



---

# Monitoring Cisco Unified Communications Manager

Cisco: CUCM Unified Communications Manager PowerPack version 111 (Revision 2)

---

# Table of Contents

<b>Introduction</b> .....	<b>3</b>
What is Cisco Unified Communications Manager? .....	3
What Does the Cisco: CUCM Unified Communications Manager PowerPack Monitor? .....	4
Supported Versions .....	4
Installing the Cisco: CUCM Unified Communications Manager PowerPack .....	4
<b>Configuration and Credentials</b> .....	<b>6</b>
Prerequisites for Monitoring CUCM .....	6
Configuring the ScienceLogic Platform to Monitor CUCM .....	7
Enabling the CUCM AXL Web Service .....	10
Configuring a CUCM User Account .....	11
Configuring Prime License Manager .....	18
Creating a CUCM Credential .....	20
Testing the CUCM Credential .....	21
Manually Creating Host File Entries for CUCM Nodes .....	23
<b>Discovery</b> .....	<b>25</b>
Discovering a CUCM Cluster .....	26
Discovering a CUCM Cluster in the SL1 Classic User Interface .....	28
Verifying Discovery and Dynamic Application Alignment .....	30
Manually Aligning Dynamic Applications .....	32
Viewing Component Devices .....	34
Viewing Component Devices in the SL1 Classic User Interface .....	35
<b>Dashboards</b> .....	<b>37</b>
Installing the CUCM Dashboards .....	37
Cisco: CUCM Performance Dashboard .....	38
Cisco: CUCM Locations LBM .....	39
Cisco: CUCM Media Resources .....	40
Cisco: CUCM Media Resources (Simple) .....	41
Cisco: CUCM Tomcat .....	42
Cisco: CUCM Overall Cluster Health .....	43
Cisco: CUCM Active Calls .....	44
<b>Troubleshooting</b> .....	<b>46</b>
Resolving Network Connectivity Issues .....	46
Resolving Credential Issues .....	47
Basic/Snippet (AXL User) Credentials .....	47
SNMP Credentials .....	48
Resolving NAT Issues .....	48
Resolving Error Messages .....	48
Running Dynamic Applications in Debug Mode .....	49

---

# Chapter

# 1

## Introduction

---

### Overview

This chapter describes how to monitor a Cisco Unified Communications Manager (CM) system in SL1.

The following sections provide an overview of Cisco Unified CM and the *Cisco: CUCM Unified Communications Manager PowerPack*:

<a href="#">What is Cisco Unified Communications Manager?</a> .....	3
<a href="#">What Does the Cisco: CUCM Unified Communications Manager PowerPack Monitor?</a> .....	4
<a href="#">Supported Versions</a> .....	4
<a href="#">Installing the Cisco: CUCM Unified Communications Manager PowerPack</a> .....	4

**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 is Cisco Unified Communications Manager?

Cisco Unified Communications Manager, also known as CallManager, is a unified call control and communications platform that provides services such as session management, voice, video, messaging, mobility, and web conferencing. Multiple CallManager servers can be grouped together into a cluster, which enables the CallManagers to share resources and features for better system scalability.

---

## What Does the Cisco: CUCM Unified Communications Manager PowerPack Monitor?

To monitor Cisco Unified CM using SL1, you must install the *Cisco: CUCM Unified Communications Manager PowerPack*. This PowerPack enables you to discover, model, and collect data about your Cisco Unified CM system and clusters.

The *Cisco: CUCM Unified Communications Manager PowerPack* includes:

- An example credential you can use as a template to create a Basic/Snippet credential to connect to the Cisco Unified CM clusters you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics and collect configuration data for Cisco Unified CM clusters
- Device Classes for each of the Cisco Unified CM clusters that SL1 monitors
- Event Policies and corresponding alerts that are triggered when Cisco Unified CM clusters meet certain status criteria
- Dashboards that display graphical information about Cisco Unified CM clusters
- Run Book Actions and Run Book Automation policies that assign the Cisco Unified CM cluster root device to the appropriate Device Class, merge subscriber and physical component devices, and clear any unregistration events for a device when the same device is registered on another node in the cluster

**NOTE:** The Run Book Action that assigns the root device disables the Cisco Unified CM cluster root device's *Auto-Update* option.

---

## Supported Versions

You can use this PowerPack to configure versions 8.x, 9.x, 10.x, 11.x, and 12.x of Cisco Unified CM.

---

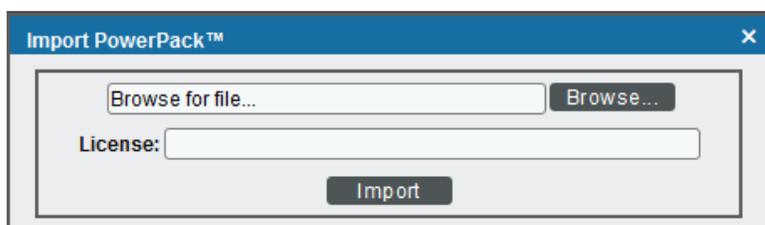
## Installing the Cisco: CUCM Unified Communications Manager PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *Cisco: CUCM Unified Communications Manager PowerPack*.

**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 **System Administration** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the [ScienceLogic Support Site](#).
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.
4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

**NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** 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 a Cisco Unified Communications Manager (CM) system for monitoring by SL1 using the *Cisco: CUCM Unified Communications Manager PowerPack*:

<i>Prerequisites for Monitoring CUCM</i> .....	6
<i>Configuring the ScienceLogic Platform to Monitor CUCM</i> .....	7
<i>Enabling the CUCM AXL Web Service</i> .....	10
<i>Configuring a CUCM User Account</i> .....	11
<i>Configuring Prime License Manager</i> .....	18
<i>Creating a CUCM Credential</i> .....	20
<i>Testing the CUCM Credential</i> .....	21
<i>Manually Creating Host File Entries for CUCM Nodes</i> .....	23

---

### Prerequisites for Monitoring CUCM

During the discovery process, SL1 automatically aligns the IP addresses and hostnames for each node in a Cisco Unified CM cluster via DNS.

If you do not have access to DNS for the Cisco Unified CM systems that you want to monitor with SL1, ensure that you know or have access to the following information about each node:

- IP address
- Hostname

# Configuring the ScienceLogic Platform to Monitor CUCM

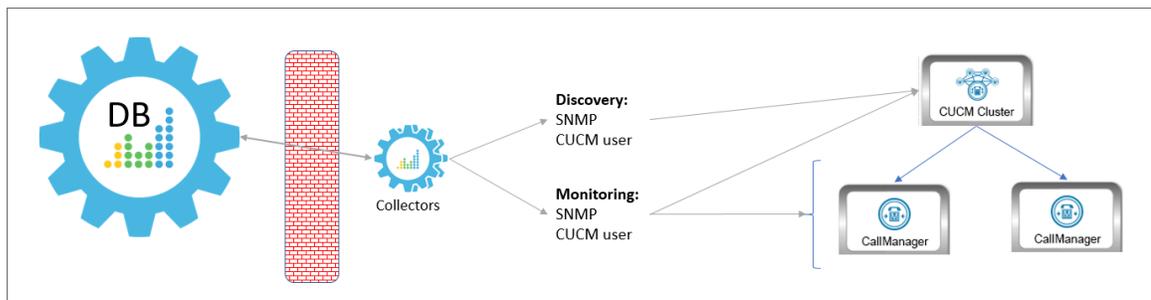
You can choose from several different possible configurations when using SL1 to monitor Cisco Unified CM:

- You can have the ScienceLogic Data Collector either in front of a firewall or behind a firewall.
- You can define the CallManager nodes either by hostname or by IP address in the Cisco Unified CM database.
- In some scenarios, you can also use network address translation (NAT) when defining the CallManagers.

These various methods are described in this section.

## **Method 1**

In the first scenario, the Data Collector sits in front of the firewall and you define the CallManagers by hostname:

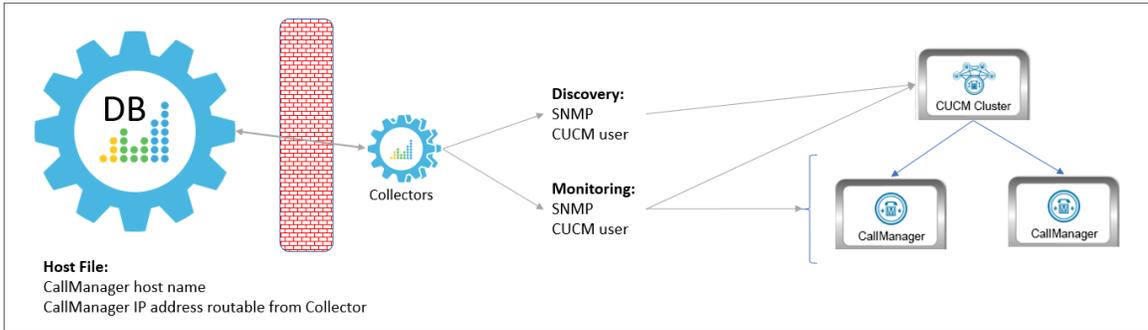


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7705	TCP

## Method 2

In the second scenario, the Data Collector sits in front of the firewall and you define the CallManagers by IP address. This method requires you to *create a host file* that includes the CallManager hostname and IP address:

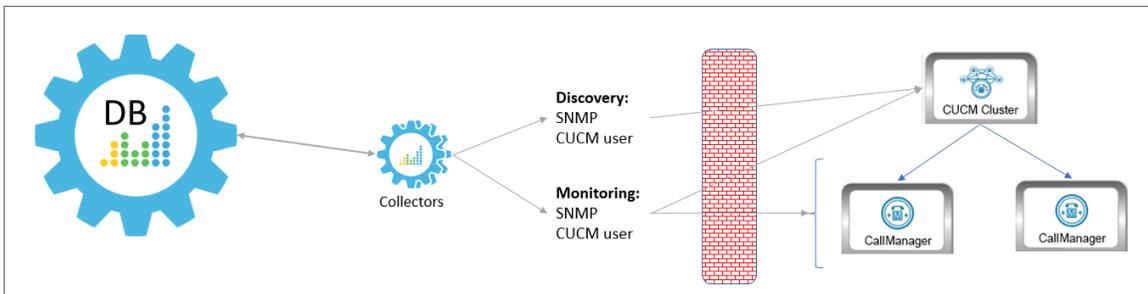


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7705	TCP

## Method 3

In the third scenario, the Data Collector sits behind the firewall and you define the CallManagers by hostname:

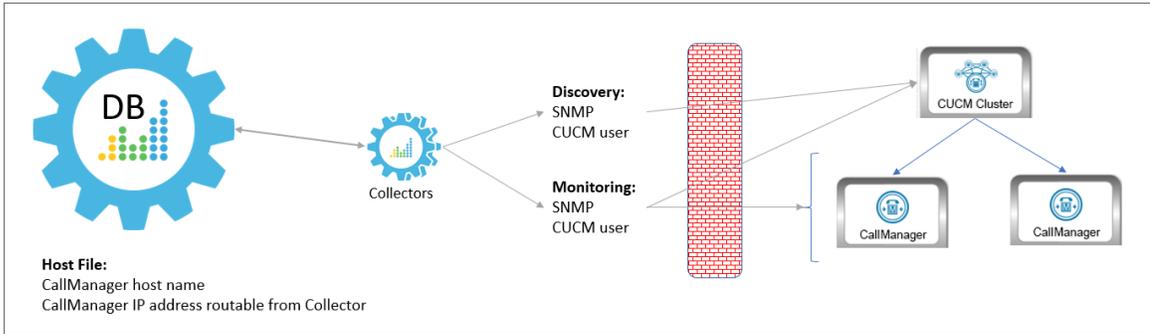


In this scenario, you must have the following ports open for the firewall:

Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

### Method 4

In the fourth scenario, the Data Collector sits behind the firewall and you define the CallManagers by hostname, with NAT. This method requires you to [create a host file](#) that includes the CallManager hostname and the IP address the Data Collector can use to access the device:

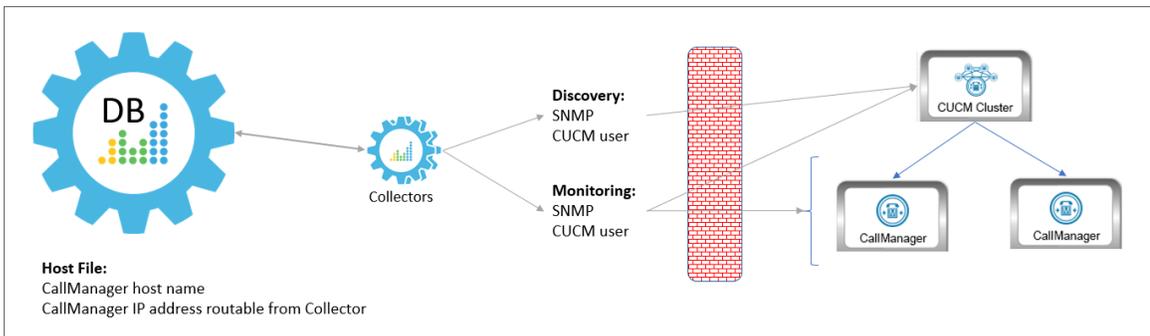


In this scenario, you must have the following ports open for the firewall:

Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

### Method 5

In the final scenario, the Data Collector sits behind the firewall and you define the CallManagers by IP address, with NAT. This method requires you to [create a host file](#) that includes the CallManager host name and IP address the Data Collector can use to access the device:



**NOTE:** This method is not supported by versions of the *Cisco: CUCM Unified Communications Manager PowerPack* prior to version 109.

