors*. This tab lets you define monitoring policies for the device.
- *Notes*. Displays notes and attachments associated with the device. You can also edit and create notes.
- *Performance Metrics*. Displays performance graphs for hardware, monitoring policies, and Dynamic Applications aligned with the device.
- *Ports*. Displays a list of all open ports on the device.
- *Processes*. Displays a list of system processes running on the device.
- *Redirects*. Allows you to redirect logs entries from an IP-based device to the current device. This is most useful when the current device is a virtual device, but you can also redirect log entries from one IP-based device to another IP-based device.
- *Relationships*. Displays information about parent-child relationships between devices.
- *Schedules*. Allows you to view and manage all the scheduled processes you have defined in your system.
- *Services*. Displays a list of all services enabled on the device.
- *Software*. Displays a list of all the software installed on the device.
- *Summary*. Displays an overview of device details through device dashboards and widgets that display various metrics.
- *Thresholds*. Lets you define space and performance thresholds for a device.
- *Tickets*. Displays all open, pending, or working tickets associated with the device.
- ***More***. This drop-down lets you select additional tabs to display on the **Device Investigator** page by clicking the star icon next to the tab name. You can search for specific items on a tab, such as Device Class, Uptime, or Category, and the relevant tab will appear in the search results. You can also remove a tab by clicking the star icon again, turning it from blue to white. Your tab selections are saved and remain in place even after you log out:



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

Using the Info Drawer on the Device Investigator Page

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



The ***Info*** drawer displays the following information for the device:

- ***Status***. The status of the device.
- ***Collector***. The Collector Group that was last used to collect data from the device. For All-In-One Appliances, this field will contain the name of the default, built-in Collector Group.
- ***Collecting***. Indicates that the device collection is "Collecting" with a green check mark icon ( ), meaning Skylar One is periodically collecting data from the device, or "Not Collecting" with a prohibition icon ( ), meaning the Skylar One is not currently collecting data from the device.
- ***IP***. IP address of the device.
- ***Organization***. The organization to which this device belongs. Click the organization name to view a detail page for the organization.
- ***Device Class***. Device class for the device. A device class usually describes the manufacturer of the device.
- ***Category***. The device category associated with the device. The device category usually describes the primary function of the device, such as a "server", "switch", or "router".
- ***Device Type***. Specifies whether the device is a physical device or a virtual device.
- ***Location Name***. The device's location name as it might appear in a geographic map. Depending on your access, you might be able to edit or just view this field.

> **NOTE:** The ***Location Name*** field appears if you have installed AP2 9.13.1-14 (Quesito) or later.

- ***Collection Time***. Date and time of the most recent collection.
- ***Uptime***. The number of days and hours that the device has been continuously up and communicating with Skylar One.
- **More Attributes**. This lower section lists any custom attributes that might be aligned with this device.

Running a Device Report

From the **Devices** page or from the **Device Investigator** page for a specific device, you can generate a detailed report for a single device. You can specify the information to include in the report and the format that Skylar One will use to generate the report, including HTML, PDF, XLS, and more.

To run a device report:

1. Do one of the following:
    - On the **Devices** page, click the **Actions** button (⋮) for a specific device and select *Device Report*.
    - On the **Device Investigator** page for a specific device, click the **[Report]** button in the top navigation bar.

    The **Device Report** modal page appears.
2. In the ***Type*** drop-down, select the type of report you want to generate. Your options include:
    - **[Full Report]**. Includes information about device status, status of all device policies, status of all monitors, status of hardware components, status of all thresholds defined for the device, a list of all active events associated with the device, and information about the last collection time and last entry to the device log.
    - **[Status]**. Includes information about device status, status of all monitors, status of hardware components, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
    - **[Config]**. Includes status of all monitors, status of all thresholds defined for the device, and information about the last collection time and last entry to the device log.
    - **[Contact]**. Includes contact information for the device's organization and contact information for all vendors and warranty or support accounts.
    - **[Hardware]**. Includes overview of hardware components for the device.
    - **[Notes]**. Includes all notes created in the **Notepad Editor** page.
    - **[Software]**. Displays a list of software installed on the device.
    - **[Processes]**. Displays a list of all processes running on the device.
    - **[Network]**. Includes information about network ports and network configuration.
    - **[Events]**. Includes a list of all active events associated with the device.
    - **[Health]**. Includes information about device status, status of all monitors, status of all Dynamic Applications associated with the device, status of all thresholds defined for the device, and a list of all active events associated with the device.
3. In the ***Format*** drop-down, select the format for the report. Your options include:
    - ***HTML***. Create the report as an HTML document.
    - ***PDF***. Create the report as a PDF document.
    - ***DOC***. Create the report as a Microsoft Word document.

- ***XLS***. Create the report as Microsoft Excel spreadsheet.
- ***CSV***. Create the report using comma-separated values.

4. Click **[Create Report]** to generate the report.

Using Device Tools in the Action Runner

On the **Device Investigator** page, you can click the **Tools** menu to display the **Action Runner**. The **Action Runner** enables you to run a set of diagnostic tools or user-initiated actions, or to click on custom links that will open in a separate browser window.

NOTE: The tools and actions that are available in the **Action Runner** are based on the device type and your user permissions, as determined by your organization assignment and access hooks. For example, if a device does not have an IP address, only the Availability tool will be available.

NOTE: For more information about user-initiated actions, see the chapter on "Automation Policies" in the ***Run Book Automation*** manual. For more information about custom links, see the chapter on "Custom Links" in the ***Customizing the User Experience*** manual.

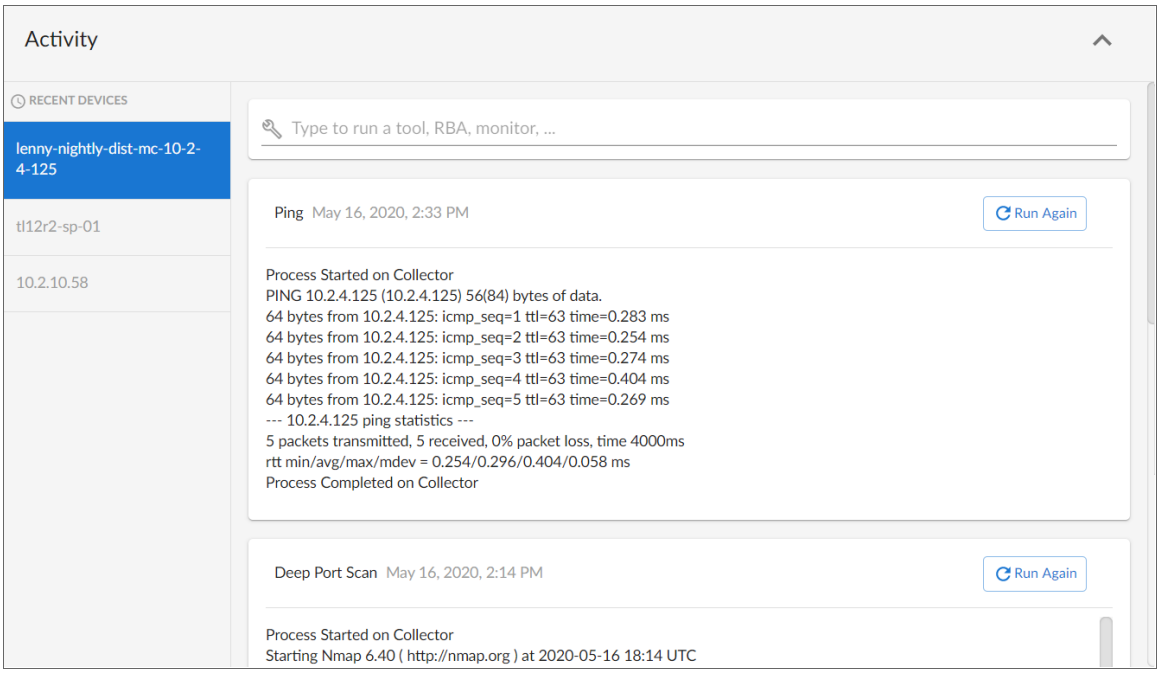
To use the **Action Runner**:

1. Access the **Action Runner** for devices in one of the following ways:
   - On the **Devices** page, open the Device Drawer for a particular device. Click the search bar in the **Tools** pane.
   - On the **Device Investigator** page, click the **[Tools]** button in the top navigation bar.
   - Click **[Activity]** in the navigation bar at the top of any page in Skylar One. Click the search bar.
2. When you click the search bar, a list appears of the default tools, actions, or custom links that are available for the selected device. Click one of these tools, actions, or custom links, or use the search bar to search for a tool or action that is not listed. The following default tools are available in the **Action Runner**:
   - ***Availability***. Displays the results of an availability check of the device, using the port and protocol specified in the ***Availability Port*** and ***Availability Protocol*** fields on the **[Settings]** tab for this device.
   - ***Ping***. Displays statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by Skylar One to communicate with the device) and waits for a reply. Skylar One then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, Skylar One uses the appropriate IPv6 ping command.
   - ***Who Is***. Displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
   - ***Port Scan***. Displays a list of all open ports on the device at the time of the scan.

- ***Deep Port Scan***. Displays a list of all open ports and as much detail about each open port as the deep port scanner can retrieve.
- ***ARP Lookup***. Displays a list of IP addresses for the device and the resolved Ethernet physical address (MAC address) for each IP address.
- ***ARP Ping***. Displays the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it uses the ARP protocol instead of ICMP. The ARP Ping tool can be used only on the local network.
- ***Trace Route***. Displays the network route between Skylar One and the device. The tool provides details on each hop to the endpoint. If the device has an IPv6 address, Skylar One uses the appropriate IPv6 traceroute command.

TIP: The tools found in the **Action Runner** can also be found in the Device Toolbox in the classic Skylar One user interface.

3. If you clicked a custom link, the link opens in a new browser window. If you clicked on a tool or action, then as it runs, its progress and results appear in a log in the **Activity Center**.
4. After the tool or action has run, if you want to run it again, click the **[Run Again]** button. This button appears only for activities completed during your current session.



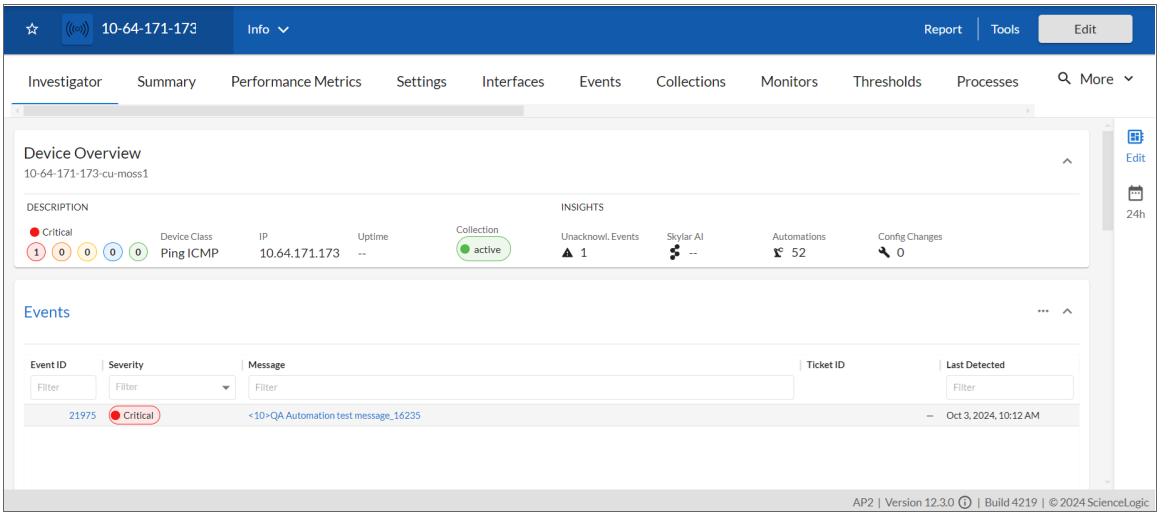
NOTE: The left pane of the **Activity Center** displays a list of devices for which you have most recently used the **Action Runner**, with the current device at the top of the list. To use the **Action Runner** for any of the other recently used devices or to view historical logs for the tools or actions that have been run on those devices, click on the device name.

Overview of the Device Investigator Tabs

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

The Investigator Tab

The **[Investigator]** tab of the **Device Investigator** page displays a customizable set of metrics about the selected device.



The device type determines which metrics appear in the **[Investigator]** tab. For most devices, the following panels appear by default:

- ***Device Overview***. Displays a panel that includes basic information about the device, including its current state, device class, IP address, uptime, collection status, unacknowledged event count, Skylar AI insights, automated actions count, and configuration changes count.

  > **NOTE:** The device's Skylar AI insights count displays the sum of all open root cause analysis events (accepted, suggested, or custom) plus all open anomaly index score events plus all open predictive alert events. The Skylar AI insights count is hidden if your Skylar One system is not connected to Skylar AI.

- ***Events***. Displays a panel with the list of events aligned with this device. In the right-hand pane, you can click the **ID** or **Message** field to view the **Event Investigator** page for that event. You can also click the **Events** panel heading to go to *the **[Events]** tab* for that device.

  > **NOTE:** If your device has Skylar Automated RCA suggestions, custom alerts, or accepted alerts, you can click the **[VIEW]** link on the banner that appears at the top of the **Device Investigator** page to go to the **[Events]** tab for that device to review the Skylar Automated RCA content.

  > **TIP:** From the **Event Investigator** or **Service Investigator** pages, if you click the name of the device where an event has occurred, you are redirected to the **Device Investigator** page for that device, with an event context panel displaying at the top of the page. From this panel, you can acknowledge, clear, or view causes and resolutions relating to that specific event.

- ***Logs***. Displays a panel with a list of the logs for the device, sorted from newest to oldest by default. You can use the **Search** field to search device logs for specific event messages, event IDs, date ranges, source types, and other relevant text for troubleshooting. You can also click on the column headers for ***Date/Time***, ***Source***, ***Event ID***, ***Severity***, and ***Message*** to sort by that column.
- ***Relationships and Membership***. Displays a panel that includes details about the other devices that have relationships to the selected device, as well as the device groups and services to which the device belongs or has membership.
  - The **[Device Relationship]** tab displays the name, relationship type, relationship discovery method, and health for each device that has a relationship with the selected device. You can click the hyperlink in the ***Device Name*** column to go to the **Device Investigator** for the related device.
  - The **[Device Groups]** tab displays the name, device count, and ID for each device group to which the selected device belongs or has membership.
  - The **[Services]** tab displays the name, type, status, description, health, availability, and risk for each service to which the selected device belongs or has membership. You can click the hyperlink in the ***Service Name*** column to go to the **Service Investigator** for the related service.

- ***Map***. Displays a panel with a map of the device and all of the devices with which the device has relationships. You can also click the **Map** panel heading to go to the **[Map]** tab for that device. This panel is disabled by default, but can be enabled by clicking the **[Edit]** button, and then selecting the ***Map*** checkbox.

NOTE: You can customize the appearance of the widgets on the page, including changing their height or width. For more information, see the section on *Customizing the Appearance of Widgets on the Investigator Tab*.

The **Device Investigator** page also includes the following sidebar buttons:

- ***Edit***. Click the **[Edit]** button on the right panel to edit the content that appears on the **[Investigator]** tab and its layout. For example, you can *add or remove metrics*, *edit the metric panel order*, or *combine charts on the **[Investigator]** tab*.
- ***Timespan***. Click the timespan button on the right panel to adjust the timespan of data that appears in all of the metric panels on the **[Investigator]** tab. The default timespan is *Last 24 Hours*.

NOTE: Select the ***Always display raw data*** checkbox at the top of the timespan selector to ensure that the metric data that appears in the panels on the **[Investigator]** tab always includes the most recent data available. If you do not select that checkbox, Skylar One will still display raw data when you select a timespan of less than 2 days, but will automatically display rolled up hourly data for timespan selections of 2-45 days and rolled up daily data for timespan selections of more than 45 days.

Customizing the Appearance of Widgets on the Investigator Tab

The **[Investigator]** tab panel layout is responsive. Panels are automatically resized or relocated whenever you add or remove a pane, rearrange the panels on the page, or change the size of the the browser window.

You can customize a widget's appearance on the **[Investigator]** tab by clicking the menu icon () for that widget and then doing one of the following:

- To change the widget's name, select *Edit Widget Name* and then enter a new name.
- To change the widget's height, select *Small*, *Medium*, or *Large*.
- To change the widget's width, select either *Columns* or *Full width*.

You can also click the contract icon ( ) in the widget header to display only the header or click the expand icon ( ) to display the widget's full contents.

For leaderboard widgets for interfaces, file systems, and Dynamic Applications, you can click the Leaderboard Bar Chart icon ( ) to switch from a bar chart to a line chart, or click the Line Chart icon ( ) to switch from a line chart to a leaderboard bar chart.

Adding and Removing Metrics on the Investigator Tab

Optionally, you can add metrics to the **[Investigator]** tab for Dynamic Applications, interfaces, and the Skylar One Agent (if applicable), among other things. You can also remove metrics from the **[Investigator]** tab.

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

1. To add a metric panel that is not currently on the **[Investigator]** tab, click the **[Edit]** button on the right sidebar to expand the layout panel, click **[Edit Panels]**, and then click the ***Add a metric*** field. A list of metrics appears:
2. Select a metric from the list, or type the name of a metric and select it from the list. The metric is added to the right pane, and a corresponding widget appears in the left pane.
3. Some metrics might require you to make additional selections, such as the network interfaces associated with a device. Click the field and add one or more additional metrics, as needed.

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

4. To remove a metric panel from the **[Investigator]** tab, uncheck the corresponding box in the right panel. The metric remains listed in the right panel, but the panel is removed from the **[Investigator]** tab.
5. To completely remove the metric and its corresponding panel from the **[Investigator]** tab, click the **[Remove from Layout]** button (✕) for that metric in the right panel.

> **NOTE:** The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Editing the Metric Panel Order on the Investigator Tab

On the **[Investigator]** tab of the **Device Investigator** page, the order in which the metric panels appear in the right panel when you click the **[Edit]** button mirrors the order in which the corresponding metric panel widgets appear in the left panel. You can drag and drop the panels up or down in the right panel to edit the order in which the metric panels appear on the left panel. This enables you to prioritize the information that appears on the page.

To edit the order in which widgets appear on the **[Investigator]** tab:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel and then click **[Edit Panels]**.
2. Hover your mouse over the "Panel" heading of the panel that you want to move until you see an open hand icon appear.

3. Click and hold down the left button on your mouse to grab the panel, and then use your mouse to drag the panel to a different location in the list. When you do so, the open hand icon becomes a closed hand icon, and a blue dotted box appears around the panel.
4. Release the left mouse button to drop the panel in your desired location. The new right-hand panel order will be reflected in the left-hand widget panel.

> **NOTE:** The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Combining Charts on the Investigator Tab

On the **[Investigator]** tab of the **Device Investigator** page, you can combine charts for different time-series metrics to see all of the combined data for those metrics in a single chart.

To combine charts:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel, and then click **[Edit Panels]**.
2. Hover your mouse over a time-series metric name until you see an open hand icon appear.
3. Click and hold down the left button on your mouse to grab the metric, and then use your mouse to drag the metric into the panel of a different time-series metric in the list. When you do so, the open hand icon becomes a closed hand icon, and the panel containing the combined metrics turns blue.
4. Release the left mouse button to drop the metric into the desired panel. The newly combined metric panel will be reflected in a "Combined Charts" widget in the left-hand widget panel.

> **NOTE:** The **[Investigator]** tab retains any changes you made to the set of device metrics displayed for each device, on a per-user basis. To reset these changes to their default settings, click the **[Reset]** button at the bottom of the right panel. Optionally, you can apply these changes to other Device Categories, Device Classes, or devices. For more information, see the section on *Applying a Custom Device Investigator Layout to Other Devices*.

Applying a Custom Device Investigator Layout to Other Devices

The device **[Investigator]** tab has a default layout that includes Device Overview, Events, and Logs widgets. Initially, this layout is assigned to all devices.

You can also create custom **[Investigator]** tab layouts and apply those layouts to individual devices, entire device classes, or entire device categories, and then apply those updates either to only yourself or to all system users.

To apply a custom device **[Investigator]** layout to other devices:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel. When you do so, the **[Investigator]** tab name will appear at the top of the layout panel, along with one of the following labels:
    - ***Default***. Indicates the layout has not been changed from the default settings.
    - ***Private***. Indicates the layout has been changed from the default settings but only applied to the logged in user.
    - ***Public***. Indicates the layout has been changed from the default settings and has been applied to all system users.
2. From this panel, you can do one or more of the following:
    - *Create a new custom Investigator layout*.
    - *Select an existing custom Investigator layout*.
    - *Manage the custom Investigator layouts*.

Creating a New Custom Investigator Layout

To create a new custom device **[Investigator]** layout:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel and then click **[Edit Panels]**.
2. Make updates to the **[Investigator]** layout as needed, such as by *adding or removing metrics*, *editing the metric panel order*, or *combining one or more charts into a single panel*. When you do so, the label at the top of the layout panel will change to "Private", if it was not already labeled as such.
3. To save the custom **[Investigator]** layout for other devices, device classes, or device categories, and/or to save the layout for all system users, click the **[Apply To...]** button, and then proceed to step 4. Otherwise, do one of the following:
    - To save the custom **[Investigator]** layout for only the current device and your user account, leave the page. When you do so, Skylar One automatically saves the custom layout, and will display the custom layout when you return to the **[Investigator]** for that device.
    - To revert your **[Investigator]** layout changes to the default settings, click the **[Reset]** button.
4. On the **Apply "Custom Investigator" to...** modal, use the following tabs and fields to specify the devices and users to which you want to apply the custom **[Investigator]** layout, as well as its name:
    - ***Categories, Classes, and Devices tabs***. Click the appropriate tab or tabs at the top of the modal page and then use the search field to locate the specific Device Categories, Device Classes, or individual devices to which you want to apply the custom **[Investigator]** layout. Select the checkbox for each category, class, or device that you want to select.
    - ***Name***. Type a new name for the custom **[Investigator]** layout.
    - ***Apply Investigator for***. Select one of the following options:
        - *Myself*. Applies the custom **[Investigator]** layout to only your user account.
        - *All System Users*. Applies the custom **[Investigator]** layout to all users in your Skylar One system.
5. Click **[Review]**. A summary of your selections appears.
6. To confirm your selections, click **[Apply To Selected Types]**.

Selecting an Existing Custom Device Investigator Layout

To select an existing custom device **[Investigator]** layout:

1. On the **[Investigator]** tab of the **Device Investigator** page, click the **[Edit]** button on the right sidebar to expand the layout panel and then click **[Choose Layout]**. The **[Choose Layout]** tab displays a list of **[Investigator]** layouts that you have access to or own.
2. Click the radio button for the layout that you want to select. When you do, the **[Investigator]** page automatically updates to use that layout.

> **TIP:** You can also bulk-align device **[Investigator]** layouts to multiple devices. For more information, see the section on *Performing Bulk Actions on One or More Devices*.

Managing Custom Device Investigator Layouts

You can view and manage the list of custom device **[Investigator]** layouts that you own or have access to on the **Device Investigator Layouts** page.

> **NOTE:** To view the **Device Investigator Layouts** page, your user account must be aligned to an access key that includes the DEV_VIEW access hook. To delete layouts from this page, your user account must have an access key that includes the DEVICE_INVESTIGATOR_REMOVE or DEVICE_DASH_EDIT access hooks.

To manage the list of custom device **[Investigator]** layouts:

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

> **NOTE:** You can also access this page by from the **[Investigator]** tab of the **Device Investigator** page by clicking the **[Edit]** button on the right sidebar and then clicking Choose Layout > Manage Layouts.

2. For each layout, the following information displays:
    - ***Layout Name***. The name assigned to the layout. This name displays as a hyperlink. Click the hyperlink to view or update the list of devices, device classes, and device categories to which the layout is aligned.
    - ***ID***. The unique ID for the layout, generated by Skylar One.
    - ***Owner***. The owner of the layout. Typically, the creator of the layout is the owner.
    - ***Categories***. The number of device categories aligned to the layout.
    - ***Classes***. The number of device classes aligned to the layout.
    - ***Devices***. The number of devices aligned to the layout.
    - ***Alignment Last Edited By***. The user who configured or last edited the layout alignment.
    - ***Alignment Last Edited***. The date and time the layout alignment was configured or last edited.

> **TIP:** To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

> **TIP:** You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

3. From the **Device Investigator Layouts** page, you can take the following actions:
    - You can view or edit the device, device class, or device category alignment for layouts that you own. Proceed to steps 4-7.
    - You can delete layouts that you own. When you do so, any devices that are currently using the selected layouts will default to the next applicable layout. Proceed to steps 8-9.
4. To view or update the list of devices, device classes, and device categories to which a layout is aligned, click the hyperlink in the ***Layout Name*** field for that layout on the **Device Investigator Layouts** page. On the layout page that appears, you can click the **[Categories]**, **[Classes]**, and **[Devices]** tabs to view the layout's current alignments in read-only format.
5. To update the layout's current alignments, click **[Edit]** and then select the checkbox next to any device category, device class, or device that you want to align to the selected layout.

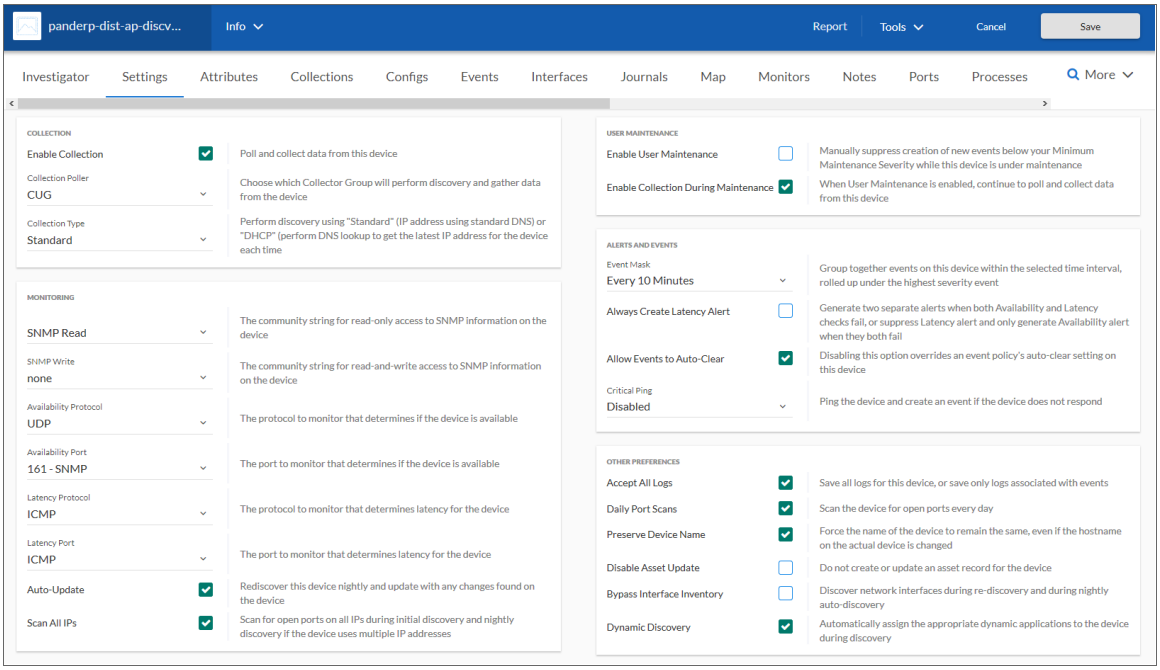
> **TIP:** You can select the checkbox at the top of the table to select all of the rows in that table.

6. If you are the layout owner and you want to edit the layout's name, click its name at the top of the page and then type a new name.
7. To save your changes, click **[Save]**.

8. To delete one or more layouts that you own, select their checkboxes on the **Device Investigator Layouts** page and then click **[Delete Layouts]**. When you do so, a warning appears informing you that any devices that are currently using the selected layouts will default to the next applicable layout.
9. To confirm that you want to delete the selected layouts, click **[Delete]**.

The Settings Tab

On the **[Settings]** tab of the **Device Investigator** page, you can manage your preferences for that device, such as whether to auto-clear events, accept all logs, run daily port scans, and more.



Click the **[Edit]** button to change your settings. When you are done making changes, click **[Save]**.

> **NOTE:** The **Agent** section appears only for agent-type devices.

Set the following **Agent** data collection preferences:

- ***Disk Space***. Specify the amount of disk space in MB that the agent can use to store data. If the agent loses connectivity to Skylar One, this disk space will be used to store collected data until the connection to Skylar One is restored. When connectivity is re-established, the agent uploads all of its stored data.
- ***Excludes***. Type a list of processes and directories, separated by semi-colons, that you do not want the agent to monitor.

- ***Includes***. Type a list of processes and directories, separated by semi-colons, that you want the agent to monitor. This field ensures that specific processes are monitored.

> **NOTE:** If a process or directory is included in both the ***Excludes*** field and the ***Includes*** field, the item in the ***Includes*** field will override the item in the ***Excludes*** field.

- ***Collect File Information***. Select this option if you want the agent to report the names of files accessed by each monitored process.
- ***Collect Named Pipe Information***. Select this option if you want the agent to collect named pipe information.
- ***Collect Socket Information***. Select this option if you want the agent to collect socket information.
- ***Collect Thread Information***. Select this option if you want the agent to collect thread information.
- ***Collect Non-Intercepted Processes***. Select this option if you want the agent to collect limited information for processes that do not contain the agent library.
- ***Processes Aggregation***. Specify how you want the agent to collect limited information for processes that do not have the agent library in them, and how to aggregate short-lived processes. Your options include the following:
    - *All*: Aggregate every short-lived process into its parent.
    - *None*: Do not aggregate any short-lived process.
    - *Without Sockets*: Aggregate short-lived processes unless those processes have sockets.
- ***Upload Interval***. Specify how often the agent should upload data. Your options include the following:
    - *20 Seconds*. Upload a data snapshot every 20 seconds.
    - *60 Seconds*. Upload a data summary every 60 seconds. This is the default setting. This option uses an improved data format that requires fewer Skylar One resources. The Skylar One agent continues to internally collect and poll data every 20 seconds, but the agent summarizes and uploads that data every 60 seconds. There is no data loss even though the data is uploaded less frequently.

> **NOTE:** If you specify 60 seconds for the upload interval, the summary upload now will include "watched" or "monitored" files, just like the snapshot upload does.

    - ***300 seconds***. Upload a data summary every 300 seconds (five minutes).

Set the following **Collection** preferences:

- ***Enable Collection***. Select this option to enable collection using the collector group specified in the following field.
- ***Collection Poller***. Select the name of collector group you want to use for collection on this device.

- ***Collection Type***. Select the type of collection you want to use on this device. Your options include *Standard* or *DHCP*.

Set the following **Monitoring** preferences:

- ***SNMP Read***. Select the community string for read-only access to SNMP information on the device.
- ***SNMP Write***. Select the community string for read-and-write access to SNMP information on the device.
- ***Availability Protocol***. Select the protocol to monitor that determines if the device is available.
- ***Availability Port***. Select the port to monitor that determines if the device is available.
- ***Latency Protocol***. Select the protocol to monitor that determines latency for the device.
- ***Latency Port***. Select the port to monitor that determines latency for the device.
- ***Auto-Update***. This checkbox specifies whether or not you want 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.
- ***Scan All IPs***. If the device uses multiple IP Addresses, Skylar One will scan for open ports on all IPs during initial discovery and nightly discovery.

Set the following **Topolgy** preferences:

> **NOTE:** The device's topology settings are initially inherited from the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior), or from the topology settings for the *device's class*. However, you can change these settings on a per-device basis by editing one or more of the fields below. For more information about the system-wide topology settings, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual. For more information about the device class topology settings, see the section on *Device Classes and Device Categories* in this manual.

- ***L2***. Select the ***Override*** checkbox to override the system-wide Layer-2 topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). When selected, this field becomes editable, and you can select from the following options:

    - *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 and connects network devices to each other using methods other than the standard SNMP protocol 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 advanced 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 advanced 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.

- ***L3***. Select the ***Override*** checkbox to override the system-wide Layer-3 topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). When selected, this field becomes editable, and you can select from the following options:

    - *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. This option requires all hops in a traceroute to respond and match devices within Skylar One 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. This option requires all hops in a traceroute to respond and match devices within Skylar One to form the relationship.

    - *Enhanced Processing Enabled*. Enables advanced Layer-3 topology processing for the device, where the system forms 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 advanced Layer-3 topology processing and collection for the device, where the system forms relationships between any two hops that respond and match devices in Skylar One rather than discarding incomplete traceroutes or results that include unmatched hops.

- ***CDP***. Select the ***Override*** checkbox to override the system-wide Cisco Discover Protocol (CDP) topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). When selected, this field becomes editable, and you can select from the following options:

    - *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 neighbors, and are managed devices in Skylar One. This option 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 neighbors, and are managed devices in Skylar One.

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

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

- ***LLDP***. Select the ***Override*** checkbox to override the system-wide Link Layer Discovery Protocol (LLDP) topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). When selected, this field becomes editable, and you can select from the following options:

    - *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 neighbors, and are managed devices in Skylar One. This option 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 neighbors, and are managed devices in Skylar One.

    - *Enhanced Processing Enabled*. Enables advanced 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 managed device in Skylar One.

    - *Collection and Enhanced Processing Enabled*. Enables advanced 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 managed device in Skylar One.

Set the following **User Maintenance** preferences:

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

Set the following **Alerts and Events** preferences:

- ***Event Mask***. Specify the time frame for masking events. When a device uses the Event Mask setting, Skylar One groups together events that occur on that device within the specified span of time.
- ***Always Create Latency Alert***. Select this option to generate two alerts when availability and latency checks fail. Deselect to generate only an availability alert and suppress latency alerts.
- ***Allow Events to Auto-Clear***. Deselect this option to override an event policy's auto-clear setting for this device.

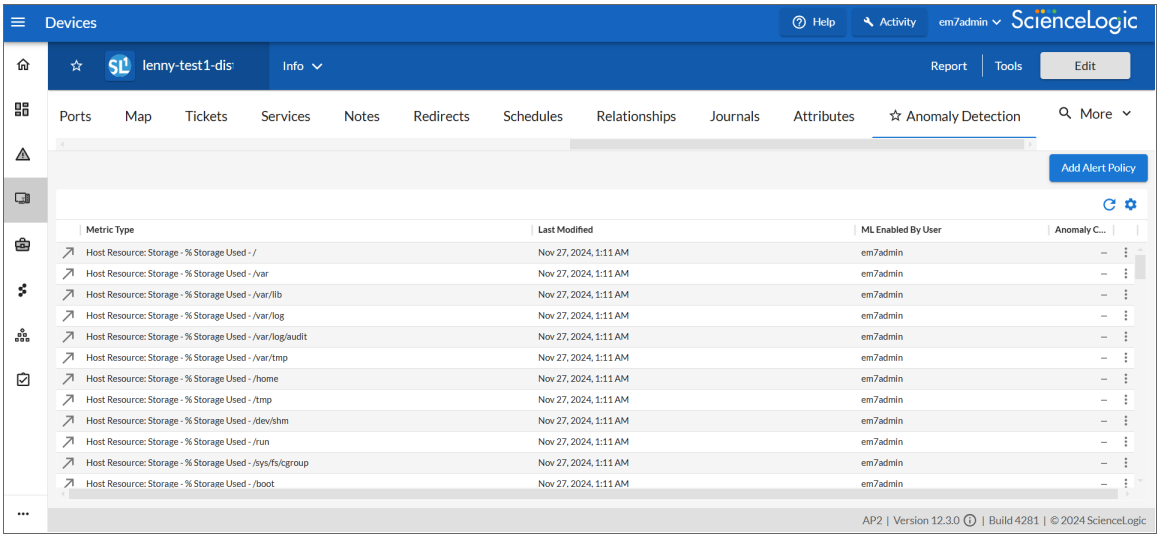
- ***Critical Ping***. Pings the device and creates an event if the device does not respond. When enabled you can select between 5 and 120 seconds.

Set the following **Other** device preferences:

- ***Accept All Logs***. This checkbox specifies whether or not you want to keep and save all logs for this device. If you want to retain only logs associated with events, uncheck this field.
- ***Daily Port Scans***. This checkbox specifies whether or not you want Skylar One to perform a daily scan of the device for open ports.
- ***Preserve Device Name***. 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, Skylar One will not automatically create a new asset record for the device or update the existing asset record for the device. For the single device, this checkbox over-rides any settings defined in the **Asset Automation** page (System > Settings > Assets).
- ***Bypass Interface Inventory***. Specifies whether or not the discovery session should discover network interfaces. Your options include:
    - *Selected*. Skylar One will not attempt to discover interfaces for this device during re-discovery and nightly auto-discovery.
    - *Not Selected*. Skylar One will attempt to discover network interfaces for this device during re-discovery and nightly auto-discovery using the ***Interface Inventory Timeout*** value and ***Maximum Allowed Interfaces*** value specified in the **Device Thresholds** page.
- ***Dynamic Discovery***. If selected, Skylar One will automatically assign the appropriate dynamic applications to the device during discovery.

The Anomaly Detection Tab

On the **[Anomaly Detection]** tab of the **Device Investigator**, you can view a list of anomaly detection metrics that are enabled for the device.

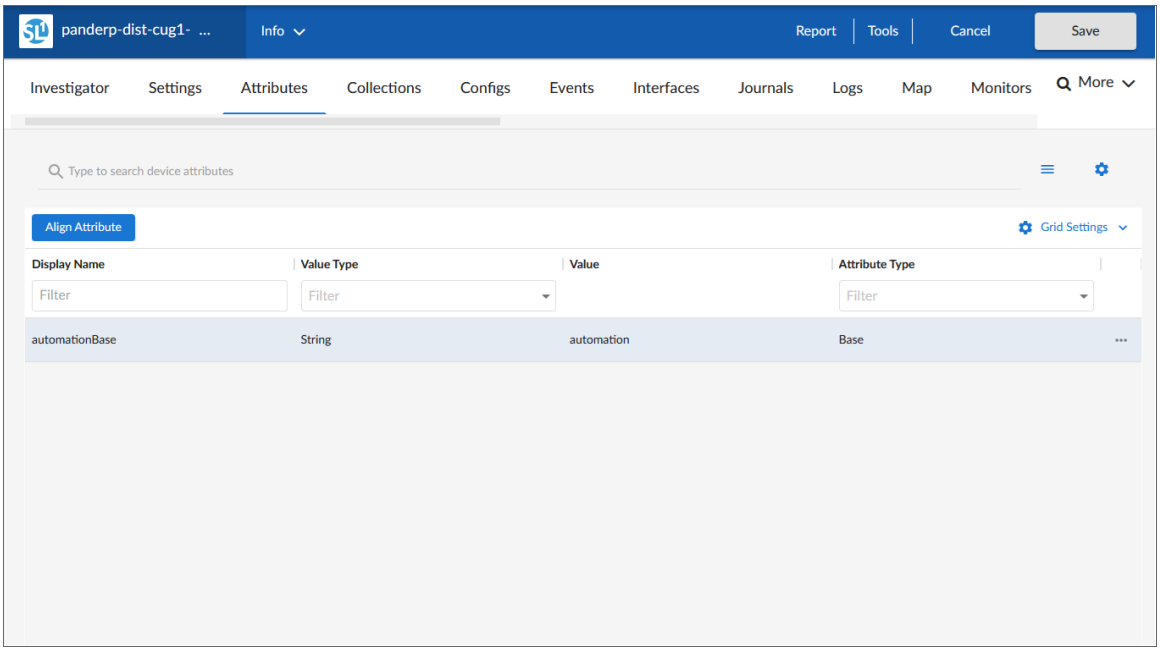


NOTE: The **[Anomaly Detection]** tab appears only if the device is collecting data for Skylar Analytics.

NOTE: For more information about this tab, see the section on "Enabling Anomaly Detection Events on the Device Investigator Page" in the ***Skylar AI Product Documentation***.

The Attributes Tab

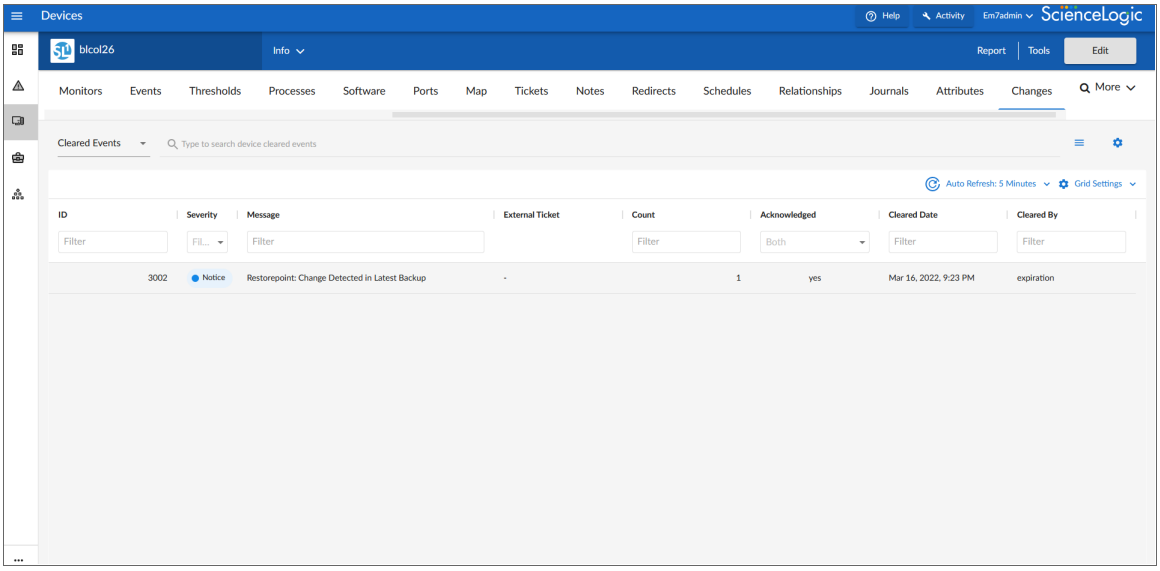
On the **[Attributes]** tab of the **Device Investigator**, you can view a list of list of custom attributes that are already aligned with that device, and you can also add and remove extended custom attributes for the device:



NOTE: For more information about this tab, see the section on *Adding Custom Attributes for a Device*.

The Changes Tab

On the **[Changes]** tab of the **Device Investigator**, you can view a list of the active and cleared change events for a device.



Skylar One PowerFlow users can use the **[Changes]** tab to view a list of events that are created when PowerFlow pulls change data from ServiceNow and Restorepoint SyncPacks.

Based on your third-party integrations, the tab displays the following information:

- ServiceNow planned change events
- ServiceNow emergency change events
- Restorepoint configuration change events

About the Changes Widget

The **Changes** tab uses data from the **Changes** widget, which is also used on the **Service Investigator** page to show change events for Business Services.

The **Changes** widget is available to customers who have purchased Configuration and Change Management as part of their Skylar One Standard or Premium subscription. This widget displays a list of events that are created when PowerFlow pulls change data from ServiceNow or Restorepoint, including both active and cleared change events.

The **Changes** widget tile displays the number of active change events that are impacting the service. Events on the widget will automatically clear after 30 minutes.

From the **Changes** widget, you can do the following:

- Use the drop-down menu to choose which type of change events display in the widget: *Active Events* or *Cleared Events*.
- Filter and search for events by their date; either by 5, 7, 14, 30 days, or more than 30 days.

- Use the ***Search*** field to search for specific change events.
- For active events that are aligned to devices, click the down-arrow icon (⌄) next to the event to open the Event Drawer panel, which displays the following panes:
    - ***Vitals***. A widget displaying the past 24 hours of CPU and memory usage for the device related to the event. You can zoom in on a shorter time frame by clicking and dragging, and you can go back to the original timespan by clicking the **[Reset zoom]** button.
    - ***Tools***. A set of network diagnostic tools or user-initiated actions that you can run on the device associated with the event. Click the search bar to search for a tool or action to run, or click one of the default tools or actions that are available based on the device type and your user permissions.
    - ***Logs***. A list of the log entries from the device's log file, sorted from newest to oldest by default.
- View the **Organizational Summary** page for the organization aligned with an active event by clicking the link in the ***Organization*** column.
- View the **Service Investigator** or **Device Investigator** page for the service or device aligned with an active event by clicking the link in the ***Name*** column.
- View the **Event Investigator** page for an active event by clicking the link in the ***Message*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with an active event by clicking the link in the ***Ticket External Reference*** column.
- For ServiceNow integrations, view the ServiceNow ticket associated with a cleared event by clicking the link in the ***External Ticket*** column.
- Acknowledge an active event by clicking the **[Acknowledge]** button. When you acknowledge an event, you let other users know that you are aware of that event, and you are working on a response.
- Clear an active event by clicking the **[Clear]** button. When you clear an event, you let other users know that the event has been addressed.
- Create a ticket from an active event.
- View the event policy for an active event.
- Select multiple active events for action using the check boxes next to the events.

Configuring and Enabling the Changes Widget

To use the **Changes** widget, you must first configure and enable the widget. To do so, perform the following steps:

1. Ensure that you are running Skylar One version 11.2.0 or later and have *Business Services Base Pack* PowerPack version 2.2.0 or later installed in Skylar One. For more information, see the chapter on "Installing a PowerPack" in the ***PowerPacks*** manual.
2. Ensure that you are running Skylar One PowerFlow Platform version 2.2.2 or greater and one or more of the following PowerPacks, depending on your integration:
    - ***For a ServiceNow integration***:
        - *ServiceNow CMDB* SyncPack version 3.2.0 or later installed in PowerFlow. For more information, see the ***ServiceNow CMDB Synchronization PowerPack*** manual.

