ScienceLogic

Monitoring Cisco Unified Communications Ancillary Devices

Cisco: UC Ancillary PowerPack version 104

Table of Contents

Introduction 1

What are Ancillary Cisco UC Devices? 1

What Does the Cisco: UC Ancillary PowerPack Monitor? 2

Installing the Cisco: UC Ancillary PowerPack 2

Configuration and Credentials 4

Prerequisites for Monitoring Ancillary Cisco Unified Communications Devices 4

Creating an SNMP Credential 5

Creating an SSH/Key Credential 5

Creating an SSH/Key Credential in the SL1 Classic User Interface 6

Discovery 8

Discovering Ancillary Cisco UC Devices 8

Discovering Cisco UC AncillaryComponent Devices 9

Manually Aligning Dynamic Applications 10

Viewing Ancillary Cisco UC Devices 11

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco UC Ancillary devices in SL1 using the "Cisco: UC Ancillary" PowerPack.

This chapter covers the following topics:

What are Ancillary Cisco UC Devices? 1

What Does the Cisco: UC Ancillary PowerPack Monitor? 2

Installing the Cisco: UC Ancillary PowerPack 2

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

What are Ancillary Cisco UC Devices?

SL1 enables you to monitor ancillary Cisco UC devices, including Cisco Unified Border Element (CUBE)-enabled devices and Cisco Emergency Responder.

CUBE is a Session Border Controller that extends Session Initiation Protocol-based voice and video connectivity between networks. It can run on a variety of Cisco routers or can be deployed virtually.

Emergency Responder supplements the emergency 9-1-1 functionality offered by Cisco Unified Communications Manager (CUCM) by helping CUCM pinpoint the location of emergency callers.

What Does the Cisco: UC Ancillary PowerPack Monitor?

To monitor ancillary UC devices using SL1, you must install the "Cisco: UC Ancillary" PowerPack. The PowerPack includes:

- An example credential you can use as a template to create SSH/Key credentials to connect to the devices you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and/or collect configuration data for ancillary UC devices
- Device classes for each of the ancillary UC devices that SL1 monitors
- Event policies that are triggered when ancillary UC devices meet certain status criteria
- A device dashboard that displays host resource and interface information about ancillary UC devices

Installing the Cisco: UC Ancillary PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Cisco: UC Ancillary" PowerPack.

IMPORTANT: Ensure that you are running version 12.1.0 or later of SL1 before installing this PowerPack. For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the section on *Global Settings*.

NOTE: For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Credentials

Overview

The following sections describe how to configure ancillary Cisco Unified Communications devices for monitoring by SL1 using the "Cisco: UC Ancillary" PowerPack:

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

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

This chapter covers the following topics:

Prerequisites for Monitoring Ancillary Cisco Unified Communications Devices 4

Creating an SNMP Credential 5

Creating an SSH/Key Credential 5

Prerequisites for Monitoring Ancillary Cisco Unified Communications Devices

To configure SL1 to monitor ancillary Cisco Unified Communications (UC) devices using the "Cisco: UC Ancillary" PowerPack, you must have already properly installed and configured the ancillary Cisco UC devices that you want to monitor. You must also note the following information, as appropriate, for each of the ancillary UC devices you want to monitor:

- SNMP community string
- Secure Shell (SSH) username and password to monitor Cisco voice components

Creating an SNMP Credential

SL1 uses SNMP to collect information about the devices that can be monitored using the Dynamic Applications in the "Cisco: UC Ancillary" PowerPack. To monitor these devices, you must first define an SNMP credential that enables SL1 to communicate with the devices.

To configure an SNMP credential:

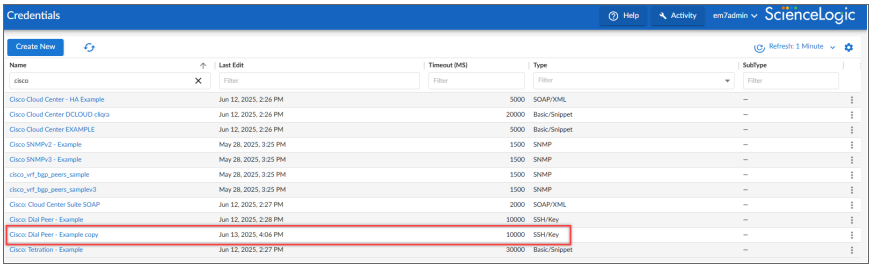
1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click **[Create]**.
3. In the drop-down list that appears, select *SNMP Credential*. The **Credential Editor** page appears.
4. In the ***Profile Name*** field, type a name for the credential.
5. In the ***SNMP Version*** field, select *SNMP V2*.
6. In the ***SNMP Community (Read Only)*** field, type the community string for the device you want to monitor.
7. Optionally, supply values in the other fields in this page. In most cases, you can accept the default values for the other fields.
8. Click **[Save]**.

