Monitoring Cisco Unified Communications Manager

Cisco: CUCM Unified Communications Manager PowerPack version 110

Table of Contents

Chapter 1

Introduction

Overview

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

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 the ScienceLogic platform, 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 the ScienceLogic platform 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
- A Run Book Action that assigns the Cisco Unified CM cluster root device to the appropriate Device Class

NOTE: The Run Book Action 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.

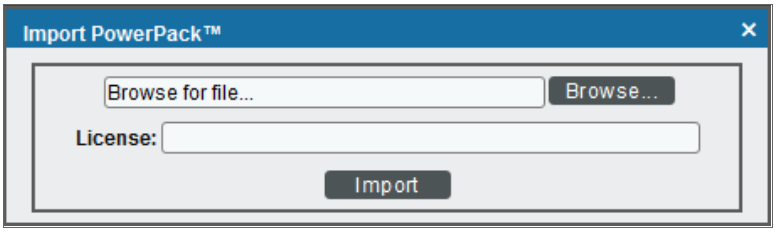
Installing the Cisco: CUCM Unified Communications Manager PowerPack

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 in 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 Customer Portal.
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 page appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal page 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 page. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuring Cisco Unified Communications Manager for Monitoring

Overview

The following sections describe how to configure a Cisco Unified Communications Manager (CM) system for monitoring by the ScienceLogic platform using the *Cisco: CUCM Unified Communications Manager* PowerPack:

Prerequisites for Monitoring Cisco Unified CM

During the discovery process, the ScienceLogic platform 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 the ScienceLogic platform, ensure that you know or have access to the following information about each node:

- IP address
- Hostname

Configuring the ScienceLogic Platform to Monitor Cisco Unified CM

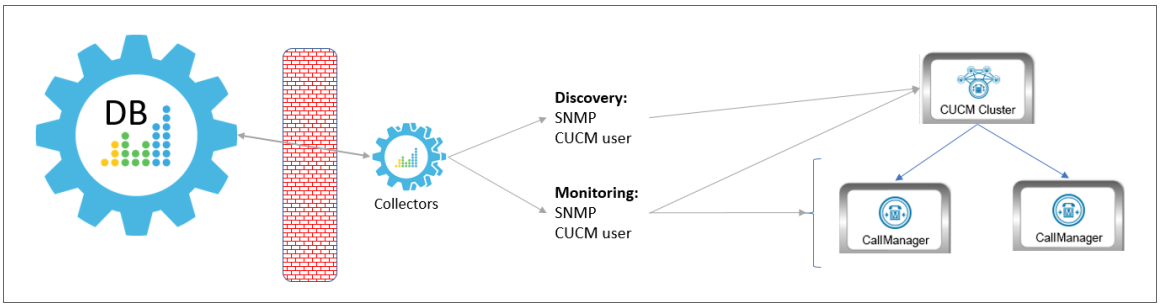
You can choose from several different possible configurations when using the ScienceLogic platform to monitor Cisco Unified CM:

- 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:

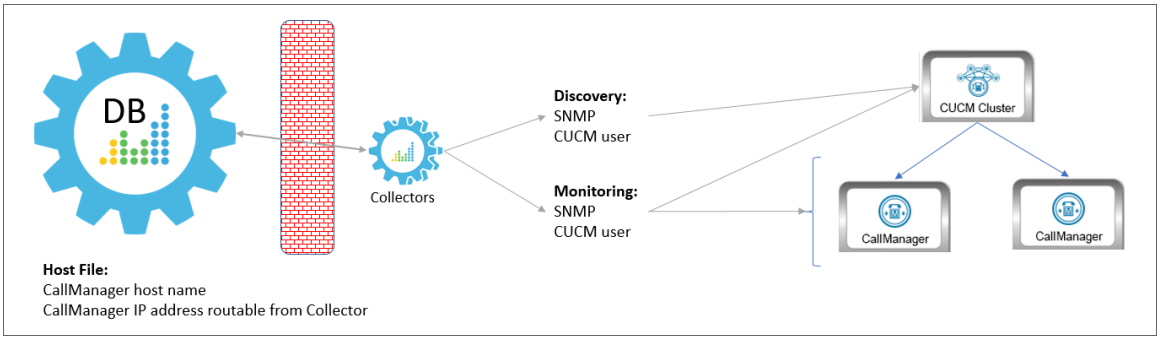


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7706	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:

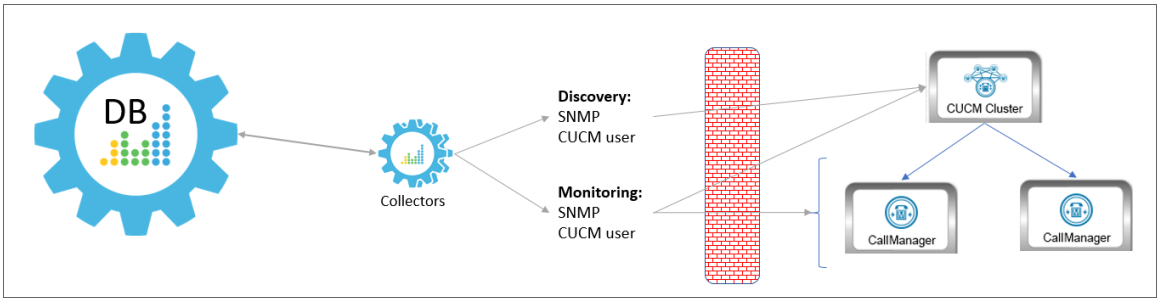


In this scenario, you must have the following ports open for the firewall:

Direction	Port	Protocol
ScienceLogic Database Server to the Data Collector	7707	TCP
PhoneHome Collector to the Database Server	7706	TCP

Method 3

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

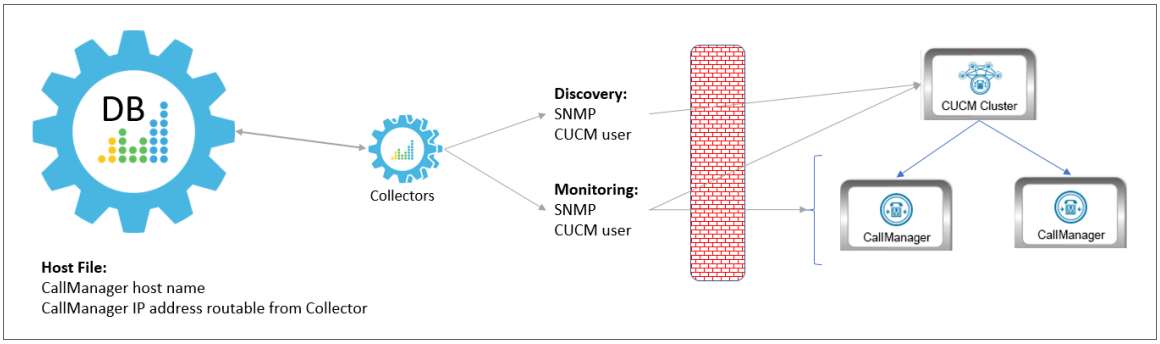


In this scenario, you must have the following ports open for the firewall:

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:

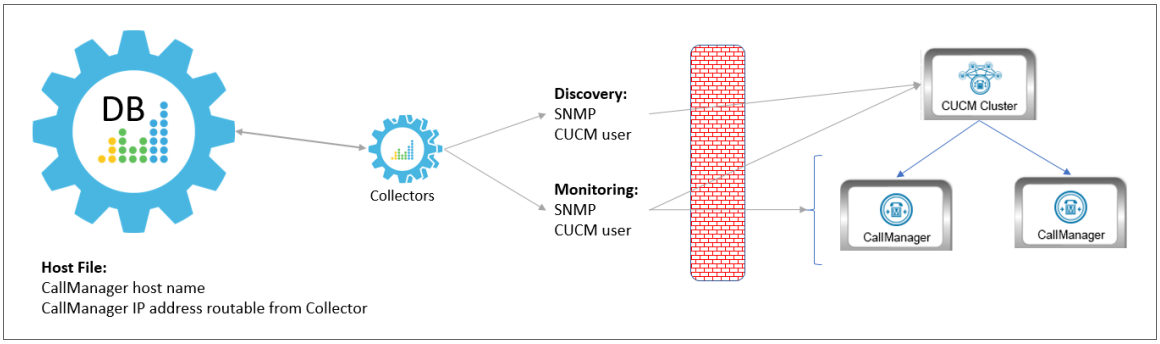


In this scenario, you must have the following ports open for the firewall:

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 Cisco Unified CM AXL Web Service

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

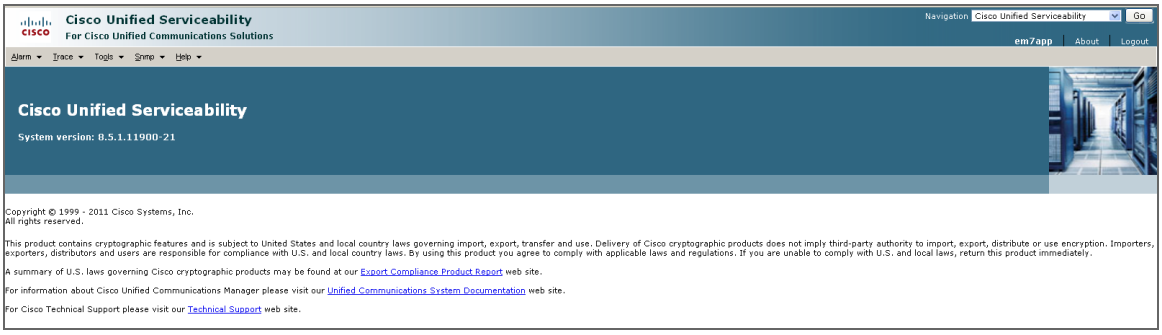
The Cisco Unified CM AXL web service is disabled by default. To enable the AXL web service, perform the following steps:

1. In a browser window, navigate to the following address:

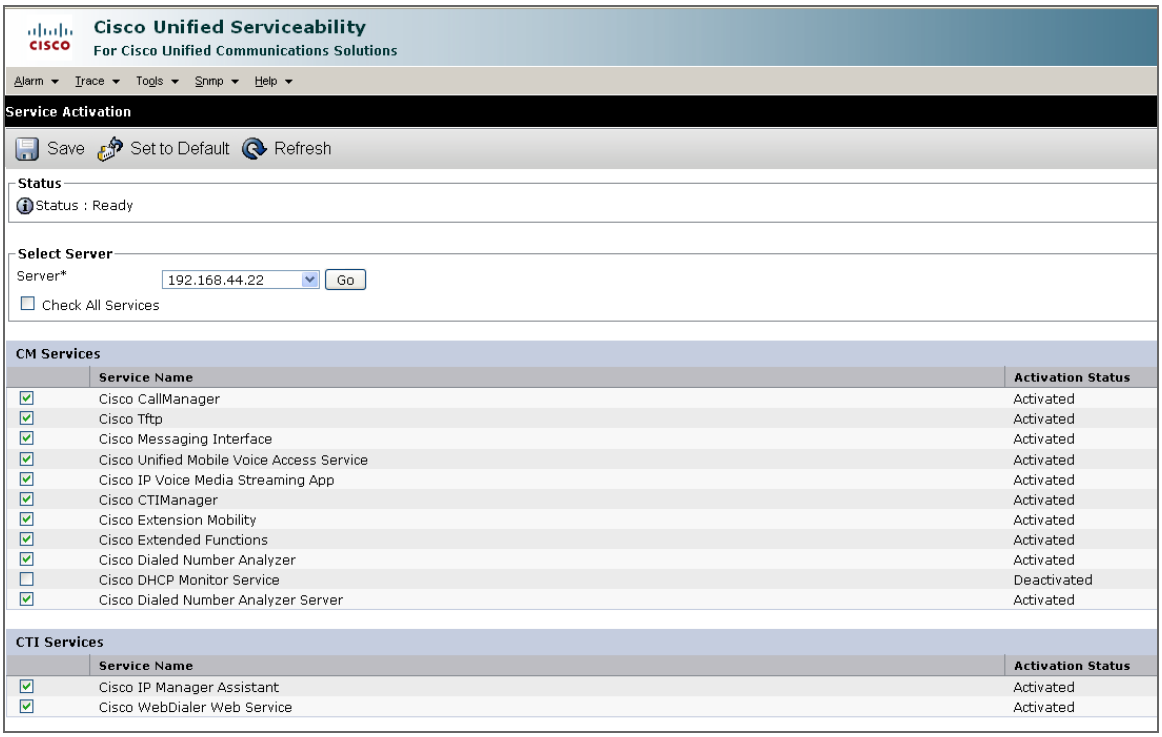
   `https://ip-address-of-CM-system:8443/ccmadmin/showHome.do`

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:



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



5. 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.
6. 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.
7. If the *Activation Status* of the ***Cisco AXL Web Service*** is not "Activated", select the checkbox for the **Cisco AXL Web Service**.

8. 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 Cisco Unified CM User Account

ScienceLogic recommends that you create a Cisco Unified CM user account that will be used only by the ScienceLogic platform 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:

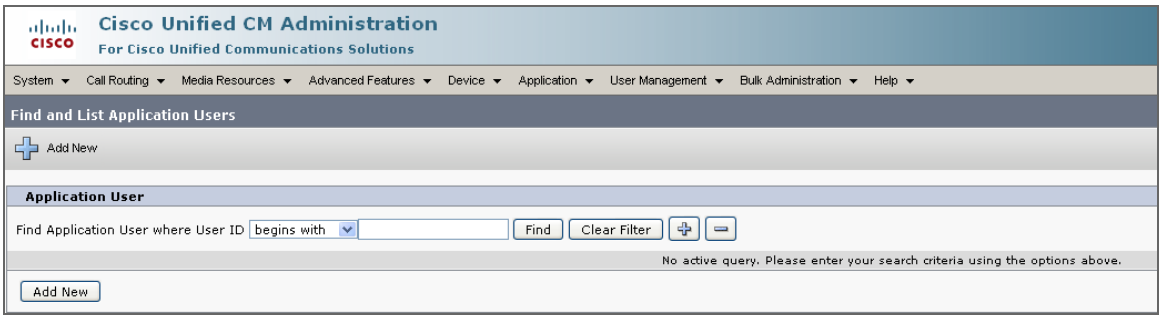
- Create a user account.
- Create a user group that includes the user account and has permission to access only the AXL web service.