In this scenario, you must have the following ports open for the firewall:

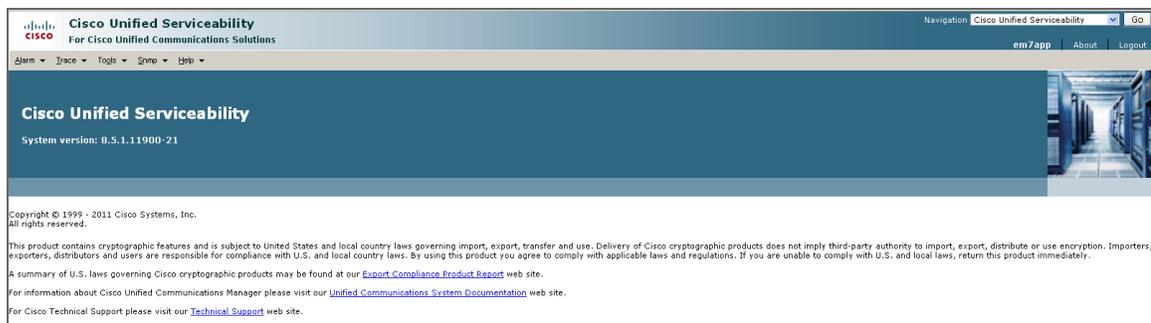
Direction	Credential	Port	Protocol
ScienceLogic Data Collector to the Cisco Unified CM Cluster and CallManagers	SNMP	161	UDP
	Cisco Unified CM user	8443	TCP

## Enabling the CUCM AXL Web Service

SL1 can monitor a Cisco Unified CM system by requesting detailed information about the system from the Cisco Unified CM AXL Web Service.

The Cisco Unified CM AXL web service is disabled by default. To enable the AXL web service, perform the following steps:

1. In a browser window, navigate to the following address:  
`https://ip-address-of-CM-system:8443/ccmadmin/showHome.do`
2. Log in to the Cisco Unified CM Administration site as an administrator.
3. In the **Navigation** drop-down list at the top-right corner of the page, select *Cisco Unified Serviceability*, and then click the **[Go]** button. The **Cisco Unified Serviceability** page appears:



- In the navigation bar at the top-left of the page, hover over **Tools**, then select **Service Activation**. The **Service Activation** page appears:

**Cisco Unified Serviceability**  
For Cisco Unified Communications Solutions

Alarm Trace Togs Smp Help

**Service Activation**

Save Set to Default Refresh

**Status**  
Status : Ready

**Select Server**  
Server\* 192.168.44.22 Go  
 Check All Services

**CM Services**

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco CallManager	Activated
<input checked="" type="checkbox"/>	Cisco Tftp	Activated
<input checked="" type="checkbox"/>	Cisco Messaging Interface	Activated
<input checked="" type="checkbox"/>	Cisco Unified Mobile Voice Access Service	Activated
<input checked="" type="checkbox"/>	Cisco IP Voice Media Streaming App	Activated
<input checked="" type="checkbox"/>	Cisco CTIManager	Activated
<input checked="" type="checkbox"/>	Cisco Extension Mobility	Activated
<input checked="" type="checkbox"/>	Cisco Extended Functions	Activated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer	Activated
<input type="checkbox"/>	Cisco DHCP Monitor Service	Deactivated
<input checked="" type="checkbox"/>	Cisco Dialed Number Analyzer Server	Activated

**CTI Services**

	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco IP Manager Assistant	Activated
<input checked="" type="checkbox"/>	Cisco WebDialer Web Service	Activated

- In the **Server** drop-down list, select the Cisco Unified CM server for which you want to enable the AXL web service, and then click the **[Go]** button.
- In the list of services, locate the **Database and Admin Services** section. If the *Activation Status* of the **Cisco AXL Web Service** is "Activated", the AXL web service is already enabled.
- If the *Activation Status* of the **Cisco AXL Web Service** is not "Activated", select the checkbox for the **Cisco AXL Web Service**.
- Click the **[Save]** button at the bottom of the page to save your changes, and then click the **[OK]** button in the pop-up window that appears.

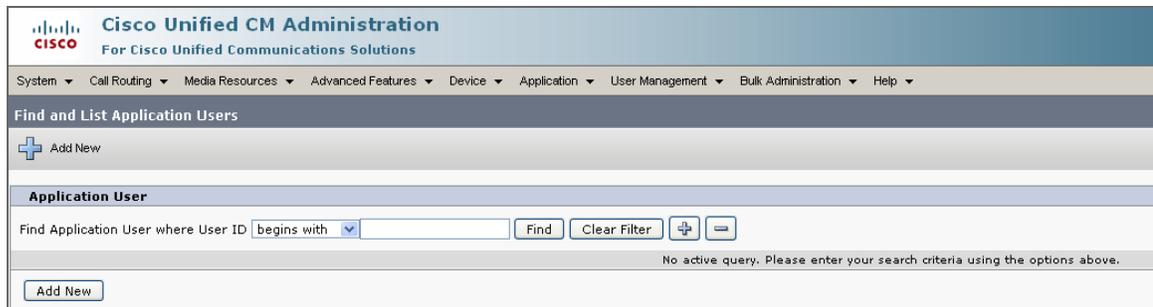
## Configuring a CUCM User Account

ScienceLogic recommends that you create a Cisco Unified CM user account that will be used only by SL1 to access the AXL web service. To create a user account in Cisco Unified CM that can access only the AXL web service, perform these two steps:

- Create a user account.
- Create a user group that includes the user account and has permission to access only the AXL web service.

To create a new Cisco Unified CM user group and user account, perform the following steps:

1. In a browser window, navigate to the following address:  
`https://ip-address-of-CM-system:8443/ccmadmin/showHome.do`
2. Log in to the Cisco Unified CM Administration site as an administrator.
3. In the navigation bar at the top-left of the page, hover over **User Management**, then select **Application User**. The **Find and List Users** page appears:



4. Click the [+ Add New] button. The **Application User Configuration** page appears:

The screenshot shows the Cisco Unified CM Administration interface for configuring an application user. The page title is "Application User Configuration". At the top, there is a navigation menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. Below the navigation menu is a "Save" button. The main content area is divided into three sections: "Status", "Application User Information", and "Device Information".

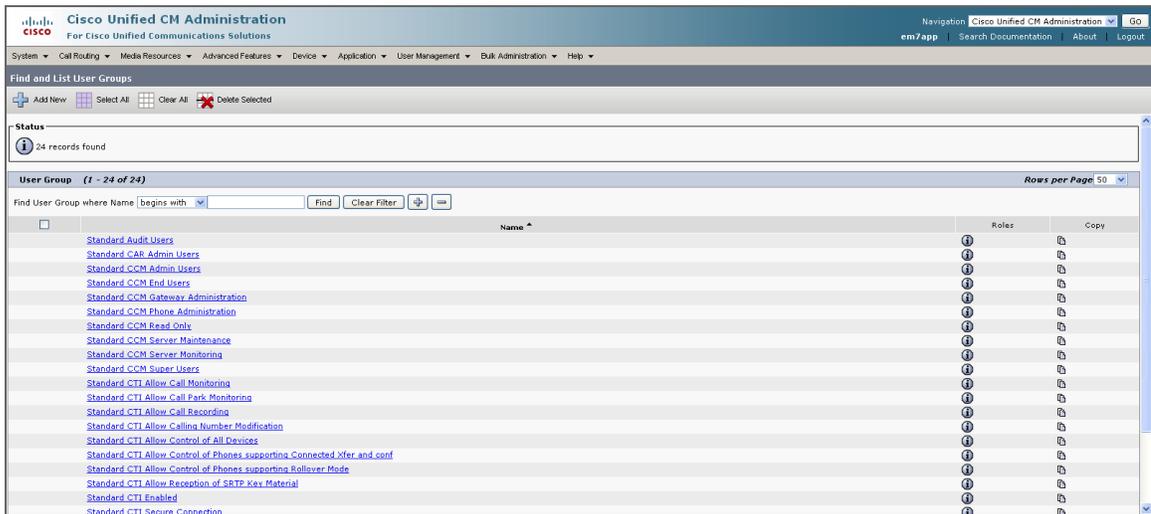
**Status**  
Status: Ready

**Application User Information**  
User ID\* [text input]  
Password [text input]  
Confirm Password [text input]  
Digest Credentials [text input]  
Confirm Digest Credentials [text input]  
Presence Group\* [dropdown menu: Standard Presence group]  
 Accept Presence Subscription  
 Accept Out-of-dialog REFER  
 Accept Unsolicited Notification  
 Accept Replaces Header

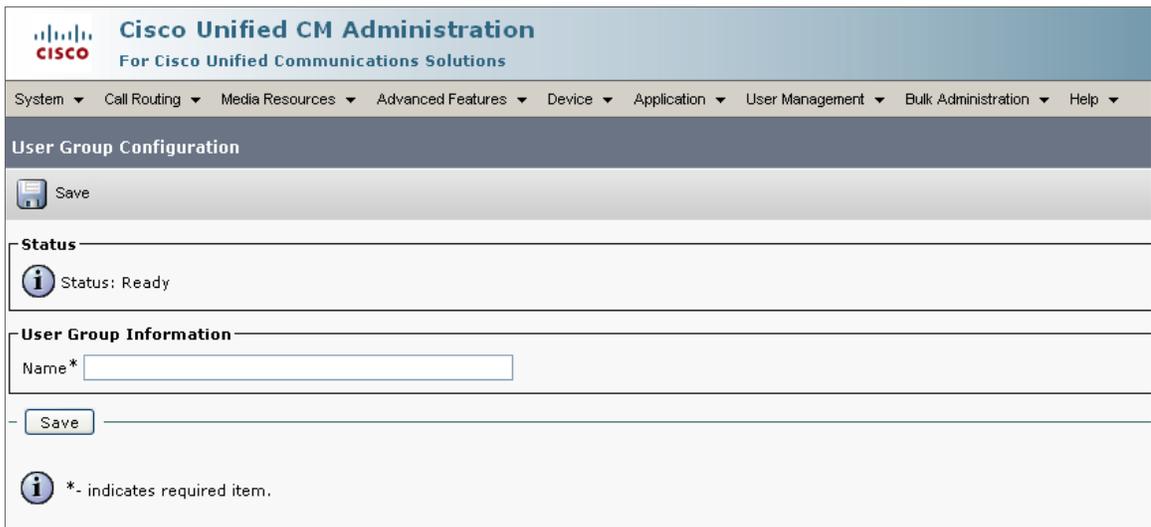
**Device Information**  
Available Devices [list box: Assistant\_RP, SEP000F909341F2, SEP001A6C8AC697, SEP04C5A4B0AD9F, SEP44E4D945EF47]  
Controlled Devices [empty list box]  
[Find more Phones] [Find more Route Points]

5. Supply values in the following fields:
  - **User ID**. Type a username for the new user.
  - **Password**. Type a password for the new user.
  - **Confirm Password**. Type the password for the new user again.
6. Click the [Save] button.