Creating an SSH/Key Credential

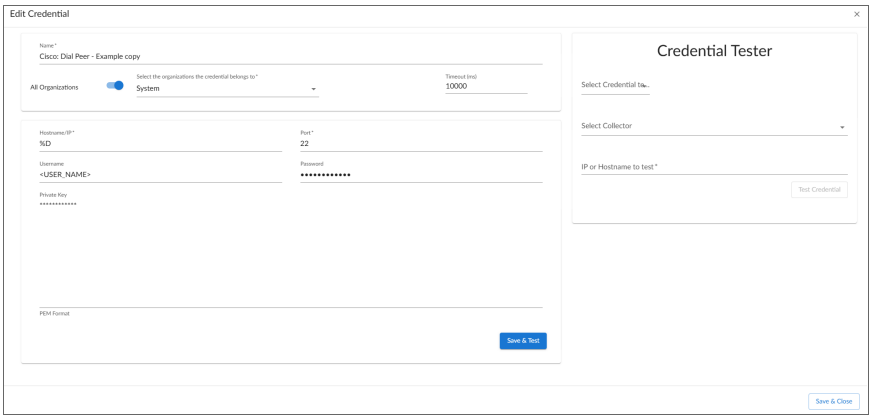
To configure SL1 to monitor ancillary Cisco Unified Communications (UC) devices, you must first create an SSH/Key credential that allows the Dynamic Applications in the "Cisco: UC Ancillary" PowerPack to connect with these devices. An example SSH/Key credential that you can edit for your own use is included in the "Cisco: UC Ancillary" PowerPack.

To create an SSH/Key credential to access ancillary Cisco UC devices:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "Cisco: Dial Peer - Example" credential, then click its **[Actions]** icon (⋮) and select *Duplicate* from the drop-down field. The "Cisco: Dial Peer - Example copy" credential appears.



3. Click the **[Action]** icon (⋮) for the "Cisco: Dial Peer - Example copy" credential and then select *Edit*. The **Edit Credential** page appears.



4. Enter values in the following fields:
    - ***Name***. Type a new name for the credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***Select the organizations the credential belongs to*** drop-down field to align the credential with those specific organizations.
    - ***Timeout***. Enter the time, in milliseconds, after which SL1 will stop trying to communicate with the Cisco UC Ancillary device. The default value is *10000*. This field is required.
    - ***Hostname/IP***. Keep the default value of %D.
    - ***Port***. Type "22".
    - Username. Type the username for the user account that you configured in the Cisco UC Ancillary Manager.
    - ***Password***. Type the password for the user account that you configured in the Cisco UC Ancillary Manager.
5. Click **[Save & Close]** to update your credential.

Creating an SSH/Key Credential in the SL1 Classic User Interface

To configure SL1 to monitor ancillary Cisco Unified Communications (UC) devices in the classic user interface, you must first create an SSH/Key credential that allows the Dynamic Applications in the "Cisco: UC Ancillary" PowerPack to connect with these devices. An example SSH/Key credential that you can edit for your own use is included in the "Cisco: UC Ancillary" PowerPack.

To create an SSH/Key credential to access ancillary Cisco UC devices in the classic user interface:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the "Cisco: Dial Peer - Example" credential, and then click its wrench icon (🔧). The **Edit SSH/Key Credential** modal page appears.
3. Type values in the following fields:
    - ***Credential Name***. Type a new name for the credential.
    - ***Hostname/IP***. Type "%D".
    - ***Port***. Type "22".

- ***Username***. Type the administrator username used to connect to the dial peers via SSH.
- ***Password***. Type the password used to connect to the dial peers via SSH.
- ***Private Key (PEM Format)***. Leave this field blank.

> **NOTE:** The private key can have a maximum of 64 characters per line. Therefore, you cannot use keys in the OpenSSH format, because that format uses 70 characters per line. When you attempt to save the credential, SL1 will validate that the private key entered is in the correct format. You will be able to save the credential only if the private key is correctly formatted.