- *ServiceNow Change Management* SyncPack version 3.2.1 or later installed in PowerFlow. For more information, see the ***ServiceNow Change Management Synchronization PowerPack*** manual.

- ***For a Restorepoint integration***:
  - *Restorepoint* SyncPack version 1.2.0 or later installed in PowerFlow.
  - *Restorepoint* PowerPack version 102 or later installed in Skylar One.
  - *Restorepoint Automation* PowerPack version 102 or later installed in Skylar One. For more information, see the ***Restorepoint Integrations*** manual.

3. In Skylar One, *create a SOAP/XML credential* to connect with PowerFlow and make note of its credential ID.
4. ***For a ServiceNow integration***:
   a. In PowerFlow, *sync Skylar One devices with ServiceNow* and make note of the ***Configuration*** field value in the Sync Devices from Skylar One to ServiceNow application.
   b. In Skylar One, open the "ServiceNow: Send Change Request Event to PowerFlow" Run Book Action (which is included in the *Business Services Base Pack* PowerPack v2.1 and greater) and *edit the input parameters* to include the credential ID from step 3 and the ***Configuration*** field value from step 4.
5. ***For a Restorepoint integration***, follow the steps in "Sync Devices with Restorepoint" section in the ***Device Management*** manual.
6. Finally, do one of the following:
   - Permanently enable the **Changes** widget by *editing the NextUI configuration file* on your Skylar One system.
   - Temporarily enable the **Changes** widget by *running a GraphQL mutation* on your Skylar One system.

Creating a SOAP/XML Credential for Skylar Automation (PowerFlow)

To create a SOAP/XML credential to connect Skylar One with Skylar Automation (PowerFlow):

1. Follow the steps in the section on "Creating a SOAP/XML Credential for Skylar Automation" in the ***Monitoring Skylar Automation*** manual.
2. After saving the credential, make note of the credential ID. This number can be found at the top of the **Edit SOAP/XML Credential** modal or in the ***ID*** column on the **Credentials** page (Manage > Credentials) or **Credential Management** page (System > Manage > Credentials).

Syncing Skylar One Devices with ServiceNow

To sync Skylar One devices with ServiceNow:

1. Follow the steps in the section on "Running a Device Sync" in the ***ServiceNow CMDB Synchronization*** PowerPack manual.

2. In the **Configuration** pane of the "Sync Devices from Skylar One to ServiceNow" application, make note of the value in the ***Configuration*** field.

Editing the Run Book Action (ServiceNow Integrations only)

To edit the input parameters in the "ServiceNow: Send Change Request Event to PowerFlow" run book action:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Locate the "Business Services Base Pack" PowerPack and click its wrench icon (🔧). The **Editing PowerPack** modal appears.
3. In the **Editing PowerPack** modal, click ***Run Book Actions*** in the left Navbar. The **Embedded Run Book Actions** page appears in the modal.
4. Click the wrench icon (🔧) for the "ServiceNow: Send Change Request Event to PowerFlow" run book action. The **Policy Editor** modal appears.
5. In the **Policy Editor** modal, make the following edits to the ***Input Parameters*** field:
   - Replace `<sll credential id for powerflow>` with the credential ID of the *SOAP/XML credential you created for PowerFlow*.
   - Replace `<pf config id>` with the ***Configuration*** field value from the *"Sync Devices from Skylar One to ServiceNow" application in PowerFlow*.
6. Click **[Save]**, then exit the **Policy Editor** modal.
7. Exit the **Editing PowerPack** modal.

Syncing Skylar One Devices with Skylar Compliance

To sync Skylar One devices with Skylar Compliance:

1. Follow the steps in the section on "Running a Device Sync" in the ***Skylar Compliance Integrations*** manual.
2. In Skylar Automation, open the **Configuration** pane for the "Restorepoint: Sync Devices" application and select *Enable* for the ***restorepoint_config*** field to allow device change detection.
3. Make a note of the ***restorepoint_id*** value on the **Configuration** pane for the "Restorepoint: Sync Devices" application.
4. In Skylar One, go to the **Device Investigator** page for the devices synced from Restorepoint, click on the **[Attributes]** tab, and ensure that the same ***restorepoint_id*** value was added to the ***Values*** column.

Permanently Enabling the Widget

To permanently enable the **Changes** widgetusing the NextUI configuration file, run the following steps on all appliances, including the Administration Portal, the Data Collector, the Database Server, the Data Engine, and the All-In-One Appliance.

To permanently enable the **Changes** widget:

1. Start an SSH session into one of the Skylar One appliances.
2. Using vi or another text editor, edit the `/opt/em7/nextui/nextui.conf` file. To do so, enter the following at the shell prompt:

   ```
   sudo vi /opt/em7/nextui/nextui.conf
   ```

3. Add the following line at the bottom of the NextUI configuration file:

   ```
   BUSINESS_SERVICES_CHANGE_EVENTS_TAB=enabled
   ```

4. Save your changes, and then restart the NextUI service by running the following command:

   ```
   sudo systemctl restart nextui
   ```

5. Repeat steps 1-4 for the remaining Skylar One appliances.

Temporarily Enabling the Widget

To temporarily enable the **Changes** widget using GraphQL:

1. To access the GraphiQL interface, type the URL or IP address for Skylar One in a browser, add **/gql** to the end of the URL or IP address, and press **[Enter]**. The GraphiQL interface appears.
2. In the main query pane, type the following mutation:

```
mutation updateChangeEventsTab {
        updateFeatureToggle(
                id: "system:BUSINESS_SERVICES_CHANGE_EVENTS_TAB"
                value: "enabled"
        ) {
                id
                value
        }
}
```

> **TIP:** Click the **[Prettify]** button to format the mutation and to add syntax highlighting to make the mutation easier to read. Note that the *Prettify* process removes the `query` syntax if only one query is present in the main query pane.

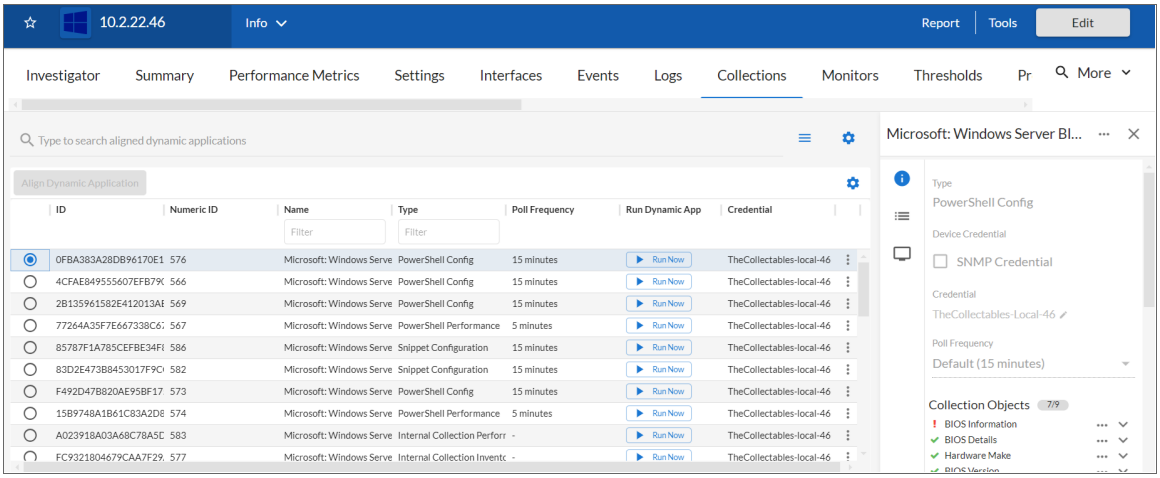
3. Click the **[Execute Query]** (Play) button. The mutation executes, and the results appear in the pane on the right side.

> **NOTE:** If the **Changes** widget does not appear in Skylar One after executing the mutation, refresh the page using the **[F5]** key or by clicking the refresh button in your web browser.

> **NOTE:** For more information about GraphQL, see the GraphQL documentation. For more information about the GraphiQL user interface, see the GraphiQL user interface documentation.

The Collections Tab

On the **[Collections]** tab of the **Device Investigator**, you can view a list of the Dynamic Applications associated with the device.

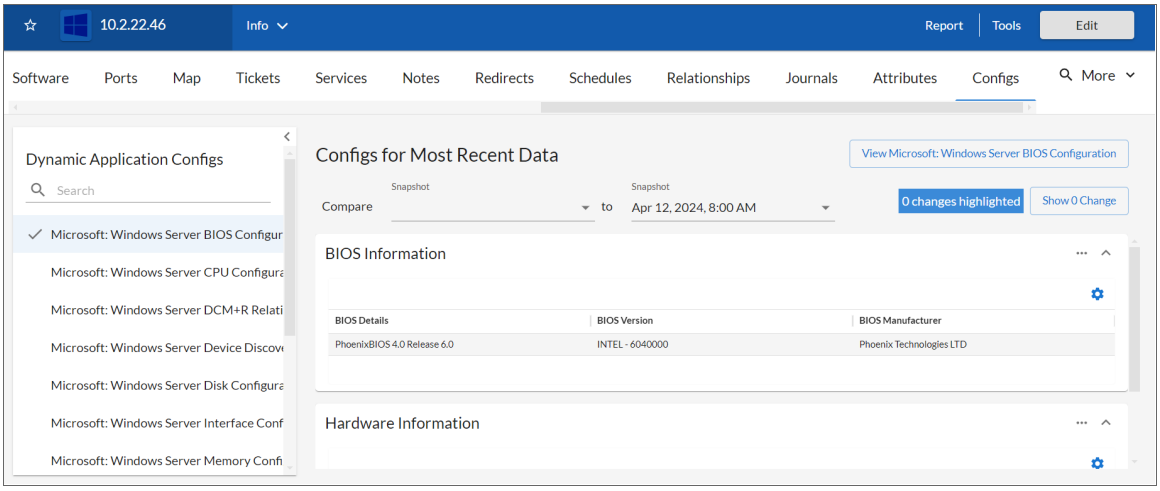


NOTE: For more information about this tab, see the section on *Managing the Dynamic Applications Associated with a Device*.

IMPORTANT: Even if you turn off data collection for a device, that device still consumes a single ScienceLogic device license. For more information, see the *Non-billable Devices* section.

The Configs Tab

On the **[Configs]** tab of the **Device Investigator**, you can view configuration information that has been collected from the device by Dynamic Applications. You can also view a list of all changes that occurred with a Dynamic Application between two specific snapshot reference points.



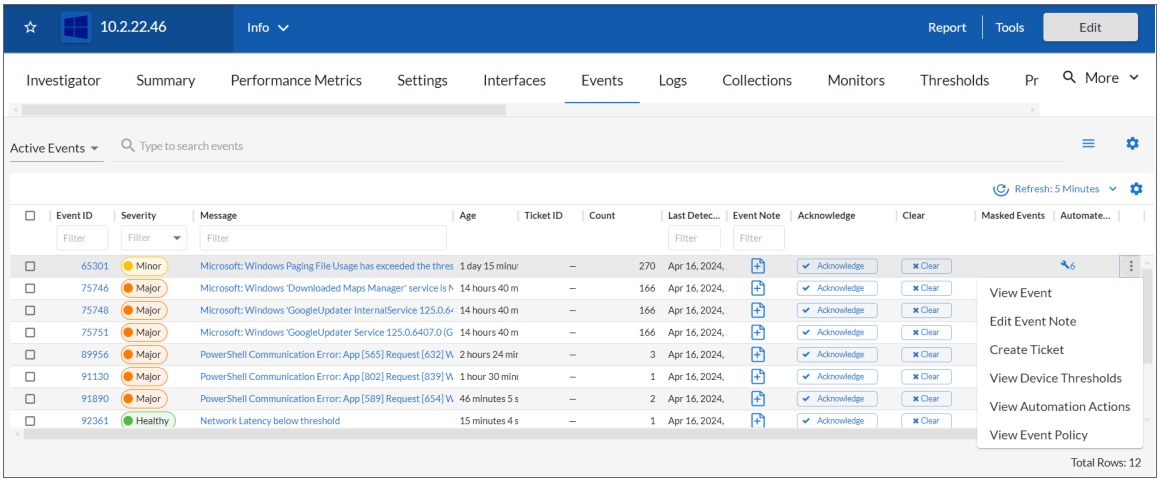
All objects of type "config" are included on the **[Configs]** tab. Usually, "config" objects contain static information about hardware and configuration settings, such as serial numbers, version numbers, and hardware status.

NOTE: You can also see all changes between two snapshots of a Dynamic Application in the **[Configs]** tab of the **Device Investigator** page. For more information, see the section on "Viewing Device Snapshot Data" in the ***Monitoring Device Infrastructure Health*** manual.

NOTE: For more information about this tab, see the chapter on "Viewing Configuration & Journal Data" in the ***Monitoring Device Infrastructure Health*** manual.

The Events Tab

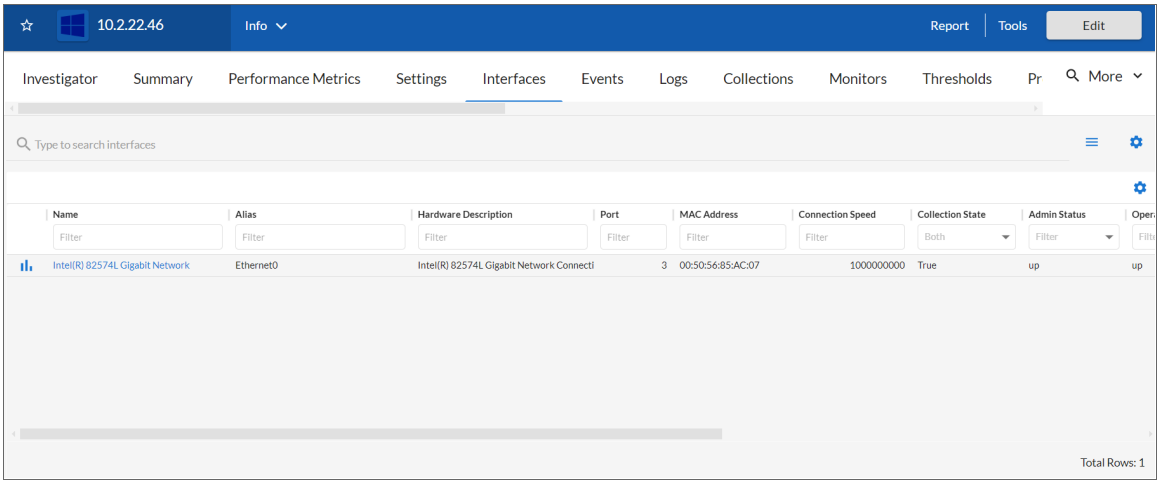
On the **[Events]** tab of the **Device Investigator**, you can view a list of events associated with the device.



NOTE: For more information about this tab, see the chapter on "Viewing Events" in the ***Events*** manual.

The Interfaces Tab

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



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

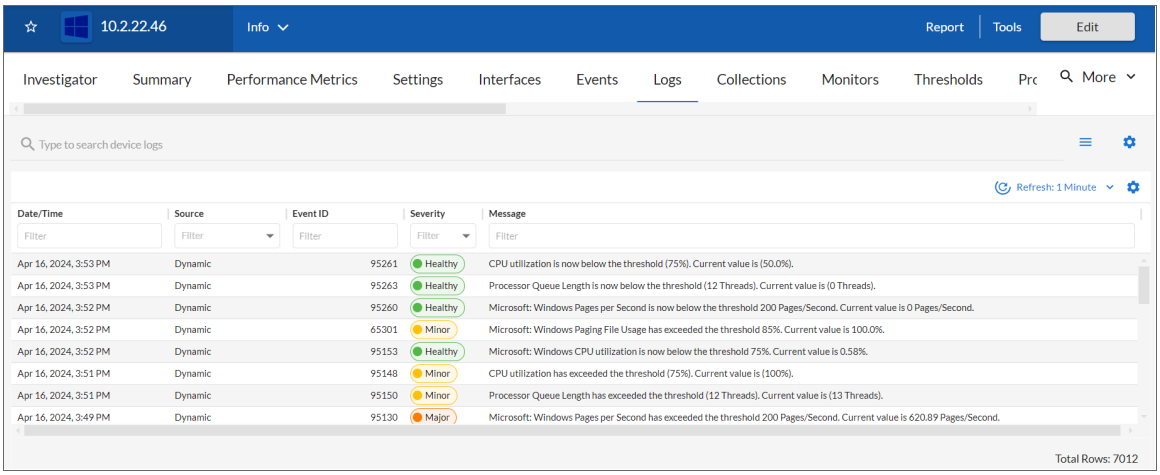
The Journals Tab

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

NOTE: For more information about this tab, see the chapter on "Viewing Configuration & Journal Data" in the ***Monitoring Device Infrastructure Health*** manual.

The Logs Tab

You can view logs and messages for a device in the **[Logs]** tab of the **Device Investigator** page. This is the same set of logs that display on the **[Investigator]** tab for this device.



The **Logs** tab displays all of the messages Skylar One and the Skylar One Agent, if applicable, have collected from the device. If the system has collected the same message multiple times, the log indicates how many times the message has repeated. You might find it helpful to view these log entries during troubleshooting or to manually check on the status of a device.

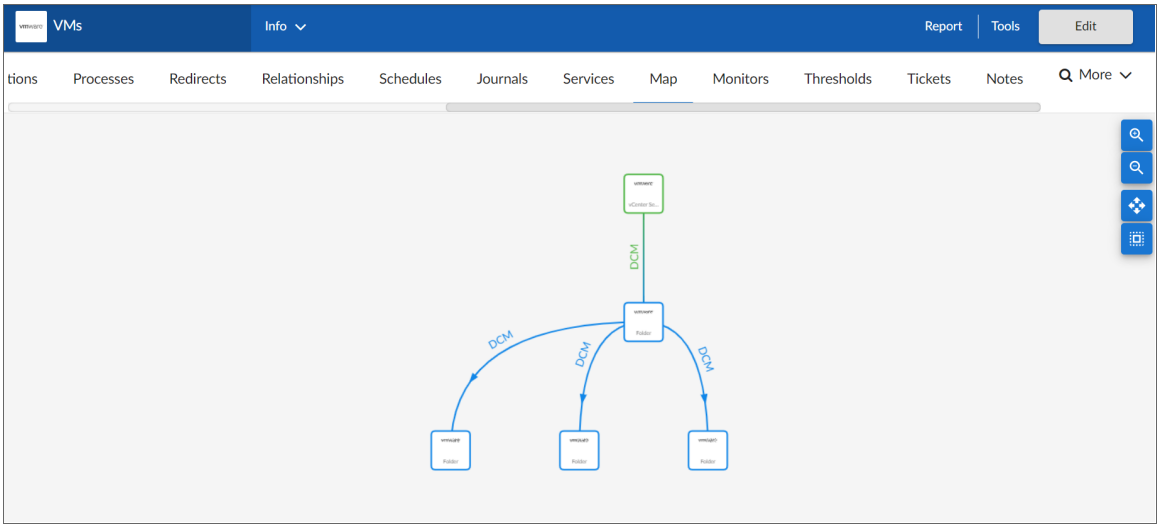
TIP: To sort the list, click on a column heading. The list will be sorted by the column value, in ascending order. To sort the list by descending order, click the column heading again. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

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

The Map Tab

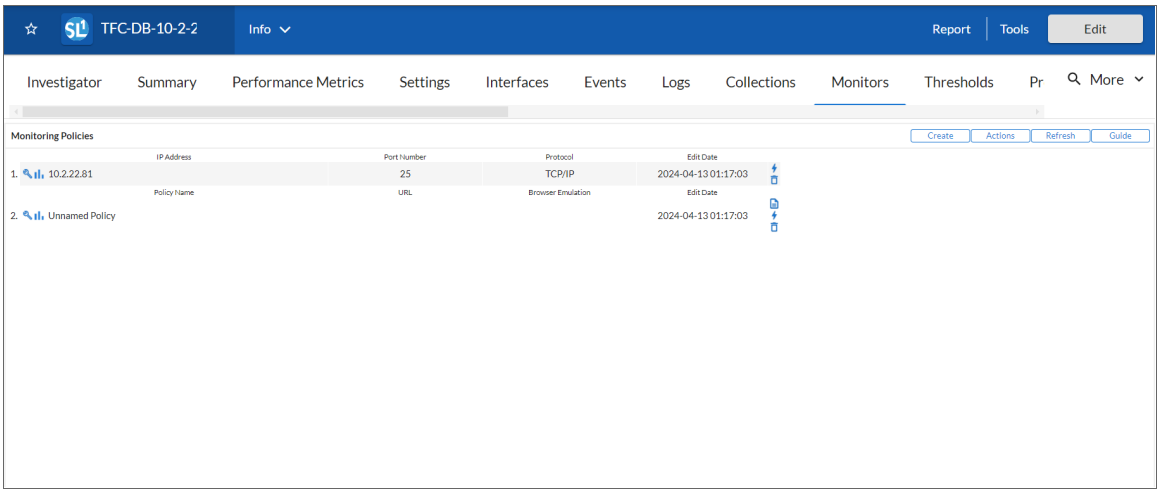
On the **[Map]** tab in the **Device Investigator**, you can view a map of the selected device and all of the devices with which the device has relationships.



NOTE: For more information about this tab, see the section on *Viewing Device Topology settings*. For more information about maps, see the ***Maps*** manual.

The Monitors Tab

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



The **[Monitors]** tab allows you to define policies that monitor:

- ***System processes***. Monitors the device and look for the specified system process. For more information, see the chapter on "Monitoring Device Processes" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Domain-name availability and lookup speed***. Monitors the availability and lookup time for a specific domain-name server and a specific record on a domain name server. For more information, see the chapter on "Monitoring Domain Servers and DNS Records" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Email round-trip speed***. Monitor the amount of time it takes to send an email message from Skylar One to an external mail server and then back to Skylar One. For more information, see the chapter on "Monitoring Email Round-Trips" in the ***Monitoring Device Infrastructure Health*** manual.
- ***SOAP and XML transaction speeds***. Monitors any server-to-server transactions that use HTTP and can post files or forms. (for example, SOAP/XML or email). Periodically, Skylar One sends a request and some data and then examines the result of the transaction and compares it to a specified expression match. For more information, see the chapter on "Monitoring SOAP and XML Transactions" in the ***Monitoring Device Infrastructure Health*** manual.
- ***TCP/IP port availability***. Monitors ports for availability every 5 minutes. If a port is not available, Skylar One creates an event. The data gathered by the port policy is used to create port-availability reports. For more information, see the chapter on "Monitoring Ports" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Web-content availability***. Monitors a website for specific content. 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. For more information, see the chapter on "Monitoring Web Content" in the ***Monitoring Device Infrastructure Health*** manual.
- ***Services***. Monitors the device and look for the specified service. For more information, see the chapter on "Monitoring Services" in the ***Monitoring Device Infrastructure Health*** manual.

> **NOTE**: All of these monitoring policies can generate events. Skylar One uses the data collected by these policies to create performance reports and graphs.

The Notes Tab

On the **[Notes]** tab of the **Device Investigator**, you can add and view notes and other attachments associated with the device.

To add a note to a device:

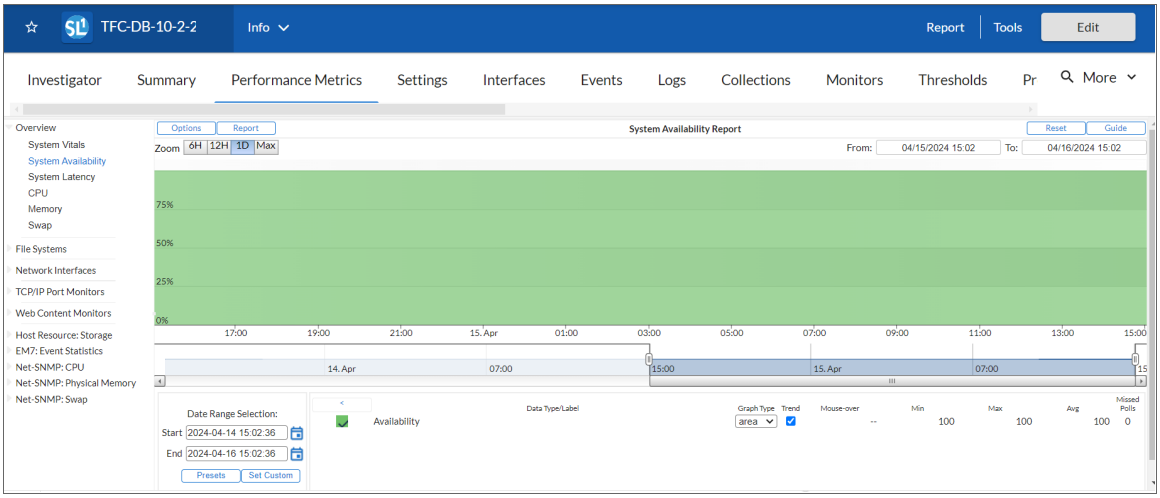
1. Go to the **[Notes]** tab of the **Device Investigator**.
2. Click the **[Actions]** button and then select *Notepad Editor*. The **Notepad Editor** modal page appears.
3. In the **Notepad Editor** modal page , you can enter notes or comments about the device.
    - You can format the text and include links, images, and videos in the note.
    - You can also include a document template (System > Customize > Document Templates) in the field.

4. When you are finished adding content to the note, click **[Save]**. The note will appear in the **[Notes]** tab, along with any other notes about the device. Each note includes the username, date and time, and text of the comment. You can perform the following on each note entry:
    - ***To view a note's attachment***, click the paperclip icon ( ).
    - ***To edit the content of a note***, click the wrench icon ( ). The **Notepad Editor** modal page appears. You can update the note; format the text; insert content from a saved template; and add an attachment, image, or video to the note. Click the **[Save]**button to save your changes.
    - ***To delete a note***, click its delete icon ( ).

NOTE: For information about adding a note to a device in the classic Skylar One user interface, see the section on *Adding a Note in the Device Administration Panel*.

The Performance Metrics Tab

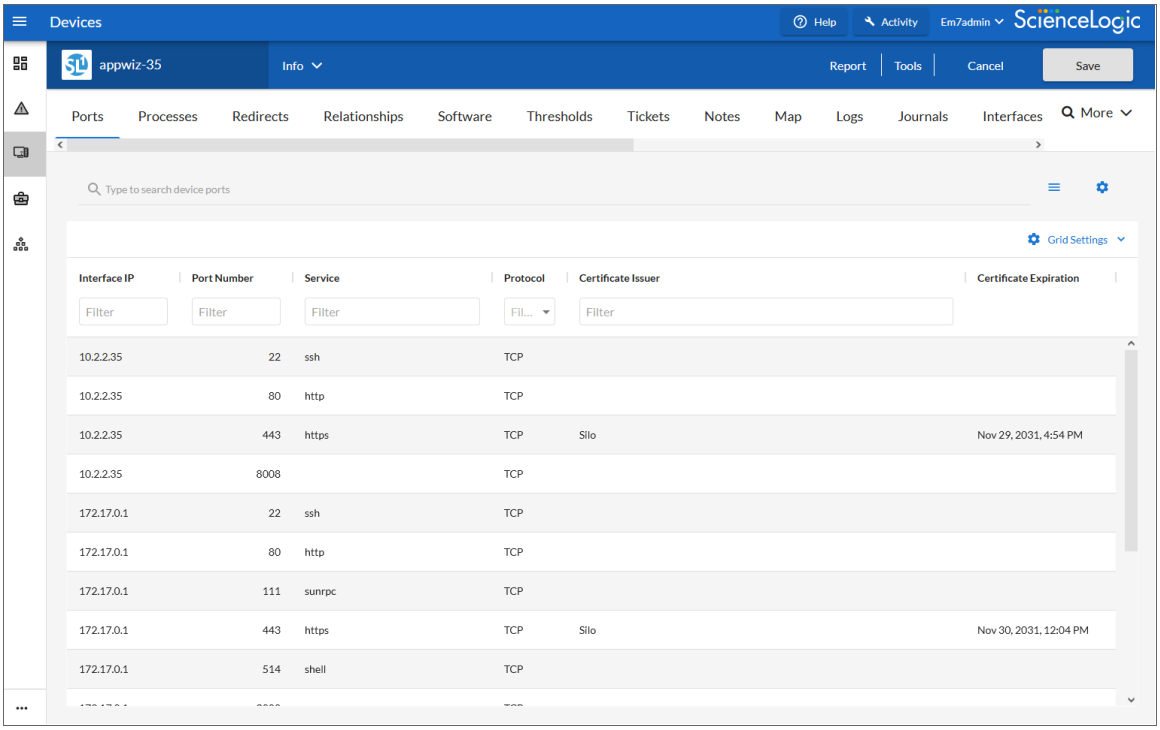
On the **[Performance Metrics]** tab of the **Device Investigator**, you can view performance graphs for hardware, monitoring policies, and Dynamic Applications aligned with the device.



NOTE: For more information about this tab, see the chapter on "Viewing Performance Graphs" in the ***Monitoring Device Infrastructure Health*** manual.

The Ports Tab

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



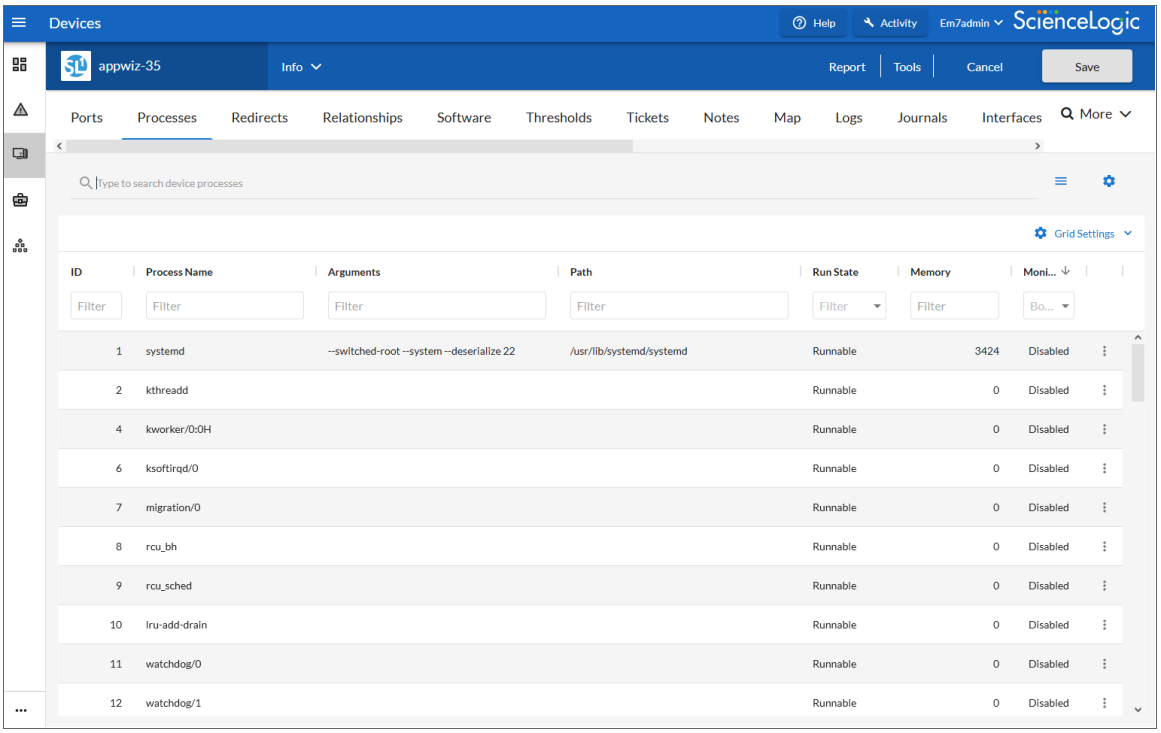
Every night, Skylar One scans all the ports of each managed device. If any new ports are opened, Skylar One adds the port to the list on the **[Ports]** tab.

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

The Processes Tab

A ***process*** is a program that is currently running on a monitored device or has been run in the past and is currently idle. Sometimes a process is called a task.

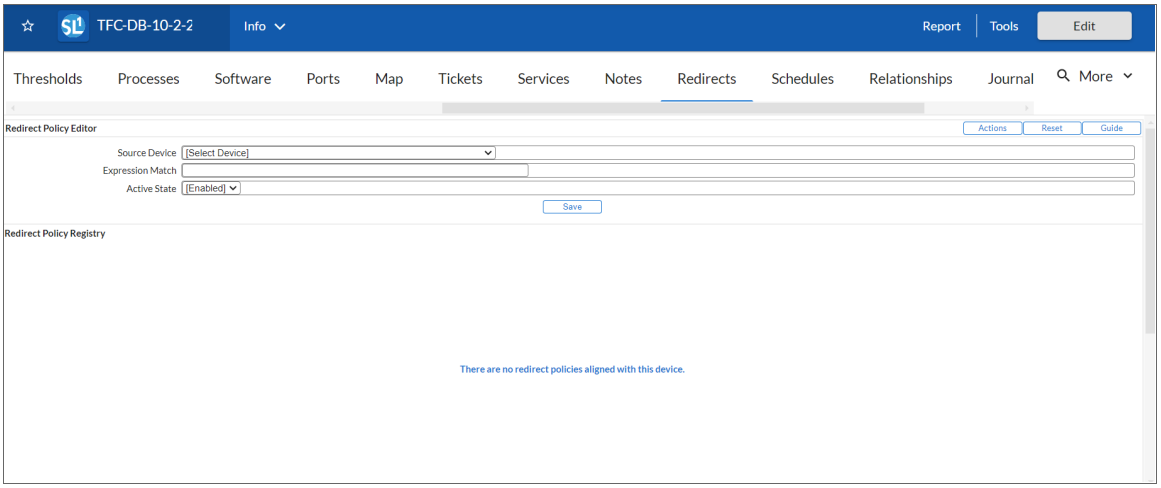
On the **[Processes]** tab of the **Device Investigator**, you can view information about the processes running on the device. The **[Processes]** tab displays a combined list of processes collected via SNMP and the agent, where applicable.



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

The Redirects Tab

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



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

The Relationships Tab

On the **[Relationships]** tab of the **Device Investigator**, you can view information about parent-child relationships between the selected device and other devices.

NOTE: For more information about this tab, see the section on *Viewing Relationships for a Single Device*.

The Schedules Tab

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

NOTE: For more information about this tab, see the section on *Scheduling Maintenance for a Single Device*.

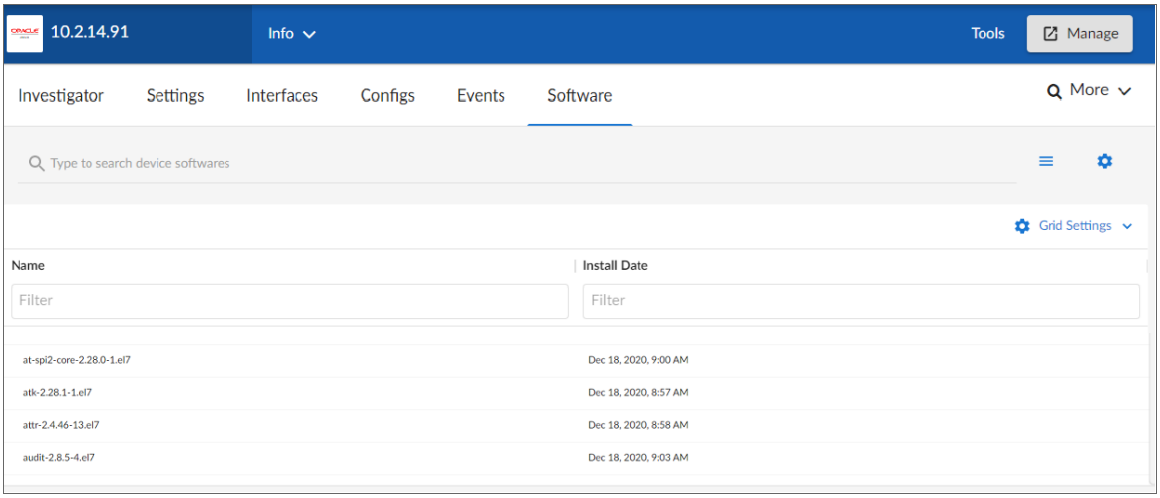
The Services Tab

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

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

The Software Tab

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



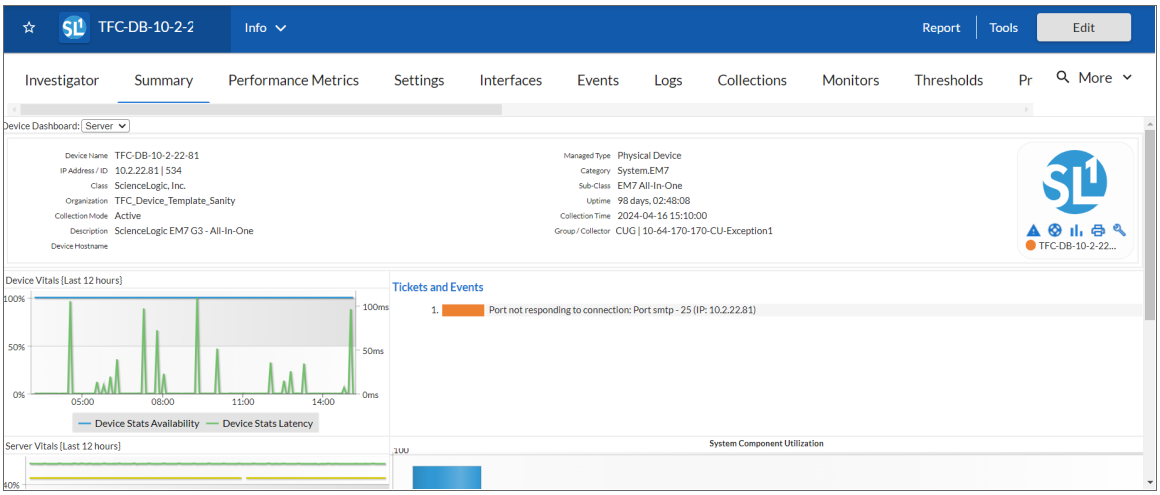
For each installed software title, the **[Software]** tab displays the following information:

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

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

The Summary Tab

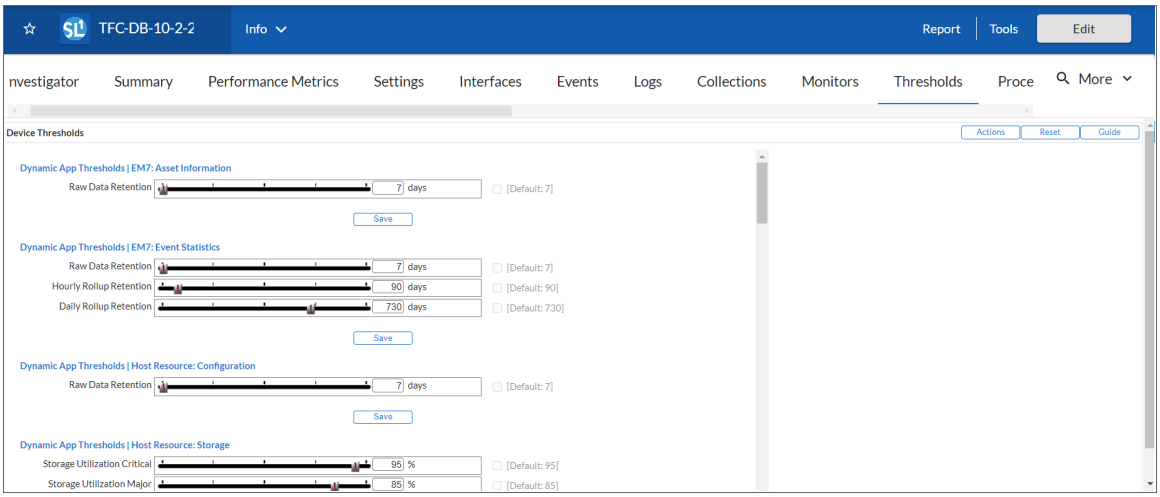
On the **[Summary]** tab of the **Device Investigator**, you can view an overview of device details through device dashboards and widgets that display various metrics.



NOTE: For more information about this tab, see the chapter on "The Default Device Summary Page" in the ***Monitoring Device Infrastructure Health*** manual.

The Thresholds Tab

On the **[Thresholds]** tab of the **Device Investigator**, you can define usage and performance thresholds and data retention thresholds for a device.



When performance thresholds are exceeded, Skylar One will generate an event for the device. When space thresholds are exceeded, Skylar One will remove the oldest data from the database. For each of these thresholds, Skylar One defines a default value. You can edit the thresholds to meet your needs.

NOTE: For more information about this tab, see the section on *Device Thresholds*.

The Tickets Tab

On the **[Tickets]** tab of the **Device Investigator**, you can view all tickets associated with the device and create new tickets to associate with the device.

The **[Tickets]** tab displays critical information about each ticket. If you require more detail, you can access the **Ticket Editor** from this page by clicking on the ticketing icon ( ) for that ticket.

You can also create a new ticket from this page.

To create a new ticket for a device:

1. Go to the **[Tickets]** tab of the **Device Investigator**.
2. Click the **[Actions]** button and then select *Create a Ticket*. The **Ticket Editor** page appears.
3. On the **Ticket Editor** page that appears, define the basic parameters for the ticket. For information about the fields on this page, see the chapter on "Creating and Editing Tickets" in the ***Ticketing*** manual.

> **NOTE:** The ***Description*** and ***Element*** fields are automatically populated with information about the device.

4. When you are finished, click **[Save]**.

Chapter 4

Using the Device Manager Page

Overview

After running discovery for the first time, you can view the list of discovered devices on the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface) in Skylar One.

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

This chapter covers the following topics:

Viewing the List of All Devices 83

Generating a Report for Multiple Devices 87

Generating a Report for a Single Device 87

Viewing the List of Component Devices 88

Bulk Actions in the Device Management Page 92

Bulk Actions for Component Devices 94

Bulk Merging and Unmerging of Devices in the Classic User Interface 95

Viewing the List of All Devices

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

TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

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

- ***Device Name***. Name of the device. For devices running SNMP or with DNS entries, the name is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***Device Hostname***. For devices that are discovered and managed by hostname (instead of IP address), this field displays the fully qualified hostname for the device.
- ***IP Address***. The IP address of the device.
- ***Device Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, and printers, among others. The category is automatically assigned during discovery, at the same time as the as Device Class/Sub-Class.
- ***Device Class/Device Sub-Class***. The manufacturer (device class) and type of device (sub-class). The Device Class/Sub-Class is automatically assigned during discovery, at the same time as the Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by Skylar One.
- ***Organization***. The Organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. The appearance of the ***Current State*** field depends upon the value of the ***Show Severity Badges*** field in your user preferences. If the ***Show Severity Badges*** field is enabled, the value in the ***Current State*** column will be displayed as a color-coded badge. If the ***Show Severity Badges*** field is not enabled, the value in the ***Device Name*** column and the value in the ***Current State*** column will be painted with the severity color. The condition can be one of the following:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.

- *Notice*. Device has an informational event associated with it.
- *Healthy*. Device is running with no problems.

- ***Collection Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in the **Collector Group Management** page (System > Settings > Collector Groups) and specify a primary Data Collector and an optional failover collector. A Data Collector server is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).
- ***Collection State***. Specifies the current condition of data collection for the device. 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*. The collection state can be one of the following:
  - *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.
- ***SNMP Credential***. The primary credential used by Skylar One to retrieve SNMP information about the device. Your organization membership(s) might affect the display in the ***SNMP Credential*** column. For details, see the ***Discovery and Credentials*** manual.
- ***SNMP Version***. The version of SNMP used by the ***SNMP Credential***.
- ***SL Agent***. Indicates if the Skylar One Agent is installed on the device. If the agentis installed on the device, the SL Agent column displays a gear icon that can be used to access agent settings. For more information about editing Agent settings, see the ***Monitoring Using the Agent*** manual. The ***SL Agent*** column does not appear on the **Device Manager** page by default. For more information about adding or removing columns on the **Device Manager** page, see the *Device Manager Preferences* section.
- ***Tools***. Displays icons for managing devices. The choices are:
  - *Device Administration* (🔧). Leads to the **Device Properties** page, where you can define basic device parameters and parameters for discovery. From the **Device Properties** page, you can also access the other pages in the *Device Administration* tools.

- *Device Management* ( ). Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the **Device Reports** panel. For details on Device Reports, see the manual ***Monitoring Device Infrastructure Health***.
- *Root Device* ( ). Indicates that the device is a ***component device***. Leads to the **Device Properties** page of the root device for the component device. In Skylar One, the ***root device*** is the physical device that hosts the system that manages the component device.
- *Parent Device* ( ). Indicates that the device is a ***component device***. Leads to the **Device Properties** page of the parent device for the component device. In Skylar One, the ***parent device*** can be either another component device or a physical device. A parent device can be either: the component device between the current component device and the next layer in the component-device hierarchy or a root device.
- *Interfaces* ( ). Leads to the **Interfaces Found** page, where you can view details about each network interface on the device.
- *View Historical Events* ( ). Leads to the **Viewing Cleared Events** page, which displays a list of all cleared events associated with the device.
- *View Current Events* ( ). Leads to the **Viewing Active Events** page, which displays a list of all active events associated with the device.
- *Print Report* ( ). Generates a report for the selected icon. Spawns the **Report Selector** page, where you can specify the information to include in the report (Full Report, Status, Config, Hardware, Notes, Software, Processes, Network, Events, and Health) and the format in which the report will be generated (Create Report as HTML Document, Create Report as PDF Document, Create Report as MS Word Document, or Create Report as MS Excel Document).
- *Create Ticket* ( ). Leads to the **Ticket Editor** page, where you can define and file a new ticket for the device. For details on creating tickets, see the ***Ticketing*** manual.
- *View Asset Record*( ). This icon appears if an asset record has already been defined for the device. This icon leads to the **Asset Properties** page, where you can view the asset record for the device.
- *Create Asset Record* ( ). This icon appears if an asset record has not been defined for the device. This icon leads to the **Asset Properties** page, where you can create an asset record for the device.
- *Schedule Maintenance* ( ). Leads to the **Schedule Maintenance** page. On this page, you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, Skylar One will not generate events about the selected devices. You can choose to disable or enable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate events for the devices. For details on scheduling maintenance, see the section on *Maintenance*.
- *Checkbox* ( ). Applies the action in the ***Select Action*** drop-down list to the device. To select all checkboxes (i.e., to select all devices), select the empty checkbox icon ( ) at the top of the column.