- In the navigation bar at the top-left of the page, hover over **User Management**, then select **User Group**. The **Find and List User Groups** page appears:

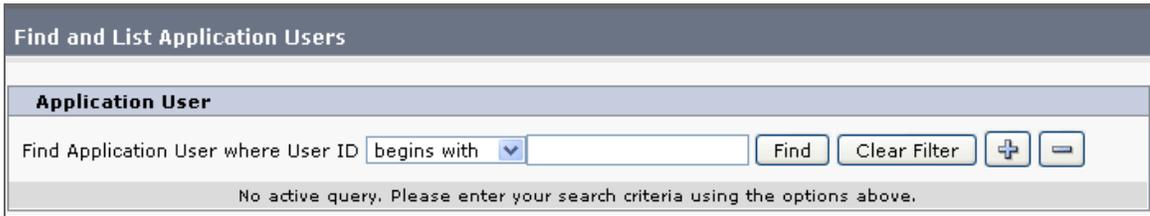


- Click the [+ Add New] button. The **User Group Configuration** page appears:

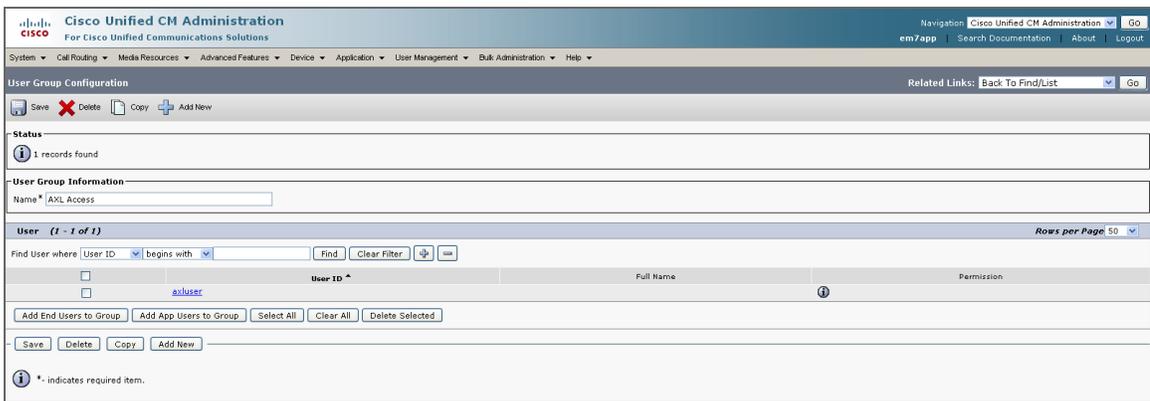


- In the **Name** field, type a name for the user group. For example, you could call the user group "AXL Access".
- Click the **[Save]** button.

11. Click the **[Add App Users to Group]** button. The **Find and List Application Users** window appears:



12. Click the **[Find]** button. In the list of users, select the checkbox for the user account that you created, then click the **[Add Selected]** button at the bottom of the page.
13. The **Find and List Application Users** window closes. In the **User Group Configuration** page, the user account is included in the list of users:



- In the **Related Links** drop-down list at the top-right hand corner of the page, select *Assign Role to User Group*, and then click the **[Go]** button. The **User Group Configuration** page appears:

- Click the **[Assign Role to Group]** button. The **Find and List Roles** window appears:

16. Click the **[Find]** button. A list of roles appears:

**Find and List Roles**

Select All Clear All Add Selected Close

**Status**  
 39 records found

**Role (1 - 39 of 39)** Rows per Page 50

Find Role where Name begins with Find Clear Filter + -  
 Select item or enter search text

<input type="checkbox"/>	Name ^	Application	Description	Copy
<input type="checkbox"/>	<a href="#">Standard AXL API Access</a>	Cisco Call Manager AXL Database	Access the AXL APIs	
<input type="checkbox"/>	<a href="#">Standard Admin Rep Tool Admin</a>		Administer CAR	
<input type="checkbox"/>	<a href="#">Standard Audit Log Administration</a>	Cisco Call Manager Serviceability	Serviceability Audit Log Administration	
<input type="checkbox"/>	<a href="#">Standard CCM Admin Users</a>		All users with access to CCM web site	
<input type="checkbox"/>	<a href="#">Standard CCM End Users</a>		Access to CCM User Option Pages	
<input type="checkbox"/>	<a href="#">Standard CCM Feature Management</a>	Cisco Call Manager Administration	Standard CCM Feature Management	
<input type="checkbox"/>	<a href="#">Standard CCM Gateway Management</a>	Cisco Call Manager Administration	Standard CCM Gateway Management	
<input type="checkbox"/>	<a href="#">Standard CCM Phone Management</a>	Cisco Call Manager Administration	Standard CCM Phone Management	
<input type="checkbox"/>	<a href="#">Standard CCM Route Plan Management</a>	Cisco Call Manager Administration	Standard CCM Route Plan Management	
<input type="checkbox"/>	<a href="#">Standard CCM Service Management</a>	Cisco Call Manager Administration	Standard CCM Service Management	
<input type="checkbox"/>	<a href="#">Standard CCM System Management</a>	Cisco Call Manager Administration	Standard CCM System Management	
<input type="checkbox"/>	<a href="#">Standard CCM User Management</a>	Cisco Call Manager Administration	Standard CCM User Management	

17. Select the checkboxes for the following roles:

- *Standard AXL API Access*
- *Standard CCM Admin Users*
- *Standard SERVICEABILITY Read Only*

18. Click the **[Add Selected]** button at the bottom of the page.

19. The **Find and List Roles** window closes. In the **User Group Configuration** page, the **Roles** field includes the *Standard AXL API Access* role:

The screenshot displays the Cisco Unified CM Administration interface for User Group Configuration. The top navigation bar includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main content area is titled 'User Group Configuration' and contains a 'Save' button. Below this is a 'Status' section showing 'Status: Ready'. The 'User Group Information' section shows 'Name \* AXL Access'. The 'Role Assignment' section features a dropdown menu with three roles: 'Standard AXL API Access', 'Standard CCM Admin Users', and 'Standard SERVICEABILITY Read Only'. To the right of the dropdown are two buttons: 'Assign Role to Group' and 'Delete Role Assignment'. At the bottom left is another 'Save' button. Below the form are three information icons with text: '\*- indicates required item.', '\*\*The role Standard CCM Admin Users must be assigned to a user group to enable its members to logon to CCMAdmin web site', and '\*\*\*The role Standard CCM End Users must be assigned to a user group to enable its members to logon to CCMUser web site'.

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

---

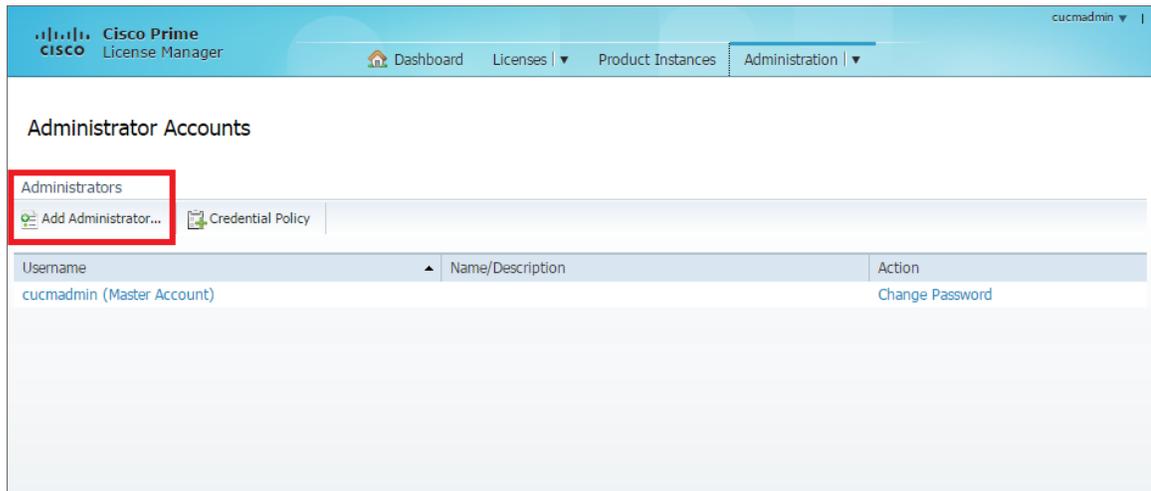
## Configuring Prime License Manager

If you want to monitor Cisco Unified CM license information from Cisco Prime License Manager (PLM), you must create an administrator user account that SL1 can use to access PLM.

To create an administrator user in PLM:

1. In a browser window, navigate to the following address:  
`https://ip-address-of-plm-server/elm-admin/`
2. Log in to the Cisco PLM site as an administrator.
3. In the **Administration** drop-down menu, select *Administrator Accounts*.

4. Click the **[Add Administrator]** button.



5. In the **Add Administrator Account** modal page, make entries in the following fields:

The screenshot shows a modal dialog box titled 'Add Administrator Account'. It contains a warning message: '- The minimum password length is 1.' Below the message are four input fields: 'Name/Description:', '\*Username:', '\*Password:', and '\*Re-enter Password:'. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

- **Name/Description.** Type a name or description for the account.
- **Username.** Type the account username.
- **Password.** Type the account password.
- **Re-enter Password.** Type the account password again.

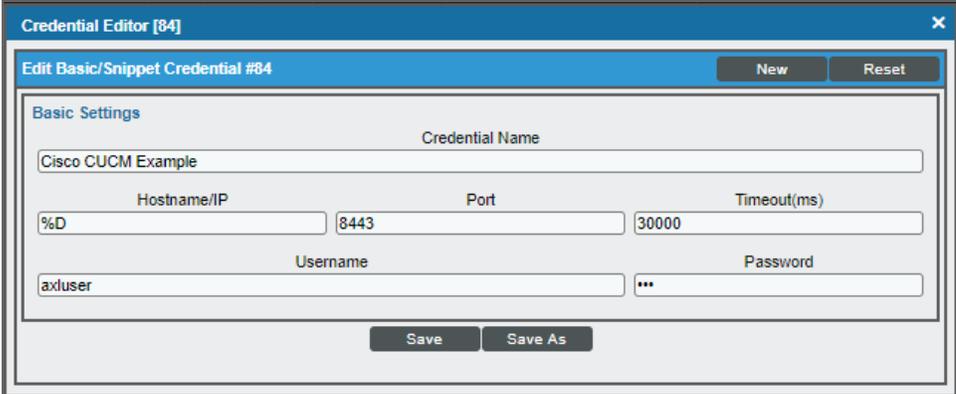
6. Click **[OK]**.

## Creating a CUCM Credential

To use the Dynamic Applications in the *Cisco: CUCM Unified Communications Manager PowerPack*, you must first define a Basic/Snippet Cisco Unified CM credential in SL1. This credential allows SL1 to communicate with the Cisco Unified CM cluster. The *Cisco: CUCM Unified Communications Manager PowerPack* includes a template you can use to create this Basic/Snippet credential.

To modify the Cisco Unified CM Basic/Snippet Credential template for use with your Cisco Unified CM cluster:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the wrench icon (🔧) for the *Cisco CUCM Example* credential. The **Credential Editor** modal window appears:



The screenshot shows the 'Credential Editor [84]' modal window. The title bar includes a close button (X). Below the title bar, there is a sub-header 'Edit Basic/Snippet Credential #84' and two buttons: 'New' and 'Reset'. The main content area is titled 'Basic Settings' and contains several input fields: 'Credential Name' (with the value 'Cisco CUCM Example'), 'Hostname/IP' (with the value '%D'), 'Port' (with the value '8443'), 'Timeout(ms)' (with the value '30000'), 'Username' (with the value 'axluser'), and 'Password' (with masked characters '\*\*\*'). At the bottom of the form are two buttons: 'Save' and 'Save As'.

3. Supply values in the following fields:
  - **Credential Name.** Type a new name for the credential.
  - **Hostname/IP.** Type the hostname or IP address, or you can type the variable "%D".
  - **Port.** Type the port number.

**NOTE:** The example credential included in older versions of the *Cisco: CUCM Unified Communications Manager PowerPack* used "80" as the default **Port** number. If your Cisco Unified CM credential specifies port 80, SL1 will automatically override that value and use port 8443 instead. If your Cisco Unified CM credential specifies any port other than 80, SL1 will use that specified port.

- **Timeout (ms).** Type the timeout value of each request, in milliseconds. The default value is "30000".
- **Username.** Type the username for the Cisco Unified CM user account that you created to access the AXL web service. For details, see the [Configuring a Cisco Unified CM User Account](#) section.
- **Password.** Type the password for the username you entered in the **Username** field.

4. Click the **[Save As]** button.

**NOTE:** If you are monitoring Cisco Unified CM license information with the Cisco Prime License Manager (PLM) and your PLM administrator username and password are the same as the user account you created to access the AXL web service, then you can use the same credential to access PLM. However, if your PLM administrator user information is different, then repeat these steps to create a credential to access PLM.