4. Click **[Save As]**.
5. When the confirmation message appears, click **[OK]**.

Chapter 3

Discovery

Overview

The following sections describe how to discover ancillary Cisco Unified Communications devices for monitoring by SL1 using the "Cisco: UC Ancillary" PowerPack:

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

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

This chapter covers the following topics:

Discovering Ancillary Cisco UC Devices 8

Discovering Cisco UC AncillaryComponent Devices 9

Manually Aligning Dynamic Applications 10

Viewing Ancillary Cisco UC Devices 11

Discovering Ancillary Cisco UC Devices

To create and run a discovery session that will discover ancillary Cisco UC devices, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
2. In the **Discovery Control Panel**, click **[Create]**.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields:
    - ***IP Address/Hostname Discovery List***. Type the IP addresses for the devices you want to discover.
    - ***SNMP Credentials***. Select the SNMP credential you created for the ancillary devices.

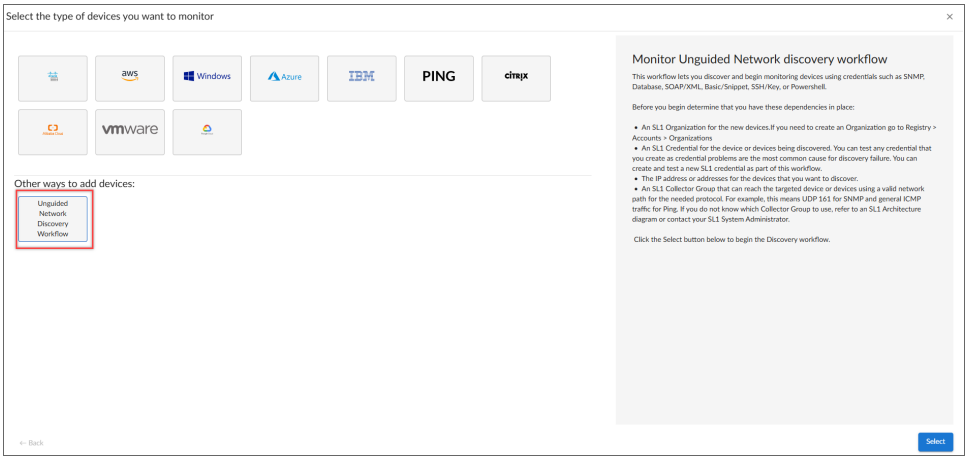
- ***Other Credentials***. Select the SSH/Key credential you created for the ancillary devices.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click **[Save]** to save the discovery session, and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning bolt icon ( ) to run the discovery session.
7. The **Discovery Session** window appears. When the ancillary devices are discovered, click the device icon ( ) to view the **Device Properties** page for each device.

Discovering Cisco UC AncillaryComponent Devices

To create and run a discovery session that will discover a Cisco UC Ancillary appliance:

1. Go to the **Devices** page ( ) or the **Discovery Session** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.



3. Click **[Select]**. The **Add Devices** page appears.
4. Complete the following fields:
   - ***Discovery Session Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Session]** tab.
   - ***Description***.Optional. Type a short description of the discovery session. You can use the test in this description to search for the discovery session on the **[Discovery Session]** tab.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears.
6. On the **Credentials** page, locate and select the SSH/Key credential you created for Cisco UC Ancillary appliances.
7. Click **[Next]**. The **Discovery Session**page of the **Add Devices** wizard appears.
8. Complete the following fields:
    - ***List of IP/Hostnames***. Type the IP address for the Cisco UC Ancillary appliance.
    - ***Which collector will monitor these devices?***. Required. Select an existing collector to monitor the discovered devices.
    - ***Run after save***. Select this option to run this discovery session as soon as you save the session.
    - ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
        - ***Discover Non-SNMP***. Enable this setting.
        - ***Model Devices***. Enable this setting.
        - ***Select Device Template***. If you configured a Cisco UC Ancillary device template, select it here. Otherwise, leave the default selection.
9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Session** page (Devices > Discovery Sessions) will display the new discovery session.

Manually Aligning Dynamic Applications

When you run the discovery session for ancillary UC devices, SL1 automatically aligns the necessary Dynamic Applications to the devices.

To verify that the Dynamic Applications aligned to the devices correctly:

1. After discovery has completed, click the device icon ( ) for any of the discovered devices. The **Device Properties** page appears.
2. From the **Device Properties** page, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
3. All applicable Dynamic Applications for the device are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

If the "Cisco: Dial Peer Voice Summary" or "Cisco: Active Voice Call Legs Performance" Dynamic Applications did not automatically align to a voice device, you might need to manually align the SSH/Key credential to the physical router running the Cube feature set and then run discovery again.