Device Manager Preferences

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

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

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

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

Using the Advanced Filter with the List of Devices

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

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

> **TIP:** To select multiple entries in the Advanced Filter Tool, hold down the **<Ctrl>** key and left-click the entries. After selecting all filters, click the **[Apply]** button to apply the filters to the list of devices. To reset each field and apply no filters, click the **[Reset]** button.

To access the Advanced Filter Tool:

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

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

4. In the Advanced Filter Tool, filter by one or more of the available parameters.
5. After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
6. To reset each field and apply no filters, select the **[Reset]** button.

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

Generating a Report for Multiple Devices

From the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), you can generate a report on all devices in Skylar One or on multiple devices in Skylar One. The report will contain all the information displayed in the **Device Manager** page.

To generate a report about all or multiple devices:

1. In Skylar One, go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. To filter the list of devices, use the "search as you type" fields at the top of each column. You can filter the list of devices by one or more column values. Only the devices displayed in the **Device Manager** page will appear in the report.
3. Click the **[Report]** button.
4. When prompted, specify the output format for the report and if you want to save the report.
5. Click **[Generate]**. The report displays.

Generating a Report for a Single Device

From the **Device Investigator** page of the Skylar One user interface or the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), you can generate a detailed report on a single device. You can specify the information to include in the report and the format in which the report will be generated, such as PDF, HTML, XLSX, ODS, or CSV.

To generate a detailed report on a single device:

1. In Skylar One, go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
    - If you are on the **Devices** page, click the device name to open the**Device Investigator** page for that device. Click the **[Reports]** button. The **Device Report** modal page appears.
    - If you are on the **Device Manager** page, select the printer icon ( ) for the device for which you want to generate a detailed report. The **Report Creator** modal page appears.
2. On the modal page, select one of the following to specify the information to include in the device report:
    - **[Full Report]**. Includes information about device status, status of all device policies, status of all monitors, status of hardware components, status of all thresholds defined for the device, a list of all active events associated with the device, and information about the last collection time and last entry to the device log.

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

3. Select from the following list of formats in which the report can be generated:
   - ***HTML***. Create the report as an HTML document.
   - ***PDF***. Create the report as a PDF document.
   - ***DOC***. Create the report as a Microsoft Word document.
   - ***XLS***. Create the report as Microsoft Excel spreadsheet.
   - ***CSV***. Create the report using comma-separated values.
4. Click **[Create Report]**. The report displays in the format you selected.

Viewing the List of Component Devices

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

1. Go to the **Device Components** page (Devices > Device Components).
2. The **Device Components** page displays the following about each device:

TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

- ***Plus-sign icon*** (+). Clicking on this icon expands the device and displays the child devices underneath the device. Each device that displays a plus-sign icon has child devices.
- ***Minus-sign icon*** (−). Clicking on this icon collapses the device and hides the child devices for this device. Each device that displays a minus-sign icon has child devices.
- ***Device Name***. Name of the device. For devices running SNMP, component devices, or devices with DNS entries, the name is discovered automatically. For root devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The IP address of the device. Appears only for physical devices.
- ***Device Category***. The category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the as Device-Class/Sub-Class.
- ***Device-Class/Device Sub-Class***. The manufacturer (device class) and type of device (sub-class). The Device-Class/Sub-Class is automatically assigned during discovery, at the same time as the as Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by Skylar One.
- ***Organization***. The Organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. Condition can be one of the following:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.
    - *Notice*. Device has an informational event associated with it.
    - *Healthy*. Device is running with no problems.
- ***Collector Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in System > Settings > Collector Groups and specify one or more Data Collectors. A Data Collector is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups)

- ***Collection State***. 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 Administration* (). Leads to the **Device Properties** page, where you can define basic device parameters and parameters for auto-discovery. From the **Device Properties** page, you can also access the other pages in the Device Administration tools
  - *Device Management* (). Leads to the **Device Summary** page, where you can see reports and logs related to the device. From the **Device Summary** page, you can also access the other pages in the Device Management tools.
  - *Interfaces* (). Leads to the **Interfaces Found** page, where you can view details about each network interface on the device.
  - *Print Report* (). Generates a report for the selected device. Opens the **Report Selector** modal, where you can specify the information to include in the report (Full Report, Status, Config, Hardware, Notes, Software, Processes, Network, Events, Health) and the format in which the report will be generated (HTML Document, PDF Document, MS Word Document, MS Excel Document, or CSV File).
  - *Create Ticket* (). Leads to the **Ticket Editor** page, where you can define and file a new ticket for the device.
  - *View Asset Record* (). This icon appears if an asset record has already been defined for the device. This icon leads to the **Asset Properties** page, where you can view the asset record for the device.
  - *Create Asset Record* (). This icon appears if an asset record has not been defined for the device. This icon leads to the **Asset Properties** page, where you can create an asset record for the device.
  - *Merge with Physical Device* (). Leads to the **Merge Devices** modal, where you can view a list of devices that are available for merging with the selected device. For more information, see the section on *Merging Devices*.
  - *Checkbox* (). Applies the action in the **[Select Action]** drop-down to the device. To select all the checkboxes, select the large red checkmark icon.

Availability for Component Devices

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

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

Viewing Child Devices

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

1. Go to the **Device Components** page (Devices > Device Components).
2. In the **Device Components** page, find the root device for which you want to view its component children. Select its plus sign icon (+).
3. The device will be expanded to display the component child devices below the root device:
4. You can select the plus sign icon for each component child device that also serves as a root device. To collapse the component child devices, select their minus sign icon (−).

Using the Advanced Filter with the List of Component Devices

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

TIP: To select multiple entries in the Advanced Filter tool, hold down the <Ctrl> key and left-click the entries. After selecting all filters, click the **[Apply]** button to apply the filters to the list of devices. To reset each field and apply no filters, click the **[Reset]**button.

To access the Advanced Filter tool:

1. Go to the **Device Components** page (Devices > Device Components).
2. Click on the funnel icon ( ).
3. In the Advanced Filter Tool, filter by one or more of the available parameters.
4. After selecting the desired filters, click the **[Apply]**button to filter the list of devices.
5. To reset each field and apply no filters, click the**[Reset]** button.

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

Bulk Actions in the Device Management Page

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

To apply an action to multiple devices:

1. In the **Device Manager** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the checkbox at the top of the page.
2. In the ***Select Action*** drop-down list, select one of the following actions:
    - ***Delete Devices***. Deletes all selected devices from Skylar One. Tickets associated with the device are unlinked from the device, but are not deleted.
    - ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device template to all selected devices. You can also make one-time changes to the template, and those changes will be applied only to the selected devices. For details on using device templates, see the manual ***Device Groups and Device Templates***.
    - ***Clear Device Logs***. Deletes data from the device's log files. For details on device logs, see the manual ***Monitoring Device Infrastructure Health***.

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

Bulk Actions for Component Devices

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

To apply an action to multiple devices:

1. In the **Device Components** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the checkbox at the top of the page.
2. In the ***Select Action*** drop-down list, select one of the following actions:
    - ***Delete Selected Devices***. Deletes all selected devices from Skylar One. Tickets associated with the device are unlinked from the device, but are not deleted.
    - ***Delete Selected Devices (recursive)***. Deletes all selected devices from Skylar One. If one or more of the selected devices is a root device with one or more component devices as children, this option deletes the root device and the component devices. Tickets associated with the deleted device are unlinked from the device, but are not deleted. To delete a root device and its associated component devices, use the option ***Delete Selected Devices (recursive)***.
    - ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device templates to all selected devices. You can also make one-time changes to the template, that will be applied only to the selected devices.
    - ***Clear Device Logs***. Deletes data from the device's log files.
    - ***Schedule Maintenance***. Leads to the **Maintenance Schedule** page. In this page, you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, Skylar One will not generate events about the selected devices. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate events for the devices.
    - ***Create Asset Record***. Automatically creates an asset record for the device. Skylar One automatically populates as many fields as possible, using retrieved data.
    - ***Change Collection State***. Changes the status of the device in Skylar One. The choices are:
        - *Active*. Skylar One polls the device on a regular basis and updates the data displayed in Skylar One.
        - *Active (recursive)*. Skylar One polls the device on a regular basis and updates the data displayed in Skylar One. Skylar One also polls all children devices (of the selected device) on a regular basis and updates their data.
        - *Disabled*. Skylar One does not poll the device. Data displayed in Skylar One is not updated.
        - *Disabled (recursive)*. Skylar One does not poll the device. Skylar One does not update data about the device. Skylar One also does not poll any children devices (of the selected device) and does not update data about the children devices.

- ***Change Collector Group***. Changes the collector group used to collect data from the device. Choose from the list of all collector groups and virtual collector groups in Skylar One. When you select one of the collector groups, each selected device will by polled by the collectors in the collector group. For All-In-One Appliances, you can select only the built-in Collector Group and any virtual Collector Groups.

    - If you align a device with a virtual Collector Group, Skylar One will store all historical data from all aligned devices, but will no longer perform collection on those devices or trigger events for these devices.
- ***Move to Organization***. Associates a device with an organization. The list of choices will include all organizations in Skylar One.
- ***Align SNMP Read Credential***. This option applies the selected credential to all selected devices. The selected devices will use the selected credential as their primary credential. Secondary credentials will remain unchanged. Choose from a list of all SNMP Read credentials in Skylar One (defined in System > Manage > Credentials).
- ***Add to Device Group***. This option aligns the selected devices with the selected device group. The selected devices will then appear in **Device Group Views** and will inherit the properties of the device group, including scheduling, access, and visibility.

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

Bulk Merging and Unmerging of Devices in the Classic User Interface

If your Skylar One system includes a physical device and a component device that both represent the same device, you can merge those device records into a single record for easier monitoring. Merging does not remove, replace, or add any data; merging simply groups data together.

There are several benefits to merging physical and component devices:

- Merging consolidates the devices and their data—device fields, values, graphs, behaviors, and other user interface elements—providing you with a single set of data for the device.
- Merging reduces the number of duplicated events and administrative tasks.
- Merged devices consume only a single device license.

For example, you might discover a virtual machine device component representing a server, and then later discover an IP-based device from the same server. To prevent duplicate events from occurring for the same server, minimize administrative tasks, and prevent a negative impact on your licensing by inflating the number of devices being monitored by Skylar One, you could merge the virtual machine component and the corresponding IP-based device into a single device record.

NOTE: You ***cannot*** merge a component device with a physical device that acts as the root device for a dynamic component map (DCM) tree.

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

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

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

NOTE: You can merge only two individual devices together into a single merged device. To do so, you must have user permissions that allow merging and unmerging on both devices. For more information about user access permissions, see the ***Access Permissions*** manual.

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

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

TIP: Use consistent device hostnames to make device merging easier.

Performing a Bulk Device Merge in the Classic User Interface

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

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

To perform a bulk device merge:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

2. Select the **[Actions]** menu and then choose ***Merge Devices***.

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

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

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

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

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

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

5. A modal window displays that asks you to confirm the merge. Select the **[Yes]** button.
6. Skylar One begins merging the selected devices. When the message, "Device Bulk Merge complete" displays, select the **[Close/Esc]** button.

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

Performing a Bulk Device Unmerge in the Classic User Interface

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

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

For details on unmerging a vanished device, see the chapter in this manual on *Vanishing & Purging Devices*.

To unmerge multiple devices:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Select the **[Actions]** menu and then choose ***Unmerge Devices***.
3. The **Device Bulk Unmerge** page displays a list of merged devices. Each numbered row indicates a pair of merged devices that can be unmerged. Select the checkboxes in the last column of each row of devices that you want to unmerge, then select the **[Unmerge]** button.
4. A modal window displays that asks you to confirm the unmerging. Select the **[Unmerge]** button.
5. When the message, "Device Bulk Unmerge complete" displays, select the **[Close/Esc]** button.

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

Chapter 5

Managing a Single Device with the Device Administration Panel

Overview

This chapter describes how to use the **Device Administration** panel in Skylar One.

This chapter covers the following topics:

What is the Device Administration Panel? 100
Actions Menu 101
Device Properties 104
Viewing Read-Only Information About the Device 105
Editing Device Settings 106
Adding an IP Address to a Device 116
Removing an IP Address from a Device 117
Managing Device IPs 117
Clearing the Device Cache 119
Aligning a Secondary Credential 119
Adding the Device to a Device Group 120
Creating a Ticket About the Device 122
Adding a Note to a Device 122

Aligning Custom Attributes with a Device 123
Associating a Product SKU with the Device 125
Merging Devices 126
Performing Administrative Tasks for One or More Devices 130
Shortcut Keys for the Device Administration Panel 132

What is the Device Administration Panel?

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

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

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device for which you want to access the **Device Administration** panel and select its wrench icon (). The **Device Properties** page is displayed. From this page, you can access all the pages in the **Device Administration** panel.
3. 'The **Device Administration** tools include the following tabs and pages:

Tab	Description
Properties	In the **Device Properties** page, you can edit parameters that affect how Skylar One "sees" and monitors the device.
Thresholds	The **Device Thresholds** page allows you to define usage and performance thresholds and data retention thresholds for a device. When these thresholds are exceeded, Skylar One will generate an event for the device.
Collections	The **Dynamic Application Collections** page displays all the Dynamic Applications associated with the device. For Dynamic Applications of type "performance," the page displays report policies for each Dynamic Application. For Dynamic Applications of type "configuration," the page displays objects monitored by each Dynamic Application. You can specify a credential for use with the Dynamic Application for the selected device only. You can enable or disable one or more report policies for the selected device only. You can enable or disable monitoring of one or more objects for the selected device only.
Monitors	The **Monitoring Policies** page allows you to define monitoring policies for a device. The **Monitoring Policies** page allows you to define policies that monitor: system processes, domain-name availability and lookup speed, email round-trip speed, SOAP and XML transaction speeds, TCP/IP port availability, web-content availability, and services.

Tab	Description
	NOTE: All these monitoring policies can generate events. Skylar One uses the data collected by these policies to create performance reports and graphs. Additionally, the Monitoring Policies page allows you to create, edit, and delete webhook receivers. For more information, see the chapter on "Using Webhooks to Generate Events" in the **Events** manual.
Schedule	In the **Maintenance Schedule** page you can view, edit, and schedule downtime for the device.
Logs	The **Device Logs & Messages** page displays all the messages Skylar One has collected from the device and from Skylar One about the device.
Toolbox	The **Device Toolbox** page provides access to common network tools. The list of tools available depends upon the type of device and the configuration of the device. This page allows you to access and run diagnostics on a device without leaving the Compute Nodes.
Interfaces	The **Device Interfaces** page displays detailed information about each network interface on the device. From this page, you can view details about each individual interface and define bandwidth monitoring for the interface.
Relationships	The **Device Relationships** page displays information about parent-child relationships between devices. From this page, you can view details on the relationships between layer-2 and layer-3 devices, hypervisors and their virtual machines, and other relationships.
Tickets	The **Ticket History** page displays all tickets associated with the device. This page displays critical information about each ticket. If you require more detail, you can access the**Ticket Editor** from this page.
Redirects	This page allows you to redirect log entries from one IP-based device to another IP-based device, or from an IP-based device to a virtual device.
Notes	The **Notes & Attachments** page displays a list of all comments and attachments associated with the device properties. When you select the *Notepad Editor* option in the **Device Properties** page, the notes appear in this page.
Attributes	The **Attributes** page displays a list of custom attributes that are already aligned with the device. Additionally, the **Attributes** page enables you to assign a value to those custom attributes, create and align a new extended custom attribute with the device, or delete a custom attribute from a device.

Actions Menu

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

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

- ***Add IP Address***. Leads to the **Add IP Address** modal, where you can define an additional IP address for the device. Skylar One will continue to use the primary IP Address for communication with the device. For details, see the section on *Adding an IP Address to a Device*.
- ***Select Primary IP Addresses***. Leads to the **Select Primary IP Addresses** modal, where you can define primary IP addresses and secondary IP addresses for the device. A primary IP address allows Skylar One to align traps and syslog messages with the device. In the case of duplicate primary IP addresses, you can promote a secondary IP address to a primary IP address and demote the duplicated primary IP address.
- ***Clear Device Cache***. Selecting this option clears data about this device from the cache. For details, see the section on *Clearing the Device Cache*.
- ***Device Class***. Leads to the **Device Class** modal, where you can select a device class to associate with the device. For details, see the section on *Device Classes and Device Categories*.
- ***Secondary Credentials***. Leads to the **Secondary Credentials** modal, where you can associate additional credentials with the device. Skylar One will then use the primary credential and the additional credentials during discovery for the device. For details, see the section on *Aligning a Secondary Credential*.
- ***Merge Device***. Allows you to merge the data from a component device and a non-root physical device into a single record. When you merge a physical device and a component device, the device record for the component device is no longer displayed in the user interface; the device record for the physical device is displayed in user interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page and the **Component Map** page. All existing and future data for both devices will be associated with the physical device.

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

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

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

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

NOTE: You can merge only one component device with a physical device. You ***cannot*** merge a component device with a physical device that acts as the root device for a dynamic component map (DCM) tree.

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

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

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

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

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

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

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

Device Properties

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

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

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

- ***View Information about the Device***. This is described in the section on *Read-Only Information about the Device*.
- ***Edit the Discovery Parameters for the Device***. This is described in the section on *Editing Device Settings*.
- ***Edit the Device Class for the Device***. This is described in the section on *Device Classes*.
- ***Associate an Additional IP Address with the Device***. This is described in the section on *Adding an IP Address to a Device*.
- ***Remove an IP Address from the Device***. This is described in the section on *Removing an IP Address from a Device*.
- ***Manage Primary and Secondary IP Addresses for the Device***. This is described in the section on *Managing Device IPs*.
- ***Clear the Device Cache***. This is described in the section on *Clearing the Device Cache*.
- ***Define Child Devices***. This is described in the section on *Defining Device Relationships*.
- ***Associate a Secondary Credential with the Device***. This is described in the section on *Aligning a Secondary Credential*.
- ***Add the Device to a Device Group***. This is described in the section *Adding the Device to a Device Group*.
- ***Create a Ticket About the Device***. This is described in the section *Creating a Ticket About the Device*.
- ***Define Custom Navigation for the Device***. This is described in the section *Customizing the User Interface for a Device*.
- ***Add a Note to the Device***. This is described in the section *Adding a Note to a Device*.
- ***Associate a Product SKU with the Device***. This is described in the section *Associating a Product SKU with the Device*.
- ***Create or Edit an Asset Record for the Device***. This is described in the ***Asset Management*** manual.
- ***View Resource Usage for the Device***. This is described in the manual ***Monitoring Device Infrastructure Health***.
- ***Create a Report About the Device***. This is described in the manual ***Monitoring Device Infrastructure Health***.

Viewing Read-Only Information About the Device

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

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

Editing Device Settings

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

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

Identification

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

Monitoring & Management

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

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

- ***SNMP Read /Write***. The first drop-down lets you select an SNMP Read credential for read access to SNMP information on the device. The second drop-down let you select a n SNMP Write credential for read-and-write access to SNMP information on the device.

> **NOTE:** Devices that do not support SNMP ("pingable" devices) display the value *None* in both fields. Also, Your organization membership(s) might affect the list of credentials you can see in these fields.

- ***Availability Port***. Specifies the protocol (first drop-down menu) and specific port (second drop-down menu) that Skylar One should monitor to determine if the device is available. The list of ports will contain all the ports discovered by Skylar One. The data collected from this port will be used in device availability reports. Protocol options include:
    - *TCP*. Availability is based on whether the Skylar One can connect to the device using the specified TCP port.
    - *ICMP*. Availability is based on whether the device responds to an ICMP ping request from Skylar One. If you select *ICMP* as the protocol, you can use the ***ICMP Availability Thresholds*** fields in the ***Device Thresholds*** page to further define how Skylar One will test the device's availability.
    - *SNMP*. Availability is based on whether the device responds to an SNMP get request from Skylar One.
    - *ScienceLogic Agent*. Availability is based on whether the Skylar One agent is reporting data to Skylar One. The agent must be installed on the device to use this option.

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

- ***Run Availability Policy*** ( ). When you select this icon, Skylar One immediately checks the availability of the device, using the port and protocol specified in the ***Availability Port*** fields. Skylar One displays a **Session Logs** modal page that displays a detailed description of each step of the availability policy. This information is helpful when troubleshooting availability problems with a device.
- ***Latency Port***. Specifies the protocol and specific port Skylar One should monitor to determine latency for the device. The list of ports will contain all the ports discovered by Skylar One and the option *ICMP*, for which Skylar One performs a ping request. The data collected from this port or ping request will be used in device latency reports.
    - If you select *ICMP* as the protocol, you can use the ***ICMP Availability Thresholds*** in the ***Device Thresholds*** page to further define how Skylar One will test the device's latency.
- ***Avail + Latency Alert***. Specifies how Skylar One should respond when the device fails an availability check, when the device fails a latency check, and when the device fails both. These options allow you to create separate events when SNMP fails on a device and when a device is not up and running. Choices are:
    - *Enabled*. 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 the event "Device Failed Availability Check: UDP - SNMP". The event "Network Latency Exceeded Threshold: No Response" is suppressed under the availability event.

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

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

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

  - *Disabled*. Device will not be set to "user maintenance" mode.
  - *Enabled*. Device will be set to "user maintenance" mode. When you make this selection, a second field is enabled where you can specify whether Skylar One should poll the device during the "user maintenance" mode. During normal operation, Skylar One polls each device as specified by each device's policies and aligned Dynamic Applications. Choices are:
    - *Maintenance Collection Enabled*. During "user maintenance" mode, Skylar One will continue to poll the device.
    - *Maintenance Collection Disabled*. During "user maintenance" mode, Skylar One will not poll the device.

- ***Collection*** . Specifies if device will be monitored by Skylar One. To edit this field, select one of the following from the drop-down list:
  - *Disabled*. Device will not be monitored by Skylar One.
  - *Enabled*. Device will be monitored by Skylar One. When you make this selection, a second field is enabled where you can specify which Collector Group will perform discovery and gather data from the device. The drop-down list contains a list of available collector groups. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups). For details on Collector Groups, see the ***System Administration***manual.

- ***Coll. Type***. Specifies how Skylar One should perform collection. 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 a DNS lookup for the device each time Skylar One retrieves information from the device. This allows Skylar One to get the latest IP address for the device.
- ***Critical Ping***. Frequency with which Skylar One should ping the device in addition to the five minute availability poll. If the device does not respond, Skylar One creates an event. The choices are:
    - *Disabled*. Skylar One will not ping the device in addition to the five minute availability poll.
    - *Intervals from every 120 seconds - every 5 seconds*.

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

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

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

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

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

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

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

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

Topology Settings

NOTE: The device's topology settings are initially inherited from the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior), or from the topology settings for the *device's class*. However, you can change these settings on a per-device basis by editing one or more of the fields below. The field labels will include either "Inherited" or "Override" to indicate whether the topology setting is inherited from either the system or the device class, or if the device's topology setting overrides the system or device class setting. For more information about the system-wide topology settings, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual. For more information about the device class topology settings, see the section on *Device Classes and Device Categories* in this manual.

- ***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 and connects network devices to each other using methods other than the standard SNMP protocol 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 advanced 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 advanced 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.
    - *Inherit Class Value*. 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. This option requires all hops in a traceroute to respond and match devices within Skylar One 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. This option requires all hops in a traceroute to respond and match devices within Skylar One to form the relationship.
    - *Enhanced Processing Enabled*. Enables advanced Layer-3 topology processing for the device, where the system forms 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 advanced Layer-3 topology processing and collection for the device, where the system forms relationships between any two hops that respond and match devices in Skylar One rather than discarding incomplete traceroutes or results that include unmatched hops.
    - *Inherit Class Value*. 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 neighbors, and are managed devices in Skylar One. This option 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 neighbors, and are managed devices in Skylar One.
    - *Enhanced Processing Enabled*. Enables advanced CDP topology processing for the device, but using methods other than standard SNMP for collection. This advanced processing can form CDP relationships between two devices if at least one of those devices responds with CDP neighbor data and is a managed device in Skylar One.
    - *Collection and Enhanced Processing Enabled*. Enables advanced CDP topology processing and collection for the device using standard SNMP collection methods. This enhanced processing can form CDP relationships between two devices if at least one of those devices responds with CDP neighbor data and is a managed device in Skylar One.
    - *Inherit Class Value*. 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 neighbors, and are managed devices in Skylar One. This option 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 neighbors, and are managed devices in Skylar One.
    - *Enhanced Processing Enabled*. Enables advanced 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 managed device in Skylar One.
    - *Collection and Enhanced Processing Enabled*. Enables advanced 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 managed device in Skylar One.
    - *Inherit Class Value*. If selected, the device inherits the LLDP topology collection and processing settings assigned to its *device class*.

- ***ARP Topology***. Select from the following Address Resolution Protocol (ARP) topology options for the device:
    - *Disabled*. Disables ARP topology collection and processing for the device.
    - *Processing Enabled*. Enables ARP topology processing for the device using the "Enterprise Database: Topology Crunch" process to determine ARP topology relationships between two devices that are routers or switches on the same local network, are managed devices in Skylar One, and include a device with an IP address and another with a physical MAC address.
    - *Collection and Processing Enabled*. Enables ARP topology collection and processing for the device using standard SNMP collection methods and the "Enterprise Database: Topology Crunch" process to determine ARP topology relationships between two devices that are routers or switches on the same local network, are managed devices in Skylar One, and include a device with an IP address and another with a physical MAC address.
    - *Enhanced Processing Enabled*. Enables advanced ARP topology processing for the device. This enhanced processing can form ARP relationships between two devices of any device class so long as at least one of those devices responds with ARP data and is a managed device in Skylar One.
    - *Collection and Enhanced Processing Enabled*. Enables advanced ARP topology processing and collection for the device using standard SNMP collection methods. This enhanced processing can form ARP relationships between two devices of any device class so long as at least one of those devices responds with ARP data and is a managed device in Skylar One.
    - *Inherit Class Value*. If selected, the device inherits the ARP topology collection and processing settings assigned to its *device class*.

Preferences

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

- ***Scan All IPs***. If the device uses multiple IP Addresses, Skylar One can scan for open ports on all IPs during nightly discovery. Check this box to enable scanning of all IP Addresses for open ports every night.
- ***Dynamic Discovery***. If selected, Skylar One will automatically assign the appropriate Dynamic Applications to the device during nightly 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 name for the device will be updated if the name of the actual device is changed.
- ***Disable Asset Update***. If selected, Skylar One will ***not*** automatically update the asset record associated with the device. For a single device, this checkbox overrides any settings defined in the **Asset Automation** page (System > Settings > Assets).

Adding an IP Address to a Device

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

To define additional IP addresses for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to define additional IP address. Select the wrench icon (🔧) for the device.
3. In the **Device Properties** page, find the ***IP Address*** field.
4. To the right of the ***IP Address*** field, click on the plus-sign icon (+).
5. Alternately, you can also select the **[Actions]** menu and choose ***Add IP Address***.
6. The **Add IP Address** modal page appears. The **Add IP Address** modal page allows you to define an additional IP address for the device.
7. The **Add IP Address** modal allows you to define an additional IP address for the device. Skylar One will continue to use the Admin Primary IP address for communication with the device. However, Skylar One will also collect data about the additional IP address(es). To associate an additional IP address with the device, supply values in the following fields:
    - ***IP Address***. Supply the IP address. This can either be a numeric IPv4 address that uses dots or an alphanumeric IPv6 address that colons.
    - ***Subnet Mask***. Supply the subnet mask associated with the IP address. This field is optional.
8. Select the **[Add]** button.
9. In the **Device Properties** page, you will now see the additional IP address in the ***IP Address*** field. During auto-discovery, Skylar One will verify that this IP address exists on the device and will append the label "verified" to the value in the ***IP Address*** field.

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

Removing an IP Address from a Device

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

There are two exceptions to this ability:

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

To delete an IP address:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device from which you want to delete an IP address. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, find the ***IP Address*** field.
4. To the right of the ***IP Address*** field, select the delete icon ( ). The **Remove IP Address** modal page displays:
5. Select the checkbox for the IP address you want to delete.
6. Select the **[Remove]** button. The IP address is deleted.

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

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

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

Managing Device IPs

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

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

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

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

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

- Although Skylar One will not allow duplicate IP addresses within a single Collector Group, Skylar One does allow duplicate IP addresses if each device is aligned with a different Collector Group.
- If a single Message Collector is aligned with multiple Collector Groups, the single Message Collector might be aligned with two or more devices (each in a separate Collector Group) that use the same primary IP address or the same secondary IP address. If this happens, Skylar One will generate an event. To fix this situation, you can go to the **Select Primary IP Addresses** modal page for one of the devices and change the primary IP address in question. You can demote the primary and promote a secondary IP address for the device. This will fix the problem with duplicate IPs and allow the Message Collector to align messages with the device.

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

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

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

4. The **Select Primary IP Addresses** modal page appears. There are three types of IP addresses that can be associated with a device:
    - ***Admin Primary***. This is the IP address that Skylar One uses to communicate with a device. This IP address is always the admin primary address and cannot be demoted to a secondary address.
    - ***Primary***. One or more IP addresses that Skylar One uses to match incoming messages (traps and syslog messages) with a device. When you select an IP address in the Select Primary IP Addresses modal page, that IP address becomes a primary. You can also unselect an IP address in the Select Primary IP Addresses modal. When you unselect an IP address, that IP address becomes a secondary.
    - ***Secondary***. Skylar One gathers information about this IP address and uses the IP address to match incoming log messages (traps and syslog messages) with a device if it cannot match them first to a primary IP address.

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

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

Clearing the Device Cache

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

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device whose data you want to clear from the cache. Select its wrench icon ( ).
3. In the **Device Properties** page for the device, select the **[Actions]** menu and select *Clear Device Cache*. Data about the device will be cleared from the cache.

Aligning a Secondary Credential

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

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

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

To associate one or more additional credentials with a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to define additional credentials. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, select the **[Actions]** menu and choose *Secondary Credentials*. The **Secondary Credentials** modal page appears.
4. The **Secondary Credentials** modal page displays a list of all credentials defined in Skylar One:

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

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

Adding the Device to a Device Group

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

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

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

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

To add a device to an existing device group:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device that you want to add to a device group. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, select the **[Actions]** menu and choose *Device Groups*. The **Device Groups** modal page appears.
4. The **Device Groups** modal page allows you to assign a device to a device group or remove a device from a device group.
    - ***To add the device to a device group***, in the **Available Device Groups** pane, select one or more device groups. After selecting the **[Save]** button, the device group will appear in the **Member Device Groups** pane.
    - ***To remove the device from a device group***, in the **Member Device Groups** pane, select one or more device groups. After selecting the **[Save]** button, the device group will appear in the **Available Device Groups** pane.

    > **NOTE:** The **Member Device Groups** pane displays device groups for which the device is a static member as well as device groups where the device matches a dynamic rule for membership.

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

Creating a Ticket About the Device

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

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

To create a ticket for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device about which you want to create a ticket. Click the wrench icon ( ) for the device.
3. In the **Device Properties** page, click the **[Actions]** menu and select ***Create a Ticket.*** The **Ticket Editor** page appears.
4. In this page, you can define the basic parameters for a ticket. Notice that the ***Description*** field and ***Element*** field are automatically populated with the device name.
5. Click the **[Save]** button to save the ticket.

Adding a Note to a Device

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

To add a note to a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device that you want to add a note to. Click the wrench icon ( ) for the device.
3. In the **Device Properties** page, click the **[Actions]** menu and select *Notepad Editor*.
4. The **Notepad Editor** modal page appears. In this page, you can enter and format text, include images and links in the message, and include an attachment. Click the **[Save]** button to save the note.
5. The **Notepad Editor** modal page allows you to enter notes or comments about the device.
    - You can format the text and include links, images, and videos in the note.
    - You can also include a document template (System > Customize > Document Templates) in the field.
6. The note will appear in the **[Notes]** tab, in the **Notes & Attachments** page.

7. The **Notes & Attachments** page displays all the notes about the device that were created with the **Notepad Editor** modal page. In the **Notes & Attachments** page, each entry includes the username, date and time, and text of the comment. You can perform the following on each note entry:
    - ***To view a note's attachment***, click the paperclip icon ( ).
    - ***To edit the content of a note***, click the wrench icon ( ). The **Notepad Editor** modal page appears. You can update the note; format the text; insert content from a saved template; and add an attachment, image, or video to the note. Click the **[Save]**button to save your changes.
    - ***To delete a note***, click its delete icon ( ).

NOTE: For information about adding a note to a device on the **[Notes]** tab of the **Device Investigator**, see the section on *The Notes Tab*.

Aligning Custom Attributes with a Device

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

NOTE: For more information on custom attributes, see the chapter on *Custom Attributes*.

To align custom attributes with a device:

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

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

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

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

Creating a New Extended Custom Attribute

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

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device for which you want to create a new custom attribute. Click its wrench icon ().
3. Click the **[Attributes]** tab.
4. In the **Attributes** page, click the plus icon () in the bottom-most row, then supply a value in the following fields:
    - ***Label***. User-defined name for the custom attribute. This value appears in the user interface. If the value in this field does not comply with XML rules for names, Skylar One will convert the value to a name that complies with XML rules and store the converted value as the ***Internal Field Name*** for the custom attribute.

NOTE: Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character or an extending character. If a value in the ***Internal Field Name*** column does not conform to XML standards, Skylar One will replace non-valid characters with an underscore plus the hexadecimal value of the illegal character plus an underscore. So "serial number" would be replaced with "serial_X20_number".

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

Deleting an Extended Custom Attribute from a Device

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

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

To delete an extended custom attribute from a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device for which you want to delete a custom attribute. Click its wrench icon ( ).
3. Click the **[Attributes]** tab.
4. In the **Attributes** page, find the extended custom attribute you want to delete. Click its delete icon ( ).
5. A message appears asking you to confirm that you want to delete the value and unalign the custom attribute from the device.
6. Click the **[OK]** button.

Associating a Product SKU with the Device

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

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

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

To associate a product SKU with a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device that you want to add a note to. Select the wrench icon ( ) for the device.
3. In the **Device Properties** page, select the **[Actions]** menu and choose *Product Catalog*.
4. The **Product Catalog** modal page appears. In this page, you can associate one or more product SKUs with the device:
    - ***To associate a product SKU with the device***, in the **Available Products** pane, select one or more product SKUs.

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

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

Merging Devices

If your Skylar One system includes a physical device and a component device that both represent the same device, you can merge those device records into a single record for easier monitoring. Merging does not remove, replace, or add any data; merging simply groups data together.

There are several benefits to merging physical and component devices:

- Merging consolidates the devices and their data–device fields, values, graphs, behaviors, and other user interface elements–providing you with a single set of data for the device.
- Merging reduces the number of duplicated events and administrative tasks.
- Merged devices consume only a single device license.

For example, you might discover a virtual machine device component representing a server, and then later discover an IP-based device from the same server. To prevent duplicate events from occurring for the same server, minimize administrative tasks, and prevent a negative impact on your licensing by inflating the number of devices being monitored by Skylar One, you could merge the virtual machine component and the corresponding IP-based device into a single device record.

NOTE: You ***cannot*** merge a component device with a physical device that acts as the root device for a dynamic component map (DCM) tree.

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

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

NOTE: You can merge only two individual devices together into a single merged device. To do so, you must have user permissions that allow merging and unmerging on both devices. For more information about user access permissions, see the ***Access Permissions*** manual.

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

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

TIP: Use consistent device hostnames to make device merging easier.

Skylar One enables you to merge and unmerge devices from the **Devices** page using a single workflow that supports both individual and bulk operations. For the current workflow, see *Merging and Unmerging Devices from the Devices Page*.

For legacy workflows in the classic Skylar One user interface, see *Merging Individual Devices in the Classic User Interface* to merge individual devices and *Unmerging Individual Devices in the Classic User Interface* to unmerge them. To merge or unmerge multiple devices at once in the classic Skylar One user interface, refer to *Bulk Merging and Unmerging of Devices in the Classic User Interface*.

Merging and Unmerging Devices from the Devices Page

You can merge or unmerge physical and component device records that represent the same device directly from the **Devices** page. This workflow supports both single and multiple device selections, allowing you to merge or unmerge one device pair or multiple device pairs.

Merging Devices from the Devices Page

You can merge physical and component device records that represent the same device on the **Merge Devices** modal from the **Devices** page.

To open the **Merge Devices** modal:

1. Go the **Devices** page.
2. Click the drop-down arrow button next to the **[Add Devices]** button and select *Merge Devices*. The **Merge Devices** modal appears.

The **Merge Devices** modal displays two tables: **Physical Device** and **Component Device**. Each table includes columns such as ***Device Name***, ***IP Address***, ***Device Category***, ***Device Class***, ***Device ID***, and ***Organization***, along with column filters to help you locate devices.

At the top of the **Merge Devices** modal, you can control how devices are matched using the fields displayed above the device tables. By default, the **Merge Devices** modal allows you to manually select physical and component devices to merge. In this mode, Skylar One does not apply any matching logic, and no comparison criteria are displayed.

Optionally, you can enable ***Suggested Device Matches*** to allow Skylar One to automatically generate device merge suggestions based on selected matching criteria.

When **Suggested Device Matches** is not enabled, the modal displays the following matching fields:

- ***Name***
- ***IP Address***

- *Organization*
- *Device Class*

For each field, you can manually review and select one of the following options to define how the physical device and component device values are compared:

- *Ignore*. Skylar One does not evaluate this criterion when generating suggested matches.
- *Match*. Skylar One suggests device pairs only when the selected values on the physical device and component device are the same.
- *Does Not Match*. Skylar One suggests device pairs only when the selected values on the physical device and component device are different.

When you enable ***Suggested Device Matches***, the **Merge Devices** modal switches to an assisted matching mode and displays additional options for defining how Skylar One should generate merge suggestions. In this mode, Skylar One compares physical and component devices based on selected criteria and suggests device pairs that meet those conditions. In this view, additional matching fields become available:

- *Collection State*
- *Collection Group*

> **NOTE:** When ***Suggested Device Matches*** is enabled, the **Merge Devices** modal automatically preselects the suggested physical-component device pairs. You can review these selections and remove individual pairs before clicking **[Merge]**.

Skylar One uses the selected fields to automatically generate suggested physical-component device pairs. Fields set to *Ignore* are excluded from matching. Fields set to *Match* or *Does Not Match* determine how suggested matches are generated.

To merge one device pair or multiple device pairs:

1. From the **Merge Devices** modal, select one or more physical-component device pairs.
2. Review the selected pairs, then click **[Merge]**.

You can merge a single device pair or multiple device pairs in the same operation. To review previous merge activity, click **[View Merge Device Logs]**.

Unmerging Devices from the Devices Page

You can unmerge previously merged physical and component device records on the **Unmerge Devices** modal from **Devices** page.

To open the **Unmerge Devices** modal:

1. Go the **Devices** page.
2. Click the drop-down arrow button next to the **[Add Devices]** button and select *Unmerge Devices*. The **Unmerge Devices** modal appears.

The **Unmerge Devices** modal displays two tables: **Physical Device** and **Component Device**.

- The **Physical Device** table includes columns such as ***Device Name***, ***IP Address***, ***Device Category***, ***Device Class***, and ***Device ID***.
- The **Component Device** table includes columns such as ***Device Name***, ***Device Category***, ***Device Class***, ***Device ID***, ***Merged Date***, and ***Merged By***. These columns indicate when the device was merged and the user who performed the merge.

To unmerge one device pair or multiple device pairs:

1. From the **Unmerge Devices** modal, select one or more merged device pairs.
2. Review the selected pairs, then click **[Unmerge]**.

You can unmerge a single device pair or multiple device pairs in the same operation. To review previous merge and unmerge activity, click **[View Merge Device Logs]**.

> **NOTE:** You can click the**[Merge Devices]** button to open the **Merge Devices** modal.

Merging Individual Devices in the Classic User Interface

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

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

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

To merge individual devices:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Click the wrench icon ( ) for the physical device that you want to merge with a component device.
3. On the **Device Properties** page, click the **[Actions]** menu and then select *Merge Device*.
4. A list of component devices that are available for merging with the physical device displays. Click the merge icon ( ) for the component device you want to merge with the physical device. Information for the component device then displays in the **Selected Device** panel.
5. Click the **[Merge]** button. A pop-up message appears that asks you to confirm the merge.
6. Click the **[OK]** button.

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

Unmerging Individual Devices in the Classic User Interface

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

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

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

NOTE: For details on unmerging a vanished device, see the chapter in this manual on *Vanishing & Purging Devices*.

To unmerge individual devices:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Select the wrench icon (🔧) for the device that you want to unmerge.
3. On the **Device Properties** page, select the **[Actions]** menu and then choose ***Unmerge Device***.
4. A modal window displays that asks you to confirm the unmerging. Select the **[Unmerge]** button.

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

Performing Administrative Tasks for One or More Devices

The **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface) contains a drop-down field in the lower right called ***Select Action***. This field allows

you to apply an action to multiple devices at once.

To apply an action to multiple devices:

1. In the **Device Manager** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the checkbox at the top of the page.
2. In the ***Select Action*** drop-down list, select one of the following actions:
    - ***Delete Devices***. Deletes all selected devices from Skylar One. Tickets associated with the device are unlinked from the device, but are not deleted.
    - ***Modify by Template***. Displays the **Applying Template to Device** page, where you can apply the settings in a device templates to all selected devices. You can also make one-time changes to the template, that will be applied only to the selected devices.
    - ***Clear Device Logs***. Deletes data from the device's log files.
    - ***Create Asset Record***. Automatically creates an asset record for the device. Skylar One automatically populates as many fields as possible, using retrieved data.
    - ***Schedule Maintenance***. Leads to the **Maintenance Schedule** page. In this page, you can specify a date and time to put each selected device into "maintenance mode". During maintenance mode, Skylar One will not generate events about the selected devices. You can choose to enable or enable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate events for the devices.
    - ***Find Collection Label Duplicates***. Leads to the **Duplicates** page. In this page, you can view a list of devices where the Collection Labels have more than possible presentation object aligned. From this page, you can manually align a single presentation object with a Collection Label for a device.
    - ***Change Collection State***. Changes the status of the device in Skylar One. The choices are:
        - *Active*. Skylar One polls the device on a regular basis and updates the data displayed in Skylar One.
        - *Disabled*. Skylar One does not poll the device. Data displayed in Skylar One is not updated.
    - ***Change Maintenance Mode***. These options allow you to enable User-Initiated-Maintenance and disable both User-Initiated-Maintenance and scheduled Maintenance.

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

    - *Enabled without Collection*. One or more devices are set to User-Initiated-Maintenance mode. During User-Initiated-Maintenance mode, Skylar One will not poll the device.
    - *Disabled*. User-Initiated-Maintenance mode is disabled for each selected device.
- ***Change Collector Group***. Changes the collector group used to collect data from the device. Choose from the list of all collector groups in Skylar One. When you select one of the collector groups, each selected device will be polled by the collectors in the collector group. For All-In-One Appliances, you can select only the built-in Collector Group and any virtual Collector Groups.
- ***Move To Organization***. Associates a device with an organization. The list of choices will include all organizations in Skylar One.
- ***Align SNMP Read Credential***. This option applies the selected credential to all selected devices. The selected devices will use the selected credential as their primary credential. Secondary credentials will remain unchanged. Choose from a list of SNMP Read credentials (defined in System > Manage > Credentials). The list will include only credentials that you are allowed to use.
- ***Add to Device Group***. This option aligns the selected devices with the selected device group. The selected devices will then appear in **Device Group Views** and will inherit the properties of the device group, including scheduling, access, and visibility.
- ***Align to Device Dashboard***. This option aligns the selected devices with the selected device dashboard. The selected device dashboard will appear as the default view in the **Device Summary** page.

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

Shortcut Keys for the Device Administration Panel

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

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

Page or Tab	Shortcut Keys
Administer Bookmarks page	Ctrl + Alt + B
Dynamic Application Collectionspage	Ctrl + Alt +C
Device Groups page	Ctrl + Alt + D
Guides page	Ctrl + Alt + G
Device Thresholds page	Ctrl + Alt + H
Device Interfaces page	Ctrl + Alt + I ("eye")

Page or Tab	Shortcut Keys
Device Logs & Messages page	Ctrl + Alt + L
Monitoring Policies page	Ctrl + Alt + M
Notes & Attachments page	Ctrl + Alt + N
Device Toolbox page	Ctrl + Alt + O ("oh")
Device Properties page	Ctrl + Alt + P
Maintenance Schedule page	Ctrl + Alt + S
Ticket History page	Ctrl + Alt + T
Resource Usage page	Ctrl + Alt + U
Exit Device Administration panel	Ctrl + Alt + X
Device Properties page	Ctrl + Alt + . ("period")
Ticket Editor page	Ctrl + Alt + <Enter>

Chapter

6

Device Toolbox

Overview

This chapter describes the **Device Toolbox** page in Skylar One.

This chapter covers the following topics:

What is the Device Toolbox? *134*

Accessing the Device Toolbox page *134*

Viewing the Session Logs *136*

What is the Device Toolbox?