**NOTE:** If SNMP is enabled on the Cisco Unified CM cluster, then you can also create an optional SNMP credential that will be used only during discovery to classify the cluster device class. If SNMP is not available on the Cisco Unified CM cluster, then you **do not** need an SNMP credential. For more information on SNMP credentials, see the *Discovery and Credentials* manual.

---

## Testing the CUCM Credential

SL1 includes a Credential Test for Cisco Unified CM. Credential Tests define a series of steps that SL1 can execute on demand to validate whether a credential works as expected.

The CUCM Credential Test can be used to test a Basic/Snippet credential for monitoring Cisco Unified CM using the Dynamic Applications in the *Cisco: CUCM Unified Communications Manager PowerPack*. The CUCM Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to see if the device is reachable.
- **Test Name Resolution.** Checks to see if nslookup can resolve the IP address or hostname.
- **Test Port Availability.** Performs an NMAP request to see if the appropriate port is open.
- **Test Accessibility to Publisher.** Checks to see if the common API service URLs on the publisher device can be queried.
- **Test Accessibility to Subscribers via Publisher.** Checks to see if data on a CUCM subscriber can be queried via the publisher.
- **Test Accessibility to All Subscribers.** Checks to see if the status of services on a CUCM subscriber can be queried.

To test the CUCM credential:

1. Go to the **Credential Test Management** page (System > Customize > Credential Tests).

2. Locate the **CUCM Credential Test** and click its lightning bolt icon (⚡). The **Credential Tester** modal page appears:

3. Supply values in the following fields:

- **Test Type**. This field is pre-populated with the credential test you selected.
- **Credential**. Select the credential to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
- **Hostname/IP**. Enter the IP address or hostname for the device.

**NOTE:** The credential being tested cannot include more than 32 characters in the **Hostname/IP** field.

- **Collector**. Select the All-In-One Appliance or Data Collector that will run the test.

4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

Step	Description	Log Message	Status	
1	Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 2.662ms	Passed
2	Test Name Resolution	Check to see if nlookup can resolve the IP and hostname	Name resolution succeeded: Reverse returned 1 result, Forward returned 1 result	Passed
3	Test Port Availability	Check to see if the appropriate port is open	Port 8443 is open	Passed
4	Test Accessibility to Publisher	Check to see if common API service URLs on the publisher device can be queried	CUCM API resource requests succeeded	Passed
5	Test Accessibility to Subscribers via Publisher	Check to see if data on a CUCM subscriber can be queried via the publisher	CUCM subscriber query through the publisher succeeded	Passed
6	Test Accessibility to All Subscribers	Check to see if the status of services on a CUCM subscriber can be queried	CUCM subscriber is accessible with this credential	Passed

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- **Step**. The name of the step.
- **Description**. A description of the action performed during the step.
- **Log Message**. The result of the step for this credential test.
- **Status**. Whether the result of this step indicates the credential or the network environment is configured correctly (Passed) or incorrectly (Failed).

- **Step Tip.** Mouse over the question mark icon (  ) to display the tip text. The tip text recommends what to do to change the credential or the network environment if the step has a status of "Failed".

## Manually Creating Host File Entries for CUCM Nodes

During the discovery process, SL1 automatically aligns the IP addresses and hostnames for each CallManager server (node) in a Cisco Unified CM cluster via DNS.

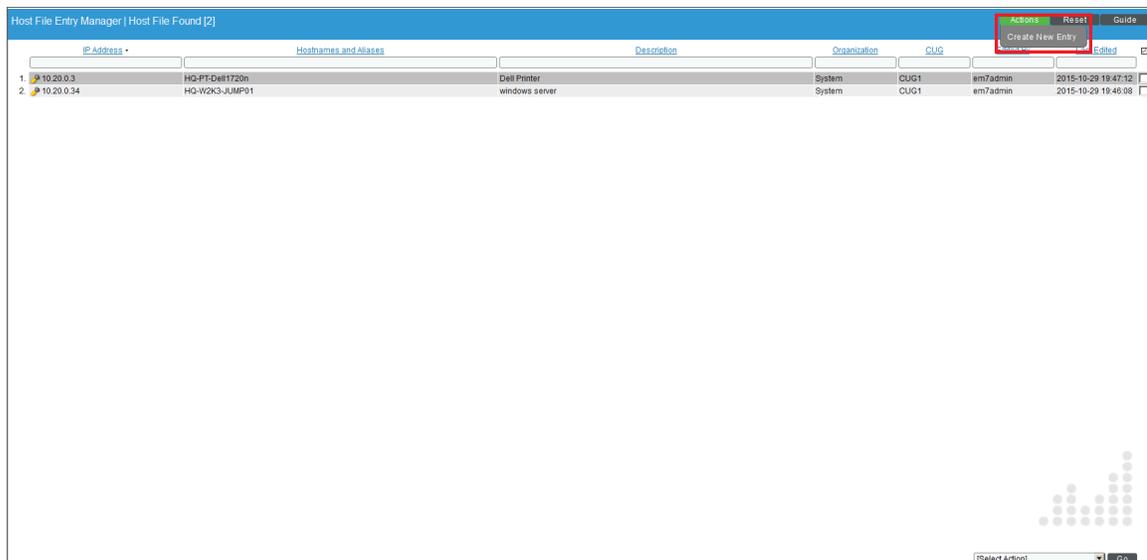
If you do not have access to DNS for the Cisco Unified CM system you want to monitor, you must manually create host file entries in SL1 for each node in the Cisco Unified CM cluster. Each host file entry must contain the IP address and hostname of a node in the Cisco Unified CM cluster.

**NOTE:** If you have access to DNS for the Cisco Unified CM system you want to monitor with SL1, you do not need to perform the steps to manually configure host file entries. Continue to the section on [Discovering a Cisco Unified CM Cluster](#).

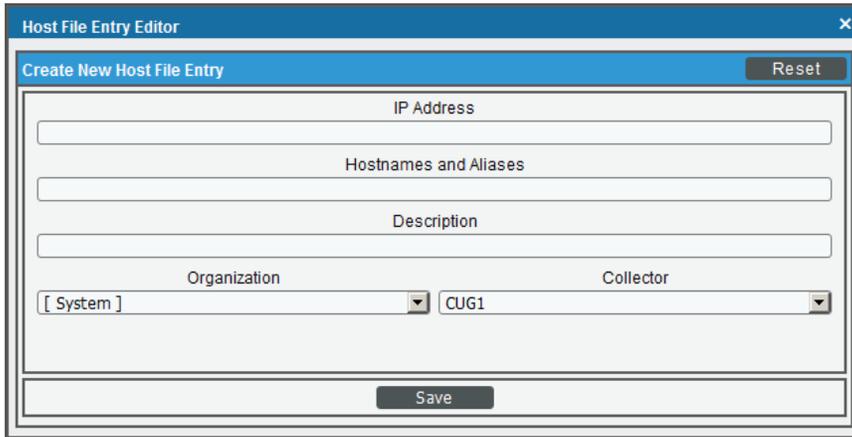
Repeat the following steps for each node in the Cisco Unified CM cluster.

To create a host file entry:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



2. Click the **[Action]** menu and choose **Create New Entry**. The **Create New Host File Entry** modal page appears.



3. In the **Create New Host File Entry** modal page, supply values in the following fields:
  - **IP Address**. The IP address to resolve with the hostname.

**NOTE:** Server hostnames should be aligned to external IP addresses when supporting Network Address Translation (NAT) environments.

- **Hostnames and Aliases**. The hostname to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
- **Description**. Description of the host entry. This field is not written to the host file. This field is for administrators to use when managing host file entries.
- **Organization**. Organization associated with the host. You can select from a list of all existing organizations. This field is not written to the host file. This field is for administrators to use when managing host file entries. For example, a service provider could assign each customer its own organization and then use this field to manage host file entries for each customer.

4. Click the **[Save]** button to save the new host entry.

---

# Chapter

# 3

## Discovery

---

### Overview

The following sections describe how to discover Cisco Unified Communications Manager (CUCM) clusters in SL1 using the *Cisco: CUCM Unified Communications Manager PowerPack*:

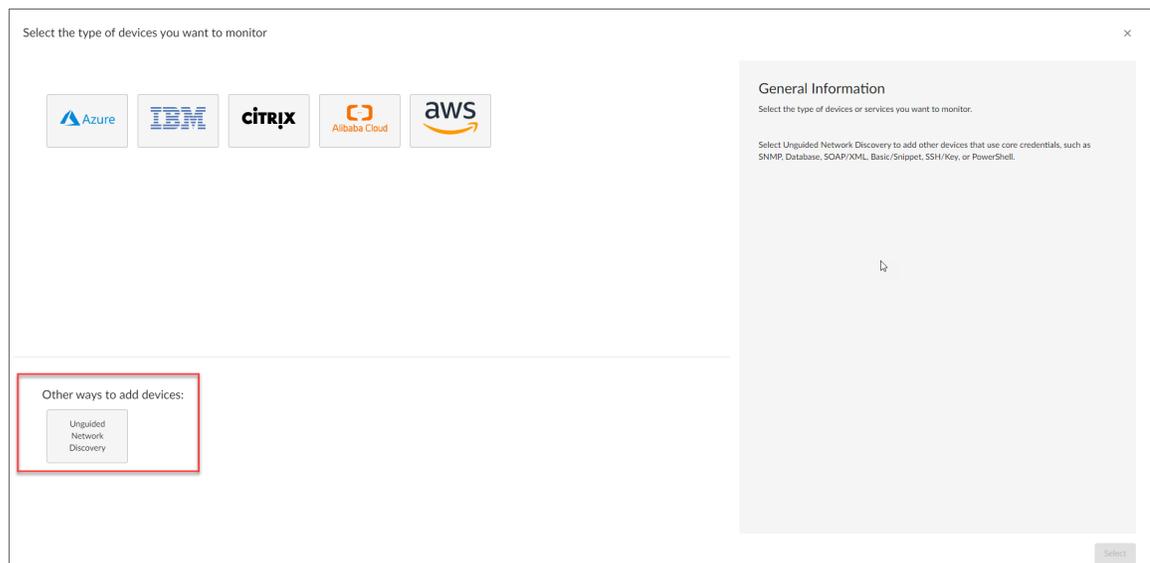
<b>Discovering a CUCM Cluster</b> .....	<b>26</b>
<i>Discovering a CUCM Cluster in the SL1 Classic User Interface</i> .....	28
<b>Verifying Discovery and Dynamic Application Alignment</b> .....	<b>30</b>
<i>Manually Aligning Dynamic Applications</i> .....	32
<b>Viewing Component Devices</b> .....	<b>34</b>
<i>Viewing Component Devices in the SL1 Classic User Interface</i> .....	35

## Discovering a CUCM Cluster

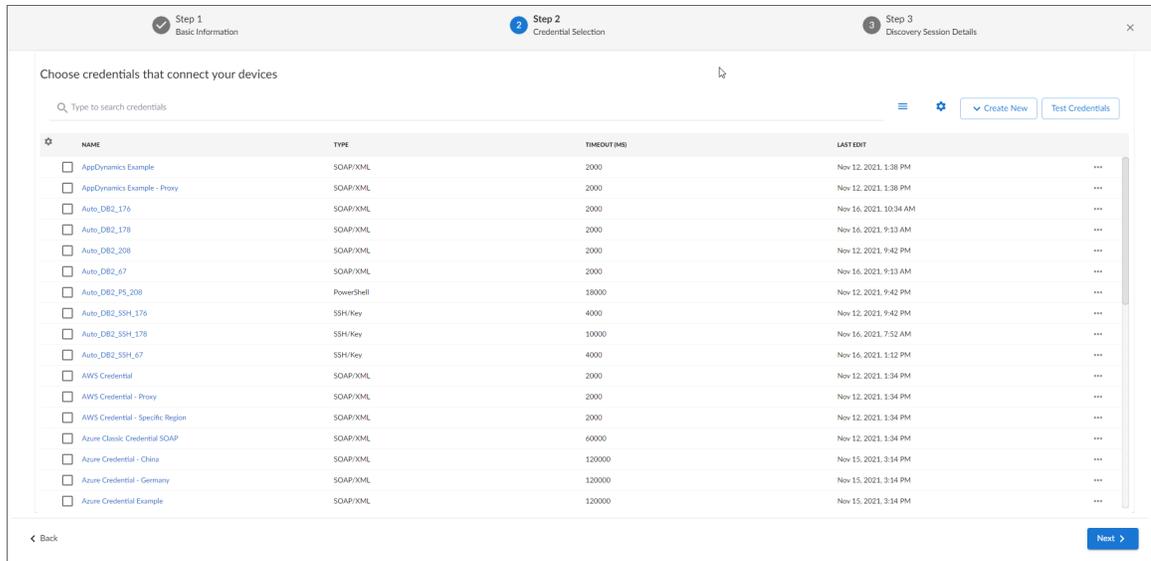
When you use the *Cisco: CUCM Unified Communications Manager PowerPack* to discover Cisco Unified CM devices, SL1 creates a device representing your Cisco Unified CM cluster. This cluster device acts as the root device for the remaining servers and component devices in your Cisco Unified CM system.