To manually align the SSH/Key credential to the router:

1. Go to the Device Manager page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface).
2. Locate the physical router running the Cube feature set and click its wrench icon (). The **Device Properties** page appears.
3. Select the SSH/Key credential you created for ancillary UC devices.

> **NOTE:** If there are other credentials (for example, an SNMP credential) already aligned to the device, hold the <Ctrl> or <Command> key when selecting the SSH/Key credential to keep the other credentials aligned to the device as well.

4. Click **[Save]**.
5. Close the **Device Properties** page and go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
6. Locate the discovery session for ancillary UC devices and click its lightning bolt icon () to re-run the discovery session.

If any of the other Dynamic Applications did not automatically align to a device during discovery, you can align them manually to the device.

To manually align a Dynamic Application to a device:

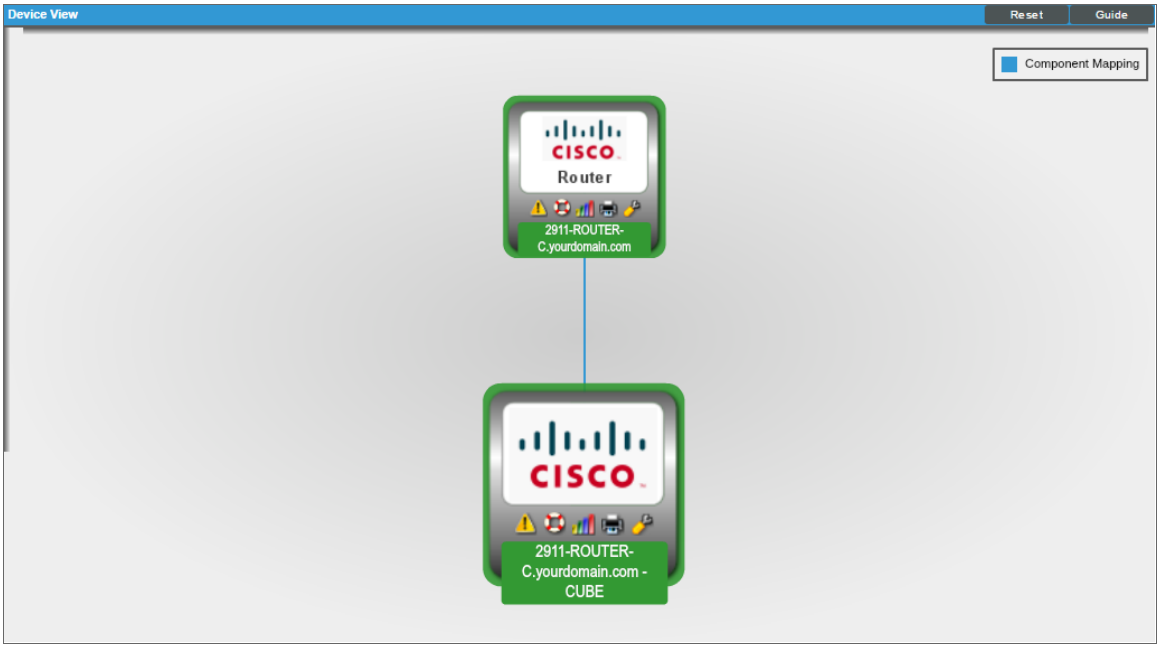
1. From the **Dynamic Application Collections** page (Registry > Devices > wrench icon > Collections), click the **[Action]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears.
2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
3. In the ***Credentials*** field, select one or more of the credentials you created for the ancillary UC devices.
4. Click **[Save]**.
5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