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

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

Accessing the Device Toolbox page

To access the **Device Toolbox** page:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

2. In the **Device Manager** page, find the device for which you want to access the **Device Toolbox** page and select its wrench icon ( ).
3. In the **Device Administration** panel, select the Toolbox tab.
4. Depending on the device, the **Device Toolbox** page can display one or more of the following buttons. These tools run on the Data Collector that is currently monitoring the device unless otherwise noted:
    - ***FTP***. Opens a new browser window and attempts to make an FTP connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 21) is detected as open by Skylar One.
    - ***SSH***. Opens an SSH session on the device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 22) is detected as open by Skylar One.

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

    - ***Telnet***. Opens a browser session or terminal session using the IP address of the current device and prompts you for the telnet username and password. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 23) is detected as open by Skylar One.
    - ***Terminal***. Opens the **Terminal Services Client Web Connection** modal page, where you can enter the login information for the terminal services session. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 3389) is detected as open by Skylar One.
    - ***Web***. Opens a new browser window and attempts to make an http connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector.
    - ***Secure Web***. Opens a new browser window and attempts to make an HTTPS connection to the current device. This tool is initiated from the user's machine and does not run on a Data Collector. This tool appears only if the correct port (port 443) is detected as open by Skylar One.
    - ***SNMP Walker***. Opens the SNMP Walker modal page, where you can perform an SNMP walk on the device. If the device has an IPv6 address, Skylar One will use the appropriate IPv6 SNMP command.
    - ***Port Scan***. Leads to the **Port Scan** modal page, where you can view a list of all open ports on the device at the time of the scan.
    - ***Deep Port Scan***. Leads to the **Deep Port Scan** modal page, where you can view a list of all open ports and view as much detail about each open port as the deep port scanner can retrieve.
    - ***Traceroute***. Leads to the **Traceroute** modal page, where you can view the network route between Skylar One and the device. If the device has an IPv6 address, Skylar One will use the appropriate IPv6 traceroute command.

- ***Ping Tool***. Leads to the **Ping_Tool** modal page, where you can view the statistics returned by the ping tool. The ping tool sends a packet to the device's IP address (the one used by Skylar One to communicate with the device) and waits for a reply. Skylar One then displays the number of seconds it took to receive a reply from the device and the number of bytes returned from the device. If the device has an IPv6 address, Skylar One will use the appropriate IPv6 ping command.
- ***Forward DIG***. Leads to the **Forward DIG** modal page, where you can view the output from the DIG utility. This tool automatically finds all available DNS information about the domain associated with the current device.
- ***Reverse DIG***. Leads to the **Reverse DIG** modal page, where you can view the output from the reverse DIG utility. The reverse DIG tool retrieves the domain name that is associated with the device's IP.
- ***ARIN Whois***. Leads to the **ARIN Whois** modal page, where you can view the output from the Whois utility. The Whois utility displays information about the device's IP, including the organization that registered the IP and contacts within that organization.
- ***ARP Lookup***. Leads to the **ARP Lookup** modal page, where you can view the results from the ARP Lookup tool. The ARP Lookup tool displays a list IP addresses for the device and the resolved Ethernet or Token Ring physical addresses (MAC addresses) for each IP address.
- ***ARP Ping***. Leads to the **ARP Ping** modal page, where you can view the results from the ARP Ping tool. The ARP Ping tool is similar in function to ping, but it operates using ARP instead of ICMP. The ARP Ping tool can be used only on the local network.
- ***SNMP Dump***. Leads to the **SNMP Dump** modal page, where you can view the results of the SNMP Dump. The SNMP Dump tool retrieves each OID and its corresponding value from the device.
- ***Web Policy***. Leads to the **Web Policy** modal page, where you can manually run a web-content policy on the device. This tool is initiated from the user's machine and does not run on the collector. This tool appears only if a Web Content Monitoring Policy has been configured for the device.

Viewing the Session Logs

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

For each session, you can view the following:

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

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

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

Chapter 7

Device Classes and Device Categories

Overview

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

This chapter covers the following topics:

Device Classes 139
Viewing the List of Device Classes 141
Creating Device Classes 143
Managing Device Classes 160
Managing Device Classes in the Classic Skylar One User Interface 162
Device Categories 165
Viewing the List of Device Categories 166
Creating a New Device Category 167
Editing a Device Category 168
Duplicating a Device Category 168
Assigning an Icon to a Device Category 168
Managing Device Categories in the Classic Skylar One User Interface 169

Device Classes

Device classes determine:

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

Administrators can define new or legacy device classes and customize properties of existing device classes on the **Device Classes** page (Devices > Device Classes), or on the **Device Class Editor** page (System > Customize > Device Classes) in the classic Skylar One user interface.

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

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

The following sections describe the types of device classes used in Skylar One.

Generic | SNMP Device Class

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

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

Non-SNMP Device Classes

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

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

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

Component Device Classes

Skylar One includes device classes for component devices. Skylar One discovers management systems and the component devices they manage. Skylar One uses Dynamic Applications to retrieve data from a

management system and discover each component device managed by that management system. Device classes for components are aligned with the Dynamic Applications that discover component devices.

Agent-Only Device Classes

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

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

Based on this information, Skylar One assigns the corresponding device classes to a device monitored only by an agent.

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

Legacy ICMP Device Classes

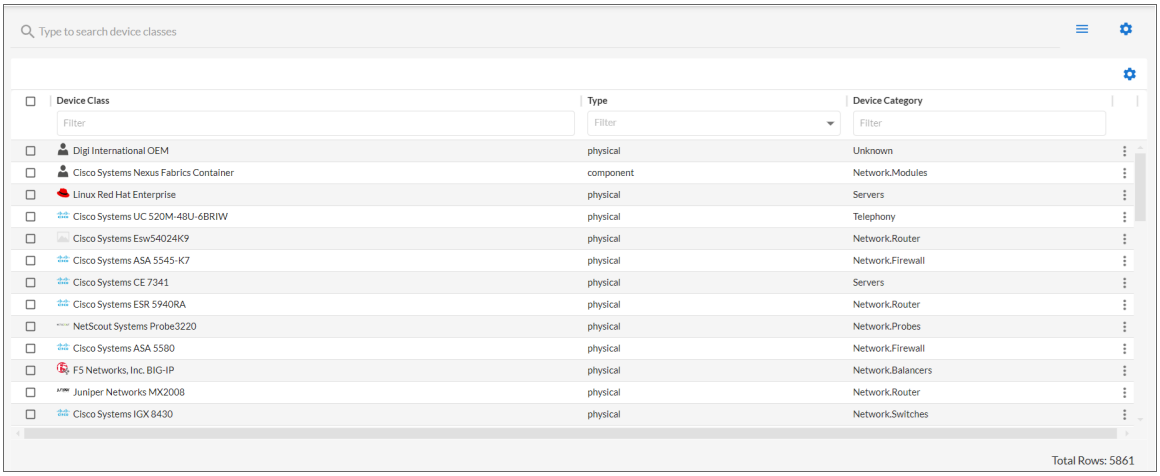
Skylar One includes legacy device classes of type ***SNMP Enabled*** for "pingable" devices (that is for devices that don't support SNMP). Skylar One includes the following legacy, ***SNMP Enabled*** device classes for "pingable" devices:

- Cisco Systems | ICMP
- FreeBSD | ICMP
- Linux | ICMP
- Microsoft | ICMP
- Novell | ICMP
- Ping | ICMP
- Sun Microsystems | ICMP
- Tektronix, Inc. | ICMP

NOTE: Best practice is to define "pingable" devices as those that do not support SNMP. For "pingable" devices that do not support SNMP, ScienceLogic recommends you use the new "deep discovery" feature and then create device classes of type "pingable".

Viewing the List of Device Classes

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



TIP: If you are looking for a very specific set of device classes, click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

For each device class, the **Device Classes** page displays the following information:

- ***Device Class***. The name of the device class.
- ***Type***. The device type. Can be "physical", "virtual", or "component".
- ***Device Category***. The device category. A device category is a way to categorize devices by primary function. Skylar One uses device categories to group related devices in reports and views. The list of device categories is defined in the **Device Category Editor** page (System > Customize > Device Categories).
- ***Model***. The device model.
- ***Vendor***. The device manufacturer.

TIP: To rearrange the columns in the list, click and drag the column name to a new location. You can adjust the width of a column by clicking and dragging the right edge of the column. For more information about editing and adding columns, see "Editing the Settings for an Inventory Page" in the ***Introduction to Skylar One*** manual.

Viewing the List of Device Classes in the Classic Skylar One User Interface

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

To view the list of device classes:

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

   TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

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

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

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

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

- ***Device Class Tier***. This field is no longer used for Subscription Billing. For information regarding billing, see *Viewing and Managing Subscription Data*.

> **NOTE**: If you create a custom device class, please contact ScienceLogic Customer Support to define the Device Class Tier for the new device class. Failure to contact will result in the device remaining in the default bucket and being billed at the full rate. ScienceLogic recommends to include the PowerPack name that should include the new devices. For more information, see *Custom Device Class Process*.

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

Creating Device Classes

The following sections describe how to create new device classes for:

- *Devices that support SNMP*
- *Devices with Device Class "Generic | SNMP"*

- *Devices that do not support SNMP*
- *Devices with a Device Class of "Component"*

Creating a New SNMP-Enabled Device Class

In the **Device Class Editor** page, you can define a new device class. Skylar One can then use this device class during discovery and users can assign this device class to devices.

You can use an existing device class as a template when defining a new device class. To do this, follow the steps in the Editing an *SNMP-Enabled Device Class* section, but supply a new name in the ***Device Class*** field and click **[Save As]** to save your changes.

The ***Device Class Tier*** is no longer used for Subscription Billing. For information regarding billing, see *Viewing and Managing Subscription Data*. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class. For more information, see *Custom Device Class Process*.

When you create a new device class of type ***SNMP Enabled***, you are defining a device class that uses the ***SNMP SysObjectID*** to identify member device.

To create a new device class of type ***SNMP Enabled***:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes).
2. Click **[Reset]** to clear the fields in the **Device Class Editor** pane.
3. Select *SNMP Enabled* in the ***Device Type*** drop-down list. You can now define the value in the following fields:
    - ***Root Device***. If selected, this checkbox specifies that this device can have children devices. Ensures that root devices are included in nightly re-discovery.
    - ***Weight***. If two device-class definitions are similar, a device might meet the criteria for both device classes. In this case, the ***Weight*** field tells Skylar One which device class to align with the device. The ***Weight*** field allows you to define both detailed, non-SNMP device-class definitions, as well as less detailed, catch-all device classes.

      Skylar One will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, Skylar One will align the device with the device class that appears first in the alphabetical list of device classes.

      For example, you could define a detailed device class with a weight of "1" and a similar but less detailed device class with a weight of "10". Skylar One will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, Skylar One will then try to assign the discovered device to the device class with a weight of "10".
    - ***Device Class***. The name of the manufacturer who created the device and/or agent. Can be any combination of alphanumeric characters, up to 48 characters in length.
    - ***Discovery Identifier (SysObjectID)***. The SNMP OID, in numeric form, that is returned when querying the device's sysObjectID. Can be up to 64 characters in length. Refer to the appropriate MIB file to determine this value.

- ***Discovery Qualifier (SNMP OID)***. Optional field. Secondary SNMP OID, in numeric form, used to further qualify device types. Can be up to 255 characters in length. If a device matches both the ***Discovery Identifier*** and responds to the ***Discovery Qualifier***, the device will be assigned to the device class.
- ***Tabular***. If you want to use a tabular value in the ***Discovery Qualifier*** field, select this checkbox. When you select this checkbox, Skylar One will perform an SNMP walk of the ***Discovery Qualifier*** (as opposed to an SNMP "get" request) and then search for the value that matches the ***Qualifier Match*** field.
- ***Qualifier Match***. Optional field. String that must be present in returned value for the ***Discovery Qualifier*** OID. If a device matches the ***Discovery Identifier***, responds to the ***Discovery Qualifier***, and the response matches the ***Qualifier Match***, the device will be assigned to the device class. Can be up to 64 characters in length.
- ***Description***. The model name of the device. Can be any combination of alphanumeric characters, up to 48 characters in length. For ease-of-use, ScienceLogic recommends that you follow this convention: If you are creating a device class for an entire manufacturer, rather than for a specific product, enter "OEM" as the device description.
- ***Device Icon***. The icon used to display the device in the graphical interface. To view the available icons, click **[Icons]**. Select an icon from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device icon for all existing members of the device class.
- ***Device Category***. A logical categorization of device by primary function. This field allows Skylar One to group related devices in reports and views. Select a value from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device category for all existing members of the device class.
- ***System Uptime OID***. Specifies the OID to monitor to determine system uptime. Choices are:
    - *sysUpTime (.1.3.6.1.2.1.1.3.0)*. EM7 Default. From the System group of MIB RFC 1213. Returns uptime of the device's SNMP Agent. The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
    - *hrSystemUptime (.1.3.6.1.2.1.25.1.1.0)*. From the HR-MIB. The amount of time since this host was last initialized.
    - Any additional OIDs defined in the **System Uptime OIDs** page (System > Customize > Uptime OIDs).
- ***Correlation Method***. Used for special topological correlation. Allows Skylar One to support event correlation and mapping for VMware and Microsoft hypervisors.
- ***Collection Type***. Specifies whether the device is a hardware-based device (physical) or a virtual device.
- ***PDU Packing***. If your managed network includes a large number SNMP elements such as interfaces that you want to monitor, select this checkbox. PDU packing enables quicker collection of voluminous SNMP data. For more information, see the section on *Additional Configuration for Concurrent Network Interface Collection* in the ***Monitoring Device Infrastructure Health*** manual.

- ***Process Collection***. Specifies how Skylar One will retrieve process information for the device. Skylar One will use this method to gather information on the system processes. Choices are:
    - *n/a*. Don't monitor processes.
    - *Host Resource*. Specifies that the Host Resources MIB will be used to collect information on processes.
    - *HP/UX*. Specifies that HP agents will provide information on processes.
    - *Solaris (prior to Solaris 10)*. Specifies that Solaris agents will provide information on processes.
    - *Extended User Information*. Specifies that ScienceLogic's custom extension to net-SNMP will provide process information. Users must have installed the extension before selecting this option.
- ***Service Collection***. Specifies how to collect information on services. Choices are:
    - *n/a*. This is not an applicable device class.
    - *Windows Basic*. Use the Windows MIB to gather information about Windows services.
    - *WMI Informant*. Use the WMI Informant MIB to gather information about Windows services.

- ***L2 Topology*** . Select from the following Layer-2 topology options for the device class:

    - *Disabled*. Disables Layer-2 topology collection and processing for the device class. If this is selected, devices assigned to the device class will inherit the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). For more information, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual.

    - *Processing Enabled*. Enables Layer-2 topology processing for the device class 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 standard SNMP for collection.

    - *Collection and Processing Enabled*. Enables Layer-2 topology collection and processing for the device class 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 class, but using methods other than 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 class, 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.

- ***L3 Topology***. Select from the following Layer-3 topology options for the device class:
    - *Disabled*. Disables Layer-3 topology collection and processing for the device class. If this is selected, devices assigned to the device class will inherit the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). For more information, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual.
    - *Processing Enabled*. Enables Layer-3 topology processing for the device class using the standard 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 class using the standard 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 class, 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 class, 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.

- ***LLDP Topology***. Select from the following Link Layer Discovery Protocol (LLDP) topology options for the device class:

    - *Disabled*. Disables LLDP topology collection and processing for the device class. If this is selected, devices assigned to the device class will inherit the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). For more information, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual.

    - *Processing Enabled*. Enables LLDP topology processing for the device class 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 class 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 class, 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 class, 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.

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

    - *Disabled*. Disables CDP topology collection and processing for the device class. If this is selected, devices assigned to the device class will inherit the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). For more information, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual.

    - *Processing Enabled*. Enables CDP topology processing for the device class 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 class 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 class, 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 class, 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.

- ***ARP Topology***. Select from the following Address Resolution Protocol (ARP) topology options for the device class:

    - *Disabled*. Disables ARP topology collection and processing for the device class. If this is selected, devices assigned to the device class will inherit the system-wide topology settings that are set on the **Behavior Settings** page (System > Settings > Behavior). For more information, see the section on "Global Settings for System Behavior" in the ***System Administration*** manual.

    - *Processing Enabled*. Enables ARP topology processing for the device class using the "Enterprise Database: Topology Crunch" process to determine ARP topology relationships between two devices that are routers or switches on the same local network, are managed devices in Skylar One, and include a device with an IP address and another with a physical MAC address.

    - *Collection and Processing Enabled*. Enables ARP topology collection and processing for the device class using standard SNMP collection methods and the "Enterprise Database: Topology Crunch" process to determine ARP topology relationships between two devices that are routers or switches on the same local network, are managed devices in Skylar One, and include a device with an IP address and another with a physical MAC address.

    - *Enhanced Processing Enabled*. Enables advanced ARP topology processing for the device class. This enhanced processing can form ARP relationships between two devices of any device class so long as at least one of those devices responds with ARP data and is a managed device in Skylar One.

    - *Collection and Enhanced Processing Enabled*. Enables advanced ARP topology processing and collection for the device class using standard SNMP collection methods. This enhanced processing can form ARP relationships between two devices of any device class so long as at least one of those devices responds with ARP data and is a managed device in Skylar One.

- ***Agent Identifier 1 and Agent Identifier 2***: These fields are used to align device classes to devices using the Skylar One agent. Device classes exist for every possible combination of values returned by the agent; you do not need to enter or change values in these fields when creating or editing a device class.
- ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in Skylar One. For devices with this device class, the selected device dashboard will appear as an option in the **Device Summary** page. This field is optional.
- ***Interface Index Change Detection***. On some devices, the SNMP index of an interface can change when the interface goes down and then comes back up. If you select this checkbox, Skylar One will use the combination of interface ID and ifPhysAddress to monitor interfaces on devices that use this device class and to align events with those interfaces.

4. Click **[Save]** to save the new device class or click **[Save As]** to save your changes under a new device class name.

Editing an SNMP-Enabled Device Class

In the **Device Class Editor** page, you can edit a device class for a device that supports SNMP.

When you ***select SNMP Enabled***, you are defining a device class that uses the ***SNMP SysObjectID*** to identify member devices.

To edit an existing device class:

1. Go to the**Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class. You can edit one or more of the fields described in the section *Creating a New SNMP-Enabled Device Class*.
4. Select the **[Save]** button to save your changes to the device class or select the **[Save As]** button to save your changes under a new device class name.

Creating a New Device Class for a Device with Device Class "Generic | SNMP"

After discovery, Skylar One might discover devices and assign those devices to the device class ***Generic | SNMP***. This means that Skylar One was able to retrieve a SysObjectID value from the device, but Skylar One does not include a Device Class for that SysObjectID.

The ***Device Class Tier*** is no longer used for Subscription Billing. For information regarding billing, see *Viewing and Managing Subscription Data*. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class. For more information, see *Custom Device Class Process*.

To create a new device class for a device with device class ***Generic | SNMP***:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device with the device class ***Generic | SNMP***. Select the wrench icon ( ) for the device.
3. In the **Device Administration** panel, select the **[Toolbox]** tab.
4. In the **Device Toolbox** page, select the icon for SNMP Walker.
5. In the **SNMP Walker** modal page, go to the drop-down menu in the upper left and select ***System MIB.*** Then select the **[Walk]** button.
6. The second entry in the ***Returned Value*** column is the SysObjectID. In the example above, that value is ***1.3.6.1.4.1.303.3.3.7.3***. Copy this value and save it in a document or write down this value. You will need it to create a new device class.
7. Follow the directions in the section *Creating a New SNMP-Enabled Device Class*. In the ***Discovery Identifier*** field, enter the value of the SysObjectID from the SNMP Walker. Make sure there are no blank spaces before or after the SysObjectID value.

8. To assign the new device class to a device, follow the instructions in the section *Manually Changing the Device Class for a Device*.
9. Alternately, you can re-discover the device with the device class "Generic | SNMP". To re-discover the device, go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface). Find the device you want to rediscover. Select its wrench icon (). In the **Device Properties** page for the device, select the magnifying glass icon ().
10. After the device is re-discovered, it should now be aligned with the new device class.

Creating a New Device Class for Devices That Do Not Support SNMP

Skylar One includes device classes for devices that are "pingable". By default, these devices are aligned with the device category of "pingable" and are placed in the device class "Ping | ICMP". To discover devices that have a device category of "pingable", you must select ***Discover Non-SNMP*** in the **Discovery Session Editor** page.

Devices with the device category of "pingable" are devices that meet one of the following criteria:

- Device does not support SNMP.
- SNMP has been disabled on the device.
- Either no SNMP credential was provided in the discovery session or an incorrect SNMP credential was provided in the discovery session.

In some cases, you might want to discover a "pingable" device and use XML requests, XSLT requests, WMI requests, SOAP transactions, Python snippets, or SQL queries to gather information from the device. You can do this through Dynamic Applications.

You might also want to create a more descriptive device class for these types of devices and assign a device category other than "pingable". Skylar One can use the values returned by nmap (run during discovery) to match a "pingable" device to a descriptive device class.

NOTE: You can use an existing device class as a template when defining a new device class. To do this, follow the steps in the *Editing a Device Class That is Not SNMP-Enabled* section, but supply a new name in the ***Device Class*** field and click **[Save As]** to save your changes.

NOTE: The ***Device Class Tier*** is no longer used for Subscription Billing. For information regarding billing, see *Viewing and Managing Subscription Data*. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class. For more information, see *Custom Device Class Process*.

When you create a new device class of type ***Pingable***, you are defining a device class that uses the ***XML values returned by nmap*** to identify member devices.

To create a new device class with a device category of "pingable":

1. To discover details about devices that do not support SNMP, during discovery (System > Manage > Classic Discovery), you should select an ***Initial Scan Level*** of *5. Deep Discovery* and select the checkbox for ***Discover Non-SNMP***. Skylar One will run the following nmap command on each device during discovery:

```
nmap -sS -O --host-timeout=12000ms "-p 21,22,23,25,80" -A --version-all -
oX full pathname of file in which to store XML outputIP address of device
```

NOTE: Depending on your selections in the **Discovery Session Editor** page, Skylar One might use the ***-sU*** or ***-sT*** option instead of ***-sS***. The value supplied to the ***host-timeout*** option will vary depending upon the list of ports specified in the **Discovery Session Editor**page. The list of ports supplied with the ***-p*** option will vary depending upon the list of ports specified in the **Discovery Session Editor** page. For more details on the nmap command, see the webpage http://nmap.org/book/man.html.

2. Skylar One stores the output from the nmap command in an XML file. In the ***NMAP Report XPATH*** field (described later in this section), you specify a path in that XML file. That path will specify the location of a value in the XML file. Skylar One will then examine the specified value and use the regular expression defined in the ***XPATH Match Regex*** field (described later in this section) to match devices to this device class.
3. To begin gathering information to include in the device class, find a device for which you want to create a "pingable" device class. If you have already discovered this device, it might currently have a device class of "Ping | ICMP".
4. You must now run nmap on the device. You can either log in directly to the device or log in to another device that can communicate with the device on which you want to run nmap. At the command prompt, enter the following:

```
nmap -sS -O -oX full pathname of file in which to XML output-sV --
version-all -A IP address of device
```

5. Navigate to the XML file where you stored the output from the nmap command. Examine the output and find an XML element or attribute that you can use to uniquely identify a device class for the device. Note the XPATH to the element or attribute.
6. The device data in the XML report generally uses the following element structure:
    - Information about nmap, including scan level and debugging level.
    - Information about each discovered host, including start-time and end-time for the nmap and the IP address, MAC address, and hardware vendor.
    - Specific information about each port, including the service running on the port, some stored as attributes of the Port element, some stored as child elements of the Port element
    - Specific information about the operating system, include vendor and version number, stored as attributes of the OSClass element
    - Information about uptime for the device.
    - Information about traceroute to the discovered device and round-trip time to the discovered

device.

- Performance data for this session of nmap.

7. For example, suppose we want to create a device class for each device that runs an Apache web server. After running nmap on a device that is running Apache, we might see the following elements and attributes under **Host/Ports**:

```
<port protocol="tcp" portid="80">
  <state state="open" reason="syn-ack" reason_ttl="64"/>
  <service name="http" product="Apache httpd" version -"2.2.3", extraninfo="
  (CentOS)" method="probed" conf="10" />
  <script id="html-title" output="Apache HTTP Server Test Page powered
  by CentOS" />
  <script id="http-favicon" output="" />
</port>
```

The XPATH would be **/nmaprun/host/ports/port/service/@product**

8. Go to the **Device Class Editor** page (System > Customize > Device Classes) to create a new device class. Click the **[Reset]** button to clear any values from the **Device Class Editor** page. Supply a value in the following fields:

   - ***Device Type***. Select *Pingable*.
   - ***Root Device***. Specifies that this device can have children devices. Ensures that root devices are included in nightly re-discovery. Leave this box unchecked.
   - ***Weight***. If two device-class definitions are similar, a device might meet the criteria for both device classes. In this case, the ***Weight*** field tells Skylar One which device class to align with the device. The ***Weight*** field allows you to define both detailed, non-SNMP device-class definitions, as well as less detailed, catch-all device classes.

     Skylar One will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, Skylar One will align the device with the device class that appears first in the alphabetical list of device classes.

     For example, you could define a detailed device class with a weight of "1" and a similar but less detailed device class with a weight of "10". Skylar One will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, Skylar One will then try to assign the discovered device to the device class with a weight of "10".

   - ***Device Class***. The name of the manufacturer who created the device and/or agent. Can be any combination of alphanumeric characters, up to 48 characters in length.

- ***NMAP Report XPATH***. Specifies how should parse the results of an nmap request (run during discovery) to determine whether the device should be aligned to this device class. If you select an ***Initial Scan Level*** of *5. Deep Discovery* for a discovery session, Skylar One will run the following nmap command on each device during discovery. Skylar One will include the -A option, to retrieve as much information as possible and match pingable devices with custom device classes.

    - In the ***NMAP Report Path*** field, enter the XPATH for the element or attribute you want to use to identify member devices. That path will specify the location of a value in the XML file. Skylar One will then examine the specified value and use the regular expression defined in the ***XPATH Match Regex*** field to match devices to this device class.

  In Skylar One, the XPATH must always begin with **/nmaprun/host**. Using our example from step #7 above, we would provide an XPATh of:

  /nmaprun/host/ports/port/service/@product

NOTE: In the ***NMAP Report Path*** field, we included the entire path to the attribute we want to match, ***but intentionally did not filter on the attribute value***. That is, we specified **/nmaprun/host/ports/port/service/@product** instead of **/nmaprun/host/ports/port/service/@product='Apache httpd'**. When you include the value of the attribute in the XPATH, XPATH does not return the attribute value, but instead returns the entire element that includes the attribute. **Because the element is not a text string, Skylar One cannot search the element using a regex.**

- ***XPATH Match Regex***. In this field, specify a regular expression you want to use when examining the value returned by nmap. The location of the value returned by nmap is defined in the ***NMAP Report XPATH*** field. Skylar One will align a device to a device class if the nmap response includes a value at the path specified in the ***NMAP Report XPATH*** and the value at that location matches the regular expression in the ***XPATH Match Regex*** field.

  Using our example in step #7, we would provide the value **Apache httpd**.

- ***Description***. The model name of the device. Can be any combination of alpha-numeric characters, up to 48-characters in length. For ease-of-use, ScienceLogic recommends that you follow this convention: If you are creating a device class for an entire manufacturer, rather than for a specific product, enter "OEM" as the device description.
- ***Device Icon***. The icon used to display the device in the graphical interface. To view the available icons, click **[Icons]**. Select an icon from the drop-down list.
- ***All in class***. Selecting this checkbox updates the device icon for all existing members of the device class.
- ***Device Category***. A logical categorization of device by primary function. This field allows to group related devices in reports and views. Select a value from drop-down list.
- ***All in class***. Selecting this checkbox updates the device category for all existing members of the device class.

- ***Collection Type***. Specifies whether the device is a hardware-based device (physical) or a virtual device.
- ***Weight***. If two device-class definitions are very similar, a device might meet the criteria for both device classes. In this case, the ***Weigh***t field tells which device class to align with the device. Skylar One will align the device with the device-class definition with the lowest weight. If a device matches two device-class definitions, and both device classes have the same weight, Skylar One will align the device with the device-class that appears first in the alphabetical list of device classes.

  The ***Weight*** field allows you to define detailed non-SNMP device-class definitions and still have catch-all device-classes with less-specific criteria.

  For example, you could define a detailed device class with a weight of "1" and a similar but less detailed catch-all device class with a weight of "10". Skylar One will first try to assign a discovered device to the device class with a weight of "1". If the device does not meet the criteria for that device class, Skylar One will then try to assign the discovered device to the device class with a weight of "10".

- ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in Skylar One. For devices with this device class, the selected device dashboard will appear as an option in the **Device Class Editor** page. This field is optional.

9. Click the **[Save]** button to save your changes to the device class or click the **[Save As]** button to save your changes under a new device-class name.

Applying the New Device Class

To apply a new "pingable" device class during discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery). If you are creating a new discovery session, click the **[Create]** button. If you are editing an existing discovery session, click its wrench icon ( ).
2. In the **Discovery Session Editor**page:
   - In the ***Initial Discovery Scan Level*** field, select *5. Deep Discovery*.

> **NOTE:** You can also define ***Initial Discovery Scan Level*** in the **Behavior Settings** page (System > Settings > Behavior). Because this discovery level is very compute-intensive, you might want to avoid setting this discovery level globally and instead choose this discovery level ***only for specific discovery sessions***.

   - Select the ***Discover Non-SNMP*** checkbox.
   - Select the ***Model Device*** checkbox.
3. Click the **[Save]** button.
4. When you run the discovery session, Skylar One will apply the new device class to discovered or re-discovered devices.

NOTE: You can also apply a new "pingable" device class ***during nightly auto-discovery***. You can define (nightly) ***Rediscovery Scan Level*** in the **Behavior Settings**page (System > Settings > Behavior) and select *5. Deep Discovery*. **However, because this auto-discovery level is very compute-intensive, you might not want to use this setting for global auto-discovery.**

Maintaining the New Device Class During Auto-Discovery

If you have applied a new "pingable" device class to a device, you should do the following to make sure that doesn't reset the device's device-class to "Ping | ICMP" during nightly auto-discovery.

NOTE: Skylar One will reset a pingable device's device class to "Ping | ICMP" if Deep Discovery is not enabled for nightly auto-discovery. You can enable Deep Discovery for nightly auto-discovery in the **Behavior Settings**page (System > Settings > Behavior). Go to the field ***Rediscovery Scan Level***, and select *5. Deep Discovery*. However, because this auto-discovery level is very compute-intensive, you might not want to use this setting for global auto-discovery.

You can disable auto-discovery for each device that uses Deep Discovery. Instead of using nightly auto-discovery, you can create a scheduled discovery session that will update the device class. To do this:

1. Go to the **Device Properties** page (Devices > Classic Devices > wrench icon).
2. Unselect the checkbox for ***Auto-Update***.
3. Click the **[Save]** button.
4. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery) and create a discovery session for this device (and each device that uses Deep Discovery and which you want to update regularly). When creating this discovery session:
    - In the ***Initial Discovery Scan Level*** field, select *5. Deep Discovery*.
    - Select the ***Discover Non-SNMP*** checkbox.
    - Select the ***Model Device*** checkbox.
5. Define the new discovery session as a scheduled discovery session, so you can periodically update the device's data.

Editing a Device Class That is Not SNMP-Enabled

In the **Device Class Editor** page, you can edit the parameters of an existing device class.

When you ***do not select SNMP Enabled***, you are defining a device class that does not use SNMP to identify member devices. Instead, the device class will use a value returned by nmap (run during discovery) to identify member devices.

NOTE: You can use an existing device class as a template for a new device class. To do this, follow the steps in this section, but supply a new name in the ***Device Class*** field and select the **[Save As]** button to save your changes.

To edit an existing Device Class:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class.
4. In the **Device Class Editor** page, you can edit the parameters of an existing device class. If you do not select *SNMP Enabled* in the ***Device Type*** drop-down list, you can edit the value in one or more of the fields described in the section *Creating a New Device Class for Devices That Do Not Support SNMP*.
5. Select the **[Save]** button to save you changes to the device class or select the **[Save As]** button to save your changes as a new device class. The newly selected device class is now associated with the device.

Creating a New Component Device Class

A device of type "component" is an entity that runs under the control of a management system running on a physical device. For example, Skylar One can discover a VMware ESX Server (management system) and then discover the virtual machines (component devices) running on that VMware ESX Server.

Skylar One uses Dynamic Applications to retrieve data from a management system and discover each component device managed by that system. Skylar One then uses that retrieved data to create a device record for each component device.

Device classes for components are aligned with the Dynamic Applications that discover component devices. For example, we could have a device class of type ***Component*** for "Cisco Systems | UCS Chassis". We could align the Dynamic Application for "UCS Chassis Discovery" with this device class. When Skylar One runs the "UCS Chassis Discovery" Dynamic Application and discovers a component device, Skylar One assigns each discovered component device to the device class "Cisco Systems | UCS Chassis".

When you create a new device class of type ***Component***, you are defining a device class that uses an aligned Dynamic Application to identify the member devices.

NOTE: The ***Device Class Tier*** is no longer used for Subscription Billing. For information regarding billing, see *Viewing and Managing Subscription Data*. If you create a custom device class, please contact ScienceLogic Customer Support to define the ***Device Class Tier*** for the new device class. For more information, see *Custom Device Class Process*.

To create a new device class of type ***Component***:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes).
2. Click **[Reset]** to clear the fields in the **Device Class Editor** pane.
3. Configure the device class as follows:
    - ***Device Type***. Select "Component".
    - ***Device Class***. Enter "ScienceLogic".
    - ***Device Category***. Select "Servers" from the drop-down list. This field specifies a logical categorization of devices by primary function, which allows Skylar One to group related devices in reports and views.
    - ***Root Device***. Select this checkbox if you will have additional tiers under this component device.
    - ***Description***. Enter a description for the device.
    - ***Device Icon***. Select an icon that you created or select a generic icon.
4. Click **[Save]** to save your changes to the device class.

Editing a Component Device Class

To edit an existing Device Class of Type "Component":

1. Go to System > Customize > Device Classes, or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class.
4. You can edit the value in one or more of the fields. For details on each field, see the section on *Creating a New Device Class of Type "Component"*.
5. Select the **[Save]** button to save you changes to the device class or select the **[Save As]** button to save your changes under a new device-class name.

Managing Device Classes

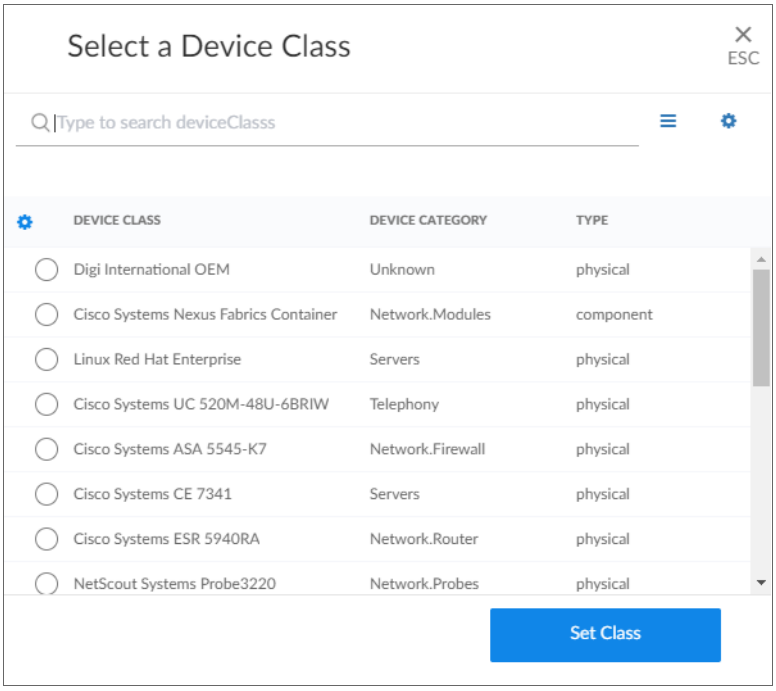
The following sections describe how to manually assign a device class to a device and how to change the icon for a device class in Skylar One.

Manually Assigning a Device Class to a Device

To manually assign a device class to a device:

1. Go to the **Devices** page and select the device to which you want to assign a device class.
2. On the **Device Investigator** page, click **[Edit]**.
3. Click the **Info** drop-down and click the ***Device Class*** field. The **Select a Device Class** window

appears:



4. The **Select a Device Class** window displays a searchable list of available device classes, and the category and type for each class.

> **TIP:** To use an advanced search to find a specific device class, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

5. Select the device class you want to assign and click the **[Set Class]** button.
6. Click the **[Save]** button on the **Device Investigator** page to save your changes.

Changing the Icon for a Device Class

You can customize the look and feel of the devices that appear on the **Devices** page by assigning an icon a device, device class, or device category.

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

1. On the **Devices** page, **Device Classes** page (Devices > Device Classes), or **Device Categories** page (Devices > Device Categories), locate the device, class, or category for which you want to add an icon.

2. Click the ***Actions*** button (⋮) for that item and select *Assign Icon*. The **Select an Icon** window appears.

> **TIP:** To assign an icon to more than one device, device class, or device category, select the checkboxes to the left of those items and click the **[Assign Icon]** button.

3. In the **Select an Icon** window, do one of the following:
   - To use an existing icon, proceed to step 7.
   - To upload a new icon from your local drive, make sure that the image file meets the following criteria, then proceed to step 4:
     - The image file should be in .SVG format.
     - The file should not be larger than 40 KB.
     - The file should not be animated.
     - The file should not contain bitmaps.
4. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears.
5. Complete the following fields in the **Add an Icon** window:
   - In the ***Icon name*** field, type a name for the icon you want to upload.
   - In the ***Add Tags*** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
   - You can click the ***Browse or Drop*** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
6. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
7. Select the icon from the list of icons and click the **[Select Icon]** button. The icon is assigned to the device, device class, or device category.

> **TIP:** You can use the ***Search*** field to search for a specific icon or narrow down the list of icons.

Managing Device Classes in the Classic Skylar One User Interface

The following sections describe:

- *Manually changing the device class for a device*
- *Changing the icon for a device class*
- *Deleting one or more device classes*

Manually Changing the Device Class for a Device in the Classic Skylar One User Interface

During discovery, Skylar One automatically assigns a device class to each discovered device. For example, Skylar One assigns the device class "Ping" to devices that do not support SNMP. You might want to manually change the device class for such a device after discovery.

In the **Device Properties** page, you can assign a different device class to the device.

To assign a different device class to the device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device you want to edit. Select its wrench icon ( ).
3. In the **Device Properties** page, find the *Device Class* field. Select the toolbox icon ( ).
4. In the **Select New Device Class** modal page, select a device class.
5. There are two other ways to align devices with the devices class:
    - You can re-run discovery for a single device. To re-discover a device, go to Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface. Find the device you want to re-discover. Select its wrench icon ( ). In the **Device Properties** page for the device, select the magnifying glass icon ( ). After the device is re-discovered, it will be aligned with the appropriate device class. You can repeat this process for each device you want to align with the new or edited device class.
    - If you re-run one or more discovery sessions (System > Manage > Classic Discovery), Skylar One will automatically apply the new or edited device class to those devices that match the criteria. Remember that to discover details about device of type "pingable", you must select the checkbox ***Discovery Non-SNMP***. Optionally, to retrieve details about "pingable" devices, in the field ***Initial Scan Level***, you can also select *5. Deep Discovery*.

Changing the Icon for a Device Class in the Classic Skylar One User Interface

You can select a new icon for a device class or import your own image as an icon. To do this:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class you want to edit. Select its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device class. To edit the icon associated with the selected device class, edit the value of the ***Device Icon*** field. The icon you select will be associated with the device class.
    - To view the list of icon names and icon images, select the **[Icon]** button in the upper right of the page.
    - The **Device Icon Browser** modal page displays a list of all icons for device class.

- To import an image to use as an icon, select the **[Import]** button. In the **Device Icon Browser** modal page, you can import a .png image for use as an icon in Skylar One.

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

Aligning One or More Device Classes with a Device Dashboard

From the **Device Class Editor** page, you can align one or more device classes with a device dashboard. You can manually align a device dashboard with a device class. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the device class will appear as the default view in the **Device Summary** page.

> **NOTE**: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

1. To align a device dashboard with one or more device classes:
2. Go to the **Device Class Editor** page (System > Customize > Device Classes).
3. In the **Device Class Register** pane at the bottom of the page, find the device class(es) you want to align. Select its checkbox.
4. In the ***Select Action*** drop-down in the lower right, select a device dashboard in the *Align Device Dashboard* section. Select the **[Go]** button.
5. Each selected device class is now aligned with the selected device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the device class will appear as the default view in the **Device Summary** page.

Deleting One or More Device Classes

From the **Device Class Editor** page, you can delete one or more device classes.

> **NOTE**: You cannot delete a device class if it is aligned to a device. To delete a device class that has devices aligned to it, you should first realign any member devices to a different device class.

To delete one or more device classes:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes), or from the **Device Properties** page, select the pencil icon ( ).
2. In the **Device Class Register** pane at the bottom of the page, find the device class(es) you want to delete. Select its checkbox.
3. In the ***Select Action*** drop-down in the lower right, select *DELETE Device Classes*. Select the **[Go]** button.
4. Each selected device class is deleted from Skylar One.

Device Categories

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

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

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

"Pingable" Device Category

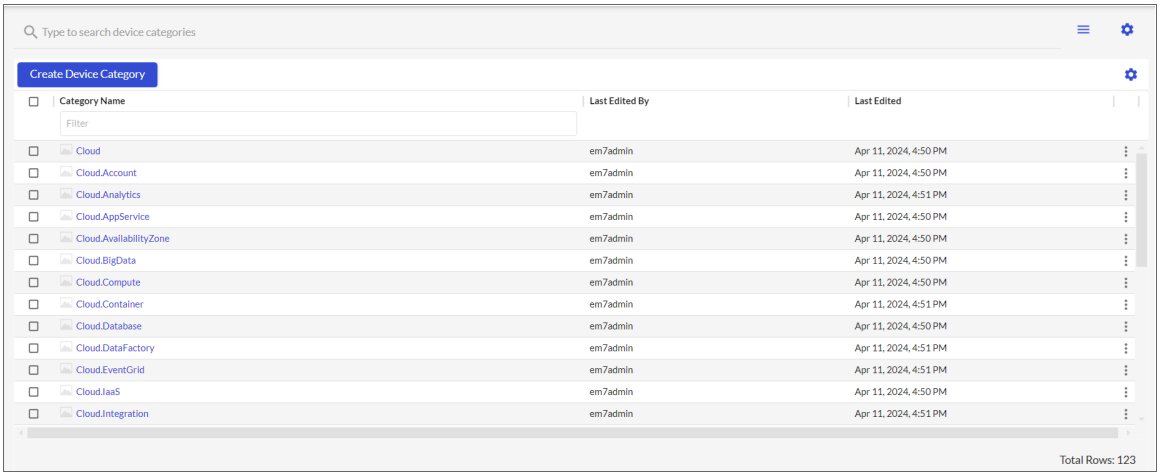
Devices that have a device category of "pingable" are devices that meet one of the following:

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

Viewing the List of Device Categories

On the **Device Categories** page (Devices > Device Categories), if you have the proper permissions, you can view a list of existing device categories, create and edit device categories, and duplicate device categories.

You can also assign an icon to a specific device category, and those icons will appear on the **Device Categories** page. The icons also appear on Maps as well as Device Investigator and Service Investigator pages.



TIP: If you are looking for a very specific set of device categories, click the gear icon ( ) to the right of the ***Search*** field and select *Advanced*. In this mode you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see the "Performing an Advanced Search" topic in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

For each device category, the **Device Categories** page displays the following information:

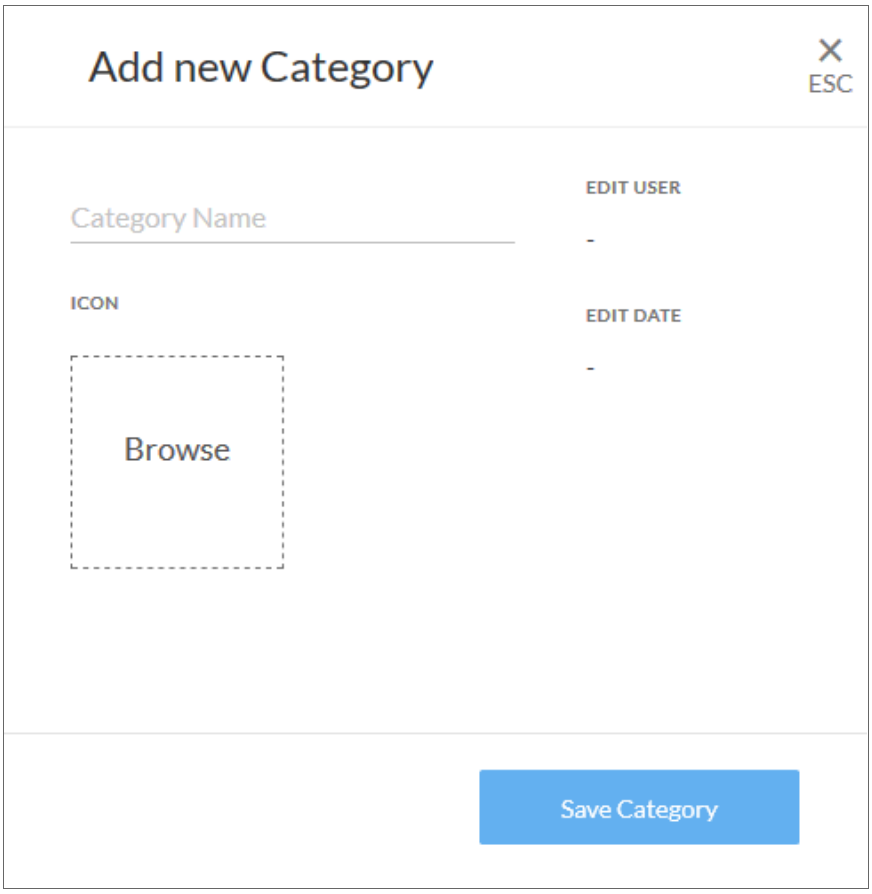
- ***Category Name***. The name of the device category.
- ***Last Edited By***. The name of the user who created or last edited the device category.
- ***Last Edited***. The date and time at which the device category was created or last edited.