To create and run a discovery session that will discover a Cisco Unified CM cluster:

1. On the **Devices** page (🖨️) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



2. Click the **[Unguided Network Discovery]** button. Additional information about the 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:
  - **Name**. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
  - **Description**. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** 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:

- Select an SNMP credential to use with the Cisco Unified CM cluster. (For more information on SNMP credentials, see the **Discovery and Credentials** manual.).

**NOTE:** An SNMP credential is needed only to properly classify the devices in the cluster. If SNMP is not available on the Cisco Unified CM cluster, then you do not need to select an SNMP credential; in that scenario, the root device will be discovered as a pingable device and you must manually change it to a Cisco Unified CM cluster.

- Select the *Cisco Cisco Unified CM Example* credential that you edited in the section on **Creating a Cisco Unified CM Credential..**

7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:

8. Complete the following fields:
  - **List of IPs/Hostnames.** Type the IP addresses for the Cisco Unified CM Publishers.
  - **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.
9. Click **[Save and Run]** if you enabled the Run after save setting, or **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

## Discovering a CUCM Cluster in the SL1 Classic User Interface

When you use the *Cisco: CUCM Unified Communications Manager PowerPack* to discover Cisco Unified CM devices, SL1 creates a device representing your Cisco Unified CM cluster. This cluster device acts as the root device for the remaining servers and component devices in your Cisco Unified CM system.

To create and run a discovery session that will discover a Cisco Unified CM cluster:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).

- Click the **[Create]** button to create a new discovery session. The **Discovery Session Editor** window appears:

- Enter values in the following fields:

- IP Address/Hostname Discovery List.** Type the IP addresses for the Cisco Unified CM Publishers.

**NOTE:** To monitor Cisco Unified CM servers that are registered by name within their clusters, you might need to go to the **Host File Entry Manager** page (System > Customize > Host Files) and map the server names to their IP addresses if you do not have access to DNS for the Cisco Unified CM system you want to monitor. For Network Address Translation (NAT) environments, server hostnames should be mapped to external IP addresses. For more information, see the section [Manually Creating Host File Entries for Cisco Unified CM Nodes](#).

- SNMP Credential.** Select an SNMP credential to use with the Cisco Unified CM cluster. (For more information on SNMP credentials, see the **Discovery and Credentials** manual.)

**NOTE:** An SNMP credential is needed only to properly classify the devices in the cluster. If SNMP is not available on the Cisco Unified CM cluster, then you do not need to select an SNMP credential; in that scenario, the root device will be discovered as a pingable device and you must manually change it to a Cisco Unified CM cluster.

- **Other Credentials.** Select the *Cisco Cisco Unified CM Example* credential that you edited in the section on [Creating a Cisco Unified CM Credential](#).
4. You can enter values in the other fields on this page, but are not required to and can simply accept the default values. For more information about the other fields on this page, see the **Discovery and Credentials** manual.
  5. Click **[Save]** 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.
  8. When the Cisco Unified CM cluster is discovered, click its device icon () to view the **Device Properties** page for the Cisco Unified CM cluster.

---

## Verifying Discovery and Dynamic Application Alignment

The Dynamic Applications for monitoring Cisco Unified CM are aligned during discovery.

To verify that SL1 has automatically aligned the correct Dynamic Applications:

1. In the **Discovery Session** page, click the device icon () for the newly discovered Cisco Unified CM cluster to view its **Device Properties** page.

- From the **Device Properties** page for the Cisco Unified CM cluster, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.

Dynamic Application	ID	Poll Frequency	Type	Credential
+ Cisco CM: Registration Counters	188	15 mins	SNMP Performance	Default SNMP Credential
+ Cisco CM: Alarm Configs	197	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Call Manager	195	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: CCM Status	196	1 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Device Pools	173	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Gateway MGCP	174	1 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Global Config	175	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: H323 Device Status	191	5 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Media Device Status	192	5 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Media Resources	177	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Phone	178	1440 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Phone Status	193	5 mins	SNMP Configuration	Default SNMP Credential
+ Cisco CM: Regions	179	1440 mins	SNMP Configuration	Default SNMP Credential
+ Host Resource: CPU Config	470	1440 mins	SNMP Configuration	Default SNMP Credential
+ Host Resource: Software	467	120 mins	SNMP Configuration	Default SNMP Credential
+ Cisco: CUCM Cluster Information	1086	15 mins	Snippet Configuration	N/A
+ Cisco: CUCM Cluster Root Cache	1085	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Gatekeeper Cache	1154	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM H323 Trunk Cache	1149	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Media Resource Big Cache	1070	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM MGCP Gateway Cache	1061	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Misc Perf Counters Fast Cache	1124	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Misc Perf Counts Slow Cache	1058	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Service Performance Cache	1076	15 mins	Snippet Configuration	Default SNMP Credential
+ Cisco: CUCM Service States Cache	1082	15 mins	Snippet Configuration	Default SNMP Credential

- The following Dynamic Applications should appear on the **Dynamic Application Collections** page for the Cisco Unified CM cluster:

**NOTE:** It can take several minutes after discovery for Dynamic Applications to display on the **Dynamic Application Collections** page. If the listed Dynamic Applications do not display on this page, try clicking the **[Reset]** button.

- Cisco: CUCM Cluster Information
- Cisco: CUCM Cluster Root Cache
- Cisco: CUCM CTI Device Cache
- Cisco: CUCM Gatekeeper Cache
- Cisco: CUCM H323 Trunk Cache
- Cisco: CUCM Media Resource Big Cache
- Cisco: CUCM MGCP Gateway Cache
- Cisco: CUCM Misc Perf Counters Fast Cache
- Cisco: CUCM Misc Perf Counts Slow Cache

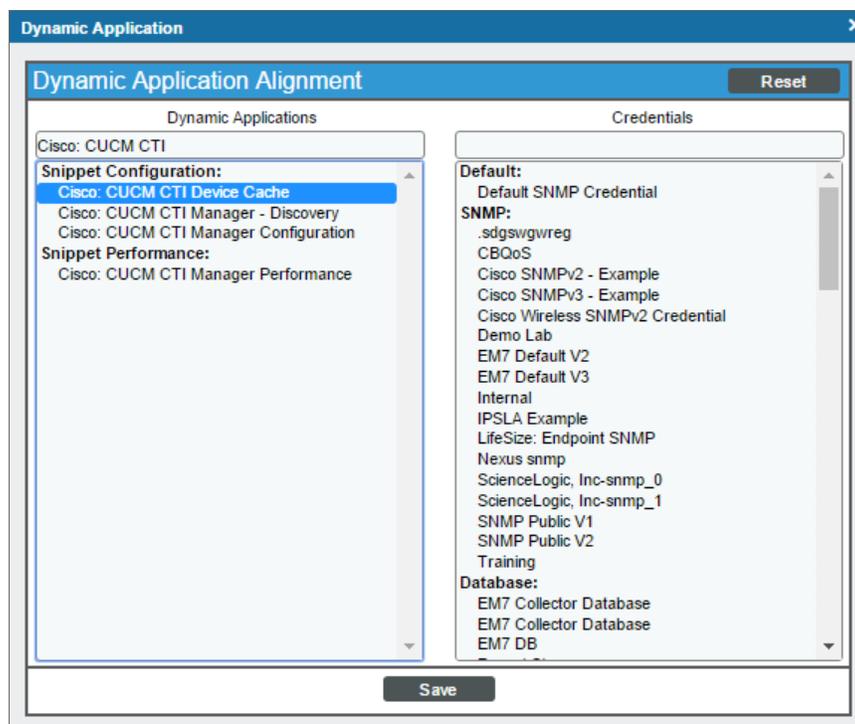
- Cisco: CUCM Partition Cache
- Cisco: CUCM Process Cache
- Cisco: CUCM Service Performance Cache
- Cisco: CUCM Service States Cache
- Cisco: CUCM SIP Trunk Cache
- Cisco: CUCM Subscriber Merge

## Manually Aligning Dynamic Applications

If the Dynamic Applications have not been automatically aligned, you can align them manually.

To manually align Dynamic Applications:

1. From the **Device Properties** page for the Cisco Unified CM cluster, click the **[Collections]** tab.
2. Click the **[Actions]** button and then click *Add Dynamic Applications*. The **Dynamic Application Alignment** page appears:



3. In the **Dynamic Applications** field, select the Dynamic Application you want to align.
4. In the **Credentials** field, select the SNMP credential you created for monitor the Cisco Unified CM cluster.
5. Repeat steps 2-4 for the remaining Dynamic Applications to align with the device.

6. After aligning the Dynamic Applications, click the **[Reset]** button and then click the plus icon (+) for the Dynamic Application. If collection for the Dynamic Application was successful, the graph icons (📊) for the Dynamic Application are enabled:

Close	Properties	Thresholds	Collections	Monitors	Schedule	Logs
Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes	Attributes
Device Name	cucm8			Managed Type	Physical Device	
IP Address / ID	10.168.44.22   1970			Category	UC.Cluster	
Class	Cisco Systems			Sub-Class	CUCM Cluster	
Organization	System			Uptime	77 days, 05:21:31	
Collection Mode	Active			Collection Time	2016-02-03 16:15:00	
Description	Hardware:7835I2, 1 Family: Xeon, 4096 MB Memory: Software:UCOS			Group / Collector	CUG   em7_a0	
Device Hostname						

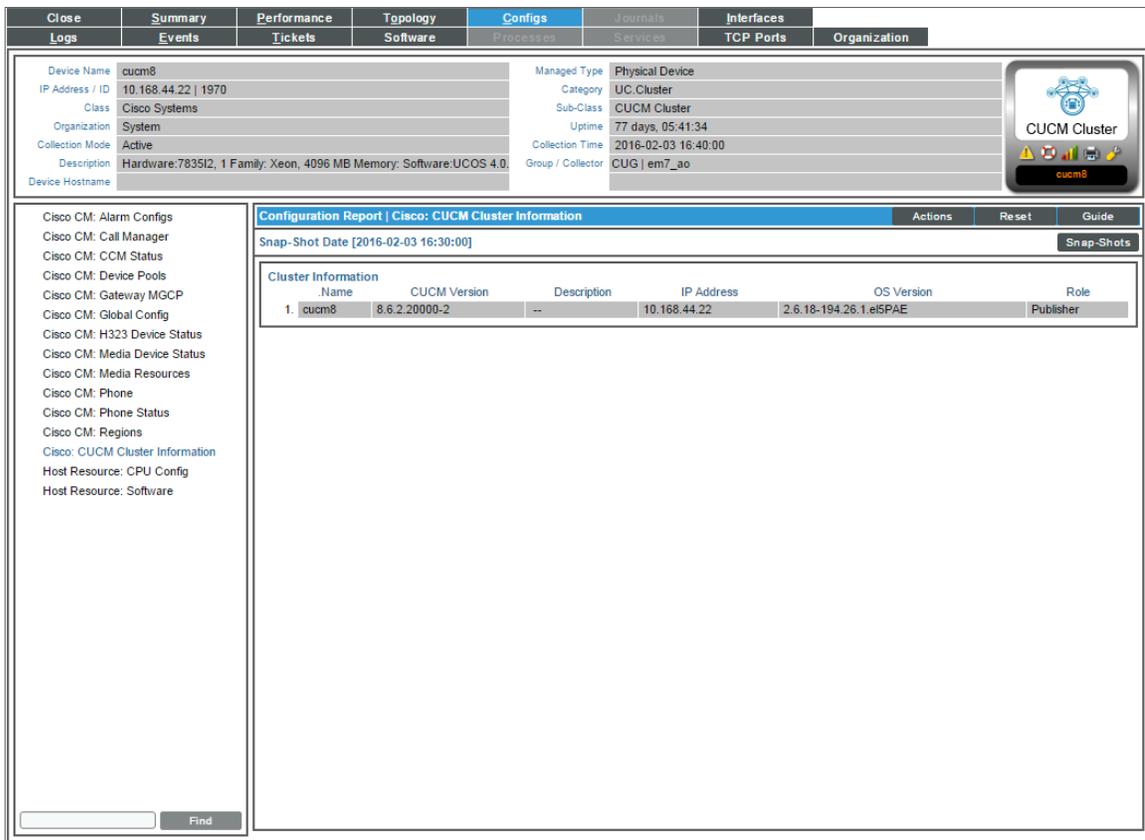


Dynamic Application™ Collections							Expand	Actions	Reset	Guide
Cisco CUCM: Cluster Information		932	15 mins	Snippet Configuration	N/A					
Name	Collection Object	Cid	Found	Collecting	Edited By					
Cluster Information		p_11751	yes	yes	--					
CUCM Version		p_12950	no	yes	--					
Description		p_11749	yes	yes	--					
Discovery Object		p_11752	yes	yes	--					
IP Address		p_15148	no	yes	--					
OS Version		p_11750	yes	yes	--					
Role		p_11754	yes	yes	--					
Unique ID 1		p_11755	yes	yes	--					
+	Cisco: CUCM Cluster Root Cache	1085	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Gatekeeper Cache	1154	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM H323 Trunk Cache	1149	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Media Resource Big Cache	1070	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM MGCP Gateway Cache	1061	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Misc Perf Counters Fast Cache	1124	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Misc Perf Counts Slow Cache	1058	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Service Performance Cache	1076	15 mins	Snippet Configuration	Cisco CUCM Example					
+	Cisco: CUCM Service States Cache	1082	15 mins	Snippet Configuration	Cisco CUCM Example					