Viewing Ancillary Cisco UC Devices

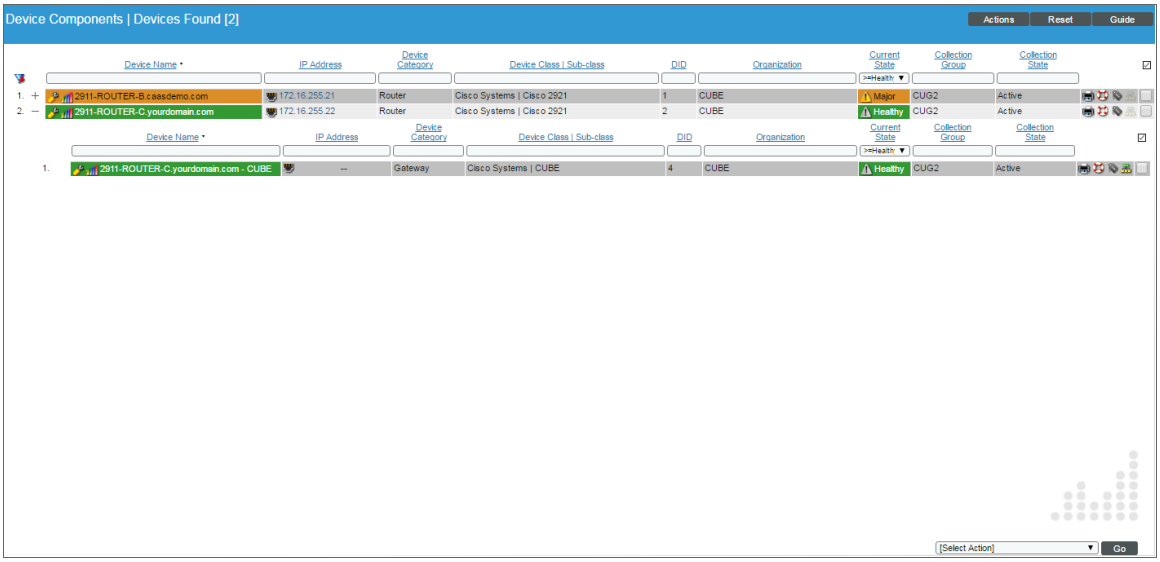
When SL1 discovers your ancillary UC devices, SL1 creates component devices that represent each component in your ancillary UC system.

In addition to the **Device Manager** page, you can view component devices in the following places in the user interface:

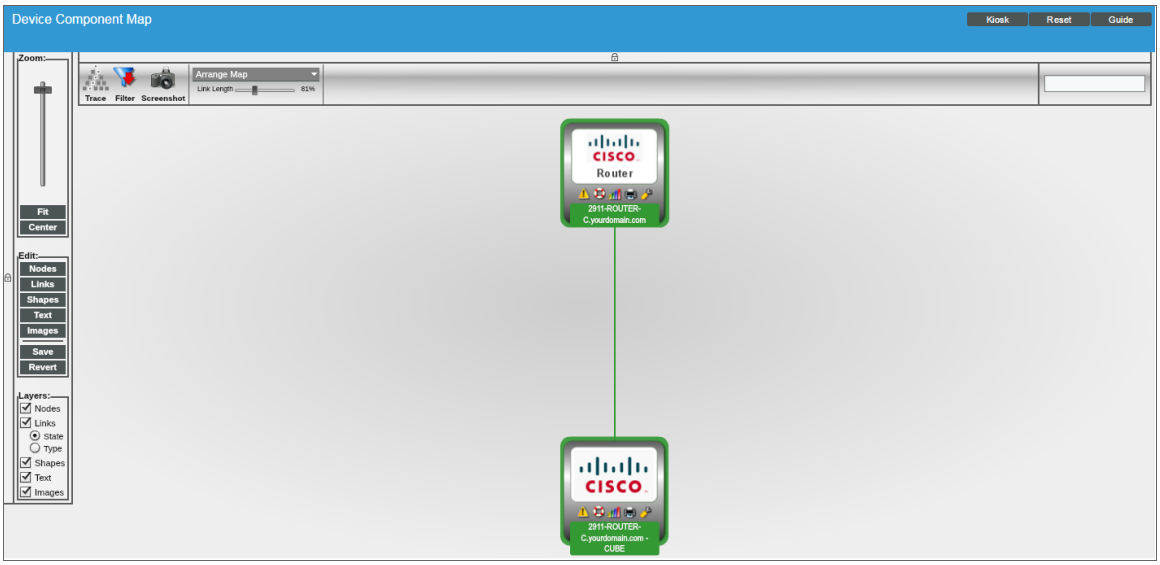
- The **Device View** modal page (click the bar-graph icon [ ] for a device, and then click the **Topology** tab) displays a map of the selected device and all of the devices with which it has parent-child relationships. Double-clicking any of the devices reloads the page with the selected device as the primary device:



- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1, in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with your ancillary UC devices, find a device cluster and click its plus icon (+):



- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for your ancillary UC devices, go to the **Component Map** page and select a map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



© 2003 - 2025, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010