TIP: To rearrange the columns in the list, click and drag the column name to a new location. You can adjust the width of a column by clicking and dragging the right edge of the column. For more information about editing and adding columns, see "Editing the Settings for an Inventory Page" in the ***Introduction to Skylar One*** manual.

Creating a New Device Category

To create a new device category:

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



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

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

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

Editing a Device Category

To edit a device category:

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

Duplicating a Device Category

To duplicate a device category:

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

Assigning an Icon to a Device Category

You can customize the look and feel of the devices that appear on the **Devices** page by assigning an icon a device, device class, or device category.

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

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

TIP: To assign an icon to more than one device, device class, or device category, select the checkboxes to the left of those items and click the **[Assign Icon]** button.

3. In the **Select an Icon** window, do one of the following:
    - To use an existing icon, proceed to step 7.
    - To upload a new icon from your local drive, make sure that the image file meets the following criteria, then proceed to step 4:
        - The image file should be in .SVG format.
        - The file should not be larger than 40 KB.
        - The file should not be animated.
        - The file should not contain bitmaps.
4. To start the upload process, click the **[Add Icon]** button. The **Add an Icon** window appears.
5. Complete the following fields in the **Add an Icon** window:
    - In the ***Icon name*** field, type a name for the icon you want to upload.
    - In the ***Add Tags*** field, type a short descriptor for the icon, without spaces. You can use this tag for searching later.
    - You can click the ***Browse or Drop*** area to browse for and select the icon, or you can drag and drop the icon file onto the **Add an Icon** window.
6. Click the **[Add Icon]** button. The icon is added to the **Select an Icon** window.
7. Select the icon from the list of icons and click the **[Select Icon]** button. The icon is assigned to the device, device class, or device category.

> TIP: You can use the ***Search*** field to search for a specific icon or narrow down the list of icons.

Managing Device Categories in the Classic Skylar One User Interface

This section describes how to view, define, and manage device categories using the **Device Category Editor** in the classic Skylar One user interface.

Viewing the List of Device Categories in the Classic Skylar One User Interface

The **Device Category Editor** page displays a list of all existing device categories. To view this page:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. For each device category, the **Device Category Editor** page displays the following:
    - ***Category Name***. The name of the device category.
    - ***Map Icon***. Pathname of the image used as an icon for the device category.

- ***Device Dashboard***. This field displays the device dashboard associated with the device category.
- ***ID***. A unique numeric identifier for the device category, automatically assigned by Skylar One.
- ***Edit User***. User who created or last edited the device category.
- ***Edit Date***. Date and time the device category was created or last edited.

TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

Creating a New Device Category in the Classic Skylar One User Interface

From the **Device Category Editor** page, you can create a new device category. To do this:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. Click the **[Reset]** button to clear any values from the fields in the editor pane.
3. In the editor pane at the top of the page, supply values in each of the following fields:
   - ***Category Name***. Enter a name for the new device category. This name can be any combination of alphanumeric characters, up to 32 characters in length. Skylar One naming convention is to create names using the following prefixes:
     - *Environmental* for environmental-monitoring devices.
     - *Network* for networking hardware like routers, switches, and firewalls.
     - *Office* for office equipment.
     - *Server* for server hardware.
     - *System* for networked hardware like servers and network stores.
     - *Telephony* for telephone hardware.
     - *Wireless* for wireless network hardware.

   However, you are not required to follow this convention.

   - ***Map Icon***. Select an icon to be associated with this device category. You can select from a list of all possible icons for device categories. The selected icon will be used to represent members of the device category in the network maps in Views and maps.
   - ***Device Dashboard***. Select a device dashboard from a list of all device dashboards in Skylar One. For devices with this device category, the selected device dashboard will appear as an option in the **Device Summary** page. This field is optional.

4. Click the **[Save]** button.
5. The new device category should now appear in the list of device categories in this page and appear in the ***Device Category*** drop-down list in the **Device Class Editor** page.

Editing a Device Category in the Classic Skylar One User Interface

In the **Device Category Editor** page, you can edit the parameters of an existing device category. To do this:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. In the register pane at the bottom of the page, find the device category you want to edit. Click its wrench icon ( ).
3. The fields in the top pane will be populated with values from the selected device category. You can edit the value in one or more of the fields.
4. For a description of each field, see the previous section on *Creating a New Device Category*.

Deleting a Device Category

From the **Device Category Editor** page, you can delete an existing device category.

> CAUTION: Do not delete device categories that are being used by managed devices. If you delete a device category to which devices have been assigned, you risk losing data from the device.

To delete a device category:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. Find the device category you want to delete. Click its delete icon ( ).
3. The device category is deleted from Skylar One.

Aligning One or More Device Categories with a Device Dashboard

From the **Device Category Editor** page, you can align one or more device categories with a device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page or in the **Device Class Editor** page, the device dashboard associated with the device category will appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with one or more device categories:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. Find the device categories you want to align. Select their checkboxes (☑).
3. In the ***Select Action*** drop-down list in the lower right, select a device dashboard under the *Align Device Dashboard* section. Click the **[Go]** button.
4. Each selected device category is now aligned with the selected device dashboard. For devices that do not have a device dashboard defined in the **Device Properties** page or in the **Device Class Editor** page, the device dashboard associated with the device category will appear as the default view in the **Device Summary** page.

Chapter 8

Device Relationships

Overview

This chapter describes device relationships in Skylar One.

This chapter covers the following topics:

What are Device Relationships? 174

Viewing the List of Device Relationships 175

Viewing Relationships for a Single Device 176

Viewing Device Topology Maps 178

Defining Device Relationships 179

Event Correlation 179

Layer-2 Topology Collection and Processing 182

CDP Topology Collection 183

LLDP Topology Collection 185

Layer-3 Topology Collection 187

ARP Topology Collection 188

What are Device Relationships?

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

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

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

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

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

Viewing the List of Device Relationships

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

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

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

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

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

You can view information for each parent-child relationship between two devices managed by Skylar One or for a single parent device managed by Skylar One and an unknown child device.

To view information on **Device Relationships**:

1. Go to the **Device Relationships** page (Registry > Networks > Device Relationships).
2. The **Device Relationships** page displays the following information:

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

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

- ***Child***. If the child device has been discovered by Skylar One, this column contains the name of the device and a link to the **Device Relationships** page for the child device.
- ***Child IP***. If the child device has been discovered by Skylar One, this column contains the IP address through which the child communicates with the parent device.
- ***Child Interface***. If the child device has been discovered by Skylar One, this column contains the name of the interface through which the child device communicates with the parent device and a link to the **Interfaces Found** page for the child interface.

- *Child Phys Addr*. The physical address (MAC address) for the interface through which the child device communicates with the parent device.
- *Child IF Manufacturer*. If included in the MAC address, the manufacturer of the child interface.
- *Parent*. The name of the parent device and a link to the **Device Relationships** page for the parent device.
- *Parent Interface*.The name of the interface through which the parent device communicates with the child device and a link to the **Interfaces Found** page for the parent interface.
- *Parent IF Alias*. Easy-to-remember, human-readable name for the interface on the parent device.
- *Parent Phys Addr*. The physical address (MAC address) for the interface through which the parent device communicates with the child device.
- *Parent IF Manufacturer*. If included in the MAC address, the manufacturer of the parent interface.
- *Type*. Describes the relationship between the parent device and child device. Possible values are:
    - ARP
    - CDP
    - Component Mapping
    - Component Relationship
    - Event Correlation
    - Layer-2
    - Layer-3
    - LLDP
    - VMware

Viewing Relationships for a Single Device

You can view all links for a single device on the **Relationships** tab of the **Device Investigator** (or on the **Device Relationships** page in the **Device Properties** panel in the classic Skylar One user interface).

To view all links for a single device:

1. Go to the **Relationships** tab of the **Device Investigator**. (Alternatively, go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), click the wrench icon for a device (🔧) and then click the **[Relationships]** tab.) The **Device Relationships** page appears.
2. The left pane of the **Device Relationships**page displays links to parent devices. The right pane of the **Device Relationships** page displays links to child devices. For each relationship, the **Device Relationships** page displays the following information:
    - *Type of relationship*. Possible values are:

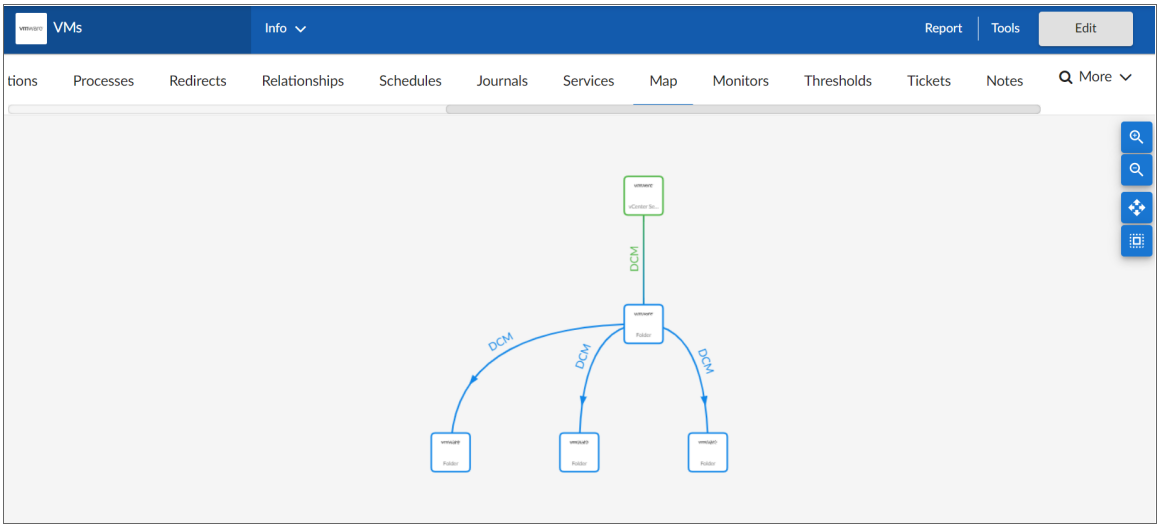
- *ARP*. Network devices that use ARP (Address Resolution Protocol) and devices that are specified as neighbors in ARP tables.
- *CDP*. Network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables.
- *Component Mapping*. Relationships defined using Dynamic Applications.
- *Event Correlation*. Relationships defined manually by users through the user interface.
- *Layer 2*. Layer-2 devices and their clients.
- *Layer 3*. Layer-3 devices and layer-2 devices.
- *LLDP*. Network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables, including those devices that respond only to LLDP v2.
- *VMware*. Hypervisors and their virtual machines.

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

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

Viewing Device Topology Maps

On the **[Map]** tab in the **Device Investigator**, you can view a map of the selected device and all of the devices with which the device has relationships.



These relationships include:

- Layer-2 devices and their clients
- Layer-3 devices and Layer-2 devices
- Component devices and their parent devices. For example, virtual machines and their hypervisors and their virtual machines.
- Network devices that use CDP (Cisco Delivery Protocol) and devices that are specified as neighbors in CDP tables
- Links between network devices that use CDP (Cisco Discovery Protocol) and devices that are specified as neighbors in CDP tables
- Network devices that use LLDP (Link Layer Delivery Protocol) and devices that are specified as neighbors in LLDP tables
- Links between network devices that use LLDP (Link Layer Discovery Protocol) and devices that are specified as neighbors in LLDP tables
- Device relationships between root devices, parent devices, and component devices (Component Mapping)
- Device relationships created with Dynamic Applications
- Manually created parent-child relationships that affect event correlation

A map includes the following graphical elements:

- ***Nodes***. Shapes that represent Devices, Topology Elements, and Business Services defined in Skylar One. The shape of a node represents its type, and the color of its outline specifies the current state of the node.
- ***Edges***. Lines with or without arrows that represent the relationships and hierarchies between nodes. All device relationships are displayed as child and parent relationships. If the nodes on a map contain arrows, then the arrows represent the direction of the relationship, pointing from the child node to its parent node. If a node does not contain an arrow, then the relationship is bi-directional, or *undirected*.

When you hover your mouse over a device icon on the map, a pop-up window appears that displays information about that device. Click the device name in the pop-up window to go to the **Device Investigator** for that device.

You can use the icons on the page to do the following:

- Increase the map size ( )
- Decrease the map size ( )
- Fit all of the map elements into the viewing pane ( )
- Center the selected elements of a map in the viewing pane ( )

Defining Device Relationships

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

To add children to a device:

1. Go to the **Relationships** tab of the **Device Investigator**. (Alternatively, go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), click the wrench icon for a device ( ) and then click the **[Relationships]** tab.) The **Device Relationships** page appears.
2. Click the **[Actions]** button and then select *Device Children*. The **Device Children** modal page appears.
3. In the **Device Children** page, select one or more devices to be children of the current device.
4. Click **[Save]**.

Event Correlation

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

- In the **Events** page, the child events are rolled up and nested under the parent event and are displayed only if you click on the magnifying-glass icon ( ).

- For the parent event, the ***Count*** column will be incremented to indicate the number of correlated child events.

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

Events that Might Appear on the Events Page

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

- ***Rolled-up events***. Multiple occurrences of the same event on the same device. When the same event occurs multiple times on a single device, Skylar One does not display each occurrence in the **Events** page. Instead, Skylar One displays a single entry and notes the number of occurrences in the ***Count*** column.
- ***Suppressed Events***. Suppressed events do not appear in the **Events** page.
- ***Topology Events***. In Skylar One, event correlation or topology suppression means the ability to build parent-child relationships between devices and between events. When events are correlated, only the parent event is displayed in the **Events** page. The magnifying-glass icon (🔍) appears to the left of the parent event. When you click on the magnifying-glass icon, the list of child events is displayed. The child events are rolled up under the parent event and are not displayed in the **Events** page. For the parent event, the count column will be incremented to indicate the number of correlated child events. Optionally, you can define event categories that allow Skylar One to more efficiently align suppressing events with suppressible events. When you align an event category to a suppressing or suppressible event, that event will be correlated with only events that are aligned with the same event category.

> **IMPORTANT:** Enabling a discovered device configured with CDP or LLDP topology in Skylar One will cause the device to provide information on its neighbor. This information only identifies that there is a neighbor device, not which is the parent or the child. This may cause the parent-child relationship to switch which requires you to manually reverse the issue within the Skylar One user interface. Skylar One allows you to manually build parent-child relationships between specific device categories. For more information, see *Defining Parent and Child Devices* in the ***Events*** manual.

- ***Event Masks***. In the **Device Properties** page for each device, you can define an Event Mask. When a device uses the Event Mask setting, events that occur on a single device within a specified span of time are grouped together. In the **Events** page, masked events are displayed under a single event, the one with the highest severity. The magnifying-glass icon (🔍) appears to the left of the event. When you click on the magnifying-glass icon, the list of all events that are masked under event is displayed.

Defining Event Correlation

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

- ***Suppressing events***. If this event occurs on a parent device, Skylar One will search all related children devices for ***suppressible*** events. On the children devices, all suppressible events will be suppressed. Only the suppressing event will appear in the **Events** page (or the **Event Console** page in the classic Skylar One user interface) . The suppressible events will not appear in the **Events** page (or the **Event Console** page in the classic Skylar One user interface) .
- ***Suppressible events***. This type of event is suppressed on a child device only when a suppressing event occurs on the parent device.

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

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

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager.
2. On the **Event Policy Manager** page, click the wrench icon (🔧) of the event that you want to define as the ***suppressing*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.
4. In the ***Topology Suppression*** field, select *Suppressing*.
5. Click **[Save]**. In the future, when this event occurs on a device, Skylar One will check if the device is a parent device. If the device is a parent device, specified events (suppressible events) with the same category will be suppressed on the children devices.

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

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page , click the wrench icon (🔧) of the event that you want to define as the ***Suppressible*** event. The **Event Policy Editor** page appears.
3. On the **Event Policy Editor** page, click the **[Advanced]** tab.
4. In the ***Topology Suppression*** field, select *Suppressible*.
5. Click **[Save]**. In the future, when this event occurs on a device, Skylar One will check if the device is a child device. If the device is a child device, Skylar One will check to see if a suppressing event with the same category has occurred on the parent device. If a suppressing event has occurred on the parent device, the specified event will be suppressed on the child device.

Example: Child Event Suppression

For example, suppose you have the following devices and event policies defined:

- A parent device, a Cisco Catalyst switch named *Boise-DMZ*.
- A child device to *Boise-DMZ*, a server named *HQ-W2K3-VC01*.
- An event policy, "Poller: Interface operationally down", defined as a suppressing event.

- A second event policy, "Poller: Device not responding", defined as a suppressible event.
- Both events are associated with the same event category.

In this scenario, if an interface goes down on the switch *Boise-DMZ*, Skylar One will not be able to communicate with the server, *HQ-W2K3-VC01*, attached to the switch.

With the above defined event topology suppression:

- The event "Poller: Interface operationally down" occurs on *Boise-DMZ*.
- The event "Poller: Device not responding" is suppressed on the server *HQ-W2K3-VC01*.
- On the **Events** page (or the **Event Console** page in the classic Skylar One user interface), the only event that would appear in this scenario will be the event "Poller: Interface operationally down" on the device *Boise-DMZ*.

Layer-2 Topology Collection and Processing

A Layer-2 topology record describes a direct network connection between a parent device (a network switch or network bridge) and a child device. The child device is either:

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

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

NOTE: Layer-2 collection should be enabled only on network devices that respond to SNMP requests for object IDs (OIDs) from the BRIDGE-MIB. Layer-2 collection is not required for the collection of MAC addresses on the interfaces of non-bridge network devices; this is done automatically as part of interface discovery.

In Skylar One 12.5.1 and later, you can enable or disable Layer-2 collection for any device, an entire device class, a device template that can be applied to one or more devices, or all devices system-wide. On network devices and device classes that do not respond to SNMP requests, you can choose to disable Layer-2 topology collection but still enable *Layer-2 standard or enhanced processing*, in which case the system will use Dynamic Applications to collect the data needed for processing.

In version 12.5.20 and later, Skylar One automatically removes stale Layer-2 topology relationships when connections no longer exist or a parent/child device becomes inactive.

During collection, Skylar One performs the following steps:

- Compiles a list of all devices to poll. Skylar One polls devices that have a ***Device Category*** of "Network.Switches" or "Network.Bridges". The ***Device Category*** is defined in the device's device class.

- If the ***Enable L2 Topology Collection from all VLANs*** checkbox is selected in the **Behavior Settings** page (System > Settings > Behavior), Skylar One compiles a list of virtual local area networks (VLANs) for which data should be collected using the CISCO-VTP-MIB. A VLAN is added to the list of VLANs only if its state is 1 (operational) and its type is 1 (ethernet). If the ***Enable L2 Topology Collection from all VLANs*** option is disabled, Skylar One performs collection for vLAN 1 only.
- For each VLAN on each device, Skylar One polls the BRIDGE-MIB to collect the list of all MAC addresses for which that network switch or bridge has forwarding information.
- Skylar One stores a MAC address record if:
    - The status of the record is "3" (learned).
    - An ifIndex value was collected successfully for the associated port index.

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

Layer-2 Topology Processing

In Skylar One 12.5.1 and later, you can choose to enable standard or enhanced processing methods for specific devices or entire device classes.

Standard Layer-2 processing, which is used by default in versions of Skylar One prior to 12.5.1, uses 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.

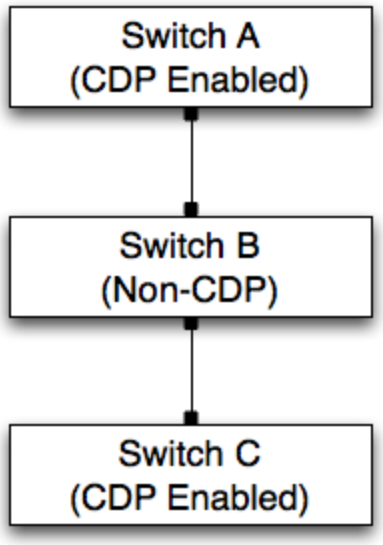
Enhanced Layer-2 processing, which is available in Skylar One 12.5.1 and later, can form Layer-2 relationships between any devices that matches a MAC address from the BRIDGE-MIB or sourced from Dynamic Applications, regardless of device category.

CDP Topology Collection

Cisco Discovery Protocol (CDP) is a proprietary standard developed by Cisco that is used by networking devices to communicate configuration information to the other devices in the network. It is not supported by all network hardware. Devices that support CDP store and report information received about their immediate neighbors.

A CDP Topology record describes a direct network connection between a parent device (a network switch or network router) and a child device. If your network includes both CDP-enabled and non-CDP network switches and routers, the topology data reported by the CDP-enabled devices might not be accurate.

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



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

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

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

NOTE: Although Skylar One polls all network switches and routers for CDP information, not all network switches and routers support CDP. To save system resources, CDP collection should be enabled only on devices that respond to SNMP and have CDP configured.

Each discovered interface can be associated with only one topology record of ***any*** type. Therefore, the same "crunch" process that creates Layer-2 topology records is also responsible for creating the CDP records based on the collected data. However, unlike Layer-2 topology records, the Cisco-CDP-MIB

reports only directly connected devices. Therefore, if all associated interfaces are valid and available, there is a 1:1 mapping between collected CDP relationships and the CDP relationships created by the "crunch" process.

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

CDP Topology Processing

In Skylar One 12.5.1 and later, you can choose to enable standard or enhanced processing methods for specific devices or entire device classes.

Standard CDP processing, which is used by default in versions of Skylar One prior to 12.5.1, requires that both devices respond with CDP neighbor data, show each other as a neighbor, and be managed devices in Skylar One in order to form a CDP topology relationship with each other.

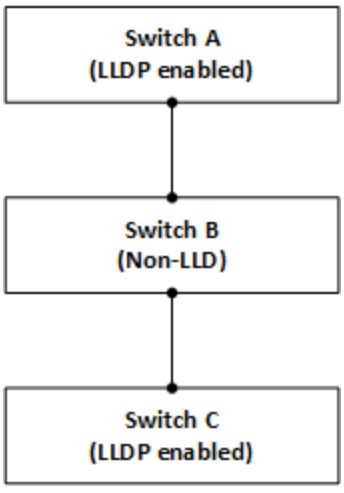
Enhanced CDP processing, which is available in Skylar One 12.5.1 and later, can form CDP relationships between two devices so long as at least one of those devices responds with CDP neighbor data and is a manged device in Skylar One. This new process also supports asynchronous collection, which increases the scale of CDP collection when devices are slow to respond or to load due to network latency.

LLDP Topology Collection

Link Layer Discovery Protocol (LLDP) is a standard used by networking devices to communicate configuration information to the other devices in the network. Devices that support LLDP store and report information received about their immediate neighbors.

An LLDP topology record describes a direct network connection between a parent device (a network switch or network router) and a child device. If your network includes both LLDP-enabled and non-LLDP network switches and routers, the topology data reported by the LLDP enabled devices might not be accurate.

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



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

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

If LLDP collection is enabled, Skylar One collects information from the LLDP MIB from all discovered network switches and routers. In Skylar One 12.5.20 and later, the system can also collect information from the LLDP-V2 MIB to discover relationships between devices that respond only to LLDP v2. Skylar One polls devices that have a ***device category*** of "Network.Switches" or "Network.Routers". The ***device category*** is defined in the device class assigned to the device. Network switches and routers that support the Cisco-LLDP-MIB report the IP address and interface information for all directly connected devices that are LLDP-enabled.

> **NOTE:** Although Skylar One polls all network switches and routers for LLDP information, not all network switches and routers support LLDP.

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

LLDP Topology Processing

In Skylar One 12.5.1 and later, you can choose to enable standard or enhanced processing methods for specific devices or entire device classes.

Standard LLDP processing, which is used by default in versions of Skylar One prior to 12.5.1, requires that both devices respond with LLDP neighbor data, show each other as a neighbor, and be managed devices in Skylar One in order to form an LLDP topology relationship with each other.

Enhanced LLDP processing, which is available in Skylar One 12.5.1 and later, can form LLDP relationships between two devices so long as at least one of those devices or its network interface responds with LLDP neighbor data and is a manged device in Skylar One. This new process also supports asynchronous collection, which increases the scale of LLDP collection when devices are slow to respond or to load due to network latency.

Layer-3 Topology Collection

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

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

For Skylar One to create Layer-3 topology records, the following requirements must be met:

- All traceroute commands for Layer-3 topology collection originate from Data Collectors or an All-In-One Appliance. Therefore, the parent node(s) in the Layer-3 topology is always a Data Collector or the All-In-One Appliance. For Skylar One to create Layer-3 topology records, all Data Collectors and All-In-One Appliances must be discovered.
- Skylar One performs traceroute commands to devices that have the ***L3 Topology*** option enabled. The ***L3 Topology*** option is defined in the device class assigned to a device. For Skylar One to perform Layer-3 topology collection, at least one device in your system must have the ***L3 Topology*** option enabled in the device class.
- Your network configuration must allow the traffic generated by the traceroute commands. To test whether your network allows this traffic, go to the **Device Toolbox** page (by clicking the **[Toolbox]** tab in the **Device Administration** panel) for a device with the ***L3 Topology*** option enabled, and then click the **Traceroute** icon.

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

Layer-3 Topology Processing

In Skylar One 12.5.1 and later, you can choose to enable standard or enhanced processing methods for specific devices or entire device classes.

Standard processing, which is used by default in versions of Skylar One prior to 12.5.1, requires all the hops in a traceroute to respond and match devices within Skylar One. The traceroute is discarded whenever the system detects hops that fail to respond or the traceroute includes hops that do not match devices in Skylar One.

Enhanced processing, which is available in Skylar One 12.5.1 and later, does not discard incomplete traceroutes or results that include unmatched hops. Instead, the system will form relationships between any two hops that respond and match devices in Skylar One.

ARP Topology Collection

Address Resolution Protocol (ARP) is a standard networking protocol used to map a logical IP address to a physical hardware MAC address within a single local area network (LAN). It works only with IPv4 addresses. Devices that support ARP store these IP-to-MAC mappings and make it easier for devices on a local network to communicate with each other.

In versions 12.5.20 and later, Skylar One can collect and store ARP data from devices that have ARP collection enabled, either at the class or device level. These devices, which are typically switches or routers, must respond to SNMP and have network interfaces discovered for Skylar One to create the ARP relationship. Only one device needs to provide ARP data for Skylar One to form the relationship.

ARP Topology Processing

In Skylar One 12.5.20 and later, you can choose to enable standard or enhanced ARP processing methods for specific devices or entire device classes.

Standard ARP processing only creates ARP relationships when both devices are routers or switches.

Enhanced processing ignores this device type restriction and creates relationships when ARP data matches, regardless of the device class.

Chapter

9

Device Maintenance

Overview

This chapter describes the ways in which you can maintain devices in Skylar One.

This chapter covers the following topics:

What is Scheduled Maintenance? *189*

What is User Maintenance? *191*

The Maintenance Minimum Severity Setting *191*

Enabling and Disabling User Maintenance for a Single Device *191*

Enabling and Disabling User Maintenance for One or More Devices *192*

Scheduling Maintenance for a Single Device *193*

Scheduling Maintenance for One or More Devices *197*

Enabling or Disabling Scheduled Maintenance for One or More Devices *197*

Deleting Scheduled Maintenance for One or More Devices *198*

What is Scheduled Maintenance?

Scheduled Maintenance is a date and time when a device is put into "maintenance mode". During maintenance mode, for the selected devices Skylar One will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during

maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate applicable events for the devices.

Skylar One includes tools that allow you to view, edit, and define scheduled maintenance for one or more devices. The **Schedule Manager** page allows you to schedule one-time and recurring maintenance tasks and downtime for a device. You can use the scheduled maintenance to:

- Specify a recurring downtime for routine maintenance (such as a database backup that occurs weekly every Tuesday at 3 AM).
- Specify a monthly schedule based on day of the week (such as a backup that occurs every third Sunday of the month at 11 PM)
- Specify one-time downtime (such as a specific day for upgrading software or hardware).

When a device is in maintenance, Skylar One will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled during maintenance, Skylar One will collect information from the device but will not generate applicable events for the device.

You can specify a "patch window" within the larger maintenance period. The "patch window" allows Skylar One to limit the suppression events to a small time-frame within the larger maintenance window. For example:

Suppose you have to patch a server that is monitored by 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 will require 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.

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. This first event within the larger maintenance window triggers the start of the patch maintenance 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.

NOTE: If you disable an active maintenance schedule, the device will be pulled out of maintenance mode; if you re-enable the schedule during the scheduled time window, the device will return to maintenance mode.

What is User Maintenance?

User maintenance is an option that allows a user to manually put a device in to "maintenance mode". During maintenance mode, for the selected devices Skylar One will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate applicable events for the devices.

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

User maintenance can be enabled and disabled in the user interface or through the API. For more information, ask your ScienceLogic contact for access to the ScienceLogic API documentation.

The Maintenance Minimum Severity Setting

The global ***Maintenance Minimum Severity*** setting specifies the minimum severity required for an event to be suppressed during device maintenance and user maintenance. The default value is *Healthy*, which causes all events to be suppressed. To change this setting:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. In the **Behavior Settings** page, select a value in the ***Maintenance Minimum Severity*** drop-down list. The choices are *Healthy*, *Notice*, *Minor*, *Major*, or *Critical*.
3. Select the **[Save]** button. Events with a severity lower than the severity you chose will now be generated for all devices in scheduled maintenance mode and user maintenance mode.

Enabling and Disabling User Maintenance for a Single Device

You can enable and disable user maintenance mode in the **Device Properties** page.

To enable or disable user maintenance mode for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

2. In the **Device Manager** page, find the device for which you want to enable or disable user maintenance. Select its wrench icon (). The **Device Properties** page is displayed.
3. In the **Device Properties** page, edit the following fields:
    - ***User Maintenance***. Specifies whether the device is in user maintenance mode. During maintenance mode, for the selected devices Skylar One will generate only events with a severity less than the system-wide ***Maintenance Minimum Severity*** setting. By default, no events are generated during maintenance. You can choose to enable or disable polling during maintenance mode. Even if polling is enabled, Skylar One will collect information from the selected devices but will not generate applicable events for the devices. Choices are:
        - *Enabled*. Device will be put in user maintenance mode. The device will remain in this state until you or another user disables user maintenance mode.
        - *Disabled*. User maintenance mode will be disabled for this device.
    - ***User Maintenance Collection***. The drop-down list to the right of the ***User Maintenance*** field specifies whether Skylar One will poll the device during user maintenance mode. Choices are:
        - *Enabled*. The device will be polled during user maintenance mode.
        - *Disabled*. The device will not be polled during user maintenance mode.
4. Select the **[Save]** button.

Enabling and Disabling User Maintenance for One or More Devices

The **Device Manager** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once. From the ***Select Action*** menu, you can enable or disable user maintenance mode for multiple devices, simultaneously.

To enable or disable user maintenance mode for multiple devices:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, select the checkbox for each device to which you want to apply the action. To select all checkboxes for all devices, select the checkbox at the top of the page.
3. In the ***Select Action*** drop-down list, select one of the following:
    - *Change User Maintenance Mode: Enabled with Collection*. This option puts the selected devices into user maintenance mode with collection enabled. The devices will remain in this state until you or another user disables user maintenance mode.
    - *Change User Maintenance Mode: Enabled without Collection*. This option puts the selected devices into user maintenance mode with collection disabled. The devices will remain in this state until you or another user disables user maintenance mode.
    - *Change User Maintenance Mode: Disabled*. This option disables user maintenance mode for the selected devices.

4. Click the **[Go]** button.
5. The changes are applied to each selected device.

Scheduling Maintenance for a Single Device

You can schedule maintenance and downtime for a device on the **Schedules** tab of the **Device Investigator** (or on the **Schedule Manager** page in the **Device Administration** panel in the classic Skylar One user interface).

NOTE: You can also view and manage all scheduled processes from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). For more information, see the ***System Administration*** manual.

Viewing the Schedule Manager

The **Schedules** tab of the **Device Investigator** (or the **Schedule Manager** page in the **Device Administration** panel in the classic Skylar One user interface) displays the following information about each scheduled or recurring device maintenance window:

- ***Schedule Summary***. Displays the name assigned to the scheduled process.
- ***Schedule Description***. Displays a description of the scheduled process.
- ***Event ID***. Displays a unique, numeric ID for the scheduled process. 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 maintenance window, click its wrench icon (🔧) and update the settings as needed on the **Schedule Editor** modal page. (For more information, see the section *Defining a Scheduled or Recurring Device Maintenance Window for a Single Device*.)

Defining a Scheduled or Recurring Device Maintenance Window for a Single Device

You can schedule a device maintenance window in Skylar One from the **Schedules** tab of the **Device Investigator** (or the **Schedule Manager** page in the **Device Administration** panel in the classic Skylar One user interface). Skylar One will automatically set the status of the device to "maintenance" at the scheduled time.

To define a scheduled or recurring device maintenance window:

1. Go to the **Schedules** tab of the **Device Investigator**. (Alternatively, in the classic Skylar One user interface, go to the **Schedule Manager** page (Devices > Classic Devices > wrench icon > Schedule, or Registry > Devices > Device Manager > wrench icon > Schedule in the classic user interface)).
2. Click **[Create]**. The **Schedule Editor** modal page appears.
3. On the **Schedule Editor** modal page, enter values in the following fields:

   Basic Settings

   - ***Schedule Name***. Type a name for the scheduled process.
   - ***Schedule Type***. Indicates the scheduled process type (such as Tickets, Reports, or Devices).
   - ***Visibility***. Select the visibility for the scheduled process. You can select one of the following:
     - *Private*. The scheduled process is visible only to the owner selected in the ***Owner*** field.
     - *Organization*. The scheduled process is visible only to the organization selected in the ***Organization*** field.
     - *World*. The scheduled process is visible to all users.
   - ***Organization***. Select the organization to which you want to assign the scheduled process.
   - ***Owner***. Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
   - ***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

- ***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 apply a patch to 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]**.

Scheduling Maintenance for One or More Devices

The **Device Manager** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple devices at once. From the ***Select Action*** menu, you can schedule maintenance for multiple devices, simultaneously.

To schedule maintenance for multiple devices:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, select the checkbox for each device for which you want to schedule maintenance. To select all checkboxes for all devices, select the checkbox at the top of the page.
3. In the ***Select Action*** drop-down list, select *Schedule Maintenance*, and then click **[Go]**. The **Schedule Editor** modal page appears.
4. To schedule maintenance for the selected devices, follow the steps described in the section *Defining a Scheduled or Recurring Device Maintenance Window for a Single Device*. The values you supply in the **Schedule Editor** modal page are applied to each selected device.

Enabling or Disabling Scheduled Maintenance for One or More Devices

You can enable or disable one or more scheduled or recurring device maintenance windows from the **Schedules** tab of the **Device Investigator** (or the **Schedule Manager** page in the **Device Administration** panel in the classic Skylar One user interface).

To do this:

1. Go to the **Schedules** tab of the **Device Investigator**. (Alternatively, in the classic Skylar One user interface, go to the **Schedule Manager** page (Devices > Classic Devices > wrench icon > Schedule, or Registry > Devices > Device Manager > wrench icon > Schedule in the classic 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 Scheduled Maintenance for One or More Devices

You can delete one or more scheduled or recurring device maintenance windows from the **Schedules** tab of the **Device Investigator** (or the **Schedule Manager** page in the **Device Administration** panel in the classic Skylar One user interface).

To delete maintenance windows:

1. Go to the **Schedules** tab of the **Device Investigator**. (Alternatively, in the classic Skylar One user interface, go to the **Schedule Manager** page (Devices > Classic Devices > wrench icon > Schedule, or Registry > Devices > Device Manager > wrench icon > Schedule in the classic 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

10

Managing Dynamic Applications

Overview

This chapter describes how to manage the Dynamic Applications aligned to a device in Skylar One.

This chapter covers the following topics:

Viewing the List of All Dynamic Applications in Skylar One 199

Managing the Dynamic Applications Aligned to a Device 203

Managing the Dynamic Applications Associated with a Device in the Classic Skylar One User Interface 211

How Skylar One Manages the Collection Status for Dynamic Applications 221

Status of Objects for Deviation 222

Bulk Un-Aligning Dynamic Applications 223

Setting Thresholds for Dynamic Applications 223

Dynamic Applications and Discovery 224

Viewing the List of All Dynamic Applications in Skylar One

The **Dynamic Applications Manager** page (System > Manage > Dynamic Applications) displays a list of all existing Dynamic Applications. For each Dynamic Application, the page displays the following fields:

TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

- ***Dynamic Application Name***. Name of the Dynamic Application, as defined in the **Dynamic Applications Properties Editor** page.
- ***Poll Rate***. Frequency, in minutes, at which Skylar One will poll all devices that use this Dynamic Application. The ***Poll Rate*** column displays the default poll frequency for the Dynamic Application, as defined in the **Dynamic Applications Properties Editor** page. You can define a ***custom*** poll frequency for one or more devices in a device template. The poll frequency defined in the device template overrides the poll frequency defined for the Dynamic Application. Devices to which the device template is applied will use the poll frequency defined in the device template.
- ***Type***. Type of Dynamic Application. The choices are:
    - *Bulk Snippet Configuration*. A *single instance of the Dynamic Application* uses custom-written Python code to collect static configuration data from *multiple devices*. This is useful for systems that include a large number of component devices. For details on creating bulk snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** manual.
    - *Bulk Snippet Performance*. A *single instance of the Dynamic Application* uses custom-written Python code to collect trendable performance data from *multiple devices*. This is useful for systems that include a large number of component devices. For details on creating bulk snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** chapter of this manual.
    - *Database Configuration*. The Dynamic Application retrieves configuration data from a database application. The Dynamic Application uses SQL queries. The queried device returns table data. For details on creating database Dynamic Applications, see the ***DatabaseDynamic Application Development*** chapter of this manual.
    - *Database Performance*. The Dynamic Application retrieves trendable performance data from a database application. The Dynamic Application uses SQL queries. The queried device returns table data. For details on creating database Dynamic Applications, see the ***DatabaseDynamic Application Development*** chapter of this manual.
    - *Internal Collection Inventory*. The Internal Collection Inventory Dynamic Application (ICDA) retrieves configuration data about filesystems and interface. For filesystem, an ICDA Inventory can retrieve data such as storage size, filesystem type, and storage used. These ICDAs can also collect configuration data about interfaces, such as physical address, operational status, and IP addresses. For details on creating ICDAs, see the ***Internal Collection Dynamic Application Development*** section of this manual.

- *Internal Collection Performance*. The Internal Collection Performance Dynamic Application (ICDA) retrieves data about availability and latency, device information (system description, system uptime, system locale), filesystem performance, and interface performance. For details on creating ICDAs, see the ***Internal Collection Dynamic Application Development*** section of this manual.
- *IT Service*. A special type of Dynamic Application that Skylar One uses to monitor IT Services. When you create and edit an IT Service in the **IT Service Editor** page, Skylar One will automatically create and maintain a Dynamic Application for that IT Service. Dynamic Applications for IT Services will appear in the **Dynamic Applications Manager** page. However, if you want to edit the settings for an IT Service, you should not edit the Dynamic Application for that IT Service. Instead, use the **IT Service Editor** page to edit IT Services. For details on creating IT Service policies, see the manual ***IT Services***.
- *PowerShell Configuration*. The Dynamic Application uses PowerShell commands to collect static configuration data from a Windows device. For details on creating PowerShell Dynamic Applications, see the chapter ***Dynamic Application Development - WMI and PowerShell***. For information on configuring Skylar One and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *PowerShell Performance*. The Dynamic Application uses PowerShell commands to collect trendable performance data from a Windows device. For details on creating PowerShell Dynamic Applications, see the chapter ***Dynamic Application Development - WMI and PowerShell***. For information on configuring Skylar One and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *Snippet Configuration*. The Dynamic Application uses custom-written Python code to collect configuration data from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** chapter of this manual.
- *Snippet Journal*. The Dynamic Application uses custom-written Python code to collect data formatted as log entries from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** chapter of this manual.
- *Snippet Performance*. The Dynamic Application uses custom-written Python code to collect trendable performance data from a device. For details on creating snippet Dynamic Applications, see the ***Snippet Dynamic Application Development*** chapter of this manual.
- *SNMP Configuration*. The Dynamic Application uses SNMP to retrieve static, configuration data from devices or applications. For details on creating SNMP Dynamic Applications, see the ***SNMP Dynamic Application Development*** chapter of this manual.
- *SNMP Performance*. The Dynamic Application uses SNMP to retrieve trendable performance data from devices or applications. For details on creating SNMP Dynamic Applications, see the ***SNMP Dynamic Application Development*** chapter of this manual.
- *SOAP Configuration*. The Dynamic Application uses XML and SOAP to retrieve static configuration data from a SOAP server. The queried device returns XML data. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter of this manual.

- *SOAP Performance*. The Dynamic Application uses XML and SOAP to retrieve trendable performance data from a SOAP server. The queried device returns XML data. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter of this manual.
- *WMI Configuration*. The Dynamic Application retrieves configuration information from either WMI or WBEM running on a managed device. WMI Dynamic Applications use a query format to request data from a managed device. WBEM Dynamic Applications use wbemcli and HTTP to request data from a managed device. For details on creating WMI Dynamic Applications, see the chapter ***Dynamic Application Development - WMI and PowerShell***. For information on configuring Skylar One and external systems to use PowerShell Dynamic Applications, see the manual ***Monitoring Windows Systems with PowerShell*** and ***Monitoring Windows Systems with WMI***.
- *WMI Performance*. The Dynamic Application retrieves trendable performance data from either WMI or WBEM running on a managed device. WMI Dynamic Applications use a query format to request data from a managed device. WBEM Dynamic Applications use wbemcli and HTTP to request data from a managed device.
- *XML Configuration*. The Dynamic Application uses HTTP GET queries. The queried device returns static configuration data in XML format. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter.
- *XML Performance*. The Dynamic Application uses HTTP GET queries. The queried device returns trendable performance data in XML format. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter.
- *XSLT Configuration*. The Dynamic Application uses XML and SOAP to retrieve static configuration data from a SOAP server. The requests used to retrieve data are generated by performing an XSLT transformation on an XML document that contains data already collected by the Dynamic Application. The queried device returns XML data, which must be changed to a specific format by performing a second XSLT transformation. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter.
- *XSLT Performance*. The Dynamic Application uses XML and SOAP to retrieve trendable performance data from a SOAP server. The requests used to retrieve data are generated by performing an XSLT transformation on an XML document that contains data already collected by the Dynamic Application. The queried device returns XML data, which must be changed to a specific format by performing a second XSLT transformation. For details on creating SOAP Dynamic Applications, see the ***XML, SOAP, and XSLT Dynamic Application Development*** chapter.

- ***State***. Specifies whether the Dynamic Application is *Enabled* or *Disabled*.
- ***Version***. Version number to assign to the Dynamic Application. You can customize this value and increment it according to your change management policies.
- ***ID***. Unique application ID, assigned by Skylar One.

- ***Subscribers***. Number of devices on which the Dynamic Application is enabled to collect data. Clicking on the icon leads to the **Application Subscribers** modal, where you can view the list of devices and access other pages for each subscriber device. You can also access this page by selecting the wrench icon (🔧) for a Dynamic Application and selecting the **[Subscribers]** tab.
- ***PowerPack***. Specifies whether or not the Dynamic Application is included in a PowerPack.
- ***Environment***. The execution environment to which the Dynamic Application is aligned, if it is a snippet or internal collection Dynamic Application. If it is not a snippet or internal collection Dynamic Application, then this column displays "n/a".
- ***Collects***. Number of objects included in the Dynamic Application. Clicking on the icon (✏) leads to the **Collection Objects** page, where you can view the list of collection objects and edit their properties.
- ***Alerts***. Number of custom alerts defined for the Dynamic Application. Clicking on the icon (✏) leads to the **Alert Objects** page, where you can view and edit each alert defined for the Dynamic Application.
- ***Events***. Number of events associated with the Dynamic Application. Clicking on the icon (✏) leads to the **Event Policy Manager** page, where you can view information about each event definition associated with the Dynamic Application definition and edit each event definition.
- ***Thresh***. Number of threshold objects defined for the Dynamic Application. Clicking on the icon (✏) leads to the **Threshold Objects** page, where you can view and edit information about each threshold object defined for the Dynamic Application.
- ***Edited By***. Username of the person who created or last edited the Dynamic Application.
- ***Last Edit***. Date that the Dynamic Application was created or last edited.

Managing the Dynamic Applications Aligned to a Device

You can view detailed data about a specific device by clicking the device name on the **Devices** page (🖥) to open the **Device Investigator** page for that device.