[Select Action] Go

Save

- Click a graph icon () to view the collected data. The **Configuration Report** page will display the number of components of each type and the total number of components managed by the Cisco Unified CM cluster:



The screenshot shows the Cisco Unified CM Configuration Report page for a CUCM Cluster. The page is divided into several sections:

- Navigation Tabs:** Close, Summary, Performance, Topology, **Configs**, Journals, Interfaces, Logs, Events, Tickets, Software, PROVISION, Services, TCP Ports, Organization.
- Device Information:**
  - Device Name: cucm8
  - IP Address / ID: 10.168.44.22 | 1970
  - Class: Cisco Systems
  - Organization: System
  - Collection Mode: Active
  - Description: Hardware:7835I2, 1 Family: Xeon, 4096 MB Memory: Software:UCOS 4.0
  - Device Hostname: [blank]
  - Managed Type: Physical Device
  - Category: UC Cluster
  - Sub-Class: CUCM Cluster
  - Uptime: 77 days, 05:41:34
  - Collection Time: 2016-02-03 16:40:00
  - Group / Collector: CUG | em7\_ao
- Configuration Report | Cisco: CUCM Cluster Information:**
  - Actions, Reset, Guide
  - Snap-Shot Date [2016-02-03 16:30:00] Snap-Shots
  - Cluster Information Table:

Name	CUCM Version	Description	IP Address	OS Version	Role
1. cucm8	8.6.2.20000-2	--	10.168.44.22	2.6.18-194.26.1.ei5PAE	Publisher
- Left Sidebar:**
  - Cisco CM: Alarm Configs
  - Cisco CM: Call Manager
  - Cisco CM: CCM Status
  - Cisco CM: Device Pools
  - Cisco CM: Gateway MGCP
  - Cisco CM: Global Config
  - Cisco CM: H323 Device Status
  - Cisco CM: Media Device Status
  - Cisco CM: Media Resources
  - Cisco CM: Phone
  - Cisco CM: Phone Status
  - Cisco CM: Regions
  - Cisco: CUCM Cluster Information
  - Host Resource: CPU Config
  - Host Resource: Software

## Viewing Component Devices

When SL1 performs collection for a Cisco Unified CM cluster, SL1 will create component devices for the components in the Cisco Unified CM cluster and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices will also be used to create additional component devices. All component devices appear in the **Device Manager** page just like devices discovered using the ScienceLogic discovery process.

In addition to the **Devices** page, you can view the Cisco Unified CM cluster and all associated component devices in the following places in the user interface

- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device.

- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1. The **Device Components** page 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. To view the component devices associated with a Cisco Unified CM cluster, find the Cisco Unified CM cluster and select 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 a Cisco Unified CM cluster, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the **Maps** manual.

## Viewing Component Devices in the SL1 Classic User Interface

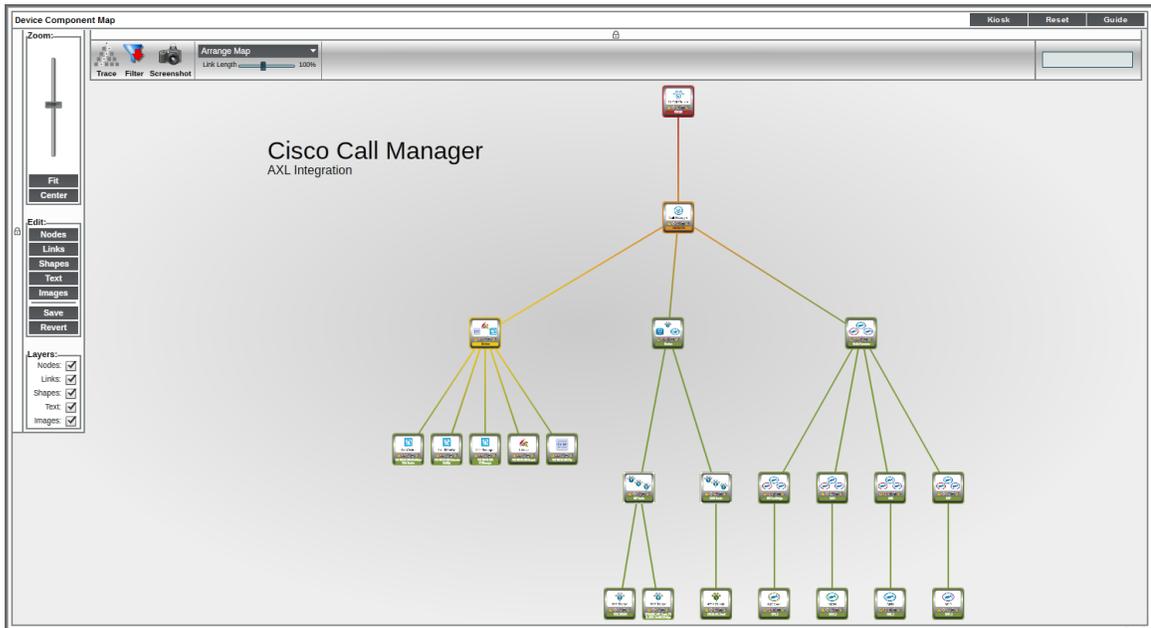
When SL1 performs collection for a Cisco Unified CM cluster, SL1 will create component devices for the components in the Cisco Unified CM cluster and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices will also be used to create additional component devices. All component devices appear in the **Device Manager** page just like devices discovered using the ScienceLogic discovery process.

In addition to the **Device Manager** page, you can view the Cisco Unified CM cluster and all associated component devices in the following places in the user interface:

- The **Device Components** page (Registry > Devices > Device Components) displays a list of all root devices and component devices discovered by the ScienceLogic platform. The **Device Components** page 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. To view the component devices associated with a Cisco Unified CM cluster, find the Cisco Unified CM cluster and select its plus icon (+):

	Device Name	IP Address	Device Category	Device Class   Sub-class	DUID	Organization	Current State	Collection Group	Collection Status	Actions	Reset	Guide
1.	+ CUCM9	10.188.84.22	Cluster	Cisco Systems   CUCM Cluster	228	Branch Office A	Healthy	CUG_LOCAL	Active			
2.	- CUCM9	192.168.53.245	Cluster	Cisco Systems   CUCM Cluster	208	Branch Office A	Critical	CUG_LOCAL	Active			
Device Name * IP Address -- Device Category Device Class   Sub-class DUID Organization Current State Collection Group Collection Status												
1.	+ CUCM-PUB		CallControl	Cisco Systems   Call Manager	262	Branch Office A	Major	CUG_LOCAL	Unavailable			
Device Name * IP Address -- Device Category Device Class   Sub-class DUID Organization Current State Collection Group Collection Status												
3.	+ nexus_a	192.168.54.10	Switches	Cisco Systems   Nexus 5548UP	155	System	Minor	CUG_LOCAL	Active			
4.	+ nexus_b	192.168.54.11	Switches	Cisco Systems   Nexus 5548UP	156	System	Minor	CUG_LOCAL	Active			

- 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. SL1 also updates each map with the latest status and event information. To view the map for a Cisco Unified CM cluster, go to Classic Maps > Device Maps > Components, and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the **Views** manual.



---

# Chapter

# 4

## Dashboards

---

### Overview

The *Cisco: CUCM Unified Communications Manager PowerPack* comes paired with the *Cisco: CUCM Dashboards PowerPack*, which contains dashboards that present data related to different aspects of Cisco Unified CM clusters.

The following sections describe how to install the *Cisco: CUCM Dashboards PowerPack* and provide a description of each dashboard:

<i>Installing the CUCM Dashboards</i> .....	37
<i>Cisco: CUCM Performance Dashboard</i> .....	38
<i>Cisco: CUCM Locations LBM</i> .....	39
<i>Cisco: CUCM Media Resources</i> .....	40
<i>Cisco: CUCM Media Resources (Simple)</i> .....	41
<i>Cisco: CUCM Tomcat</i> .....	42
<i>Cisco: CUCM Overall Cluster Health</i> .....	43
<i>Cisco: CUCM Active Calls</i> .....	44

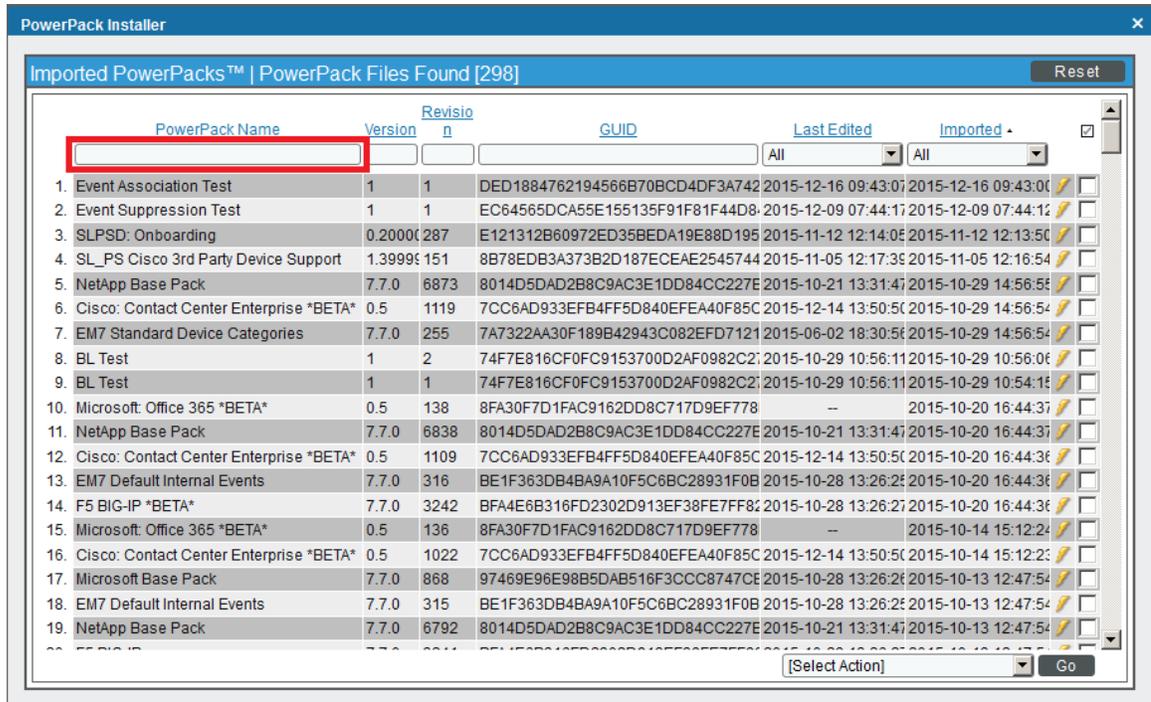
---

### Installing the CUCM Dashboards

To view the Cisco Unified CM dashboards in SL1, you must install the *Cisco: CUCM Dashboards PowerPack*. To do so:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the **[Actions]** button, then select *Install PowerPack*. The **Imported PowerPacks** modal page appears.