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

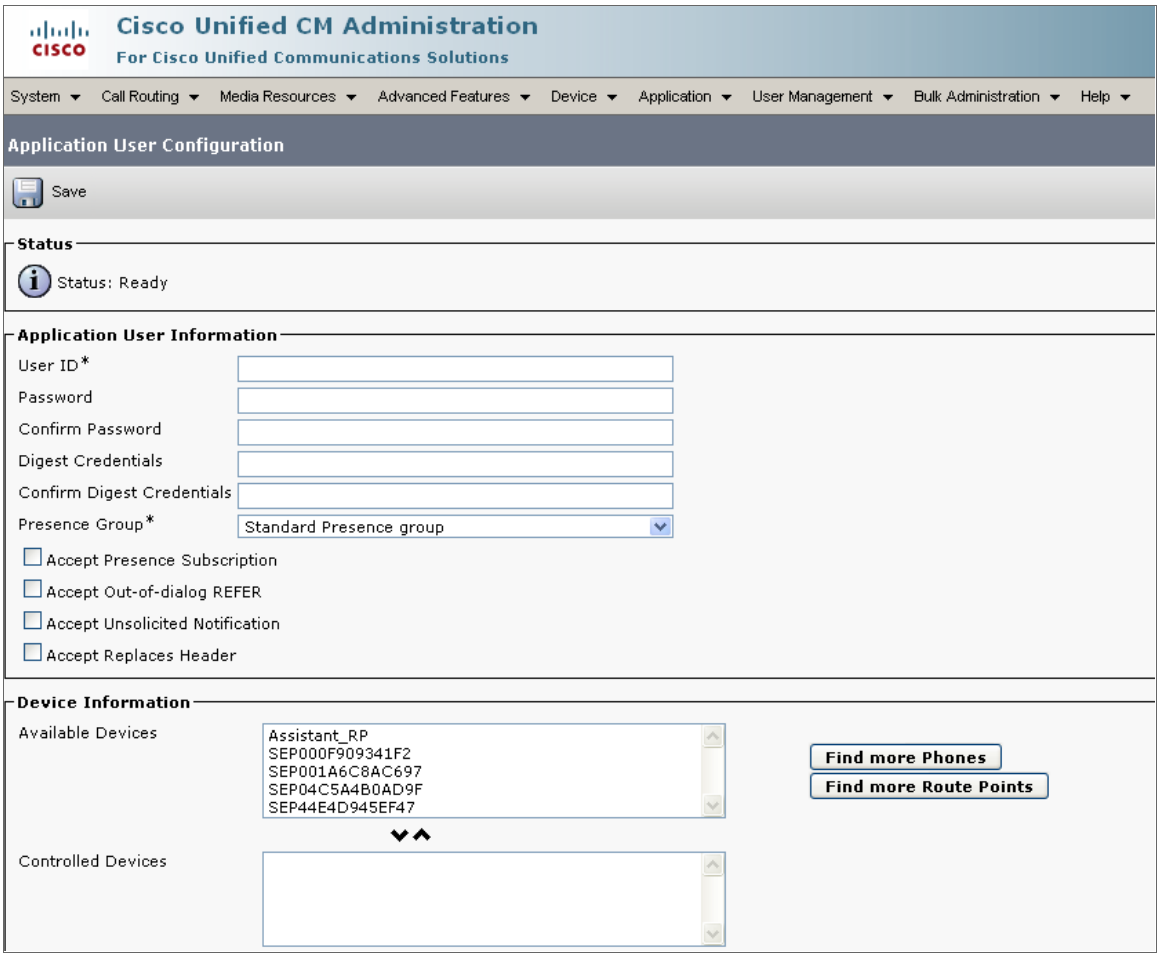
1. In a browser window, navigate to the following address:

   `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:

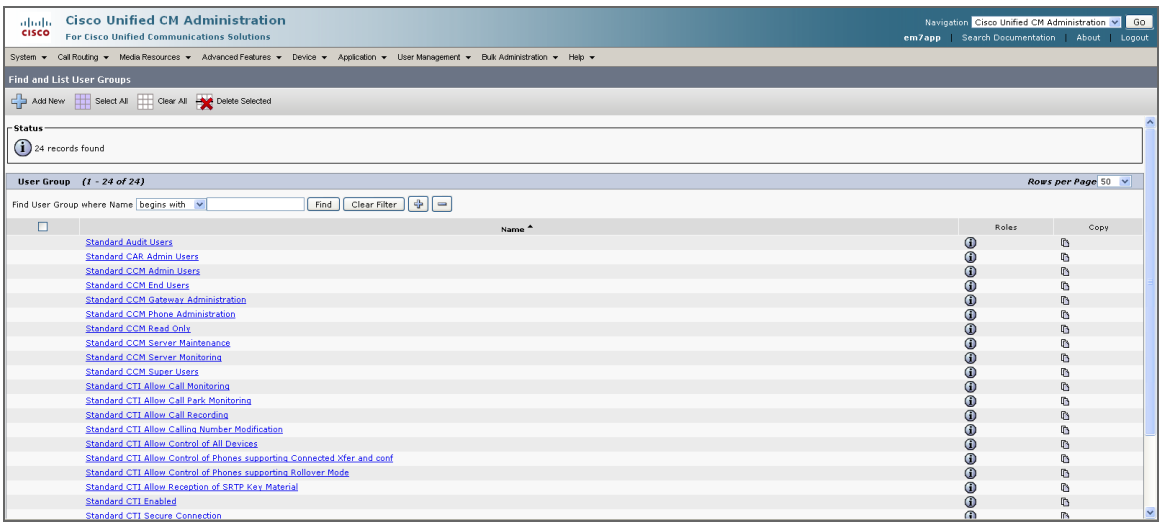


5. Supply values in the following fields:

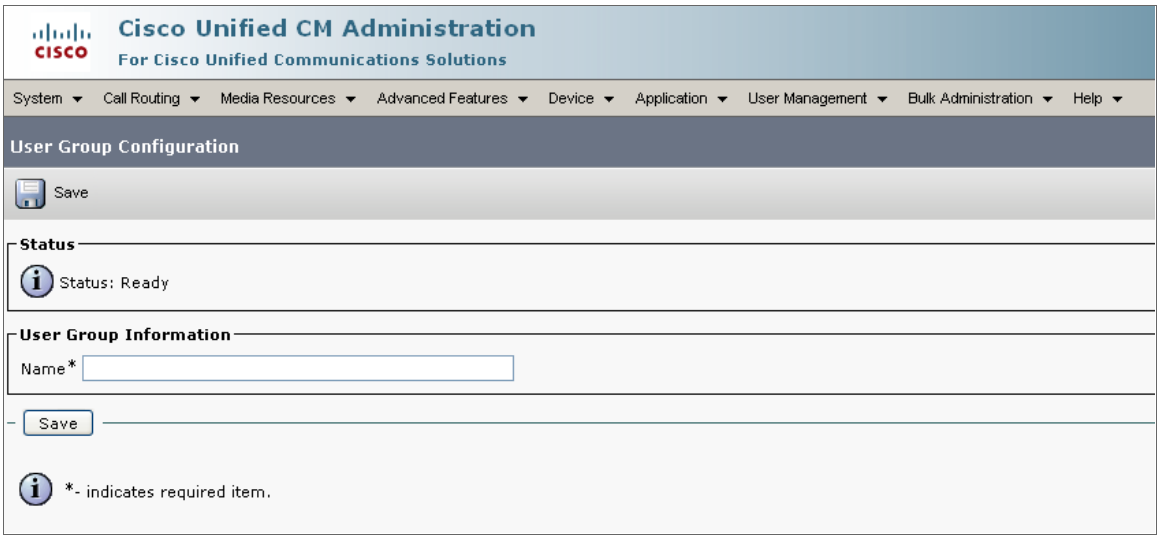
   - ***User ID***. Type a username for the new user.
   - ***Password***. Type a password for the new user.
   - ***Confirm Password***. Type the password for the new user again.