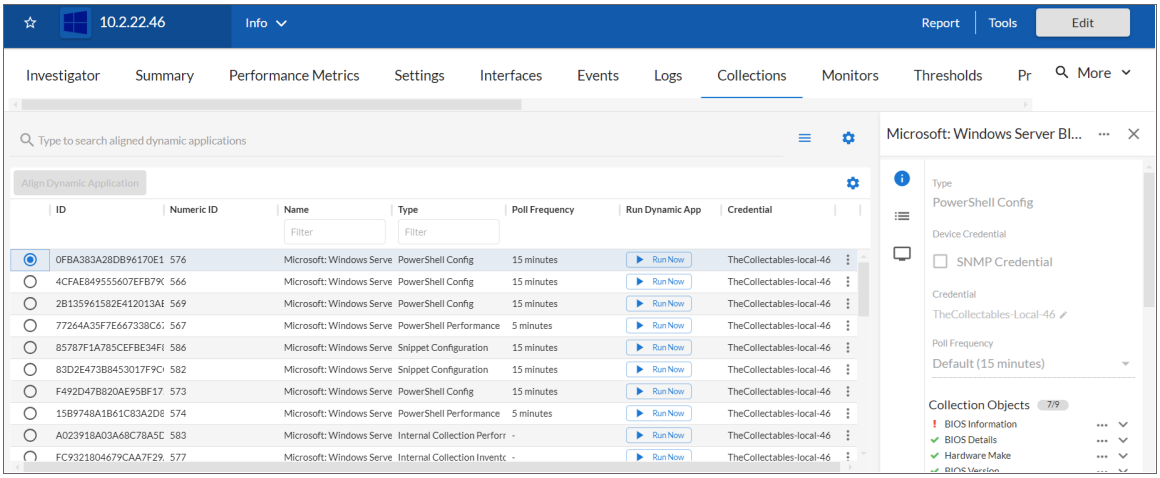
The **[Collections]** tab of the **Device Investigator** displays a list of the Dynamic Applications associated with the device.

This section describes how to view and manage the Dynamic Applications associated with a device using the **[Collections]** tab of the **Device Investigator**.

IMPORTANT: Even if you turn off data collection for a device, that device still consumes a single ScienceLogic device license. For more information, see the *Non-billable Devices* section.

Viewing the List of Dynamic Applications Aligned to a Device

On the **[Collections]** tab of the **Device Investigator**, you can view a list of the Dynamic Applications associated with the device.



TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

For each Dynamic Application in the list, the **[Collections]** tab displays the following information:

- ***ID***. The globally unique ID number (GUID) assigned to the Dynamic Application by Skylar One.
- ***Numeric ID***. The numeric integer ID number for the Dynamic Application, which can be used to correlate Dynamic Applications to system log messages.
- ***Name***. Name of the Dynamic Application.
- ***Type***. The protocol used by the Dynamic Application (Database [SQL], Internal Collection Inventory or Internal Collection Performance (ICDA), Snippet [Python], SNMP, SOAP, WMI, XML, or XSLT) and the type of data collected by the Dynamic Application (Configuration, Performance, or Journal).
- ***Credential***. Name of the credential that Skylar One uses to access the device and retrieve the data specified in the Dynamic Application.

NOTE: Cache-consuming Dynamic Applications do not require a credential. If you aligned a cache-consuming Dynamic Application in the **Align Dynamic Application** modal page, the ***Credential*** field displays *N/A* and is grayed out. You do not have to select a credential in the **Align Dynamic Application** modal page.

- ***Poll Frequency***. Frequency at which Skylar One will query the device to retrieve the data specified in the Dynamic Application. Each Dynamic Application includes a default frequency. From this page (the **[Collections]** tab), if you have the proper user permissions, you can change the poll frequency for a Dynamic Application on the current device. This edited poll frequency will override the default frequency for the Dynamic Application and the poll frequency defined for a Dynamic Application in one or more device templates.

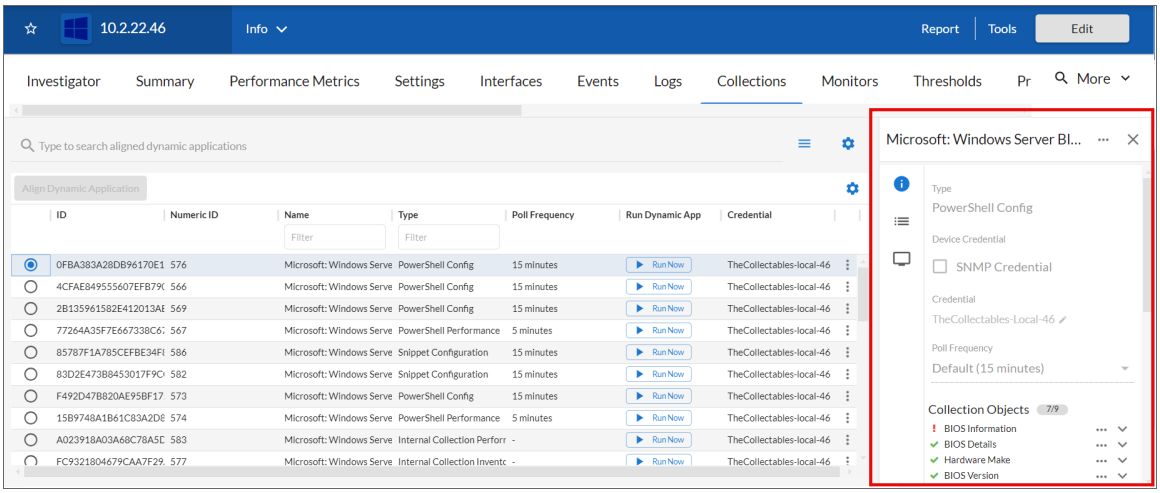
TIP: To rearrange the columns in the list, click and drag the column name to a new location. You can adjust the width of a column by clicking and dragging the right edge of the column. For more information about editing and adding columns, see "Editing the Settings for an Inventory Page" in the ***Introduction to Skylar One*** manual.

On the **[Collections]** tab, you can:

- *View information about a Dynamic Application*
- *Change the credential for a Dynamic Application*
- *Update the poll frequency for a Dynamic Application*
- *Align or unalign Dynamic Applications with the device*
- *View the collection status for a Dynamic Application*
- *Enable or disable collection for the device's Dynamic Applications*
- *Enable or disable collection for individual collection objects within a Dynamic Application*
- *Run a Dynamic Application*

Viewing Information about a Dynamic Application Aligned to a Device

To view more information about a Dynamic Application that is aligned to the device, select that Dynamic Application from the list on the **[Collections]** tab. An information pane with details about that Dynamic Application appears on the right side of the page:



This information pane includes three sections:

- ***Info*** (). This section provides basic information about the Dynamic Application. From here, if you have the proper user permissions, you can also *change the Dynamic Application's credential* and *update its poll frequency*.
- ***Collection Objects*** (). This section lists the Dynamic Application's collection objects. Each collection object in a Dynamic Application specifies a data point that Skylar One will attempt to collect.
- ***Presentation Objects*** (). This section lists the Dynamic Application's presentation objects. Presentation objects define how Skylar One should present data for performance or journal Dynamic Applications.

You can click the expand icon () next to each collection object and presentation object to see additional information about that object, including its collection status. For more information, see the section on *Viewing the Status of a Dynamic Application*.

If you have the proper user permissions, you can also enable or disable collection for certain collection objects. For more information, see the section on *Enabling and Disabling Collection for Specific Collection Objects*.

Changing the Credential for a Dynamic Application Aligned to a Device

If you have the proper user permissions, you can use the information pane for a Dynamic Application listed on the **[Collections]** tab to change the credential aligned to that Dynamic Application.

To change the credential for a Dynamic Application aligned to a device:

1. On the **[Collections]** tab of the **Device Investigator**, click **[Edit]** and select the Dynamic Application you want to update. The information pane for the Dynamic Application appears.
2. If *SNMP Credential* is checked currently in the ***Device Credential*** field, uncheck the checkbox. The ***Credential*** field appears below it.
3. In the ***Credential*** field, click the edit icon (). The **Choose Credential** modal page appears.

4. In the **Choose Credential** modal page, search for the credential you want to align with the Dynamic Application and select it from the list, then click **[Select]**. Your selected credential appears in the ***Credential*** field.
5. Click **[Save]**.

Updating the Poll Frequency for a Dynamic Application Aligned to a Device

If you have the proper user permissions, you can use the information pane for a Dynamic Application listed on the **[Collections]** tab to change the default poll frequency at which the Dynamic Application queries the device for data.

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

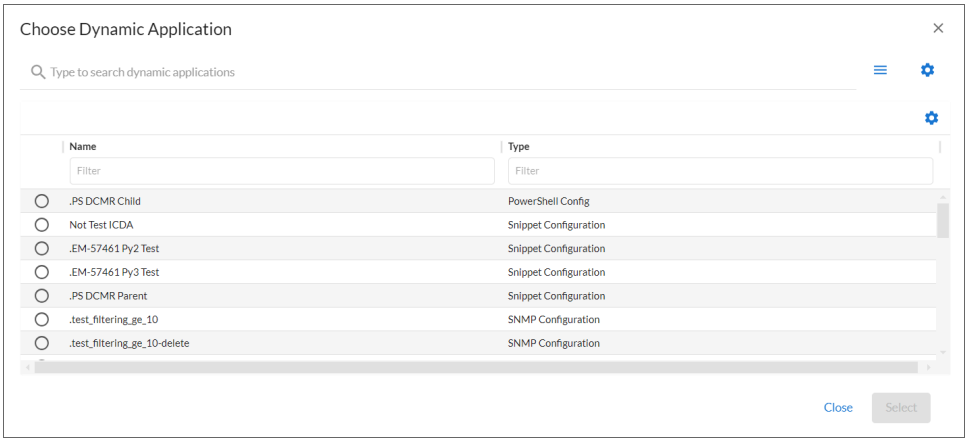
1. On the **[Collections]** tab of the **Device Investigator**, click **[Edit]** and select the Dynamic Application you want to update. The information pane for the Dynamic Application appears.
2. From the ***Poll Frequency*** drop-down, select how often you want the Dynamic Application to collect data from the device. Your options range from *1 minute* to *24 hours*, or you can select *Default* to not change the frequency.
3. Click **[Save]**.

Manually Aligning a Dynamic Application to a Device

If you have the proper user permissions, you can manually align a new Dynamic Application to a device or unalign a currently aligned Dynamic Application from a device.

To align a Dynamic Application to a device:

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



TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

TIP: You can adjust the size of the rows and the size of the row text on this inventory page. For more information, see the section on *Adjusting the Row Density* in the ***Introduction to Skylar One*** manual.

3. Select the Dynamic Application you want to align and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. If a default credential is listed below the Dynamic Application and you want to use that credential, skip ahead to step 7. Otherwise, uncheck the box next to the credential name.
5. Click *Choose Credential*. The **Choose Credential** window appears.
6. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

TIP: To *unalign* a Dynamic Application from a device, click the **[Actions]** button (⋮) for that Dynamic Application and select *Unalign Dynamic App*. However, be advised that when you unalign a Dynamic Application, you also delete the data it has collected.

Viewing the Status of a Dynamic Application Aligned to a Device

The **[Collections]** tab of the **Device Investigator** displays the status of each collection object within each Dynamic Application aligned to a device.

The following icons represent the different collection statuses:

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

For more information about these status, see the sections on the *Found status* and the *Collecting status*.

NOTE: Before determining which collection objects defined in a Dynamic Application will be collected, Skylar One determines whether the Dynamic Application itself should be collected. Dynamic Applications are not collected for devices that are unavailable (because of a failed availability check) or have collection disabled (either manually by a user or because of maintenance scheduled in Skylar One), regardless of the ***Collecting*** value of the objects.

Understanding the Found Status

The ***Found*** status for a collection object indicates whether data has ever been successfully collected for that object from that specific device.

For a presentation object, the ***Found*** status indicates whether every collection object used by that presentation object has a ***Found*** value of *Yes*.

After ***Found*** is set to *Yes* for an object, Skylar One will never automatically change the value of ***Found*** for this object.

The value of ***Found*** is used by Skylar One to determine whether icons, tabs, and Navbar links that lead to the **[Performance]** or **[Configs]** page where the collection object is used should be active.

NOTE: After the Dynamic Application is enabled, its Discovery Object displays as *Not found and collecting* in the Skylar One user interface, with a yellow question mark icon (?) next to it. No further action is needed in this situation.

Understanding the Collecting Status

The ***Collecting*** status for a collection object indicates whether Skylar One will attempt to collect data for this object when collection for this Dynamic Application occurs. For information about how Skylar One determines the ***Collecting*** status, see the section on *How Skylar One Manages the Collection Status for Dynamic Applications*.

If you have the proper user permissions, you can disable or enable collection for individual collection objects. For more information, see the section on *Enabling and Disabling Collection for Specific Collection Objects*.

For a presentation object, the ***Collecting*** status indicates whether every collection object used by that presentation object has a ***Collecting*** value of *Yes*. If a collection object has a ***Collecting*** value of *No*, then every presentation object that uses that collection object will also have a ***Collecting*** value of *No*.

Conversely, the ***Collecting*** status for a presentation object has no effect upon its collection objects. If you manually change the ***Collecting*** status for a presentation object, the ***Collecting*** status for the collection objects used by the presentation object will not change.

Enabling and Disabling Dynamic Application Data Collection for a Device

If you have the proper user permissions, you can disable data collection for a particular Dynamic Application on a specific device. This will affect collection only for that Dynamic Application on that device. For all other subscriber devices, Skylar One will continue to use the Dynamic Application to collect data.

To disable or enable all collection for a Dynamic Application:

1. On the **[Collections]** tab for the device, click **[Edit]**.
2. To disable collection for a Dynamic Application, click the **[Actions]** button (⋯) for that Dynamic Application and select *Disable Collection*. To enable collection for a disabled Dynamic Application, click the **[Actions]** button (⋯) and select *Enable Collection*.
3. Click **[Save]**.

IMPORTANT: Even if you turn off data collection for a device, that device still consumes a single ScienceLogic device license. For more information, see the *Non-billable Devices* section.

Enabling and Disabling Collection for Specific Collection Objects

If you have the proper permissions, you can disable data collection for specific collection objects within a Dynamic Application that is aligned to a device. Doing so will affect collection only for that collection object within that Dynamic Application for that specific device; the collection status will not change for any other collection objects, Dynamic Applications, or devices. For all other devices, Skylar One will use the default list of objects from the Dynamic Application's definition or will use the list of objects defined on the **[Collections]** tab for that device.

To disable or enable collection for specific collection objects within a Dynamic Application:

1. On the **[Collections]** tab for a device, click **[Edit]** and select the Dynamic Application you want to update. The information pane for the Dynamic Application appears.
2. To disable collection for an individual collection object, click the **[Actions]** button (⋯) for that object in the information pane and select *Disable Collection*. To enable collection for a disabled object, click the **[Actions]** button (⋯) and select *Enable Collection*.
3. Click **[Save]**.

Running a Dynamic Application on a Device

On a single device, you can perform a test run of collection with a single Dynamic Application, if you have the proper user permissions. During this test run, Skylar One displays details of each step of the collection process. This information can be very helpful for troubleshooting and debugging.

NOTE: During a test run of a collection with a Dynamic Application, Skylar One does not store the collected data or generate alerts. Skylar One will continue to collect data and generate alerts using the selected Dynamic Application at the frequency defined in the Dynamic Application.

To execute a test run of collection with a single Dynamic Application:

1. On the **[Collections]** tab for the device, do one of the following:
   - Click the **[Run Now]** button in the ***Run Dynamic App*** column.
   - Click the **[Actions]** button (···) for the Dynamic Application that you want to run and select *Run Now*.
   - Select the Dynamic Application from the list to open its information pane. On the information pane, click the **[Actions]** button (···) and then select *Run Now*.
2. A status window displays the status and relevant logs for the Dynamic Application.

Managing the Dynamic Applications Associated with a Device in the Classic Skylar One User Interface

This section describes how to view and manage the Dynamic Applications associated with a device using the **Dynamic Application Collections** page in the classic Skylar One user interface.

Viewing the Dynamic Applications Associated with a Device in the Classic Skylar One User Interface

To view the Dynamic Applications associated with a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to view Dynamic Applications. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Collections]** tab.
4. The **Dynamic Application Collections** page displays a list of all Dynamic Applications aligned with the current device. For each Dynamic Application, the **Dynamic Application Collections** page displays the following read-only information:
   - ***Plus Sign*** ( ). Clicking on this icon displays a list of all Presentation Objects included in Dynamic Applications of type "Performance" and "Journal" or a list of all Collection Objects included in Dynamic Applications of type "Configuration". You can click on the plus sign next to each Presentation Object to see all the Collection Objects included in the Presentation Object.
   - ***Minus Sign*** ( ). Collapses a Dynamic Application and hides the display of Presentation Objects and Collection Objects.

- ***Dynamic Application***. Name of the Dynamic Application.
- ***ID***. Numeric ID for the Dynamic Application.
- ***Poll Frequency***. Frequency at which Skylar One will query the device to retrieve the data specified in the Dynamic Application. Each Dynamic Application includes a default frequency. From this page (**Dynamic Application Collections**), you can change the poll frequency for a Dynamic Application on the current device. This edited poll frequency will override the default frequency for the Dynamic Application and the poll frequency defined for a Dynamic Application in one or more device templates.
- ***Type***. The protocol used by the Dynamic Application (Database [SQL], Internal Collection Inventory or Internal Collection Performance (ICDA), Snippet [Python], SNMP, SOAP, WMI, XML, or XSLT) and the type of data collected by the Dynamic Application (Configuration, Performance, or Journal).
- ***Credential***. Name of the credential that Skylar One uses to access the device and retrieve the data specified in the Dynamic Application.

NOTE: Cache-consuming Dynamic Applications do not require a credential. If you aligned a cache-consuming Dynamic Application in the **Dynamic Application Alignment** modal page, the ***Credential*** field displays *N/A* and is grayed out. You do not have to select a credential in the **Dynamic Application Alignment** modal page.

- ***Collector***. Name of the specific Data Collector used to collect data from the Dynamic Application.

NOTE: Based on the Dynamic Application's ***Collector Affinity*** settings, the Dynamic Application might be assigned to a different Data Collector than the Data Collector that is assigned to the device in the Device Properties page (Devices > Classic Devices > wrench icon). In the **Dynamic Application Collections** page, hover your mouse over the ***Collector*** name for any of the Collection Objects to view a tooltip that explains why the Dynamic Application is assigned to its particular Data Collector.

- ***Run Dynamic Application*** (⚡). Performs a test run of data collection for the selected Dynamic Application on the current device.

NOTE: If a device is currently unavailable, the lightning-bolt icon (⚡) will be grayed out for each Dynamic Application aligned with the device.

- ***Checkbox*** (☐). Apply an action from the ***Select Action*** field to this instance of the Dynamic Application.

Manually Associating a Dynamic Application with a Device in the Classic Skylar One User Interface

From the **Dynamic Application Collections** page, you can manually associate a new Dynamic Application with a device.

To manually associate a Dynamic Application with a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device you want to associate with a Dynamic Application. Click its wrench icon (🔧).
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Actions]** menu and select *Add Dynamic Application*.
5. The **Dynamic Application Alignment** modal page appears. To align a Dynamic Application with a device in this page:
    - Select the Dynamic Application you want to align with the device in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
    - After selecting a Dynamic Application, you must select a credential. Select a credential in the ***Credentials*** field. You can filter the list of credentials using the search field above the ***Credentials*** field.

    NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

    NOTE: Cache-consuming Dynamic Applications **do not** require a credential. If you selected a cache-consuming Dynamic Application in the **Dynamic Application Alignment** modal page, the ***Credential*** field displays *N/A* and is grayed out. You do not have to select a credential in the **Dynamic Application Alignment** modal page.

6. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
7. Skylar One will associate the Dynamic Application with the device and immediately attempt to collect the data specified in the Dynamic Application using the selected credential.
8. After the first, immediate collection, Skylar One will collect the data at the frequency defined in the ***Polling Frequency*** field in the **Application Configuration Editor** page for the Dynamic Application.

Editing the Credential Associated with a Dynamic Application in the Classic Skylar One User Interface

From the **Dynamic Application Collections** page, you can change the credential associated with a Dynamic Application. This credential will be used by Skylar One for this specific Dynamic Application associated with this specific device . For all other devices, Skylar One will use the default credential associated with the device, or will use the credential defined in the **Dynamic Application Collections** page for each device.

> **NOTE**: Cache-consuming Dynamic Applications do not require a credential. If you aligned a cache-consuming Dynamic Application with this device (you do this in the **Dynamic Application Alignment** modal page), the ***Credential*** field displays *N/A* and is grayed out.

To change the credential associated with a Dynamic Application for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to define a credential. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, find the Dynamic Application for which you want to change the credential. Select its checkbox. To apply a credential to multiple Dynamic Applications, select the checkbox for each Dynamic Application.
5. From the ***Select Action*** drop-down list, select the credential from the list of all credentials that you are allowed to use, and then select the **[Go]** button.

   > **NOTE:** Your organization membership(s) might affect the list of credentials you can see in the ***Select Action*** drop-down list.

   > **NOTE:** If this Dynamic Application has already been aligned with a credential to which you do not have access, the ***Credential*** column will display the value *Restricted Credential*. If you align the device with a different credential, you will not be able to re-align the device with the *Restricted Credential*.

6. You should see your change reflected in the ***Credential*** column in the **Dynamic Application Collections** page.

Viewing the Status of a Dynamic Application Associated with a Device in the Classic Skylar One User Interface

For each device, Skylar One maintains the collection status for each collection object in each Dynamic Application aligned with that device. The **Dynamic Application Collections** page displays the status of each collection object for a device as represented by two values: ***Found*** and ***Collect***. The **Dynamic Application Collections** page also displays the ***Found*** and ***Collect*** values for each presentation object, which are derived from the status of each collection object used by the presentation object.

Found

The ***Found*** status for a collection object has two possible values:

- *Yes*. Data has been successfully collected from this device for this object. ***Found*** is set to *Yes* the first time data is successfully collected from this device for this object.
- *No*. Data has never been successfully collected from this device for this object. *No* is the initial value of ***Found*** for every object when a Dynamic Application is initially aligned with a device.

The ***Found*** status for a presentation object also has two possible values (*Yes* and *No*).

- ***If the presentation object uses only one collection object***, the presentation object always has the same default ***Found*** and default ***Collect*** values as that collection object.
- ***If a presentation object uses multiple collection objects***, the default ***Found*** value for the presentation object will be *Yes* only if all the collection objects used by the presentation object have a ***Found*** value of *Yes*.

After ***Found*** is set to *Yes* for an object, Skylar One will never automatically change the value of ***Found*** for this object.

The value of ***Found*** is used by Skylar One to determine whether icons, tabs, and Navbar links that lead to the **[Performance]** or **[Configs]** page where the collection object is used should be active.

Collect

The ***Collect*** status for a collection object has two possible values:

- *Yes*. Skylar One will attempt to collect data for this object when collection for this Dynamic Application occurs. *Yes* is the initial value for ***Collect*** for every object when a Dynamic Application is initially aligned with a device.
- *No*. Skylar One will not attempt to collect data for this object when collection for this Dynamic Application occurs. Skylar One might set ***Collect*** to *No* automatically if no data has been collected.
- If a collection object has a ***Collect*** value of *No*, all presentation objects that use that collection object will also have a ***Collect*** value of *No*.

The ***Collect*** status for a presentation object also has two possible values (*Yes* and *No*).

- ***If the presentation object uses only one collection object***, the presentation object always has the same default ***Found*** and default ***Collect*** values as that collection object.

- ***If a presentation object uses multiple collection objects***, the default ***Collect*** value for the presentation object will be *Yes* only if ***all*** the collection objects used by the presentation object have a ***Collect*** value of *Yes*. If one or more collection objects used by the presentation object have a ***Collect*** value of *No*, the presentation object will also have a default ***Collect*** value of *No*.
- The ***Collect*** status for a presentation object has no effect upon its collection objects. If you manually change the ***Collect*** status for a presentation object, the ***Collect*** status for the collection objects used by the presentation object will not change.

> **NOTE:** Before determining which collection objects defined in a Dynamic Application will be collected, Skylar One determines whether the Dynamic Application itself should be collected. Dynamic Applications are not collected for devices that are unavailable (because of a failed availability check) or have collection disabled (either manually by a user or because of maintenance scheduled in Skylar One) regardless of the ***Collect*** value of the objects.

Performing Other Administrative Tasks for an Aligned Dynamic Application in the Classic Skylar One User Interface

You can perform the following other administrative tasks for an aligned Dynamic Application in the **Dynamic Application Collections** page:

- Enable or disable one or more collection objects or presentation objects.
- Stop data collection for the whole Dynamic Application.
- Reset the statistical data that has been stored for standard deviation alerting.
- Reset persistent session objects that have been collected and stored for a Dynamic Application.
- Test collection for a Dynamic Application.
- Remove all data collected using the Dynamic Application and optionally unalign the Dynamic Application from the device.

To perform one of these tasks:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to perform an administrative task. Select its wrench icon (🔧).
3. In the **Device Administration** panel, select the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, find the Dynamic Application for which you want to perform an administrative task. The following sections describe how to perform each task.

Enabling or Disabling Objects

From the **Dynamic Application Collections** page, you can customize the collection performed by the Dynamic Application for the current device. This customization will be used by Skylar One only for this

specific device. For all other devices, Skylar One will use the default list of objects from the Dynamic Application's definition or will use the list of objects defined in the **Dynamic Application Collections** page for that device.

> **NOTE:** If a collection object has a ***Collect*** value of *No*, all presentation objects that use that collection object will also have a ***Collect*** value of *No*.

To enable or disable collection for one or more objects in a Dynamic Application:

- ***To disable collection for one or more collection objects***, unselect the checkbox for each object for which you want to disable collection.
- For each unselected object, the ***Collect*** column should now display *No*.
- ***To enable collection for one or more collection objects***, select the checkbox for each object for which you want to enable collection.
- For each selected object, the ***Collect*** column should now display *Yes*.
- Select the **[Save]** button.

> **NOTE**: If a user **manually** sets the ***Collect*** status of a collection object or presentation object to *No*, Skylar One will **not** attempt to re-collect the object once a day and will **not** automatically set the ***Collect*** status to *Yes*.

Restarting Automatic Maintenance of Collection Objects

If a user **manually** sets the ***Collect*** status of a collection object or presentation object, Skylar One will **not** automatically change the ***Collect*** status of that object as described in the *How Skylar One Manages Collect Status* section.

If you want Skylar One to restart automatic maintenance of the objects in a Dynamic Application, perform the following steps:

1. In the **Dynamic Application Collections** page, select the checkbox for the Dynamic Application for which you want to restart automatic collection maintenance. To restart automatic collection maintenance for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the ***Select Action*** drop-down list, select *Restore System Control of Collection State* and then select the **[Go]** button.
3. Automatic collection maintenance for all objects in the Dynamic Application will now occur. The ***Collect*** status of the objects in the Dynamic Application will not change immediately.

Editing the Poll Frequency for a Dynamic Application on the Current Device

Poll Frequency is the frequency at which Skylar One will query the device to retrieve the data specified in the Dynamic Application. Each Dynamic Application includes a default frequency.

From the **Dynamic Application Collections** page, you can change the poll frequency for a Dynamic Application on the current device. For the current device, the edited poll frequency will override:

- the default frequency for the Dynamic Application.
- the poll frequency defined for a Dynamic Application in one or more device templates.

To edit the poll frequency for a Dynamic Application on the current device:

1. In the **Dynamic Application Collections** page, select the checkbox for the Dynamic Application for which you want to change the poll frequency. To change the poll frequency for multiple Dynamic Applications, select the checkbox for each Dynamic Application.
2. From the ***Select Action*** drop-down list, select *Poll Frequency* from the list of poll frequencies and then select the **[Go]** button.
3. You should see your change reflected in the ***Poll Frequency*** column in the **Dynamic Application Collections** page.

Stopping Data Collection for a Dynamic Application

You can stop data collection for a Dynamic Application on the current device. This will affect collection only for this specific device. For all other subscriber devices, Skylar One will continue to use this Dynamic Application to collect data.

To stop data collection for a Dynamic Application on this device:

1. Select the checkbox of each Dynamic Application for which you want to stop data collection.
2. From the ***Select Action*** drop-down list, select the following:
    - ***Disable All Collection Objects***. For all collection objects in the selected Dynamic Application (s), the ***Collect*** value will be set to *No*.
3. Select the **[Go]** button.

> **NOTE**: If a user manually sets the ***Collect*** status of a collection object or presentation object to *No*, Skylar One will not attempt to re-collect the object once a day and will not set the ***Collect*** status to *Yes*.

Resetting Statistical Data for a Dynamic Application

Skylar One allows you to examine the value of an object and trigger an alert if that value falls outside the range of "normal" values for that object at that hour of the day on that day of the week. The deviation function allows you to define such alerts.

To use the deviation function, you must configure Skylar One to store and calculate the mean values and standard deviation for an object. You do this by selecting the ***Enable Deviation Alerting*** field in the **Collection Objects** page. You then specify the minimum and maximum number of weeks to collect deviation data for the object. Skylar One must have already collected at least the minimum number of weeks' worth of values for an object before Skylar One will evaluate alert formulas that use the deviation function. To use the deviation function, you must specify a minimum value of at least two weeks.

In some cases, you might want to delete all the collected statistics for an object and start over. This is useful if known circumstances change the value of an object, and you no longer want to use the old data to calculate the "normal" ranges. You can do this by "resetting" the statistical data for an object.

For example, suppose you were monitoring bandwidth usage with a standard deviation alert. Suppose your company previously ran on a 09:00 to 17:00 work schedule. Suppose your company has recently added a nightshift to the schedule. In this circumstance, you might want to reset the statistical data to determine the new "normal" usage patterns.

When you reset the statistical data for an object, you are telling Skylar One to ignore all previously collected values and to use only values from today onward. When you reset the statistical data for an object, the **Dynamic Application Collections** page will again display a message like:

```
Note: object 123 not ready for deviation alerting.
```

until enough data has been collected to again calculate standard deviation for the object. Skylar One will again start collecting the minimum number of weeks of data for the object (as specified in the ***Enable Deviation Alerting*** field in the **Collection Objects** page) and calculating the "normal" ranges for those objects for each hour at each day of the week.

To delete all current statistical data for an object:

1. In the Dynamic Application, find the object for which you want to reset data.
2. In that Dynamic Application, find the object for which you want to reset data. Select its checkbox.
3. From the ***Select Action*** drop-down list, select the following option:
    - *Reset Statistical Data*. Removes all previously collected statistical data for the selected object. Skylar One will again start collecting the minimum number of weeks of data for the object (as specified in the ***Enable Deviation Alerting*** field in the **Collection Objects** page) and calculating the "normal" ranges for those objects for each hour at each day of the week.
4. Select the **[Go]** button.
5. The **Dynamic Application Collections** page will display a message like:

    ```
    Note: object 123 not ready for deviation alerting.
    ```

Resetting Persistent Session Objects for a Dynamic Application

SOAP or XSLT Dynamic Applications can contain a collection object that stores a Session ID. The value for this collection object can be defined as a persistent value. If Skylar One has already retrieved and stored a value in the collection object for the Session ID, Skylar One will not collect a new value for the collection object until a SOAP fault occurs. You can force Skylar One to re-collect a Session ID collection object by deleting the current persistent value.

To delete the current persistent value for a session object:

1. In the Dynamic Application, find the object for which you want to reset data. Select its checkbox.
2. From the ***Select Action*** drop-down list, select *Reset Persistent Session Objects*. Removes the stored value for collection objects of type ***SOAP/XSLT Session ID***. ***SOAP/XSLT Session ID*** objects are persistent across collection periods; Skylar One does not collect a ***SOAP/XSLT Session ID*** object if a collected value is available from a previous poll. After selecting this option,

Skylar One will delete the existing value for the object and collect a new value during the next collection.

3. Select the **[Go]** button.

Testing Data Collection for a Dynamic Application

On a single device, you can perform a test-run of collection with a single Dynamic Application. During this test run, Skylar One displays details of each step of the collection process. This information can be very helpful for troubleshooting and debugging.

> **NOTE:** During a test run of a collection with a Dynamic Application, Skylar One does not store the collected data or generate alerts. Skylar One will continue to collect data and generate alerts using the selected Dynamic Application at the frequency defined in the Dynamic Application.

To execute a test run of collection with a single Dynamic Application:

1. Locate the device on which you want to test the Dynamic Application and click its wrench icon ( ).
2. Click the **Collections** tab.
3. Find the Dynamic Application for which you want to test collection and click its lightning bolt icon ( ).

> **NOTE:** If a device is currently unavailable, the lightning bolt icon ( ) will be grayed out for each Dynamic Application aligned with the device.

4. Skylar One displays a **Session Logs** modal that includes details about each step of the collection process and diagnostic details about alerts in the Dynamic Application. This information can be helpful during troubleshooting.

Removing Data Collected by a Dynamic Application

You can remove the data retrieved with a Dynamic Application from the current device. You have two options for removing Dynamic Application data associated with a device:

- Remove all previously collected data, but continue to collect data at the specified polling frequency.
- Remove all normalized data, but retain all raw collected data and continue to collect data at the specified polling frequency.
- Remove all previously collected data and stop collecting data with this Dynamic Application. This unaligns the device from the Dynamic Application. The device will no longer be a subscriber to the Dynamic Application.

To remove Dynamic Application data associated with a device:

1. In the **Dynamic Application Collections** page, select the checkbox of the Dynamic Application for which you want to remove data. To remove data for multiple Dynamic Applications, select the

checkbox for each Dynamic Application.

2. From the ***Select Action*** drop-down list, select one of the following options:
   - ***Remove Data***. Removes all previously collected data, but data will continue to collect at the specified polling frequency.
   - ***Remove Normalized Data***. Removes all normalized data, but all raw collected data is retained and data will continue to collect at the specified polling frequency.
   - ***Stop Collection and Remove Data***. Removes all previously collected data and stops collection of data with this Dynamic Application. This "unaligns" the device from the Dynamic Application. The device is no longer considered a subscriber to the Dynamic Application. If you perform this option and later want to subscribe to this Dynamic Application again, you must re-align the device with the Dynamic Application.
3. Select the **[Go]** button.

How Skylar One Manages the Collection Status for Dynamic Applications

This section describes how Skylar One manages collection for Dynamic Applications, including the conditions under which it might automatically stop or restart collection. It also describes the types of collection objects for which it will never automatically change the collection status.

Stopping Collection

One of the ScienceLogic hourly maintenance tasks checks the last collection time for every collection object being collected from every device. If the last collection time for an object on a device is more than 48 hours ago, collection is stopped for that collection object on that device. Skylar One will set the ***Collect*** status of that object to *No*.

NOTE: If a device is in maintenance mode, is unavailable, or has been manually disabled by a user, Skylar One will not automatically set the ***Collect*** status of objects to *No*. Skylar One will automatically set the ***Collect*** status of objects to *No* only if the device is up and running, but Skylar One still cannot collect the object.

When Skylar One sets the ***Collect*** status of that object to *No*, Skylar One generates an event. The event will include the name of the device, the name of the Dynamic Application, the name of the collection object, and the collection object IDs. By default, this event is of severity "notice".

NOTE: For Dynamic Applications that have the ***Component Mapping*** checkbox selected in the **Dynamic Applications Properties Editor** page, Skylar One will never automatically set the ***Collect*** status to *No* for any of the collection objects in the Dynamic Application.

NOTE: For Dynamic Applications that have the ***Caching*** fields set to either *Cache Results* or *Consume cached results* in the **Dynamic Applications Properties Editor** page, Skylar One will never automatically set the **Collect** status to *No* for any of the collection objects in the Dynamic Application.

Starting Collection

For each object that has the ***Collect*** status of *No*, Skylar One will attempt to re-collect the object once a day. If re-collection is successful, Skylar One will automatically set the ***Collect*** value for that object to *Yes*.

NOTE: If a user manually sets the ***Collect*** status of a collection object or presentation object to *No*, Skylar One will **not** attempt to re-collect the object once a day and will **not** set the ***Collect*** status to *Yes*.

Collection Objects that are Excluded from Maintenance

The ***Collect*** status of the following collection objects is never changed automatically:

- Collection objects in Dynamic Applications that have the ***Component Mapping*** checkbox checked in the **Dynamic Applications Properties Editor** page.
- Collection objects in Dynamic Applications that have the ***Caching*** fields set to either *Cache Results* or *Consume cached results*, in the **Dynamic Applications Properties Editor** page.
- Collection objects that have the ***Disable Object Maintenance*** setting enabled.
- Collection objects that have a ***Collect*** status defined by a user, i.e. collection objects that were manually enabled or disabled by a user.

Status of Objects for Deviation

Skylar One allows you to examine the value of an object and trigger an alert if that value falls outside the range of "normal" values for that object at the hour of the day on that day of the week. The deviation function allows you to define such alerts.

To use the deviation function, you must configure Skylar One to store and calculate the mean values and standard deviation for an object. You do this by selecting the ***Enable Deviation Alerting*** field in the **Collection Objects** page. You then specify the minimum and maximum number of weeks to collect deviation data for the object. Skylar One must have already collected at least the minimum number of weeks' worth of values for an object before Skylar One can evaluate alert formulas that use the deviation function. To use the deviation function, you must specify a minimum value of at least two weeks.

If a Dynamic Application in the **Dynamic Application Collections** page contains one or more alerts that use the deviation function, the **Dynamic Application Collections** page displays the status of the collection objects.

For example, suppose an alert in a Dynamic Application will apply the deviation function to object "o_123". Suppose that you specified that Skylar One must collect at least two weeks' worth of deviation data for this object. Suppose that Skylar One contains only one weeks' worth of values for object "o_123". In this case, the **Dynamic Application Collections** page will display the following message:

```
Note: object 123 not ready for deviation alerting.
```

When Skylar One contains at least two weeks worth of values for object "o_123", the **Dynamic Application Collections** page will display the following message:

```
All objects ready for deviation alerting.
```

Bulk Un-Aligning Dynamic Applications

The **Application Subscribers** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to un-align a Dynamic Application from one or more subscriber-devices.

To un-align a Dynamic Application from one or more devices:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. In the **Dynamic Applications Manager** page, find an application with a subscriber icon ( ) in the ***Subscribers*** column. Click the icon.
3. The **Application Subscribers** page appears.
4. In the **Application Subscribers** page, select the checkbox for each device you want to apply the action to. To select all checkboxes for all devices, select the checkbox at the top of the page.
5. In the ***Select Action*** drop-down list, select *Unalign Device and Remove Collection Data*. This option un-aligns the device from the Dynamic Application and deletes all data collected by the Dynamic Application from the device. The device is no longer considered a subscriber to the Dynamic Application. If you perform this option and later want to subscribe to this Dynamic Application again, you must re-align the device with the Dynamic Application.
6. Click the **[Go]** button to apply the action to all selected devices.

Setting Thresholds for Dynamic Applications

If a Dynamic Application includes one or more ***thresholds***, you can change the threshold value on a per-device basis. To change a Dynamic Application threshold for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to define a threshold. Select its wrench icon ( ).
3. In the **Device Administration** panel, select the **[Thresholds]** tab.

4. The **Device Thresholds** page displays a list of thresholds defined for each Dynamic Application that is aligned to the device. To change a threshold, move the slider for that threshold or enter a value in the number field for that threshold.
5. After changing one or more thresholds, select the **[Save]** button to save your changes.

> **NOTE:** Changing a threshold in the **Device Thresholds** page affects only the current device. The threshold values defined in the Dynamic Application remain unchanged.

Dynamic Applications and Discovery

Discovery is the ScienceLogic tool that automatically discovers devices in your network. You supply the discovery tool with a range or list of IP addresses, and the discovery tool determines if a device exists at each IP address. The discovery tool also determines which (if any) Dynamic Applications to align with the device. If the discovery tool finds Dynamic Applications to align with the device, the discovery tool triggers collection for each aligned Dynamic Application.

To learn more about discovery, see the ***Discovery and Credentials*** manual.

How Does Skylar One Align Dynamic Applications During Discovery?

Most Dynamic Applications include a discovery object. A discovery object enables Skylar One to determine which devices to align with a Dynamic Application.

During discovery, Skylar One:

1. Searches the list of Dynamic Applications.
2. If a Dynamic Application includes a discovery object, Skylar One adds that Dynamic Application to the list of Dynamic Applications to try to align during discovery.
3. For each Dynamic Application that includes a discovery object, Skylar One checks the current discovery session for an appropriate credential. For example, for each database Dynamic Application, Skylar One would look for one or more database credentials that have been selected for the discovery session.
4. For each discovered device, both those that support SNMP and those that don't, discovery tries to determine which Dynamic Applications to align. For each discovered device, Skylar One tries to align each Dynamic Application in the list of Dynamic Applications to try during discovery. For each Dynamic Application in the list, Skylar One tries to connect to each device with each of the appropriate credentials (until Skylar One finds a working credential) and then tries to find the discovery object. If Skylar One is able to connect to a device with one of the credentials and can then retrieve the discovery object, Skylar One will align the Dynamic Application with the device.

NOTE: Skylar One also includes more sophisticated logic that allows you to define multiple discovery objects, validate the value of the discovery object, and to align the Dynamic Application if a discovery object is not available. However, the most common use of a discovery object is as described above (discovery object exists).

5. If discovery aligns a Dynamic Application with a device, immediately after discovery completes Skylar One will start the first collection from that device using the aligned Dynamic Application. This step is not performed for Dynamic Applications that meet all of the following three criteria:
    - Has a collection frequency of 1 minute, 2 minutes, 3 minutes or 5 minutes.
    - Does not have component mapping enabled (does not discover component devices).
    - Is aligned with a component device.

NOTE: During discovery, Skylar One tries each SNMP credential specified in the discovery session on each discovered device, to determine if Skylar One can collect SNMP details from the device. Later in the discovery session, during alignment of Dynamic Applications, discovery again tries each SNMP credential specified in the discovery session. If one of the SNMP credentials times out three times ***without any response***, discovery will stop trying to use that SNMP credential to align SNMP Dynamic Applications. Note that "no response" means that a device did not respond at all. Note that if a device reports that "no OID was found" or "the end of the OID tree was reached", these are considered a legitimate response and would not cause Skylar One to abandon the credential.

Queuing Discovery from the Dynamic Applications Manager Page

From the **Dynamic Applications Manager** page, you can manually run the Dynamic Application alignment portion of discovery for all devices in the system using one or more selected Dynamic Applications.

To manually queue discovery from the **Dynamic Applications Manager** page:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Dynamic Applications).
2. In the **Dynamic Applications Manager** page, select the checkbox for each Dynamic Application you want to use for discovery.
3. In the ***Select Action*** drop-down list, select *Discover Applications*. Select the **[Go]** button.
4. You can also run the Dynamic Application alignment portion of discovery for all devices in the system using a single Dynamic Application. To do this, select the lightning bolt icon ( ) for that Dynamic Application.

Chapter 11

Device Thresholds and Data Retention

Overview

Skylar One allows users to define performance thresholds for devices. When these thresholds are exceeded, Skylar One generates an ***event***. Events are messages that are triggered when a specific condition is met. For example, an event can signal that a CPU is at maximum capacity or that a device's hard drives are getting too full.

These events have messages like:

- CPU usage exceeded threshold
- Physical Memory usage exceeded threshold
- Virtual Memory usage exceeded threshold
- File system usage exceeded (critical) threshold
- File system usage exceeded (major) threshold
- Bandwidth usage exceeded threshold

These events notify users when hardware is starting to reach its limits. This allows users to fix the problem before a catastrophic hardware or software failure occurs.

Users can define hardware thresholds in two ways:

1. Users can define global hardware thresholds in the **Global Threshold Settings** page (System > Settings > Thresholds), in the **Operating System Thresholds** pane. These global thresholds apply to all hardware discovered by Skylar One.
2. For a single device, users can override the global hardware thresholds in the **Global Threshold Settings** page (System > Settings > Thresholds). Users can do this on the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface).

This chapter describes how to define both types of hardware thresholds.

This chapter covers the following topics:

Global Settings for Thresholds *227*

Device Thresholds *232*

Global Settings for Thresholds

The **System Threshold Defaults** page (System > Settings > Thresholds > System) allows you to define global thresholds for system latency, file system usage, counter rollovers, ICMP availability, number of component devices, interface inventory, and inbound messages.

These settings apply to all devices. However, you can override these system settings on a case-by-case basis. For example, you can define thresholds for a device's file systems in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface). The settings you define for the specific device override the settings in the **System Threshold Defaults** page.

To edit the global settings for system thresholds:

1. Go to the **System Threshold Defaults** page (System > Settings > Thresholds > System).
2. In the **System Threshold Defaults** page, you can drag sliders to change to value of each field or edit a field manually. You can edit the value for one or more of the following fields:
    - ***System Latency***. During polling, the platform initially pings monitored devices. The value in this field is the maximum number of milliseconds for the device to respond to Skylar One's ping (round-trip time divided by 2). The default value is 100 ms. When the latency threshold is exceeded, Skylar One generates an event for that device.
    - ***System Availability***. During polling, Skylar One monitors devices for availability. Availability means the device's ability to accept connections and data from the network. The value in this field is the percent availability required of each device. The default value is 99%. When a device falls below this level of availability, Skylar One generates an event for that device.

      During polling, a device has two possible availability values:

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

NOTE: Component devices use a Dynamic Application collection object to measure availability. Skylar One polls component devices for availability at the frequency defined in the Dynamic Application. For details, see the chapter on *Monitoring Device Availability and Latency* in the ***Monitoring Device Infrastructure Health*** manual.

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

- ***File System Major***. Threshold that will trigger a "low disk space" event. The default threshold is 85%. When a device has used more disk space than the specified percentage, Skylar One will generate a "file system usage exceeded threshold" event with a status of "major".
- ***File System Critical***. Threshold that will trigger a "low disk space" event. The default threshold is 95%. When a device has used more disk-space than the specified percentage, Skylar One will generate a "file system usage exceeded threshold" event with a status of "critical".

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), Skylar One does not generate events for that file system.

- ***Rollover Percent***. For any collected data that uses a 32-bit counter, you can specify how Skylar One determines that the counter has "rolled over", that is, has reached its maximum value, is reset to zero, and restarts counting. When this happens, the collected values go from the maximum value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
  - Maximum value has been exceeded and counter was reset to zero.
  - Retrieved value was manually reset to zero on the external device.
  - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.

NOTE: For 64-bit counters, when the counter values go from a higher value to a lower value, Skylar One assumes that the counter has been manually reset or that the two values were collected out of order. Skylar One does not assume that the counter has rolled over.