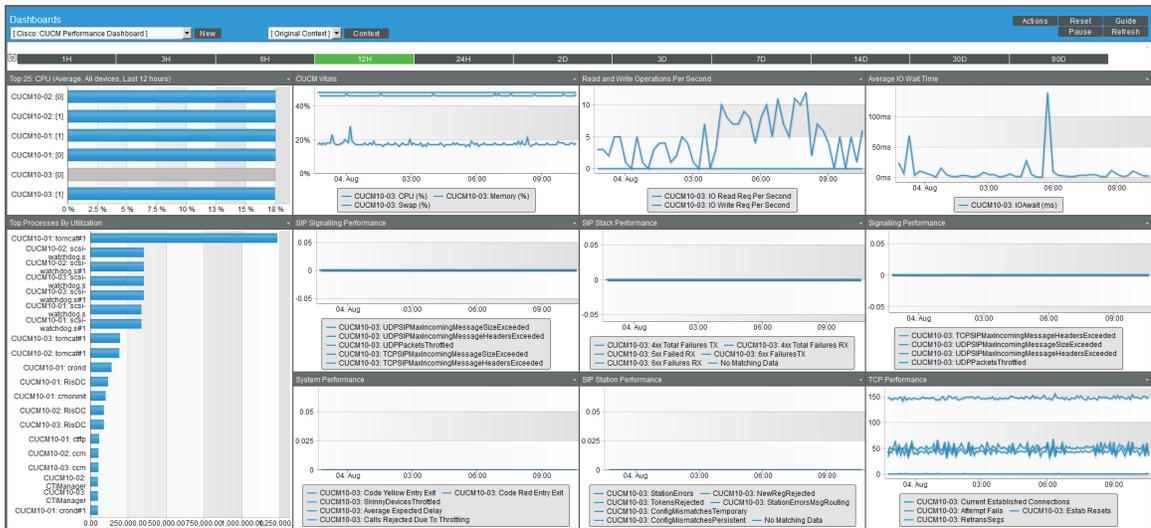
- Use the search filter in the **PowerPack Name** column heading to locate the PowerPack you want to install. To do so, enter text to match, including special characters, and the **Imported PowerPacks** modal page displays only PowerPacks that have a matching name.



- Click the lightning-bolt icon (⚡) for the PowerPack that you want to install.
- The **Install PowerPack** modal page appears. To install the PowerPack, click **[Install]**.
- The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your SL1 System.

## Cisco: CUCM Performance Dashboard

The Cisco: CUCM Performance dashboard displays 11 widgets.



The dashboard includes the following widgets:

- **Top 25: CPU (Average, All devices, Last 12 Hours).** This widget displays a bar graph that depicts the 25 Cisco CallManager devices that used the highest percentage of CPU time over the last 12 hours.
- **Top Processes By Utilization.** This widget displays a bar graph that depicts all Cisco Unified CM processes in the cluster, ordered by utilization from highest to lowest.
- **CUCM Vitals.** This widget displays a line graph that depicts the cluster's vitals by percent, including CPU time, Swap Utilization, and Memory Utilization, over time.
- **Read and Write Operations Per Second.** This widget displays a line graph that depicts read and write requests per second over time.
- **Average IO Wait Time.** This widget displays a line graph that depicts the average IO wait time over time.
- **SIP Signaling Performance.** This widget displays a line graph that depicts SIP signaling performance over time.
- **SIP Stack Performance.** This widget displays a line graph that depicts SIP stack performance over time.
- **Signaling Performance.** This widget displays a line graph that depicts overall signaling performance over time.
- **System Performance.** This widget displays a line graph that depicts multiple system performance metrics over time.
- **SIP Station Performance.** This widget displays a line graph that depicts multiple SIP station performance metrics over time.
- **TCP Performance.** This widget displays a line graph that depicts TCP performance over time.

## Cisco: CUCM Locations LBM

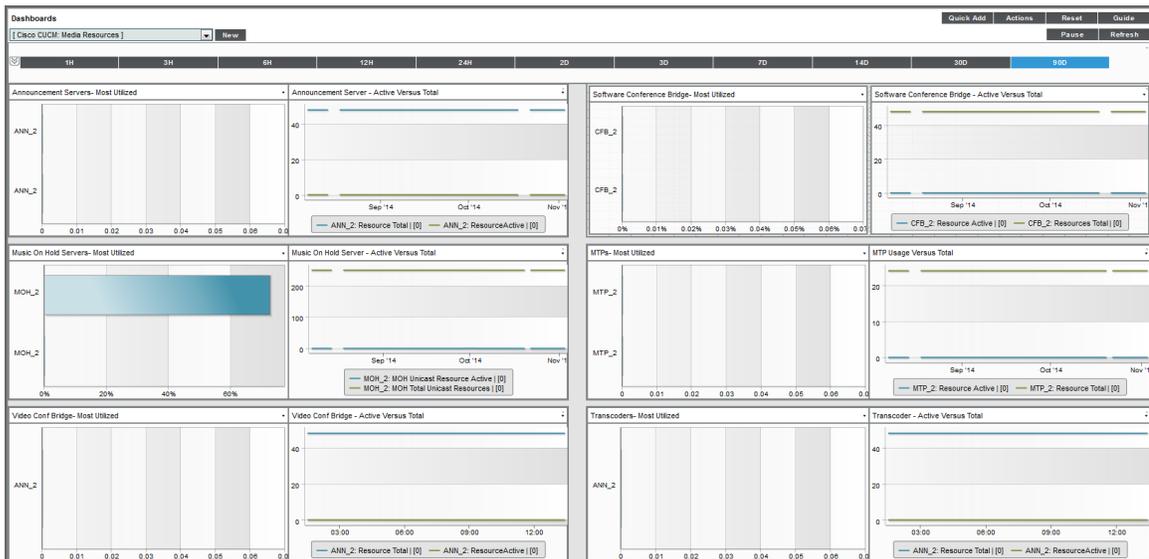
The Cisco: CUCM Locations LBM (Location Bandwidth Manager) dashboard displays eight widgets.

The dashboard includes the following widgets:

- **Top Locations by Audio Bandwidth.** This widget displays a horizontal bar graph that depicts a list of locations, ordered by audio bandwidth usage by percent, from highest to lowest.
- **Location - Audio Bandwidth Utilization.** This widget displays a line graph that depicts audio bandwidth utilization over time.
- **Top Locations by Available Bandwidth.** This widget displays a horizontal bar graph that depicts a list of locations, ordered by available bandwidth in kpbs, from highest to lowest.
- **Location - Available Bandwidth.** This widget displays a line graph that depicts available bandwidth over time.
- **Top Locations by Video Bandwidth.** This widget displays a line graph that a list of locations, ordered by video bandwidth by percent, from highest to lowest.
- **Location - Video Bandwidth Utilization.** This widget displays a line graph that depicts video bandwidth utilization over time.
- **Top Locations by Telepresence Bandwidth Utilization.** This widget displays a horizontal bar graph that depicts a list of locations, ordered by TelePresence bandwidth usage in percent, from highest to lowest.
- **Location - Telepresence BW Utilization.** This widget displays a line graph that depicts TelePresence bandwidth utilization over time.

## Cisco: CUCM Media Resources

The Cisco: CUCM Media Resources dashboard displays 12 widgets that display the most utilized and active versus total metrics for transcoding, announcement servers, streaming music to callers on hold, video, conferencing, and media termination points.



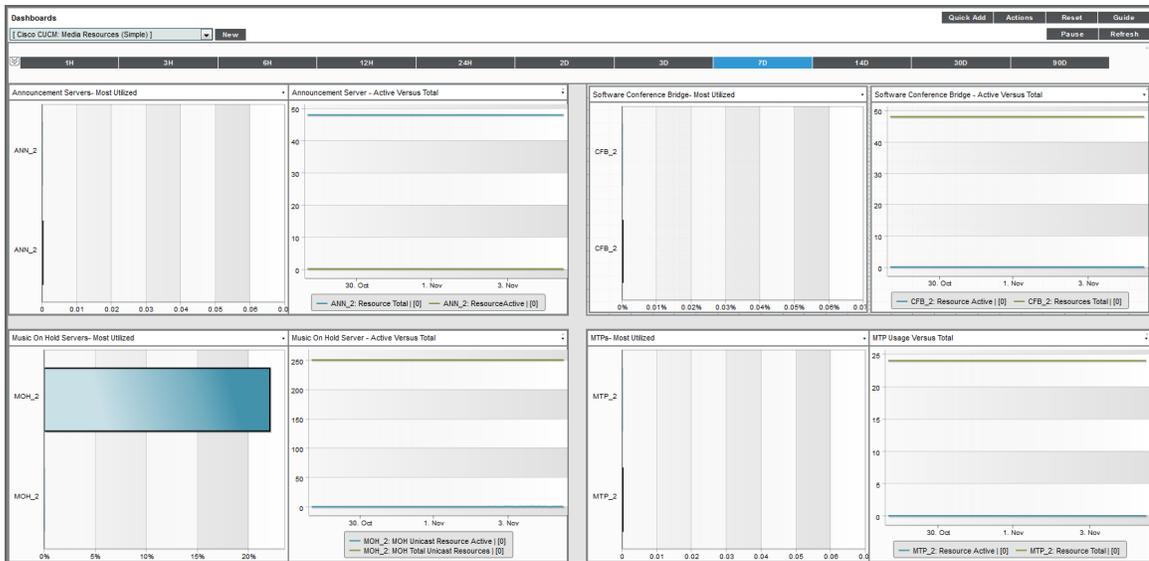
The dashboard includes the following widgets:

- **Announcement Servers - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized announcement servers.
- **Announcement Server - Active Versus Total.** This widget displays a line graph that depicts the active announcement servers versus the total announcement servers over time.
- **Software Conference Bridge - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized software conference bridges by percent.
- **Software Conference Bridge - Active Versus Total.** This widget displays a line graph that depicts the active versus total software conference bridges over time.
- **Music On Hold Servers - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized music-on-hold servers by percent.
- **Music On Hold Servers - Active Versus Total.** This widget displays a line graph that depicts the active versus total music-on-hold servers over time.
- **MTPs - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized Media Transfer Protocols (MTPs) by percent.
- **MTP Usage Versus Total.** This widget displays a line graph that depicts the usage versus total Media Transfer Protocols (MTPs) over time.
- **Video Conf Bridge - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized video conference bridges by percent.
- **Video Conf Bridge - Active Versus Total.** This widget displays a line graph that depicts the active versus total video conference bridges over time.
- **Transcoders - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized transcoders by percent.
- **Transcoders - Active Versus Total.** This widget displays a line graph that depicts the active versus total transcoders over time.

---

## Cisco: CUCM Media Resources (Simple)

The Cisco: CUCM Media Resources dashboard displays eight widgets which display the most utilized and active versus total metrics for announcement servers, streaming music to callers on hold, conferencing, and media termination points.



The dashboard includes the following widgets:

- **Top SIP Trunks by Number of Active Calls.** This widget displays a horizontal bar graph that depicts the most utilized SIP trunks.
- **SIP Trunk Active Calls (Per Trunk).** This widget displays a line graph that depicts the number of active calls per SIP Trunk over time.
- **Software Conference Bridge - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized software conference bridges by percent.
- **Software Conference Bridge - Active Versus Total.** This widget displays a line graph that depicts the active versus total software conference bridges over time.
- **Music On Hold Servers - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized music-on-hold servers by percent.
- **Music On Hold Servers - Active Versus Total.** This widget displays a line graph that depicts the active versus total music-on-hold servers over time.
- **MTPs - Most Utilized.** This widget displays a horizontal bar graph that depicts the most utilized Media Transfer Protocols (MTPs) by percent.
- **MTP Usage Versus Total.** This widget displays a line graph that depicts the usage versus total Media Transfer Protocols (MTPs) over time.

## Cisco: CUCM Tomcat

The Cisco: CUCM Tomcat dashboard displays 12 widgets that monitor servers and services that use the Tomcat Java Webserver.