The ***Rollover Percent*** field allows you to specify a threshold that indicates that a 32-bit counter has reached its maximum value and restarted counting. The default value is 20%. When Skylar One records a counter value that is lower than the previously collected value, the platform:

- Calculates the difference between the two counter values (the delta):

  2^{32} - Last Collected Value + Current Collected Value

- Examines the value of the ***Rollover Percent*** threshold. If the delta is less than the specified percentage of the maximum possible value (2^{32}), Skylar One concludes that the 32-bit counter rolled over.
- For example, if you specified "25" in this field, Skylar One would determine if the delta is less than 25% of the maximum possible value. If the delta is less than 25% of the maximum possible value, Skylar One concludes that the 32-bit counter rolled over.
- When Skylar One determines a counter has rolled over, Skylar One uses the delta value when displaying the data point for this poll period.

NOTE: The ***Rollover Percent*** field applies only to 32-bit counters. If a 64-bit counter value goes from a higher value to a lower value, the change is treated as either a manual reset or an out-of-order collection.

- ***Out-of-order Percent***. For any collected data that uses a counter, you can specify how Skylar One determines that data has been collected out of order. When this data is collected out of order, the collected values go from a higher value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
  - Maximum value has been exceeded and counter was reset to zero (for 32-bit counters only).
  - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
  - Retrieved value was manually reset to zero on the external device.

  The ***Out-of-order Percent*** field allows you to specify a threshold that indicates that data has been collected out of order. The default value is 50%. When Skylar One records a counter value that is lower than the previously collected value and the platform has determined that the value is not a rollover, Skylar One:
  - Compares the current value to the last collected value:
    current value / last collected value
  - If the ratio of current value / last collected value is greater than the percent specified in the ***Out-of-order Percent*** field, Skylar One concludes that the data was collected out of order.
  - When Skylar One determines a data point has been collected out of order, Skylar One uses the following value as the current value of the data point:
    last collected value - current collected value

NOTE: If a 32-bit counter value goes from the maximum value to a lower value, and the current collected value does not meet the criteria for a rollover AND the current collected value does not meet the criteria for out-of-order, Skylar One concludes that the 32-bit counter was manually reset to zero (0). Skylar One uses the current collected value for this data point.

NOTE: If a 64-bit counter value goes from a higher value to a lower value, and the current collected value does not meet the criteria for out-of-order, Skylar One concludes that the 64-bit counter was manually reset to zero (0). Skylar One uses the current collected value for this data point.

- ***Availability Ping Count***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices > Classic Devices > wrench icon) for a device, this field specifies the number of packets that should be sent during each availability check. The default value is "1".
- ***Avail Required Ping Percentage***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices > Classic Devices > wrench icon) for a device, 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%".
- ***Process Runtime Threshold Low***. Threshold that will trigger a "process time exceeded" event. The default threshold is 80%. When a process has used more than 80% of its allowed ***Run Length***, Skylar One will generate a "process time exceeded threshold" event with a status of "minor".
- ***Process Runtime Threshold High***. Threshold that will trigger a "process time exceeded" event. The default threshold is 100%. When a process has used 100% of its allowed ***Run Length***, Skylar One will generate a "process time exceeded threshold" event with a status of "major".

NOTE: ***Run Length*** is defined in the **Process Manager** page (System > Settings > Admin Processes).

- ***Component Purge Timeout***. This field specifies the number of hours a device can be set to "vanished" before Skylar One purges the component device. When a device is purged, Skylar One stops trying to collect data about the component device. The purged device will not appear in reports or views on in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. If you set this value to "0", component devices are never purged. You can override this threshold for a specific device in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for the device.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

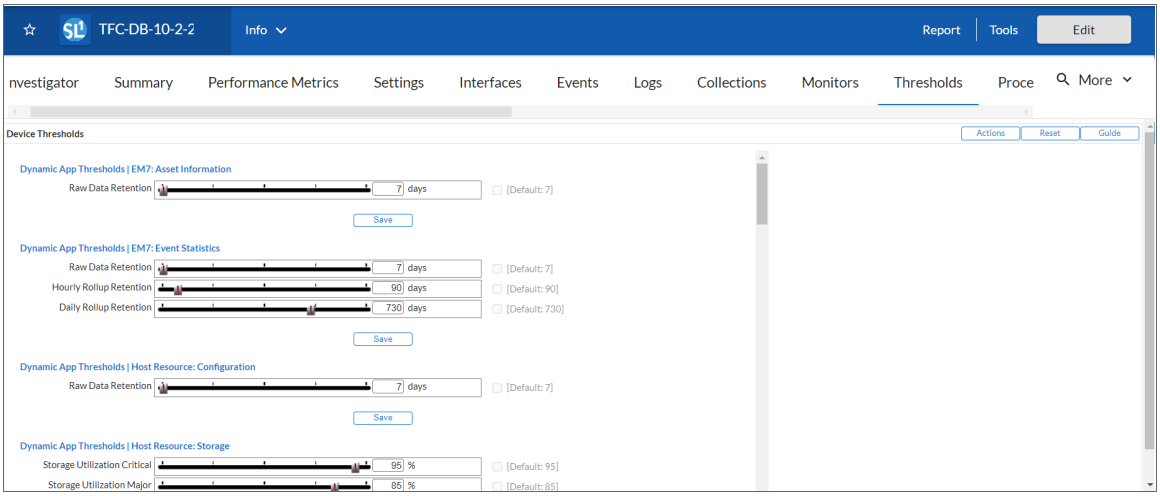
- ***Component Vanish Timeout Mins***. If Skylar One cannot retrieve information from a root device about a component device, this field specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", Skylar One stops trying to collect data about the component device. The vanished device will not appear in reports or views. The vanished device will appear in the **Vanished Device Manager** page. If you set this value to "0", component devices are never set to "vanished". You can override this threshold for a specific device in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for the device.
- ***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 polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
    - During *initial discovery*, initiated from the Discovery Session Editor page (System > Manage > Classic Discovery > Create), Skylar One uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.
    - During *re-discovery* (clicking the magnifying glass icon (🔍) in the Device Properties page), Skylar One will use the value in this field if there no value is specified in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for the device.
    - During *nightly auto-discovery* (run automatically by Skylar One every night, to update device information), Skylar One uses the value in this field if no differing value is specified in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for a device.
- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per device. If a device exceeds this number of interfaces, Skylar One will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
    - During *initial discovery*, initiated from the **Discovery Session Editor** page (System > Manage > Classic Discovery > Create), Skylar One uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.
    - During *re-discovery* (clicking the magnifying glass icon (🔍) in the Device Properties page), Skylar One will use the value in this field if there is no differing value is specified in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for the device.
    - During *nightly auto-discovery* (run automatically by Skylar One every night, to update device information), Skylar One uses the value in this field if no differing value is specified in the **[Thresholds]** tab of the **Device Investigator** (or the **Device Thresholds** page in the classic Skylar One user interface) for a device.
- ***Inbound Message Throttle Thresholds***. Specifies the maximum number of messages that can be received before Skylar One will notify the system administrator and discard the current batch of messages. The default message threshold is 25.
    - *Syslog per-IP*. Specifies the threshold for incoming syslog messages from a given IP address.

- *Dynamic Alert per-device*. Specifies the threshold for incoming alerts for a Dynamic Application on a given device.
- *SNMP Trap per-IP*. Specifies the threshold for incoming SNMP traps from a given IP address.

3. Click the **[Save]** button to save changes in this page.
4. All changes to this page are logged in the audit logs.

Device Thresholds

On the **[Thresholds]** tab of the **Device Investigator**, you can define usage and performance thresholds and data retention thresholds for a device.



When performance thresholds are exceeded, Skylar One will generate an event for the device. When space thresholds are exceeded, Skylar One will remove the oldest data from the database. For each of these thresholds, Skylar One defines a default value. You can edit the thresholds to meet your needs.

The thresholds defined for the device on the **[Thresholds]** tab override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds) and the **Data Retention Settings** page (System > Settings > Data Retention).

To define thresholds for a device:

1. Go to the **[Thresholds]** tab of the **Device Investigator**.
2. On the **[Thresholds]** tab, you can define one or more of the following thresholds:
   - ***Dynamic Application Thresholds***. If the device is a subscriber for one or more Dynamic Applications, this page can include threshold objects from those Dynamic Applications. By default, each threshold object will have the default value as defined in its Dynamic Application. However, on this page you can define a threshold value specifically for the current device. You can define a custom value for each threshold object, and Skylar One will use that custom value when evaluating Dynamic Application alerts ***for this device***. The following data retention thresholds always appear for Dynamic Applications of type performance:

- *Raw Data Retention*. Number of days to retain raw performance data collected from the device using this Dynamic Application. Raw data that is older than the specified number of days is automatically deleted.

- *Hourly Rollup Performance Data*. Number of days to retain hourly normalized data for this Dynamic Application. Hourly normalized data that is older than the specified number of days is automatically deleted.

- *Daily Rollup Performance Data*. Number of days to retain daily normalized data for this Dynamic Application. Daily normalized data that is older than the specified number of days is automatically deleted.

NOTE: The default values for the Dynamic Application Thresholds fields are defined on the **Data Retention Settings** page (System > Settings > Data Retention).

- ***File System Thresholds***. For each file system on the device that has been detected by Skylar One, you can define two thresholds:

  - *Major*. Threshold that will trigger a "low disk space" event. The default threshold is 85%. When a device has used more disk space than the specified percentage, Skylar One will generate a "file system usage exceeded threshold" event with a status of "major". ***To disable this threshold for the current device***, set the threshold to 0% (zero percent). When you disable a threshold, Skylar One does not generate an event for the threshold.

  - *Critical*. Threshold that will trigger a "low disk-space" event. The default threshold is 95%. When a device has used more disk space than the specified percentage, Skylar One will generate a "file system usage exceeded threshold" event with a status of "critical". ***To disable this threshold for the current device***, set the threshold to 0% (zero percent). When you disable a threshold, Skylar One does not generate an event for the threshold.

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), Skylar One does not monitor the thresholds on the file system and does not generate events for that file system.

- ***Interface Inventory Thresholds***. When a device has a large number of interfaces, these settings prevent Skylar One from consuming too many resources during *re-discovery* (clicking the magnifying glass icon (🔍) in the **Device Properties** page) and during *auto-discovery* (run automatically by Skylar One every night, to update device information).

  - *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. The default value is 600,000 ms (10 minutes).

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

- ***Operating System Thresholds***. You can define the following two thresholds for the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

  - *System Latency*. Every five minutes, Skylar One polls monitored devices to determine latency. The value in this field is the maximum number of milliseconds for the device to respond to Skylar One's poll (round-trip time divided by two). The default threshold value is 100ms. When the latency threshold is exceeded, Skylar One generates an event ("network latency exceeded threshold") for that device. ***To disable this threshold for the current device***, set the threshold to 0 (zero) milliseconds. When you disable a threshold, Skylar One does not generate an event for the threshold.

  - *System Availability*. Every five minutes, Skylar One polls devices for availability. The default threshold value is 99%. Availability means the device's ability to accept connections and data from the network. The value in this field is the percent availability required of each device. When a device falls below this level of availability, Skylar One generates an event for that device.

    For availability collection, a device has two possible availability values:

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

    However, you might see values other than 100 or 0 in an availability report. If a report contains any other percentage, it is an average of multiple readings. For example, if Skylar One gathered five readings and during one of those readings a device was unavailable, the average would be 80% (100 + 100 + 100 + 100 + 0 = 400; 400/5 = 80).

    NOTE: Component Devices use a Dynamic Application collection object to measure availability. Skylar One polls component devices for availability at the frequency defined in the Dynamic Application. For details, see the description of the ***Component Identifier*** field in the **Collection Objects** page. For details, see the manual ***Monitoring Device Infrastructure Health***.

- ***Data Retention Thresholds***. These thresholds specify how long Skylar One will store data collected from the device. The thresholds defined for the device on this page override the global thresholds defined in the **Data Retention Settings** page (System > Settings > Data Retention).

  - *Device Logs Max*. Maximum number of records to store in the device log. The default value is 10,000 entries. When this number is exceeded, the oldest entries will be removed.

- *Device Logs Age*. Number of days to retain device logs. Log records that are older than the specified number of days are automatically removed. The default value is 90 days.
- *Bandwidth Data*. Number of days to retain bandwidth data and CBQoS data collected from each interface on a device . Bandwidth data that is older than the specified number of days is automatically removed. The default value is 31 days.
- *Daily Rollup Bandwidth Data*. Number of days to retain daily normalized data and daily normalized CBQoS data for each interface on the device. Daily normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Hourly Rollup Bandwidth Data*. Number of days to retain hourly normalized data and hourly normalized CBQoS data for each interface on a device. Hourly normalized data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Raw Performance Data*. Number of days to retain performance data collected from the device. This setting applies to availability statistics, latency statistics, file system statistics, statistics generated by monitoring policies, and Performance Dynamic Applications for which a specific ***Raw Data Retention*** setting has not been defined. Performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Daily Rollup Performance Data*. Number of days to retain daily normalized performance data for the device. This setting applies to daily normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific ***Daily Rollup Retention*** setting has not been defined. Daily normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *Hourly Rollup Performance Data*. Number of days to retain hourly normalized performance data for the device. This setting applies to hourly normalized availability data, normalized latency data, normalized file system data, normalized data for monitoring policy statistics, and normalized data for Performance Dynamic Applications for which a specific ***Hourly Rollup Retention*** setting has not been defined. Hourly normalized performance data that is older than the specified number of days is automatically deleted. The default value is defined in the **Data Retention Settings** page.
- *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.
- *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.

- *SSL Certificate Purge Timeout*. Specifies the number of days after which SSL certificate data will be purged. The default value is 730 days.
- *Ports Data Retention*. Specifies the number of days after which expired port data will be marked for deletion during the hourly maintenance process. The default value is 730 days.

- *Services Data Retention*. Specifies the number of days after which expired services data will be marked for deletion during the hourly maintenance process. The default value is 24 hours.
- *Filesystems Data Retention*. Specifies the number of hours after which expired filesystems data will be marked for deletion during the hourly maintenance process. The default value is 24 hours.

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.

- ***Counter Rollover Thresholds***. You can define the following two thresholds for the counters on the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).
    - *Rollover Percent*. For any collected data that uses a 32-bit counter, you can specify how Skylar One determines that the counter has "rolled over", that is, has reached its maximum value, is reset to zero, and restarts counting. When this happens, the collected values go from the maximum value to a lower value. However, there are multiple circumstances under which a 32-bit counter value can go from a higher value to a lower value:

      NOTE: For 64-bit counters, when the counter values go from a higher value to a lower value, Skylar One assumes that the counter has been manually reset or that the two values were collected out of order. Skylar One does not assume that the counter has rolled over.

        - Maximum value has been exceeded and counter was reset to zero.
        - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
        - Retrieved value was manually reset to zero on the external device.

The ***Rollover Percent*** field allows you to specify a threshold that indicates that a 32-bit counter has reached its maximum value and restarted counting. The default value is 20%. When Skylar One records a counter value from a 32-bit counter that is lower than the previously collected value, Skylar One:

- calculates the difference between the two counter values (the delta):

```
maximum value (either 2^32) - Last Collected Value
+ Current Collected Value
```

- Examines the value of the ***Rollover Percent*** threshold. If the delta is less than the specified percentage of the maximum possible value (either 2^{32}), Skylar One concludes that the counter rolled over.
- For example, if you specified "25" in this field, Skylar One would determine if the delta is less than 25% of the maximum possible value. If the delta is less than 25% of the maximum possible value, Skylar One concludes that the counter rolled over.
- When Skylar One determines a 32-bit counter has rolled over, Skylar One uses the delta value when displaying the data point for this poll period.

◦ *Out-of-order Percent*. For any collected data that uses a counter, you can specify how Skylar One determines that data has been collected out of order. When this data is collected out of order, the collected values go from a higher value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value.

- Maximum value has been exceeded and counter was reset to zero (for 32-bit counters only).
- Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
- Retrieved value was manually reset to zero on the external device.

The ***Out-of-order Percent*** field allows you to specify a threshold that indicates that data has been collected out of order. The default value is 50%. When Skylar One records a counter value that is lower than the previously collected value and Skylar One has determined that the value is not a rollover, Skylar One:

- compares the current value to the last collected value:

```
current value / last collected value
```

- If the ratio of current value divided by last collected value is greater than the percent specified in the ***Out-of-order Percent*** field, Skylar One concludes that the data was collected out of order.
- When Skylar One determines a data point has been collected out of order, Skylar

One uses the following value as the current value of the data point:

```
last collected value - current collected value
```

NOTE: If a 32-bit counter value goes from the maximum value to a lower value, and the current collected value does not meet the criteria for a rollover AND the current collected value does not meet the criteria for out-of-order, Skylar One concludes that the 32-bit counter was manually reset to zero (0). Skylar One uses the current collected value for this data point.

NOTE: If a 64-bit counter value goes from a higher value to a lower value, and the current collected value does not meet the criteria for out-of-order, Skylar One concludes that the 64-bit counter was manually reset to zero (0). Skylar One uses the current collected value for this data point.

- ***ICMP Availability Thresholds***. You can define the following availability thresholds for the device. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).
    - *Availability Ping Count*. If you selected *ICMP* in the ***Availability Port*** field on the **[Settings]** tab of the **Device Investigator** (or on the **Device Properties** page in the classic Skylar One user interface), this field specifies the number of packets that should be sent during each availability check. If you selected *ICMP* in the ***Latency Port*** field in the **Device Properties** page, this field specifies the number of packets that should be sent during each latency check. The default value is "1".
    - *Avail Required Ping Percentage*. If you selected *ICMP* in the ***Availability Port*** field on the **[Settings]** tab of the **Device Investigator** (or on the **Device Properties** page in the classic Skylar One user interface), 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%".
    - *Availability Packet Size*. If you selected *ICMP* in the ***Availability Port*** field on the **[Settings]** tab of the **Device Investigator** (or on the **Device Properties** page in the classic Skylar One user interface), this field specifies the size of each packet, in bytes, that is sent during each availability check. If you selected *ICMP* in the ***Latency Port*** field in the **Device Properties** page, this field specifies the size of each packet, in bytes, that is sent during each latency check. The default value is "56 bytes".
- *Process Runtime Threshold Low*. Threshold that will trigger a "process time exceeded" event. The default threshold is 80%. When a process has used more than 80% of its allowed ***Run Length***, Skylar One will generate a "process time exceeded threshold" event with a status of "minor".
- ***Process Runtime Threshold High***. Threshold that will trigger a "process time exceeded" event. The default threshold is 100%. When a process has used 100% of its allowed ***Run Length***, Skylar One will generate a "process time exceeded threshold" event with a status of "major".

- ***Component Device Thresholds***. You can define the following thresholds for component devices. The thresholds defined for the device in this page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds).

    - *Component Vanish Timeout Mins*. If Skylar One cannot retrieve information from a root device about a component device, this field specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", Skylar One stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear in the **Vanished Device Manager** page. If you set this value to "0", the component device is never set to "vanished". For the current device, this setting overrides the ***Component Vanish Timeout*** in the **Global Threshold Settings** page.

    - *Component Purge Timeout*. If Skylar One cannot retrieve information from a root device about a component device, this field specifies how many hours to wait until purging the component device. When a device is purged, Skylar One stops trying to collect data from the component device. The purged device will not appear in reports or views on in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. If you set this value to "0", the component device is never purged. For the current device, this setting overrides the ***Component Purge Timeout*** in the **Global Threshold Settings** page.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

3. Click **[Save]**.

NOTE: If you have changed a threshold from its default value, you can return it to its default value by selecting the ***Default*** checkbox next to the appropriate field, and then clicking **[Save]**.

Defining Device Thresholds in the Classic Skylar One User Interface

The **Device Thresholds** page allows you to define space and performance thresholds for a device. When performance thresholds are exceeded, Skylar One will generate an event for the device. When space thresholds are exceeded, Skylar One will remove the oldest data from the database. For each of these thresholds, Skylar One defines a default value. You can edit the thresholds to meet your needs.

The thresholds defined for the device in the **Device Thresholds** page override the global thresholds defined in the **Global Threshold Settings** page (System > Settings > Thresholds) and the **Data Retention Settings** page (System > Settings > Data Retention).

To define thresholds for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

2. On the **Device Manager** page, find the device for which you want to define thresholds and click its wrench icon (🔧).
3. In the **Device Administration** panel, click the **[Thresholds]** tab.
4. In the **Device Thresholds** page, define one or more of the thresholds. For a description of the threshold fields, see the section on *Device Thresholds*.
5. Click the **[Save]** button to save your changes.

Chapter 12

Bulk Management with Device Groups and Device Templates

Overview

This chapter provides an overview of the device groups and device template features in Skylar One. For more information on how to use and manage device groups and device templates, see the ***Device Groups & Device Templates*** manual.

This chapter covers the following topics:

What is a Device Group? *241*

What is a Device Template? *242*

What is a Device Group?

A ***device group*** is a group of multiple devices.

Device groups allow you to:

- Use device configuration templates to perform initial configuration for multiple devices simultaneously.
- Use device configuration templates to make changes to the configuration for multiple devices simultaneously.
- On the **Device Groups** page (Devices > Device Groups), view each device group and the sub-groups and devices within each device group.

- Schedule maintenance and downtime for multiple devices simultaneously.
- Suppress events on multiple devices simultaneously.
- Include the device group in an automation policy. An automation policy allows you to trigger an automatic action if specified criteria are met on all the devices in the device group.

A device can belong to multiple device groups. For example, suppose 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.
- 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.

What is a Device Template?

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

A device template contains the following tabs and settings:

- **[Config]** tab. Contains all the fields in the **Device Properties** page (except device name and device IP) and all the fields in the **Device Thresholds** page. When you apply a device template to a device group or selected devices, you do not have to manually define any settings in the **Device Properties** page or the **Device Thresholds** page for the devices that use the template. All the devices that use the template will inherit the field values from the device template.

- **[Interface]** tab. Contains all the fields in the **Interface Properties** page that define how 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]** tab. 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]** tab. 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]** tab. Specifies one or more service policies that can be applied to devices that use the template. These 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 service policies in the **Monitoring Policies** page for those devices. All the devices that use the template will inherit the service policies from the device template; Skylar One will automatically create these service policies for each device that uses the template.
- **[Proc Policies]** tab. 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]** tab. Specifies 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.

NOTE: In a configuration template, you are not required to define all the fields in each tab. For example, you can choose to define only one or more fields in only one tab. When you apply the configuration template to devices, only those fields you defined in the template will be applied to the devices. For the remaining fields, the devices will retain their previous values or use the default values.

You can apply device templates to:

- One or more ***device groups***.
- One or more devices, selected from the **Device Manager** page.
- all the devices discovered by a specific discovery session.

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

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

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

NOTE: If you make changes to a device template or simply apply the device template a second time, 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.

Chapter

13

Creating a Physical Device without Running Discovery

Overview

Skylar One allows you to manually create physical devices without running discovery. When you do so, a device record exists in Skylar One before Skylar One can communicate with the device.

In some cases, service providers find it useful to pre-populate a Skylar One system with device records but set the status of the manually created devices to *Disabled*. When network and firewall work are completed, the provider can then enable the devices and use discovery to keep the device data up-to-date.

You can manually create a physical device in three ways:

- In the user interface
- By uploading device data via a CSV file
- With the ScienceLogic API

This chapter covers the following topics:

Requirements 246

Using the User Interface to Create a Physical Device 246

Using a CSV File to Create Multiple Physical Devices 247

Using the API to Create a Physical Device 250

Requirements

Before manually creating a device record in Skylar One, you must have the following information:

- ***Unique IP address for each device that you want to create***. The IP address must be unique in Skylar One so it can be used to communicate with the device.
- ***Organization ID***. If you use the API to manually create a physical device or if you manually create multiple devices in bulk using a CSV file, you must supply the organization ID for an existing organization.

Using the User Interface to Create a Physical Device

Creating a Physical Device from the Devices Page

To manually create a physical device from the **Devices** page:

1. Go to the **Devices** page.
2. Click the down arrow icon ( ) next to the **[Add Devices]** button and then select *Create Physical Device*. The **Create a Physical Device** modal appears.
3. In the **Create a Physical Device** modal, complete the following required fields:
    - ***IP Address***. Enter an IP address that is unique in the device's collector group and can be used to communicate with the device.

      NOTE: Skylar One will not allow a new device to be added with a public IP address that is not unique system-wide or a private IP address that is not unique to the selected Collector Group.

    - ***Device Name***. Enter a device name for the device.
    - ***SNMP Read Credential***. Select from a list of SNMP credentials.
    - ***Organization***. Select from a list of organizations.
    - ***Device Class***. Select from a list of device classes.
    - ***Collector Group***. Select from a list of collector groups.
4. Click **[Create]**.

Creating a Physical Device from the Device Manager Page

To manually create a physical device from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Click the **[Actions]** menu and select ***Create Physical Device***. The **Create Physical Device** modal page appears.
3. In the **Create Physical Device** modal page, supply the following:
    - ***IP Address***. Required. Enter an IP address that is unique in the device's collector group and can be used to communicate with the device.
    - ***Device Name***. Optional. Enter a device name for the device.
    - ***SNMP Credential***. Optional. Select from a list of SNMP credentials. If no credential is selected, the default value of *NO CREDENTIAL* is assigned to the new device.
    - ***Organization***. Optional. Select from a list of organizations. If no organization is selected, the default organization, *System*, is assigned to the new device.
    - ***Device Class***. Optional. Select from a list of device classes. If no device class is selected, the default device class, *Ping | ICMP*, is assigned to the new device.
    - ***CUG***. Optional. Select from a list of collector groups. If no collector group is selected, the collector group with the lowest ID is assigned to the new device.
4. Click **[Add]** to add the new physical device.

> **NOTE:** Skylar One will not allow a new device to be added with a public IP address that is not unique system-wide or a private IP address that is not unique to the selected Collector Group.

Managing Physical Devices Created in the User Interface

After an administrator manually creates a physical device, the device appears in the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

The new device can be managed like any physical device in Skylar One. However, the following caveats apply:

- No Dynamic Applications are automatically aligned with the device.
- No interfaces are discovered and no interface data is included with the device record.

If you want to disable ***Auto-Update*** and disable ***Collection*** for the new device, see the details in the ***Device Management*** manual.

If you want to discover the device using the Discovery tool, see the section on *Manually Re-Running Discovery for a Device*, in the manual ***Discovery and Credentials***.

Using a CSV File to Create Multiple Physical Devices

Skylar One allows users to manually create multiple physical devices simultaneously by uploading device data in a CSV file.

The fields supported differ based on whether you are uploading the CSV file from the **Devices** page or from the **Device Manager** page.

The following fields are supported if you are uploading the file from the **Devices** page:

- ***ip***. Required. An IP address that is unique in the device's collector group and can be used to communicate with the device.
- ***organization***. Required. The ID of an existing organization.
- ***name***. Optional. A name for the device.
- ***deviceClassId***. Required. The Globally Unique Identifier (GUID) of the device class.
- ***snmpCredId***. Optional. An SNMP credential associated with the device. If no SNMP credential is included, no credential is associated with the device.
- ***collectorGroupId***. Optional. The collector group (CUG) assigned to the new device. If no CUG is included, Skylar One assigns the CUG from the top of the list of all CUGs, sorted numerically by ID.

NOTE: From the **Device Manager** page, the same fields are instead labeled like this:

- ip
- organization
- name
- class_type
- snmp_cred_id
- collector_group

The explanations and examples in the rest of this section use the **Devices** page format. If you are uploading the CSV file from the **Device Manager** page, you should instead use the field labels listed here.

NOTE: Skylar One generates an error if a required field is excluded from the CSV file or if non-supported fields (for example, hostname) are included in the CSV file.

The CSV file must contain a comma-separated header line that indicates the fields used, followed by comma-separated lines for each device. The CSV file must include the ***ip***, ***organization***, and ***deviceClassId*** fields at a minimum, and can include additional fields. You must enter the field names in lowercase with no space between field names. Because the field names must match the corresponding parameters in the API, you must enter the field names exactly as follows:

- ip
- organization
- name
- deviceClassId (or class_type, if uploading from the **Device Manager** page)

- snmpCredId (or snmp_cred_id, if uploading from the **Device Manager** page)
- collectorGroupId (or collector_group, if uploading from the **Device Manager** page)

For example, to create two devices using only the required fields of IP address, organization, and device class ID, the CSV file must contain the following:

```
ip,organization,deviceClassId

10.2.9.42,1,9681

10.2.10.42,1,9681
```

To create "Device A" and "Device B" using all supported fields, the CSV file must contain the following:

```
ip,organization,name,deviceClassId,snmpCredId,collectorGroupId

10.2.9.42,1,Device A,9681,37,1

10.2.10.42,1,Device B,9681,37,1
```

NOTE: Do not include spaces between the comma-separated values in the CSV file.

Creating Multiple Physical Devices Using a CSV File from the Devices Page

To manually create multiple physical devices using a CSV file from the **Devices** page:

1. Go to the **Devices** page.
2. Click the down arrow icon ( ) next to the **[Add Devices]** button and then select *Create Physical Device From File*. The **Create a Physical Device From File** modal appears.
3. In the **Create a Physical Device From File** modal, click **[Browse Files]**, then select the desired CSV file.
4. Click **[Create]** to import the CSV file and create the physical devices. If an error occurs, the error message appears in the **Create a Physical Device From File** modal. Otherwise, if the import is successful, the **Devices** page appears with the new devices added.

NOTE: Skylar One will not allow a new device to be added with a public IP address that is not unique system-wide or a private IP address that is not unique to the selected Collector Group.

Creating Multiple Physical Devices Using a CSV File from the Device Manager Page

To manually create multiple physical devices using a CSV file from the **Device Manager** page:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Click the **[Actions]** menu and select ***Create Physical Devices From File***. The **Bulk Physical Device** modal appears.
3. In the **Bulk Physical Device** modal, click **[Browse]**, then select the desired CSV file.
4. Click **[Import]** to import the CSV file and create the physical devices. The **Bulk Physical Device** modal displays log messages as each new physical device is created or if any errors occurred while adding a device.
5. If an error occurred importing a device, select the wrench icon (🔧) for a that device to open the manually edit the settings for that device. The *Creating a Physical Device in the User Interface* section describes the user interface for adding a single device manually.

NOTE: Skylar One will not allow a new device to be added with a public IP address that is not unique system-wide or a private IP address that is not unique to the selected Collector Group.

Managing Physical Devices Created Using a CSV File

You can use the Skylar One user interface to manage the newly created devices. For details, see the section *Managing Physical Devices Created in the User Interface*.

Using the API to Create a Physical Device

Creating a Physical Device with the API

You can use a POST request to the /device API resource to manually create a physical device in Skylar One.

The following fields are supported:

- ***ip***. Required. Supply an IP address that is unique in Skylar One and can be used to communicate with the device.
- ***organization***. Required. Supply the relative API URI for an existing organization, e.g. /api/organization/0.
- ***name***. Optional. Supply a name for the device.
- ***snmp_cred_id***. Optional. Specify the relative API URI of an existing SNMP credential. If no credential is selected, no credential is assigned to the new device.
- ***class_type***. Optional. Specify the relative API URI of an existing device class. If no device class is selected, the default device class, *Ping | ICMP*, is assigned to the new device.
- ***collector_group***. Optional. Specify the relative API URI of an existing collector group. If no collector group is selected, the collector group with the lowest ID is assigned to the new device.

Example

The following example creates a physical device using the API:

```
curl -v -H 'X-em7-beautify-response:1' -H 'accept:application/json' -H
'content-type:application/json' -u 'em7admin:<password>'
"http://192.168.10.205/api/device" -d '{"name": "example-device",
"organization": "\/api\/organization\/0", "class_type": "\/api\/device_
class\/1547", "ip": "10.20.7.31", "snmp_cred_id":
"\/api\/credential\/snmp\/69","collector_group": "\/api\/collector_
group\/1"}'
```

- ***curl -v***. Executes the cURL request. The -v option tells cURL to use verbose mode (displays all header information and all status and error messages). In the response, lines that start with ">" include header data returned by cURL. Lines that start with "<" include header data received by cURL.
- ***-H 'X-em7-beautify-response:1'***. The -H option tells cURL to include an additional header in the request. In this case, we're including a ScienceLogic custom header that tells the API to include white-space in the response.
- ***-H 'accept:application/json'***. The -H option tells cURL to include an additional header in the request. In this case, we're telling the API to return responses in JSON format.
- ***-H 'content-type:application/json'***. The -H option tells cURL to include an additional header in the request. In this case, we're telling the API that the incoming data is in JSON format.
- ***-u 'em7admin:<password>'***. The -u option tells cURL to authenticate as a specified user. In our example, we authenticated as the user "em7admin". You would replace *<password>* with the appropriate password for that user.
- ***"https://192.168.10.205/api/device"***. Connect to the specified URL. In our example, we connected to the API at 192.168.10.205 and navigated to the resource for devices.
- ***-d***. Tells the API the following text is the data to submit as a POST request.
- The device is created using the following fields:

Field Name	Value
name	example-device
organization	/api/organization/0
class type	/api/device_class/1547
ip	10.20.7.31
snmp_cred_id	/api/credential/snmp/69
collector_group	/api/collector_group/1

The API returns an HTTP 201 response. The response body includes the newly created device record in JSON format.

The X-EM7-status-message header includes the device ID of the newly created device.

```
< HTTP/1.1 201 Created:

< Server: nginx/1.10.0

< Date: Thu, 28 Jul 2016 16:50:12 GMT

< Content-Type: application/json

< Transfer-Encoding: chunked

< Connection: keep-alive

< X-EM7-Implemented-methods: GET,POST,PUT,DELETE

< X-Powered-By: ScienceLogic, Inc. - EM7 API/Integration Server

< X-EM7-Authenticated-account: /api/account/1

< Location: /api/device/33

< Cache-Control: private, no-cache, must-revalidate, no-store, max-
age=0, post-c heck=0, pre-check=0
```

< X-EM7-status-message: Device :33 added successfully

```
< X-EM7-status-code: CREATED

< Vary: Accept-Encoding

<

{

"name": "example-device",

"ip": "10.20.7.31",

"hostname": null,

"snmp_cred_id": "\/api\/credential\/snmp\/69",

"snmp_w_cred_id": null,

"class_type": "\/api\/device_class\/1547",

"collector_group": "\/api\/collector_group\/1",
```

```
"organization": "\/api\/organization\/0",
```

The rest of the response includes a list of all device fields, each set to its default value.

Managing Physical Devices Created with the API

You can use the ScienceLogic user interface to manage the newly created device. For details, see the section *Managing Physical Devices Manually Created in the User Interface*.

You can also use the ScienceLogic API to manage the newly created device. For more information, ask your ScienceLogic contact for access to the ScienceLogic API documentation.

Available Actions for the Device Resource

Action	URI	Method
View/search/filter the list of devices.	/device	GET
Create a new physical device. Unlike for virtual device, must specify a valid IP address and the organization ID for an existing organization.	/device	POST
Create a new virtual device.	/device	POST
View the properties of a device.	/device/X	GET
Update the properties of a device.	/device/X	POST
Replace the properties of a device.	/device/X	PUT
Delete a device.	/device/X	DELETE
View/search/filter the list of Dynamic Applications aligned with a device.	/device/X/aligned_app	GET
Align a Dynamic Application with a device.	/device/X/aligned_app	POST
View the collection status and associated credential for a Dynamic Application aligned with a device.	/device/X/aligned_app/X	GET
Update the collection status and associated credential for a Dynamic Application aligned with a device.	/device/X/aligned_app/X	POST
Unalign a Dynamic Application from a device.	/device/X/aligned_app/X	DELETE
View/search/filter the list of available configuration data for a device.	/device/X/config_data	GET
View meta-data about data collected from a device by a configuration Dynamic Application.	/device/X/config_data/X	GET
View data collected from a device by a configuration Dynamic Application.	/device/X/config_data/X/data	GET

Action	URI	Method
View historical snapshots of data collected from a device by a configuration Dynamic Application.	/device/X/config_data/X/snapshots	GET
View general information collected from a device.	/device/X/detail	GET
View/search/filter the list of credentials aligned with a device.	/device/X/device_app_credentials	GET
View the threshold settings for a device.	/device/X/device_thresholds	GET
Update the threshold settings for a device.	/device/X/device_thresholds	POST
Replace the threshold settings for a device.	/device/X/device_thresholds	PUT
Revert all device thresholds to the global default values.	/device/X/device_thresholds	DELETE
Add an interface record to a device.	/device/X/interface	POST
View/search/filter the list of interfaces for a device.	/device/X/interface	GET
View the properties of an interface for a device.	/device/X/interface/X	GET
Update the properties of an interface for a device.	/device/X/interface/X	POST
Replace an interface record associated with a device.	/device/X/interface/X	PUT
Delete an interface record associated with a device.	/device/X/interface/X	DELETE
View data for an interface.	/device/X/interface/X/interface_data/data	GET
View daily normalized data for an interface.	/device/X/interface/X/interface_ data/normalized_daily	GET
View hourly normalized data for an interface.	/device/X/interface/X/interface_ data/normalized_hourly	GET
View/search/filter the list of logs associated with a device.	/device/X/log/	GET
View a log associated with a device.	/device/X/log/X	GET
Add a note to a device.	/device/X/note/	POST
View/search/filter the list of notes associated with a device.	/device/X/note/	GET
View a note associated with a device.	/device/X/note/X	GET
Update a note associated with a device.	/device/X/note/X	POST
Replace a note associated with a device.	/device/X/note/X	PUT
View/search/filter the list of files	/device/X/note/X/media	GET

Action	URI	Method
associated with a device note.		
Get a media file associated with a device note.	/device/X/note/X/media/X	GET
Add a media file to a device note.	/device/X/note/X/media/X	PUT
View meta-data about a media file associated with a device note.	/device/X/note/X/media/X/info	GET
View/search/filter the list of available Dynamic Application data for a device.	/device/X/performance_data	GET
View data for a Dynamic Application aligned to a device.	/device/X/performance_data/X/data	GET
View daily normalized data for a Dynamic Application aligned to a device.	/device/X/performance_ data/X/normalized_daily	GET
View hourly normalized data for a Dynamic Application aligned to a device.	/device/X/performance_ data/X/normalized_hourly	GET
View/search/filter the list of available vitals data for a device.	/device/X/vitals	GET
View availability data for a device.	/device/X/vitals/availability/data	GET
View daily normalized availability data for a device.	/device/X/vitals/availability/normalized_ daily	GET
View hourly normalized availability data for a device.	/device/X/vitals/availability/normalized_ hourly	GET
View data for a file system on a device.	/device/X/vitals/fsX/data	GET
View daily normalized data for a file system on a device.	/device/X/vitals/fsX/normalized_daily	GET
View latency data for a device.	/device/X/vitals/latency/data	GET
View daily normalized latency data for a device.	/device/X/vitals/latency/normalized_daily	GET
View hourly normalized latency data for a device.	/device/X/vitals/latency/normalized_ hourly	GET
Apply a device template to a device.	/device/X	Post a /device_ template resource.

Chapter

14

Virtual Devices

Overview

This chapter describes how to create and use virtual devices in Skylar One.

This chapter covers the following topics:

What is a Virtual Device? *256*

Defining a Virtual Device *257*

Directing Data to a Virtual Device *258*

What is a Virtual Device?

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

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

Defining a Virtual Device

NOTE: Before you create a virtual device, you must ensure that Skylar One includes a device class for virtual devices. These device classes must have a device category of "virtual" and a collection type of "virtual". If Skylar One does not include such a device class, you must *define one* on the **Device Class Editor** page (System > Customize > Device Classes).

Creating a Virtual Device from the Devices Page

To create a virtual device from the **Devices** page:

1. Go to the **Devices** page.
2. Click the down arrow icon ( ) next to the **[Add Devices]** button and then select *Create Virtual Device*. The **Create a Virtual Device** window appears.
3. In the **Create a Physical Device** window, complete the following required fields:
   - ***Device Name***. Enter the name of the virtual device. This name can be any combination of alphanumeric characters, up to 32 characters in length.
   - ***Organization***. Select the organization you want to associate with the virtual device.
   - ***Device Class***. Select the device class you want to associate with the virtual device. Only device classes with a collection type of "virtual" appear in the list.
   - ***Collector Group***. Select the collector group to which you want to assign the virtual device.
4. Click **[Create]**.

Creating a Virtual Device from the Device Manager Page

To create a virtual device from the **Device Manager** page:

5. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
6. Click the **[Actions]** menu and then select *Create Virtual Device*. The **Create Virtual Device** modal appears.
7. Supply a value in each of the following fields:
   - ***Device Name***. Name of the virtual device. Can be any combination of alphanumeric characters, up to 32 characters in length.
   - ***Organization***. Organization to associate with the virtual device. Select from the drop-down list of all organizations in Skylar One.
   - ***Device Class***. The device class to associate with the virtual device. Select from the drop-down list of device classes. Only device classes with a device category of "virtual" and a collection type of "virtual" appear in the list.

- ***Collector***. Specifies which instance of Skylar One will perform auto-discovery and gather data from the device. Can also specify a "virtual" poller. Select from the drop-down list of all collectors in Skylar One.

8. Click **[Add]**.

Directing Data to a Virtual Device

After defining a virtual device, you must tell Skylar One which data to store in the virtual device.

- For data that is pushed to Skylar One, you can *define the log data that you want to collect and redirect to the virtual device*.
- For data that is collected via SNMP or TCP/IP, you can *manually associate a Dynamic Application with the device* to ensure that data collected by the Dynamic Application is stored in the virtual device.

Redirecting Log Data to a Virtual Device

Skylar One enables you to redirect log entries from one IP-based device to another IP-based device, or from an IP-based device to a virtual device.

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

In this scenario, you can create a virtual device in Skylar One to represent the device that does not support TCP/IP. You can then move the data from the TCP/IP device that is monitored by Skylar One to the virtual device in Skylar One.

The **[Redirects]** tab of the **Device Investigator** (or the **Redirect Policy Editor** page in the **Device Administration** panel) allows you to move data and log entries generated by inbound SNMP trap, syslog, or email messages from the TCP/IP device to the virtual device.

IMPORTANT: If you move data and log entries from a TCP/IP device to a virtual device, be aware of the following:

- Log entries that are redirected to a virtual device will no longer appear in the log files for the IP-based device.
- Log entries that are redirected to a virtual device are no longer associated with the IP address of the original device.
- Log entries with a ***Source*** of *Internal*, *Dynamic*, or *API* that match a redirect policy are not moved from the IP-based device to the current device.

To redirect data from one IP-based device to another IP-based device or a virtual device:

1. From the **Devices** page, click the name of the virtual or IP-based device to which you want to redirect data to open the **Device Investigator** for that device, and then click the **[Redirects]** tab.

> **NOTE:** Alternatively, you can do this in the classic Skylar One user interface by going to the **Redirect Policy Editor** page in the **Device Administration** panel. To do so, go to the **Device Manager** page Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface), find the device to which you want to direct data, click its wrench icon (🔧), and then click the **[Redirects]** tab.

2. To move SNMP trap, syslog, or email log messages from an IP-based device to the current device, provide values in each of the following fields:
    - ***Source Device***. This is the TCP/IP device from which you want to redirect log messages. Data from this device will be moved to the current device. Select from a drop-down list of all IP-based devices discovered by Skylar One.
    - ***Expression Match***. A regular expression used to locate the log entry to redirect. This can be any combination of alphanumeric and multi-byte characters, up to 64 characters in length. Skylar One's expression matching is case-sensitive. For details on the regular-expression syntax allowed by Skylar One, see http://www.python.org/doc/howto/ .
    - ***Active State***. Specifies whether or not Skylar One will execute the redirection policy. The choices are:
        - *Enable*. Skylar One will execute the redirection policy.
        - *Disable*. Skylar One will not execute the redirection policy.
3. Click **[Save]**.
4. You can repeat steps 2 and 3 to redirect data from more than one device or from more than one type of log message.

Aligning a Dynamic Application with a Virtual Device

You can associate data that is collected by a Dynamic Application with a virtual device. Any data collected by the Dynamic Application will be stored in the virtual device.

> **NOTE:** You cannot align SNMP Dynamic Applications with a virtual device. You can align all other types of Dynamic Applications with a virtual device.

You can align a Dynamic Application with a virtual device from the *Device Investigator* or from the *Device Administration panel*.

Aligning a Dynamic Application with a Virtual Device from the Device Investigator

To align a Dynamic Application with a device from the **Device Investigator**:

1. From the **Devices** page, click the name of the virtual device that you want to align with a Dynamic Application to open the **Device Investigator** for that device, and then click the **[Collections]** tab.
2. Click **[Edit]**.
3. Click **[Align Dynamic Application]**. The **Align Dynamic Application** window appears.
4. Click **[Choose Dynamic Application]**. The **Choose Dynamic Application** window appears.
5. Select the radio button of the Dynamic Application you want to align with the virtual device, and then click **[Select]**. The **Align Dynamic Application** window appears with the selected Dynamic Application.

> **TIP:** You can use the search field or filter fields to narrow down the list of Dynamic Applications.

6. In the **Align Dynamic Application** window, an SNMP credential is automatically selected. To align the Dynamic Application using that SNMP credential, proceed to step 8. Otherwise, clear the credential checkbox and then click **[Choose Credential]**. The **Choose Credential** window appears.
7. Select the radio button of the credential you want to align with the Dynamic Application, and then click **[Select]**. The **Align Dynamic Application** window appears with the selected credential.

> **TIP:** You can use the search field or filter fields to narrow down the list of credentials.

8. Click **[Align Dynamic Application]**. The **[Collections]** tab appears with the selected Dynamic Application aligned to the virtual device.
9. To run the Dynamic Application immediately, click **[Run Now]**. Otherwise, proceed to step 10 and the Dynamic Application will run automatically based on its ***Poll Frequency***.
10. Click **[Save]**.

Aligning a Dynamic Application with a Virtual Device from the Device Administration Panel

To align a Dynamic Application with a device from the **Device Administration** panel:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device you want to associate with a Dynamic Application and then click its wrench icon ( ). The **Device Administration** panel appears.
3. In the **Device Administration** panel, click the **[Collections]** tab.
4. In the **Dynamic Application Collections** page, click the **[Action]** menu and select *Add Dynamic Application*.
5. The **Dynamic Application Alignment** modal page appears.

6. To associate an additional Dynamic Application with the device, highlight it in the ***Dynamic Applications*** field. You can filter the list of Dynamic Applications using the search field above the ***Dynamic Applications*** field.
7. After selection a Dynamic Application, you must select a credential. Select a credential in the ***Credentials*** field. You can filter the list of credentials using the search field above the ***Credentials*** field.

> **NOTE**: Your organization membership(s) might affect the list of credentials you can see in the ***Credentials*** field.

8. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.
9. Skylar One will associate the Dynamic Application with the device and immediately attempt to collect the data specified in the Dynamic Application using the selected credential.
10. After the first, immediate collection, Skylar One will collect the data at the frequency defined in the ***Polling Frequency*** field in the **Application Configuration Editor** page for the Dynamic Application.

Chapter 15

Customizing the User Interface for a Device

Overview

This chapter describes how to define custom tabs in the **Device Administration** panel in Skylar One for a specific device.

> **NOTE:** The information in this chapter applies only to the classic Skylar One user interface.

This chapter covers the following topics:

Custom Navigation in the Classic User Interface 262

Editing a Custom Navigation tab 263

Custom Navigation in the Classic User Interface

In the **Device Administration** panel you can access the **Custom Navigation** modal page.

The **Custom Navigation** modal page allows users to define custom tabs to include in the **Device Administration** panel for a specific device. Each custom tab includes one or more links. The links can be to internal pages in Skylar One or external URLs and URIs.

To define a custom tab for a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

2. In the **Device Manager** page, find the device for which you want to create a custom tab. Select its wrench icon ( ).
3. In any page in the **Device Administration** panel, select the **[Actions]** menu and choose *Custom Navigation*. The **Custom Navigation** modal page appears.
4. To create a custom tab in the **Device Administration** panel for the device, enter values in the following fields:
    - ***Title (Shown on Tab)***. Enter a name for the tab. This name will appear on a new tab in the Device Administration tools for this device.
    - ***Limit Access***. Users who will be allowed to access the custom tab, based on the type of user account. The choices are:
        - *Administrators*. Only users with account type "Administrator" are allowed to access this tab.
        - *Users*. Both users with account type "User" and users with account type "Administrator" are allowed to access this tab.
    - ***External URL / URI Link***. The URL of the page that is displayed when a user selects the tab. The page can be an internal page in Skylar One or an external web page. This field can contain any combination of alphanumeric characters, with a maximum length of 128 characters. Forward slash (/), underscore (_), and question mark (?) are allowed.

Editing a Custom Navigation tab

After you have defined one or more custom tabs in the **Device Administration** panel, each tab appears as an entry in the **Register** pane in the bottom of the **Custom Navigation** modal page.

To edit a custom tab:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. In the **Device Manager** page, find the device for which you want to edit a custom tab. Select its wrench icon ( ).
3. In any page in the **Device Administration** panel, select the **[Actions]** menu and choose ***Custom Navigation***. The **Custom Navigation** modal page appears.
4. Go to the **Register** pane. Find the custom tab you want to edit. Select its wrench icon ( ).
5. The fields in the top pane will be populated with values from the selected custom tab.
6. You can edit the values in one or more fields. Select the **[Save]** button to save your changes to the custom tab.
7. To delete the custom tab, go to the **Register** pane. Find the custom tab you want to edit. Select its delete icon ( ).

NOTE: for details on creating a custom Navigation Tab for all devices, see the manual ***Customizing User Experience***.

Chapter 16

Vanishing & Purging Devices

Overview

The **Vanished Devices** page displays a list of all component devices that have "vanished" from Skylar One.

If Skylar One cannot retrieve information about a component device for the amount of time specified in the ***Component Vanish Timeout*** field (in either the **Global Threshold Settings** page, the **Device Thresholds** page for the component device, or the **Device Thresholds** page for a device higher in the component tree), Skylar One sets the device to "vanished".

When a device is set to "vanished", Skylar One stops trying to collect data about the component device. The vanished device will not appear in reports or views. The vanished device will appear only in the **Vanished Devices** page. When a device is set to "vanished", all children of that device are also set to "vanished".

> **NOTE:** A vanished device automatically returns to a monitored state when the root device reports the device in the latest inventory of the component device discovery application.

After a device is vanished for the amount of time specified in the ***Component Purge Timeout*** field (in either the **Global Threshold Settings** page, the **Device Thresholds** page for the component device, or the **Device Thresholds** page for a device higher in the component tree), Skylar One purges the device. Purged devices are completely removed from Skylar One and all associated data is deleted. When a device is purged, all children of that device are also purged.

NOTE: The vanishing and purging functions apply only to component devices and merged physical and component devices. Physical, IP-based devices and virtual devices that have not been merged with a component device are never vanished or purged.

This chapter covers the following topics:

Setting Vanish and Purge Thresholds *266*

Viewing the List of Vanished Devices *267*

Using the Advanced Filters *269*

Unmerging Vanished Devices *269*

Manually Purging Selected Devices *270*

Setting One or More Devices to Never Purge *270*

Setting Vanish and Purge Thresholds

Two threshold settings control the vanishing and purging behavior for component devices:

- ***Component Vanish Timeout***. If Skylar One cannot retrieve information from a root device about a component device, this threshold specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", Skylar One stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear in the *Vanished Device Manager* page. If this threshold is set to zero for a component device, the component device is never set to "vanished".
- ***Component Purge Timeout***. This field specifies the number of hours a device can be set to "vanished" before Skylar One purges the component device. When a device is purged, Skylar One stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from Skylar One. If this threshold is set to zero for a component device, the component device is never purged.

Skylar One uses the following logic to determine the threshold value for a given component device when determining whether the component should be vanished or purged:

- If the threshold has been configured in the *Device Thresholds* page for the component device, that threshold value is used.
- If the threshold has not been configured in the *Device Thresholds* page for the component device, but the threshold has been configured in the *Device Thresholds* page for an ancestor of the component device (i.e., a component device in the component tree between the root device and the component device), that threshold value is used. If multiple ancestors have the threshold configured in the *Device Thresholds* page, Skylar One uses the threshold value for the component device that is closest to the root device (furthest up the tree).

- If the threshold has not been configured in the *Device Thresholds* page for the component device or an ancestor of the component device, the threshold value defined in the **Global Threshold Settings** page (System > Settings > Thresholds) is used.

Viewing the List of Vanished Devices

The **Vanished Device Manager** page (Devices > Vanished Devices) displays the following about each device:

> **TIP:** To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

- ***Device Name***. Name of the device. For devices running SNMP or with DNS entries, the named device is discovered automatically. For devices without SNMP or DNS entries, the device's IP address will appear in this field.
- ***IP Address***. The IP address of the device.
- ***Device Category***. The ScienceLogic category assigned to the device. Categories include servers, routers, switches, firewalls, printers, etc. The category is automatically assigned during discovery, at the same time as the Device Class/Sub-Class.
- ***Device Class/Sub-class***. The manufacturer (device class) and type of device (sub-class). The Device Class/Sub-Class is automatically assigned during discovery, at the same time as the as Category.
- ***DID***. Device ID. This is a unique number automatically assigned to the device by Skylar One.
- ***Organization***. The organization to which the device is assigned.
- ***Current State***. Condition of the device, based upon events generated by the device. Condition can be one of the following:
    - *Critical*. Device has a serious problem that requires immediate attention.
    - *Major*. Device has a problem that requires immediate attention.
    - *Minor*. Device has a less-serious problem.
    - *Notice*. Device has an informational event associated with it.
    - *Healthy*. Device is running with no problems.
- ***Collection Group***. Specifies the collector group to which the device belongs. Collector Groups are defined in the **Collector Group Management** page (System > Settings > Collector Groups) and specify one or more ScienceLogic Data Collectors. An ScienceLogic Data Collector is the appliance that gathers data from the device. For All-In-One Appliances, this field displays only the built-in Collector Group (and any virtual Collector Groups).

- ***Collection State***. 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 a 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 the device is currently in scheduled maintenance mode.
    - *User-Initiated-Maintenance*. Skylar One is not currently collecting data from the device because the device 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*.

- ***Vanished Date***. Date on which the device was set to "vanished". If Skylar One cannot retrieve information from a root device about component device for the amount of time specified in the ***Component Vanish Timeout*** field (defined globally in the **Global Threshold Settings** page or for an individual device in the **Device Thresholds** page), Skylar One sets the device to "vanished". When device is set to "vanished", Skylar One stops trying to collect data from the component device. The vanished device will not appear in reports or views. The vanished device will appear only in the **Vanished Device Manager** page.
- ***Hours Until Purge***. Based on the threshold ***Component Purge Timeout***, specifies the number of hours until the vanished device will be purged. When a device is purged, Skylar One stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. You can define a global threshold for ***Component Purge Timeout*** in the **Global Threshold Settings** page. You can override the global threshold and define the ***Component Purge Timeout*** threshold for a single device in the device **Device Thresholds** page.

NOTE: To ensure that one or more devices are never purged, *you can set one or more devices to never purge*.

NOTE: To manually purge a device prior to the ***Hours to Purge*** time, *you can manually purge selected devices*.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

Using the Advanced Filters

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

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

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

To access the Advanced Filter Tool:

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

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

4. In the Advanced Filter Tool, filter by one or more of the available parameters.
5. After selecting all filters, select the **[Apply]** button to apply the filters to the list of devices.
6. To reset each field and apply no filters, select the **[Reset]** button.

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

Unmerging Vanished Devices

To unmerge a vanished device:

1. Go to the **Vanished Device Manager** page (Devices > Vanished Devices, or Registry > Devices > Vanished Device Manager in the classic user interface).
2. Select the **[Actions]** menu and then choose ***Unmerge Devices***.
3. The **Device Bulk Unmerge Vanished** page displays a list of merged devices. Each numbered row indicates a pair of merged devices that can be unmerged. Select the checkboxes in the last column of each row of devices that you want to unmerge, then select the **[Unmerge]** button.
4. A window displays that asks you to confirm the unmerging. Select the **[Unmerge]** button.
5. When the message, "Device Bulk Unmerge complete" displays, select the **[Close/Esc]** button.
6. The physical device will once again appear in the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).

Manually Purging Selected Devices

You can manually purge one or more devices in the **Vanished Device Manager** page.

When a device is purged, Skylar One stops trying to collect data from the component device. The purged device will not appear in reports or views in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server.

> **NOTE**: When a device is purged, all children of that device are also purged.

To purge one or more vanished devices:

1. In the **Vanished Device Manager** page (Devices > Vanished Devices), select the checkbox for each device you want to purge. To select all checkboxes for all devices, select the checkbox at the top of the page.
2. In the ***Select Action*** drop-down list, select *Purge Selected Devices*.
3. Select the **[Go]** button.

Setting One or More Devices to Never Purge

You can specify that a vanished device should never be purged. When you define this setting for a device, the device is never purged, regardless of the global threshold for ***Component Purge Timeout*** in the **Global Threshold Settings** page or the ***Component Purge Timeout*** threshold set for the device in the **Device Thresholds** page.

To set one or more vanished devices to never be purged:

1. In the **Vanished Device Manager** page (Devices > Vanished Devices), select the checkbox for each device you want to prevent from being purged. To select all checkboxes for all devices, select the select the checkbox at the top of the page.
2. In the ***Select Action*** drop-down list, select *Set Selected Devices to Never Purge*.
3. Select the **[Go]** button.

Chapter 17

Device Dashboards

Overview

A dashboard in Skylar One is a page that displays graphical reports. Each report, called a widget, is displayed in its own pane. To define a graphical report, you select from a list of pre-defined widgets and then customize the selected widget by supplying values in the configuration fields. The customized widget then generates a graph, chart, table, or other information in a pane in the dashboard. For information on generating and viewing dashboards, see the ***Dashboards*** manual.

The **Device Summary** page, which appears when you select the graph icon ( ) for a device in the classic Skylar One user interface, displays one or more dashboards similar to the dashboards available under the **[Dashboards]** tab.

Dashboards for the **Device Summary** page are always displayed with the context set to the device being viewed. Typically, the widgets on a device dashboard are configured to read the device context. As a result, the widgets display data for the device being viewed.

The **Device Dashboards** page (System > Customize > Device Dashboards in the classic user interface only) displays a list of dashboards that can be displayed for a device in the **Device Summary** page. From the **Device Dashboards** page, you can create, edit, delete, and align device dashboards.

This chapter covers the following topics:

Viewing the List of Device Dashboards 272

Creating a Device Dashboard 273

Aligning Device Dashboards 273

Editing a Device Dashboard 276

Deleting a Device Dashboard 276

Copying a Device Dashboard 277
Defining the Global Default for Device Dashboards 277
Unaligning a Device Dashboard 278
Moving Alignment for Device Dashboards 278

Viewing the List of Device Dashboards

The **Device Dashboards** page (System > Customize > Device Dashboards in the classic Skylar One user interface only) displays a list of existing device dashboards. These dashboards include predefined device dashboards (which are installed with Skylar One or can be installed with a PowerPack) and any user-defined device dashboards.

TIP: To sort the list, 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. You can also filter the items on this inventory page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page. For more information, see *Filtering Inventory Pages* in the ***Introduction to Skylar One*** manual.

For each device dashboard, the **Device Dashboards** page displays the following information:

- ***Device Dashboard Name***. Name of the device dashboard.
- ***ID***. Unique ID that Skylar One automatically assigned to each device dashboard.
- ***Global Default***. Specifies whether the device dashboard is the default device dashboard for all devices.
- ***Categories***. Specifies the number of device categories aligned with the device dashboard.
- ***Classes***. Specifies the number of device classes aligned with the device dashboard.
- ***Devices***. Specifies the number of devices that have been manually aligned with the device dashboard.
- ***Dynamic Apps***. Specifies the number of Dynamic Applications that are aligned with the device dashboard.
- ***Edited By***. ScienceLogic user who created or last edited the device dashboard.
- ***Last Edited***. Date and time the device dashboard was created or last edited.

NOTE: By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

Creating a Device Dashboard

To create a device dashboard:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, click the **[Create]** button. The **Device Dashboard Editor** page appears.
3. Supply values in the following fields:
    - ***Device Dashboard Name***. Name of the device dashboard.
    - ***Device***. Select a device to provide sample data while you create the dashboard. This device will not be permanently associated with the dashboard.
    - ***Adding Widgets***. To add a widget, go to the big pane below the ***Device*** field. Left-click and drag with your mouse to draw a rectangle. This shape will determine the initial size and position of the widget in your dashboard. When the **Widget Configuration** page appears, configure the widget as you would for a dashboard.

NOTE: For maximum flexibility, when configuring a device-specific widget, ScienceLogic recommends that you select *Contextual Device (Auto)* in the ***Element*** field.

NOTE: For details on configuring widgets, see the manual ***Dashboards***.

4. The new device dashboard is automatically saved.

Aligning Device Dashboards

The device dashboard that is defined as the "Global Default" is the default dashboard that appears in the in the **Device Summary** page for each device.

Skylar One decides what to display in the **Device Summary** page as follows:

- If the device is manually aligned with a device dashboard (in the **Device Properties** page), that dashboard is displayed in the **Device Summary** page for the device.
- If the device is not manually aligned with a device dashboard, the device dashboard that is aligned with the Device Class is displayed.
- If the device class is not aligned with a device dashboard, the device dashboard that is aligned with the Device Category is displayed.
- If the device category is not aligned with a device dashboard, the device dashboard that is defined as the "Global Default" is displayed.

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

NOTE: Although you can align a device dashboard with a Dynamic Application, the device dashboards that are aligned with Dynamic Applications are never displayed in the **Device Summary** page as the default display. However, from the **Device Summary** page, a user can select and view any device dashboards that are aligned with Dynamic Applications for the device.

Aligning a Device Dashboard with a Device

You can manually align a device dashboard with a device. The device dashboard will then appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic user interface).
2. Find the device you want to align with a device dashboard. Click the wrench icon (🔧) for that device.
3. In the **Device Properties** page, edit the ***Dashboard*** field to select a device dashboard. The selected device dashboard will appear by default in the **Device Summary** page for this device.
4. Click the **[Save]** button.

Aligning a Device Dashboard with a Device Class

You can manually align a device dashboard with a device class. For devices that do not have a device dashboard defined in the **Device Properties** page, the device dashboard associated with the Device Class will appear as the default view in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device class:

1. Go to the **Device Class Editor** page (System > Customize > Device Classes).
2. In the **Device Class Register** pane, find the device class you want to align with a device dashboard. Click the wrench icon (🔧) for that device class.
3. In the **Device Class Editor** page, edit the ***Dashboard*** field to select a device dashboard. The selected device dashboard will be associated with all devices that use this device class and will appear as an option in the **Device Summary** page.
4. Click the **[Save]** button.

> **NOTE**: If a PowerPack updates one or more device classes, Skylar One will not overwrite the alignment between device dashboards and any updated device classes.

Aligning a Device Dashboard with a Device Category

You can manually align a device dashboard with a device category. For devices that do not have a device dashboard defined in the **Device Properties** page or a device dashboard defined in the **Device Class Editor** page, the device dashboard associated with the Device Category will appear as the default view in the **Device Summary** page.

> **NOTE**: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To align a device dashboard with a device category:

1. Go to the **Device Category Editor** page (System > Customize > Device Categories).
2. In the **Register** pane, find the device category you want to align with a device dashboard. Click the wrench icon (🔧) for that device category.
3. In the **Editor** pane, edit the ***Device Dashboard*** field to select a device dashboard. The selected device dashboard will be associated with all devices that use this device category and will appear as an option in the **Device Summary** page.
4. Click the **[Save]** button.

> **NOTE**: If a PowerPack updates one or more device categories, Skylar One will not overwrite the alignment between device dashboards and any updated device categories.

Aligning a Device Dashboard with a Dynamic Application

You can manually align a device dashboard with a Dynamic Application. For each device that subscribes to the Dynamic Application, the aligned device dashboard will appear as an option in the **Device Summary** page.

NOTE: From the **Device Summary** page, the user can select and view any device dashboards that are associated with the device, the device's device class, the device's device category, the device's Dynamic Applications, and the Global Default.

To manually align a device dashboard with a Dynamic Application:

1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
2. Find the Dynamic Application you want to align with a device dashboard. Click the wrench icon ( ) for that Dynamic Application.
3. In the **Dynamic Applications Properties Editor** page, edit the ***Device Dashboard*** field to select a device dashboard. The selected device dashboard will be associated with all devices that subscribe to this Dynamic Application and will appear as an option in the **Device Summary** page.
4. Click the **[Save]** button.

NOTE: If a PowerPack updates one or more Dynamic Applications, Skylar One will not overwrite the alignment between device dashboards and any updated Dynamic Applications.

Editing a Device Dashboard

To edit a device dashboard:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, find the device dashboard you want to edit. Click its wrench icon ( ).
3. The **Device Dashboard Editor** page appears. Edit one or more fields and/or the dashboard widgets.
4. Skylar One automatically saves your changes.

Deleting a Device Dashboard

To delete one or more device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for each dashboard you want to delete.
3. In the ***Select Action*** drop-down list, select *Delete Dashboards*.
4. Click the **[Go]**button. The selected device dashboard(s) will no longer appear in this page or be accessible in the **Device Summary** page.

NOTE: You cannot delete a device dashboard that is defined as the Global Default.

Copying a Device Dashboard

To copy one or more device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for each dashboard you want to copy.
3. In the ***Select Action*** drop-down list, select *Copy Dashboards*.
4. Click the **[Go]** button. One or more new device dashboards will appear in this page with names that start with "Copy of".

Defining the Global Default for Device Dashboards

The device dashboard that is defined as the "Global Default" is the default dashboard that appears in the in the **Device Summary** page for each device.

Skylar One decides what to display in the **Device Summary** page as follows:

- If the device is manually aligned with a device dashboard (in the **Device Properties** page), that dashboard is displayed in the **Device Summary** page for the device.
- If the device is not manually aligned with a device dashboard, the device dashboard that is aligned with the Device Class is displayed.
- If the device class is not aligned with a device dashboard, the device dashboard that is aligned with the Device Category is displayed.
- If the device category is not aligned with a device dashboard, the device dashboard that is defined as the "Global Default" is displayed.

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

NOTE: Although you can align a device dashboard with a Dynamic Application, the device dashboards that are aligned with Dynamic Applications are never displayed in the **Device Summary** page as the default display. However, from the **Device Summary** page, a user can select and view any device dashboards that are aligned with Dynamic Applications for the device.

To define the Global Default for device dashboards:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard you want to define as the Global Default.
3. In the ***Select Action*** drop-down list, select *Set Global Default Device Dashboard*.
4. Click the **[Go]** button. In the ***Global Default*** field for the selected device dashboard the value "Yes" will appear.

Unaligning a Device Dashboard

If you no longer want a device dashboard to appear as an option in the **Device Summary** page for any devices, you can remove all alignments for that device dashboard. To do this:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard you want to remove from the **Device Summary** page.
3. In the ***Select Action*** drop-down list, select *Unalign Device Dashboard(s)*.
4. Click the **[Go]** button.
5. The selected dashboards are no longer aligned with Device Categories, Device Classes, Devices, or Dynamic Applications. The selected dashboards will no longer appear as an option in the **Device Summary** page for any devices.

Moving Alignment for Device Dashboards

You can specify that you want a device dashboard to "steal" all the alignments from another device dashboard. When you do this, the device dashboard that is stolen from will no longer have any alignment. To move alignments from one dashboard to another:

1. Go to the **Device Dashboards** page (System > Customize > Device Dashboards).
2. In the **Device Dashboards** page, select the checkbox for the dashboard that you want to "steal" alignments.
3. In the ***Select Action*** drop-down list, select *Replace Dashboard Alignments with* and then select the device dashboard that you want to "steal" alignments from.
4. Click the **[Go]** button.
5. The **Device Dashboards** page shows that the alignments have been removed from the device dashboard that you chose in the ***Select Action*** drop-down. In the **Device Dashboards** page, the device dashboard for which you selected the checkbox now displays all the alignments that it "stole" from the other device dashboard.

Chapter 18

Using Custom Attributes

Overview

This chapter describes how to use custom attributes in Skylar One.

This chapter covers the following topics:

Custom Attributes 279

Viewing the List of Custom Attributes 280

Creating Custom Attributes 284

Adding Custom Attributes for a Device 285

Custom Attributes in the ScienceLogic API 287

Using the ScienceLogic API to View, Create, and Edit Custom Attributes 288

Using a Dynamic Application to Create and/or Populate Custom Attributes 288

Using Custom Attributes to Define Device Groups 290

Viewing Custom Attributes in the Custom Table Widget 291

Custom Attributes

Custom Attributes are name-value pairs. You can use custom attributes to add custom descriptive fields to assets, devices, interfaces, services, themes, and vendors. In Skylar One, you can create and update custom attributes via the API, in configuration Dynamic Applications, and in the **Custom Attribute**

Manager page. Custom attributes can be used to dynamically define device groups and can be viewed with the custom table widget.

There are two categories of custom attributes:

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

Viewing the List of Custom Attributes

The **Custom Attribute Manager** page (Manage > Custom Attributes) displays a list of all the existing custom attributes created through the user interface.

> **TIP:** You can use the ***Search*** field to look for specific items in the list. For more information, see *Using Basic Search* in the ***Introduction to Skylar One*** manual. If you are looking for a very specific set of device classes, click the gear icon (⚙) to the right of the ***Search*** field and select *Advanced*. In this mode, you can create an advanced search using "AND" or "OR" for multiple search criteria. For more information, see *Performing an Advanced Search* in the ***Introduction to Skylar One*** manual.

The same information is available on the classic **Custom Attribute Manager** page (System > Manage > Custom Attributes).

For each custom attribute, the **Custom Attribute Manager** page displays the following information:

- ***Display Name***. Name for the custom attribute. This value appears in the user interface.
- ***Internal Field Name*** (classic only). Name for the custom attribute that complies with XML naming rules. If the value in the ***Display Name*** field does not comply with XML rules, Skylar One will convert the value to a name that complies with XML rules. The ***Internal Field Name*** is the unique ID of each Custom Attribute, and you cannot change it after the custom attribute has been created.

> **NOTE:** Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character, or an extending character. If a value in the ***Display Name*** column does not conform to XML standards, Skylar One will replace non-valid characters with an underscore plus the hexadecimal value of the illegal character plus an underscore. So "serial number" would be replaced with "serial_X20_number".

- ***Value Type***. Specifies the type of value that will be saved in the custom attribute. Choice are:

- *String*. Non-numeric value
- *Integer*. Numeric value

- ***Attribute Type***. Specifies the behavior of the custom attribute. Choices are:
  - *Base*. A base custom attribute is automatically aligned to all members of the specified ***Resource Type***. For example, a base custom attribute for devices would be aligned with each and every device in your Skylar One System.
  - *Extended*. An extended custom attribute is manually assigned only to some members of the ***Resource Type*** and should not be assigned to all members of the ***Resource Type***. For example, you could apply the custom attribute cisco_ios_version only to those asset records for Cisco devices; you would not want to assign this custom attribute to all asset records.
- ***Resource Type***. Specifies the ScienceLogic element that will use the custom attribute. Choices are:
  - *Asset*. Custom attribute will be associated with one or more asset records.
  - *Device*. Custom attribute will be associated with one or more devices.
  - *Interface*. Custom attribute will be associated with one or more network interfaces.
  - *Service*. Custom attribute will be associated with one or more services.
  - *Theme*. Custom attribute will be associated with one or more user-interface themes.
  - *Vendor*. Custom attribute will be associated with one or more vendor records.
- ***Database Index***. Specifies how the custom attribute is stored in the ScienceLogic database. Choices are:
  - *None*. Custom attribute is not indexed.

    NOTE: Extended custom attributes allow only the value *None* in this field.

  - *Unique*. For base custom attributes, ensures that the value of each base custom attribute is unique within its ***Resource Type***.
  - *Index*. For base custom attributes, allows Skylar One to efficiently search for custom attributes in the ScienceLogic database.

- ***Subscribers*** (classic user interface only). Specifies the ***Resource Type*** and number of subscribers. Possible values in this field include:

> **NOTE:** For base custom attributes, the value in the ***Subscribers*** column is always "- - " (dash dash).

  - *(Asset)*. Custom attribute is associated with one or more asset records. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Asset.
  - *(Device)*. Custom attribute is associated with one or more devices. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Device.
  - *(Interface)*. Custom attribute is associated with one or more network interfaces. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Interface.
  - *(Theme)*. Custom attribute is associated with one or more user-interface themes. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Theme.
  - *(Vendor)*. Custom attribute is associated with one or more vendor records. Clicking on the icon displays the **Custom Attribute Subscribers** page, where you can view details about each subscriber of type Vendor.
- ***Subscriber Count*** (Skylar One user interface only). Lists the number of subscribers to this custom attribute.

Viewing the List of Subscribers for a Custom Attribute

To view a list of subscribers for a custom attribute:

1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes) .
2. Click the icon in the ***Subscribers*** column.
3. The **Custom Attribute Subscribers** modal page appears.
   - For (*Asset*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
     - ***Make***. Make of the asset.
     - ***Model***. Model of the asset.
     - ***Device***. If applicable, name of the device associated with the asset record.
     - ***Asset Tag***. Asset tag associated with the asset.
     - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.

- For (*Device*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
    - ***DID***. Device ID for the device. Skylar One automatically assigns this value to the device.
    - ***Device Name***. Name of the device.
    - ***IP Address***. If applicable, the IP address associated with the device.
    - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Interface*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
    - ***Device Name***. Name of the device associated with the interface.
    - ***IF Name***. Name of the interface.
    - ***IF Port***. Port number associated with the interface.
    - ***Alias.*** Alias associated with the interface.
    - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Theme*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
    - ***ID***. Unique ID associated with the theme. Skylar One automatically assigns this value to the theme.
    - ***Theme Name***. Name of the theme.
    - ***HTML Header/Title***. HTML header associated with the theme.
    - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.
- For (*Vendor*), the **Custom Attribute Subscribers** modal page displays the following for each subscriber:
    - ***ID***. Unique ID associated with the vendor. Skylar One automatically assigns this value to the vendor.
    - ***Vendor Name***. Name of the vendor.
    - ***Name of the custom attribute***. The value assigned to the custom attribute for this subscriber.

Creating Custom Attributes

You can create custom attributes on the **Custom Attributes** page (or on the **Custom Attribute Manager** page in the classic Skylar One user interface), via the ScienceLogic API, or by using a configuration Dynamic Application. The following rules apply to the creation of custom attributes:

- If you define a base custom attribute for devices on the **Custom Attributes** page (or on the **Custom Attribute Manager** page in the classic Skylar One user interface), that base custom attribute is aligned with each device in your system. The value of the base custom attribute will be null until you assign a value for each device.
- If you define an extended custom attribute for devices on the **Custom Attributes** page (or on the **Custom Attribute Manager** page in the classic Skylar One user interface), that extended custom attribute is not aligned with any devices.
- You can use the **Attributes** page in the **Device Administration** panel to assign a value or edit the value for each custom attribute aligned with a device. For more information, see the section on *Managing a Single Device with the Device Administration Panel*.
- You can use Dynamic Applications of type "configuration" to create custom attributes and/or assign values to custom attributes for devices. For details, see the section on *Using a Dynamic Application to Create and/or Populate Custom Attributes*.
- If you create a base custom attribute for asset records, network interfaces, themes, and vendor records, those custom attributes will appear in the ScienceLogic API for the specified entity. Initially, the value of the base attribute will be null. You cannot use the Skylar One user interface to assign a value to these base custom attribute. You must use the ScienceLogic API to assign values to these base custom attribute. For details, see the section on *Custom Attributes in the ScienceLogic API*.
- If you create an extended custom attribute for asset records, network interfaces, themes, and vendor records, those custom attributes can be aligned and populated using the ScienceLogic API. You cannot use the Skylar One user interface to assign a value to these extended custom attributes. You must use the ScienceLogic API to assign values to these extended custom attributes. For details, see the section on *Custom Attributes in the ScienceLogic API*.
- If you create a new "unique" custom attribute, you cannot assign the same value for that custom attribute to multiple devices. Each device must have a unique value for that custom attribute.
- You can use an API call to "unsubscribe" interfaces from the extended custom attribute. For example:

```
curl -k -v -H 'X-em7-beautify-response:1'
http://em7admin:<password>@10.2.15.81/api/device/1/interface/1 -H
'content-type:application/json' -d '{"c-apple_ext_test":null}'
```

  In this example the custom attribute is called `apple_ext_test`, and you need add `c-` at the start of the name in the API call to match how it is stored in the database. In the example above, the Device ID is 1, the Interface ID is also 1, and the Custom Attribute unique name or ID is `c-apple_ext_test`. This call sets the custom attribute to `null`, which unsubscribes the interface.

To create a custom attribute from the **Custom Attribute Manager** page:

1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes).
2. In the bottom-most row, enter a value in each field.
3. Click the **Save** icon ( ).

Deleting One or More Custom Attributes

From the **Custom Attribute Manager** page, you can delete custom attributes from Skylar One. To do this:

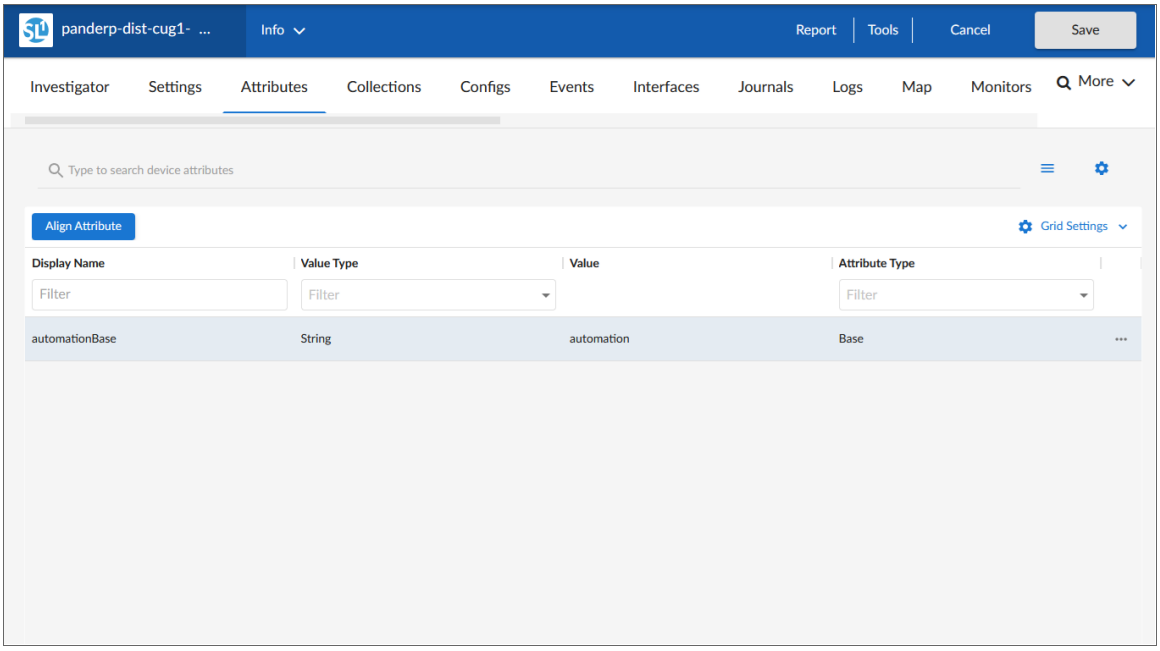
1. Go to the **Custom Attribute Manager** page (System > Manage > Custom Attributes).
2. Select the checkbox for each custom attribute you want to delete.
3. Click the ***Select Action*** field in the lower-right and select *DELETE Custom Attributes*.
4. Click the **[Go]** button.

> **NOTE:** Skylar One will not allow you to delete an extended custom attribute that is aligned with one or more subscribers. If you try to delete an extended custom attribute that is aligned with one or more subscribers, Skylar One will display the error message: "Error: Some attributes have entities aligned. Unalign entity from attribute before deleting." This message appears to the right of the page title.

Adding Custom Attributes for a Device

You can view detailed data about a specific device by clicking the device name on the **Devices** page ( ) to open the **Device Investigator** page for that device.

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



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

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

1. On the **[Attributes]** tab for the device, click **[Edit]** and then click **[Align Attribute]**. The **Align Extended Attribute** window appears.
2. Complete the following fields:
   - ***Attributes***. Select the name of the custom attribute.
   - ***Attribute value***. Specify a text or numeric value for the attribute, based on its value type.

     NOTE: If the custom attribute has a ***Database Index*** of *Unique*, each device must have a unique value for that custom attribute
3. Click **[Align Attribute]**. The custom attribute is added to the list on the **[Attributes]** tab.
4. To edit an attribute in the list, click the **[Actions]** button (⋯) for that attribute and select *Edit Attribute*.
5. To unalign an attribute, click the **[Actions]** button (⋯) for that attribute and select *Unalign Attribute*.
6. When you are done adding, editing, or unaligning attributes, click **[Save]**.

NOTE: Upon saving, your attribute changes will be reflected in the ***More Attributes*** section of the *Info drop-down*.

Adding Custom Attributes for a Device in the Classic Skylar One User Interface

For information about how to add custom attributes for a device in the classic Skylar One user interface, see the section on *Aligning Custom Attributes with a Device*.

Custom Attributes in the ScienceLogic API

The ScienceLogic API includes resources for adding custom attributes to the following resources:

- /asset
- /device
- The /interface sub-resource under /device resources
- /theme
- /vendor

When you define a custom attribute for a resource:

- For any instance of that resource (e.g., a specific device), you can perform a POST operation specifying a value for that attribute for that instance.
- If you configure the attribute as a base attribute, the attribute will appear in the list of fields for all instances of that resource. For example, if you define a custom attribute as a base attribute for the /device resource, the response to a GET request for any /device/*device_id* resource includes the custom attribute in the list of fields.
- If you configure the attribute as an extended attribute, the attribute will appear in the list of fields for instances of that resource only if a value has been specified for the attribute for that instance. For example, suppose you define a custom attribute as an extended attribute for the /device resource. The response to a GET request on the /device resource index with the extended_fetch option enabled will include the custom attribute only for devices that have a value for that custom attribute.
- GET requests for the resource index can include filter and sort criteria that use that custom attribute.

When you define a value for a custom attribute by performing a POST request to a resource, the value is available through the API and can be used in dynamic rules for device groups and viewed in the custom table widget.

Using the ScienceLogic API to View, Create, and Edit Custom Attributes

You can use the ScienceLogic API to view, edit, and create custom attributes. For more information, ask your ScienceLogic contact for access to the ScienceLogic API documentation.

Using a Dynamic Application to Create and/or Populate Custom Attributes

For details on creating a Dynamic Application or creating collection objects, see the manual ***Dynamic Application Development***.

One of the ways you can create and/or populate a custom attribute for devices is through a Dynamic Application of type *configuration*.

In Dynamic Applications of archetype *configuration*, you can:

- Use a collection object to populate the value of an existing custom attribute.
- Use a pair of collection objects to create a custom attribute and provide a value for that custom attribute. You must define a collection object to define the name of the custom attribute; this causes the Skylar One system to create a custom attribute with the name from the collection object. You must also define a second collection object to populate the value of the custom attribute.

NOTE: For details on creating and managing custom attributes, see the manual ***Using the ScienceLogic API***.

NOTE: For component devices, only assigned Collector Affinity is supported when using a Dynamic Application to populate custom attributes. If a custom attribute value is manually edited or removed for a device that is using a different collector than its root device, the Dynamic Application will not be able to update the value on subsequent polls unless the Dynamic Application is using assigned Collector Affinity. For more information, see the section on *Collector Affinity*.

The following fields in the **Collection Objects** page allow you to use one or more collection objects to define and/or populate a custom attribute:

- ***Align to Custom Attribute***. Specify the custom attribute to associate with this collection object. The custom attribute will be populated with a value from a collection object. Choices are:
    - *None*. This collection object is not associated with a custom attribute.
    - *Static*. This collection object is associated with a specific custom attribute.

- ***Static Name***. If you selected *Static* in the ***Custom Attribute*** field, the *Static Name* field appears. In this field, specify the name of the custom attribute that you want to populate with the value of the collection object. You can select from a list of existing custom attributes.
    - If the list does not include the custom attribute you want to align with the collection, select the plus-sign icon (+). The icon clears the field and allows you to manually enter a value.
    - If you manually specify a custom attribute, Skylar One will search for a custom attribute with a matching name and populate the custom attribute with the value of this collection object. If Skylar One does not find a custom attribute with a matching name and therefore creates the custom attribute, the new custom attribute will be an extended custom attribute, for devices. The data type will be integer (for numeric values) or string (for all other value types).
- *Dynamic Name*. You can use a pair of collection objects to populate the name and value of a custom attribute. You must define each collection object separately. When you select *Dynamic Name* in the ***Custom Attribute*** field, the name of the custom attribute is populated with the value of the collection object. If Skylar One does not find a custom attribute with a matching name, Skylar One will create the custom attribute. If Skylar One does not find a custom attribute with a matching name and therefore creates the custom attribute, the new custom attribute will be an extended custom attribute, for devices. The data type will be integer (for numeric values) or string (for all other value types).

NOTE: If you select *Dynamic Name* in the ***Custom Attribute*** field, you must create a second collection object that will populate the value of the custom attribute.

NOTE: Names for custom attributes must conform to XML naming standards. The attribute name can contain any combination of alphanumeric characters, a period, a dash, a combining character or an extending character. If a collected value for an attribute name does not conform to XML standards, Skylar One will replace non-valid characters with an underscore + the hexadecimal value of the illegal character + an underscore. So "serial number" would be replaced with "serial_X20_number". The attribute label will use the original, non-converted value ("serial number").

- ***Dynamic Value***. The value of the custom attribute selected in the *Dynamic Name* field is populated with the value of the collection object.
- ***Dynamic Name***. If you selected *Dynamic Value* in the ***Custom Attribute*** field, the *Dynamic Name* field appears. Select from the list of collection objects that have a ***Custom Attribute*** value of *Dynamic Name*.

NOTE: The collection object assigned to the *Dynamic Value* is added to the same ***Group*** as the collection object assigned to the associated *Dynamic Name*. If the collection object for *Dynamic Name* is not assigned to a ***Group***, you will be prompted to select a ***Group*** for the both the collection object for *Dynamic Name* and the collection object for *Dynamic Value*.

NOTE: Each group can contain only one collection object that is assigned to a *Dynamic Value* and only one collection object that is assigned to a *Dynamic Name*. The group can contain other collection objects, but should not contain more than one collection object assigned to a *Dynamic Value* and not more than one collection object assigned to a *Dynamic Name*.

Using Custom Attributes to Define Device Groups

A device group is a group of multiple devices, grouped together for ease of management. You can use custom attributes to define membership in a device group. Only devices that have a specific value for a custom attribute will be included in the device group.

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

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

In the **Device Group Rule Editor** page, the ***Active Selectors*** field includes an entry for each custom attribute you have defined with the API or with a Dynamic Application. When you select a custom attribute, the ***Selector Definitions*** pane displays a field in which you can enter a string. Skylar One will use the string to search for devices that have a matching value for this custom attribute.

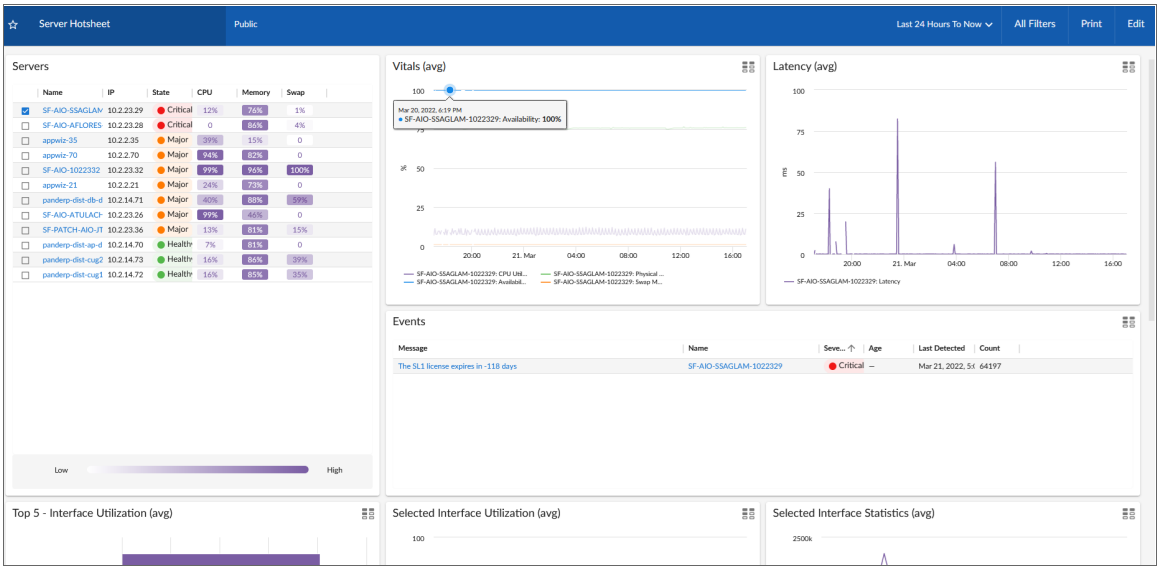
In the example above, we selected the custom attribute *Device:Color* and specified the value *red*. Our device group will include only devices that ihave the value *red* assigned to the *Device:Color* custom attribute.

For additional details on defining device groups and defining device group rules, see the manual ***Device Groups and Device Templates***.

Viewing Custom Attributes in the Custom Table Widget

A dashboard is a page that displays one or more graphical reports, called widgets. Skylar One includes pre-defined widgets that can be customized and displayed in the **Dashboards** page. These widgets are displayed in their own pane, and display graphs, tables, and/or text.

To define an instance of a widget, you first select from a list of pre-defined widget definitions, and then customize what will be displayed by the selected widget by supplying values in the option fields provided by that widget.



The **Custom Table** widget displays multiple instances of an entity in a table. The **Custom Table** widget can be configured to display a list of devices, device classes, or device groups (and also other entities).

The generated table displays information about each entity in the list. You can configure which information is included in the table in the ***Layout Editor*** pane during configuration.

The **Layout Editor** panel displays the columns that will be displayed in the widget.

In the example above, *Color* and *Device Location* are custom attributes for devices.

If you selected *Device*,or *Asset*, or *Interface* in the ***Entity Type*** field of the Custom Table Widget, the Layout Editor will include columns for the custom attributes defined in your system for that entity type.

- By default, the columns for the custom attributes are excluded from the configuration.
- If an extended custom attribute is defined in your system but has not been assigned a value for any asset, device, or interface, it will not appear in the list of columns.

You can add or remove custom attributes from the layout of the widget using the following buttons:

- **<|>** You can move columns from left to right by clicking on the arrow characters at the top of each column and dragging the column left or right. Double-clicking on the arrow moves the column out of the display past a black bar to the right. All disabled columns can be seen to the right of the black bar. Double-clicking on the arrow again moves the column back into the display.

For additional details on configuring the Custom Table Widget, see the ***Dashboards*** manual.

© 2003 - 2026, ScienceLogic, Inc.

All rights reserved.

ScienceLogic™, the ScienceLogic logo, and ScienceLogic's product and service names are trademarks or service marks of ScienceLogic, Inc. and its affiliates. Use of ScienceLogic's trademarks or service marks without permission is prohibited.

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

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

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

International: +1-703-354-1010