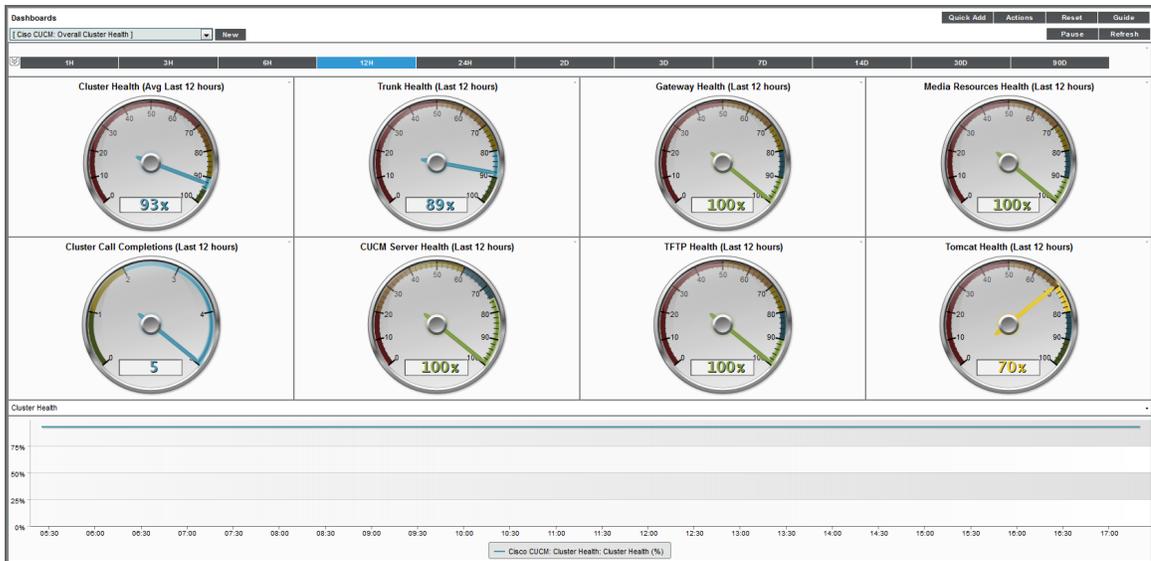
The dashboard includes the following widgets:

- **Tomcat - Top Servers by Number of Requests.** This widget displays a horizontal bar graph that depicts the servers with the highest number of requests.
- **Tomcat % Memory Utilization.** This widget displays a line graph that depicts the percentage of memory utilization over time.
- **Tomcat % Total Errors.** This widget displays a line graph that depicts the percentage of errors over time.
- **Tomcat Connector - Total Sessions Active.** This widget displays a line graph that depicts the total active Tomcat Connector sessions over time.
- **Tomcat - Top 10 Services By Number of Requests.** This widget displays a horizontal bar graph that depicts the ten services with the most requests.
- **Tomcat - Number of Requests (Per Service).** This widget displays a line graph that depicts the number of requests per service over time.
- **Tomcat - Top 10 Services by Errors.** This widget displays a horizontal bar graph that depicts the ten services with the most errors.
- **Tomcat - Errors (Per Service).** This widget displays a line graph that depicts errors per service over time.
- **Tomcat - Top 5 Services by Sessions Active.** This widget displays a horizontal bar graph that depicts the five services with the most active sessions.
- **Tomcat - Sessions Active.** This widget displays a line graph that depicts active Tomcat sessions over time.
- **Tomcat - Top Connectors By Errors/Threads Busy.** This widget displays a horizontal bar graph that depicts the Connectors with the most errors and busy threads.
- **Tomcat - Connector Errors or Threads Busy (Per Connector).** This widget displays a line graph that depicts connector errors or busy threads per connector over time.

---

## Cisco: CUCM Overall Cluster Health

The Cisco: CUCM Overall Cluster Health dashboard contains nine widgets that monitor aspects of the cluster's overall health.

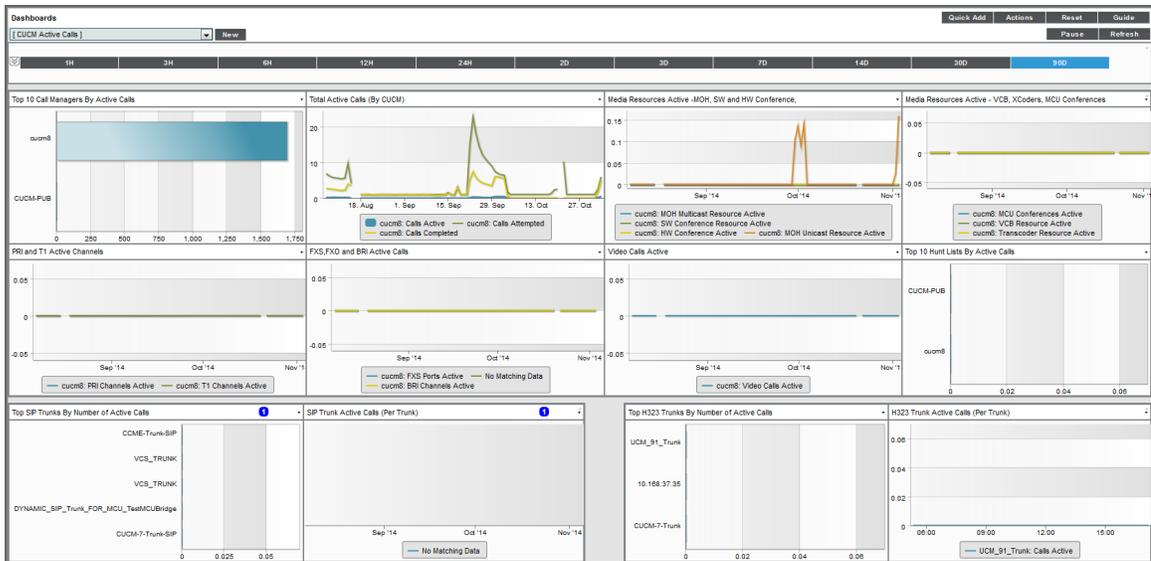


The dashboard includes the following widgets:

- Eight gauge widgets use IT Service Monitor Policies to display the following:
  - Cluster Health
  - Trunk Health
  - Gateway Health
  - Media Resources Health
  - Cluster Call Completions
  - CUCM Server Health
  - TFTP Health
  - Tomcat Health
- At the bottom of the dashboard, a line graph depicts the overall cluster health by percentage over time.

## Cisco: CUCM Active Calls

The Cisco: CUCM Active Calls widget displays 12 graphs that monitor active calls, conferences, and active channels.



The widgets display:

- **Top 10 Call Managers By Active Calls.** This widget displays a horizontal bar graph that depicts the ten call managers with the highest number of active calls.
- **Total Active Calls (By CUCM).** This widget displays a line graph that depicts total active calls by CUCM over time.
- **Media Resources Active - MOH, SW and HW Conferences.** This widget displays a line graph that depicts active MOH, SW, and HW conference media resources over time.
- **Media Resources Active - VCB, Xcoders, MCU Conferences.** This widget displays a line graph that depicts active VCB, Xcoders, and MCU conferences over time.
- **PRI and T1 Active Channels.** This widget displays a line graph that depicts the active PRI and T1 channels over time.
- **FXS, FXO, and BRI Active Calls.** This widget displays a line graph that depicts FXS, FXO, and BRI active calls over time.
- **Video Calls Active.** This widget displays a line graph that depicts active video calls over time.
- **Top 10 Hunt Lists By Active Calls.** This widget displays a horizontal bar graph that depicts the ten hunt lists with the highest number of active calls.
- **Top SIP Trunks By Number of Active Calls.** This widget displays a horizontal bar graph that depicts the SIP trunks with the highest number of active calls.
- **SIP Trunk Active Calls (Per Trunk).** This widget displays a line graph that depicts active SIP trunk calls over time.
- **Top H323 Trunks By Number of Active Calls.** This widget displays a horizontal bar graph that depicts the H323 trunks with the highest number of active calls.
- **H323 Trunk Active Calls (Per Trunk).** This widget displays a line graph that depicts active H323 trunk calls over time.

---

# Chapter

# 5

## Troubleshooting

---

### Overview

The following sections describe resolutions to some issues you might encounter when monitoring Cisco Unified Communications Manager:

<i>Resolving Network Connectivity Issues</i> .....	46
<i>Resolving Credential Issues</i> .....	47
<i>Basic/Snippet (AXL User) Credentials</i> .....	47
<i>SNMP Credentials</i> .....	48
<i>Resolving NAT Issues</i> .....	48
<i>Resolving Error Messages</i> .....	48
<i>Running Dynamic Applications in Debug Mode</i> .....	49

---

### Resolving Network Connectivity Issues

If you experience network connectivity issues, you can follow the steps in this section to diagnose the cause.

To diagnose network connectivity issues:

1. Use a Secure Shell (SSH) client software such as PuTTY to log in to the ScienceLogic Data Collector.
2. Type the following command:

```
ping <Cisco Unified CM Publisher IP>
```

If this fails, check to see if the network is blocking ICMP traffic anywhere, as this might identify a firewall that is not documented.

3. Type the following command:

```
nmap -sU -Pn -p 161 <Cisco Unified CM Publisher IP>
```

This will validate whether or not you have SNMP connectivity. If you do not, you might be on an access control list (ACL).

4. Type the following command:

```
nmap -sS -Pn -p 8443 <Cisco Unified CM Publisher IP>
```

This will determine if you have AXL connectivity.

5. Type the following command:

```
traceroute <Cisco Unified CM Publisher IP>
```

This will identify any additional unknown firewalls or unexpected routing paths.

If you cannot identify the causes of your network connectivity issues using these steps, you might be experiencing a DNS resolution issue. For more information, see the [Manually Creating Host File Entries for CUCM Nodes](#) section.

---

## Resolving Credential Issues

### Basic/Snippet (AXL User) Credentials

The following list includes commands that you can use to validate your Basic/Snippet Cisco Unified CM credentials:

- To validate that the credential can communicate with the AXL API service:

```
curl -k -u <USER>:<PASSWORD> -H "Content-type: text/xml;" https://<Cisco Unified CM Publisher IP>:8443/axl/services/AXLAPIService?wsdl
```

- To validate that the credential can communicate with the Real Time Information port:

```
curl -k -u <USER>:<PASSWORD> -H "Content-type: text/xml;" https://<Cisco Unified CM Publisher IP>:8443/realtimeservice/services/RisPort?wsdl
```

- To validate that the credential can communicate with the Performance Monitor port:

```
curl -k -u <USER>:<PASSWORD> -H "Content-type: text/xml;" https://<Cisco Unified CM Publisher IP>:8443/perfmonservice/services/PerfmonPort?wsdl
```

- To validate that the credential can communicate with the SOAP monitor service:

```
curl -k -u <USER>:<PASSWORD> -H "Content-type: text/xml;" https://<Cisco Unified CM Publisher IP>:8443/realtimeservice/services/SOAPMonitorService?wsdl
```

- To validate that the credential can communicate with the Control Center service port:

```
curl -k -u <USER>:<PASSWORD> -H "Content-type: text/xml;" https://<Cisco Unified CM Publisher IP>:8443/controlcenterservice/services/ControlCenterServicesPort?wsdl
```

## SNMP Credentials

You can use the following commands to validate your SNMP credentials:

- For SNMP v2:

```
snmpwalk -v 2c -c <read string> <Cisco Unified CM Publisher IP> system
```

- For SNMP v3:

```
snmpwalk -v3 -l authNoPriv -u <username> -a SHA -A <password> <Cisco Unified CM Publisher IP>
```

---

## Resolving NAT Issues

If a customer must have a firewall between the ScienceLogic Data Collector and the Cisco Unified CM Cluster, then check the firewall to determine if the firewall is performing network address translation (NAT).

If NAT is enabled:

1. The customer must provide a hostname and an IP address accessible from the Data Collector for the Cluster and each subscribing CallManager.
2. Add the CallManager hostnames and IP addresses to host file entries. (For more information, see the [Manually Creating Host File Entries for CUCM Nodes](#) section.)
3. Allow time for the host file to be propagated to the Data Collector.

**NOTE:** You can also follow these instructions if the CallManager is defined by an IP address but not a hostname.

---

## Resolving Error Messages

The following error message might be generated during collection for the Cisco Unified Communications Manager Dynamic Applications.

Error / Message	Cause / Resolution
When running the "Cisco: CUCM Cluster Root Cache" Dynamic Application, you receive an error message stating "[Application number, snippet number] reported a collection problem. (Explanation: The server is not specified as a Publisher.)"	SL1 cannot determine the node's IP address. You must add the node hostname and IP address to a host file. (For more information, see the <a href="#">Manually Creating Host File Entries for CUCM Nodes</a> section.)

---

## Running Dynamic Applications in Debug Mode

To identify issues with a specific Dynamic Application, go to the **Dynamic Application Collections** page (Registry > Devices > wrench icon > Collections) and run the Dynamic Application by clicking its lightning bolt icon (⚡). Doing so provides you with details about any issues the Dynamic Application might be experiencing with the provided URL, IP address, or credentials.

Another method, which will provide even more data, is to run the Dynamic Application in debug mode. To run a Dynamic Application in debug mode, type the following command from the command line interface for the Data Collector:

```
sudo -u s-em7-core SILO_DEBUG=1 /opt/em7/backend/dynamic_single.py <device ID>  
<Dynamic Application ID>
```

© 2003 - 2021, 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](mailto:legal@sciencelogic.com)



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

International: +1-703-354-1010