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

7. 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:

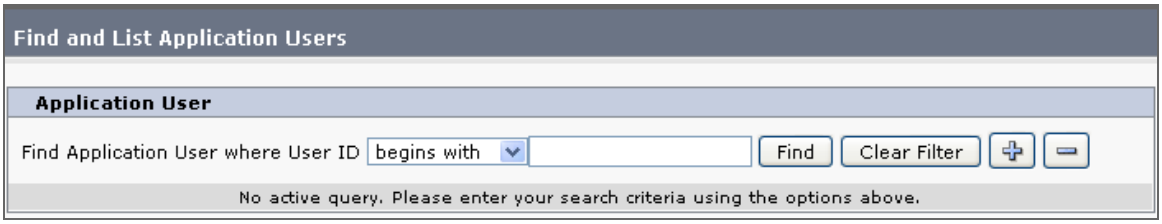


8. Click the **[+ Add New]** button. The **User Group Configuration** page appears:

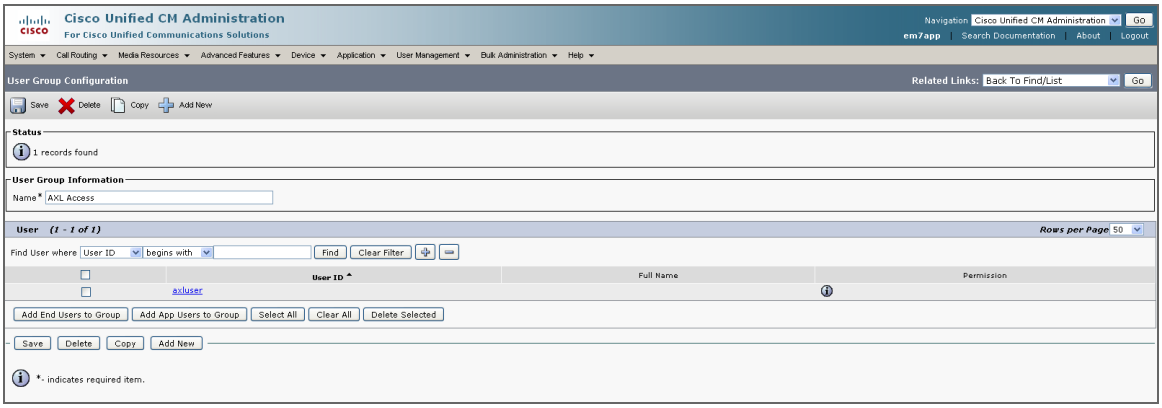


9. In the ***Name*** field, type a name for the user group. For example, you could call the user group "AXL Access".
10. Click the **[Save]** button.

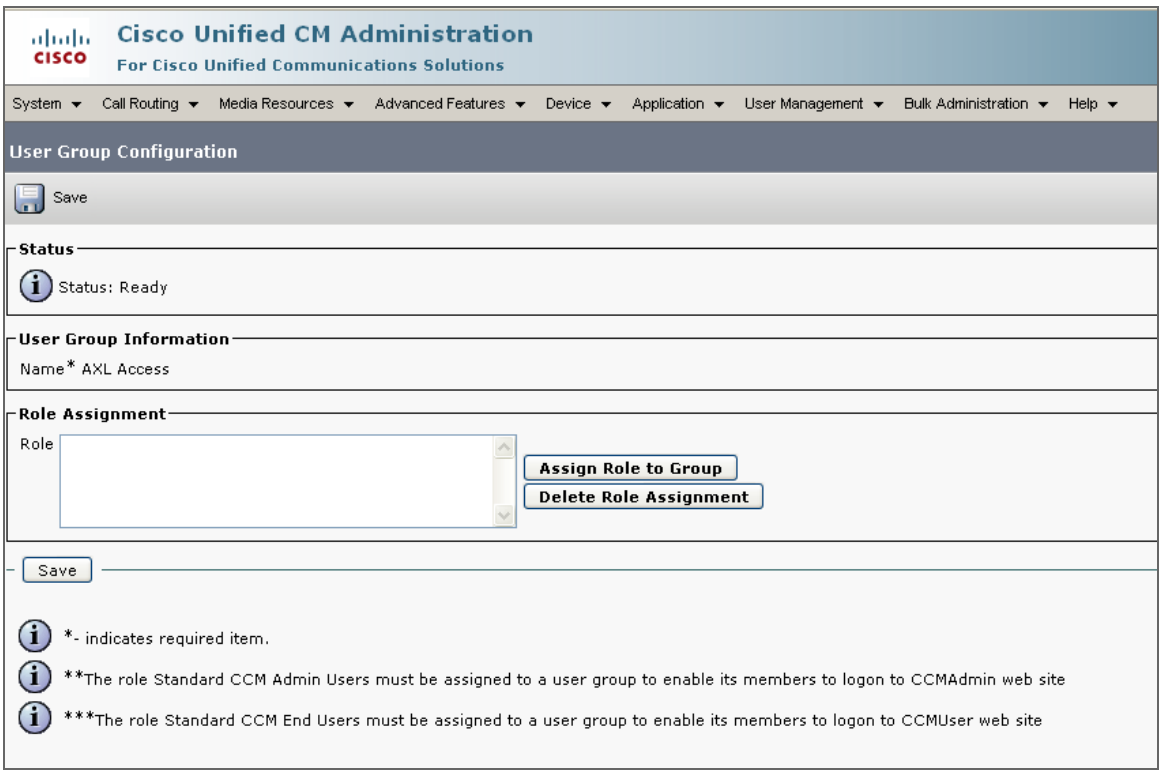
11. Click the **[Add App Users to Group]** button. The **Find and List Application Users** window appears:



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:

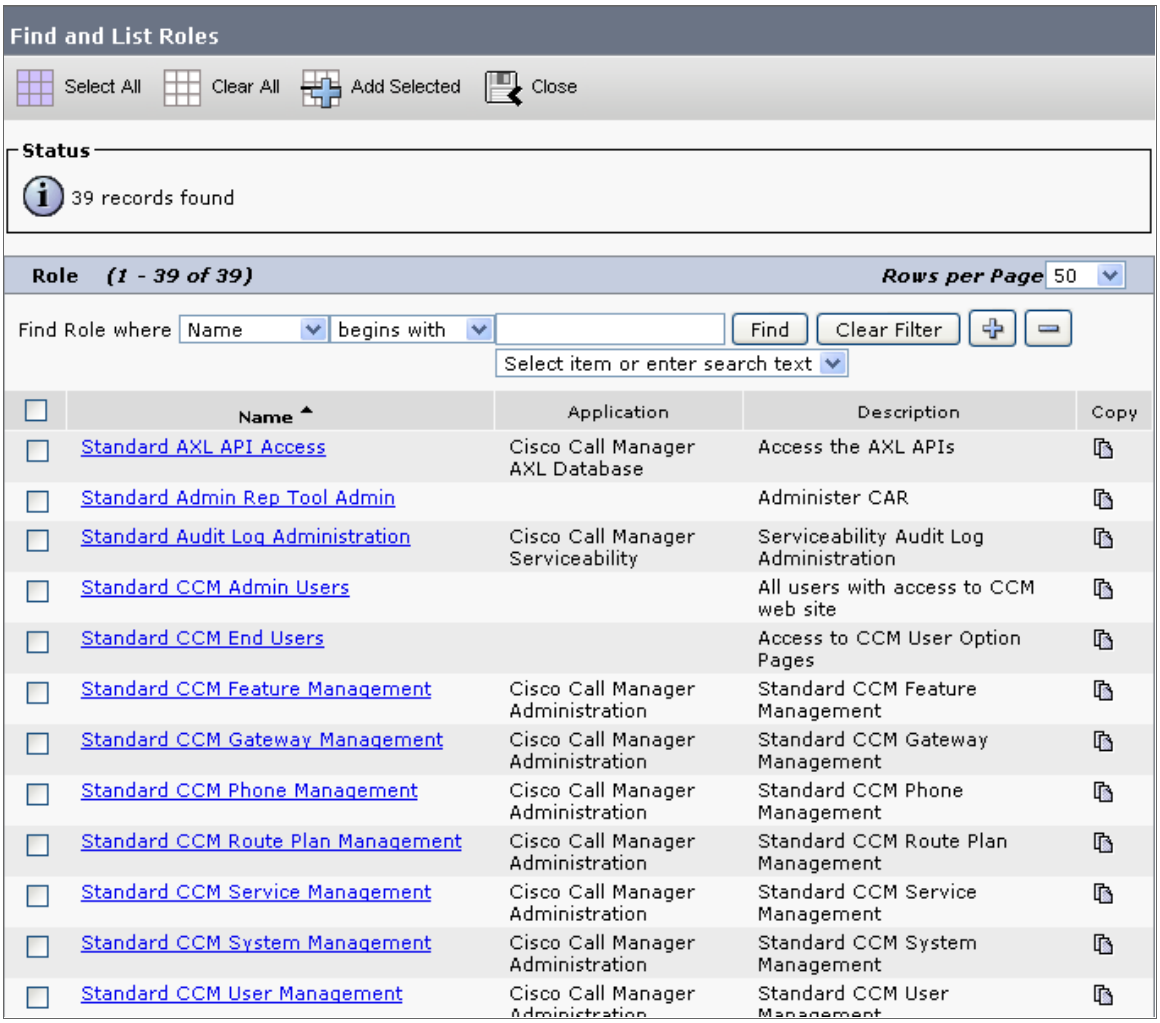


14. In the ***Related Links*** drop-down list at the top-right hand corner of the page, select *Assign Role to User Group*, and then click the **[Go]** button. The **User Group Configuration** page appears:



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

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

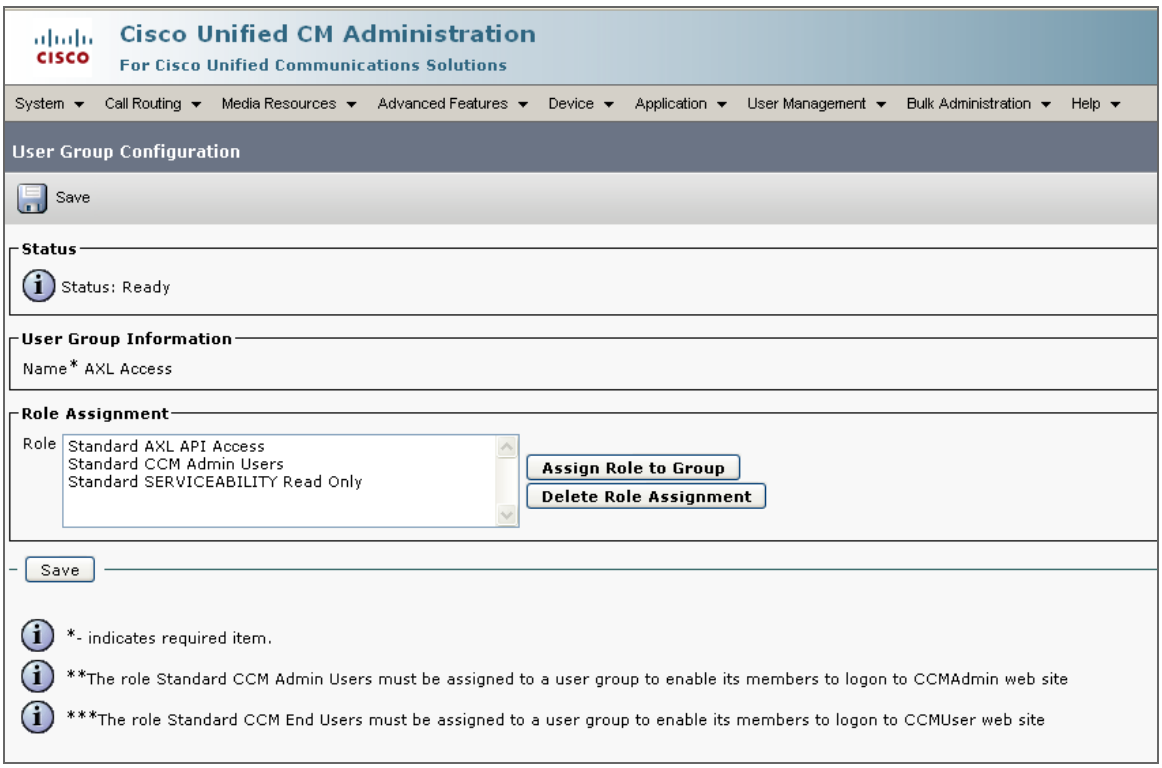


17. Select the checkboxes for the following roles:

    - *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:



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 the ScienceLogic platform can use to access PLM.

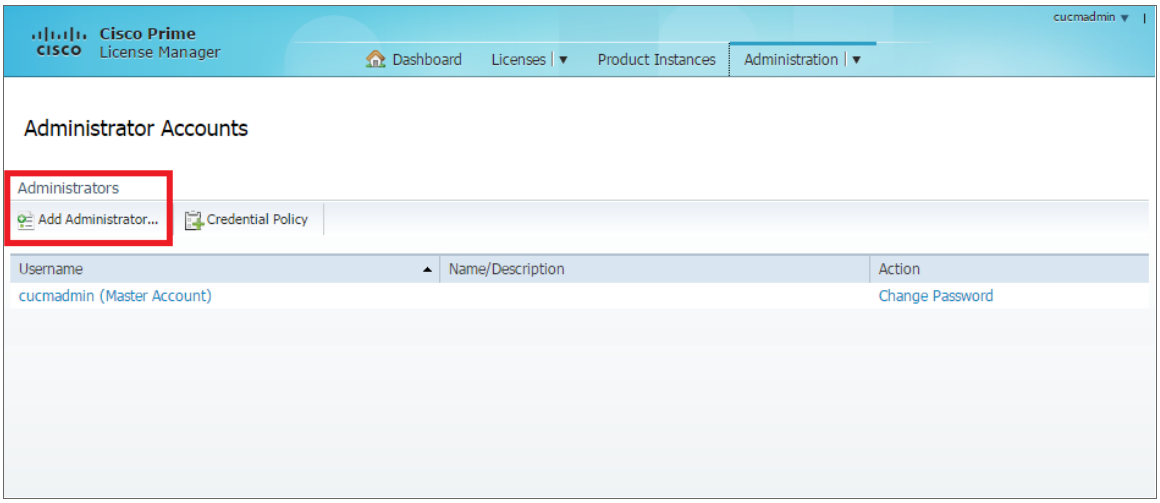
To create an administrator user in PLM:

1. In a browser window, navigate to the following address:

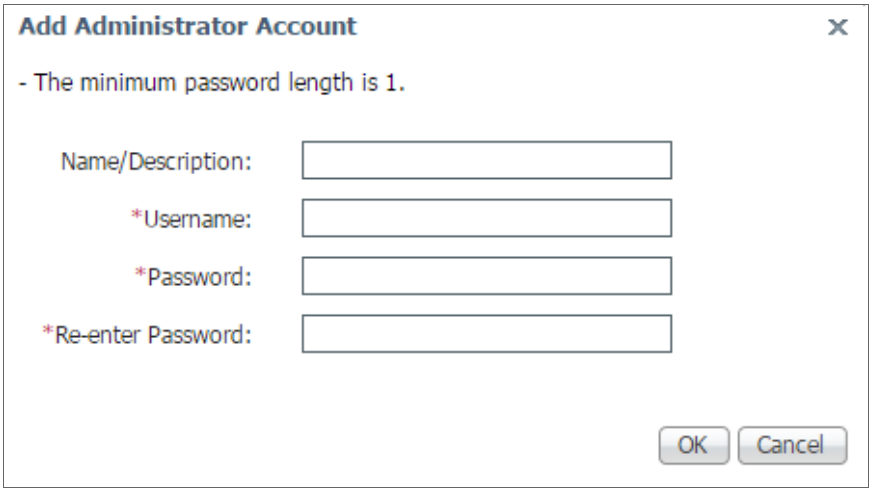
   ```
   https://ip-address-of-plm-server/elm-admin/
   ```

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:



- ***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.

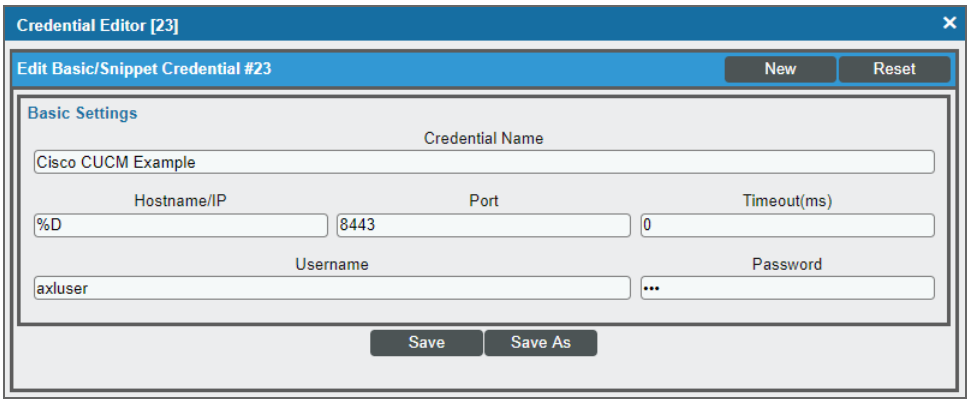
6. Click **[OK]**.

Creating a Cisco Unified CM 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 the ScienceLogic platform. This credential allows the platform 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:



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, the ScienceLogic platform will automatically override that value and use port 8443 instead. If your Cisco Unified CM credential specifies any port other than 80, the platform will use that specified port.

   - ***Timeout (ms)***. Type the timeout value of each request, in milliseconds.
   - ***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.

Manually Creating Host File Entries for Cisco Unified CM Nodes

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

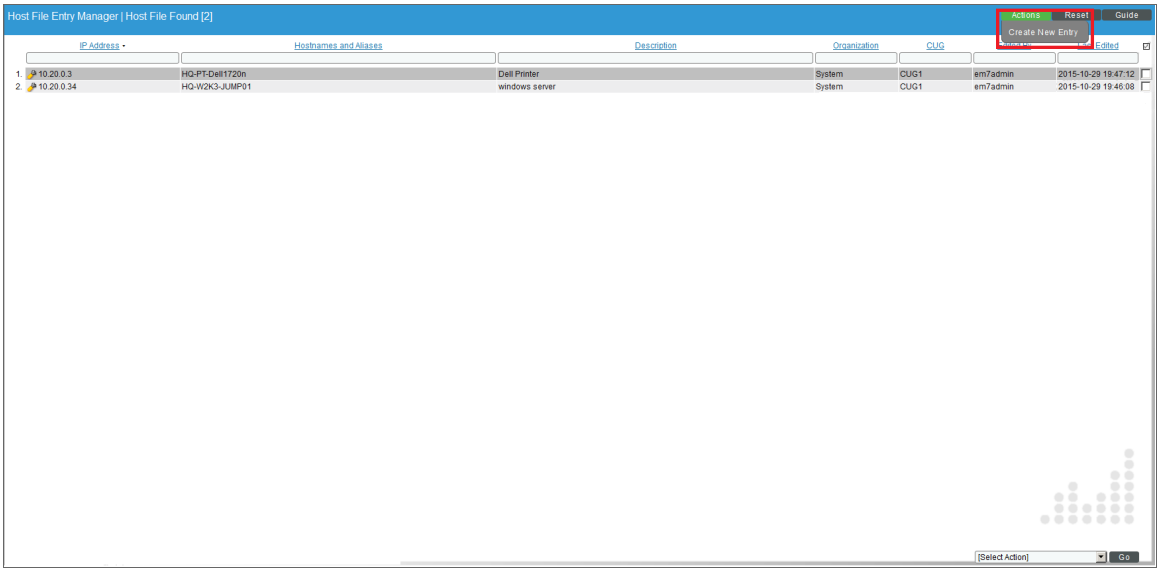
If you do not have access to DNS for the Cisco Unified CM system you want to monitor, you must manually create host file entries in the ScienceLogic platform for each node in the Cisco Unified CM cluster. Each host file entry must contain the IP address and hostname of a node in the Cisco Unified CM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

NOTE: If you have access to DNS for the Cisco Unified CM system you want to monitor with the ScienceLogic platform, 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*.

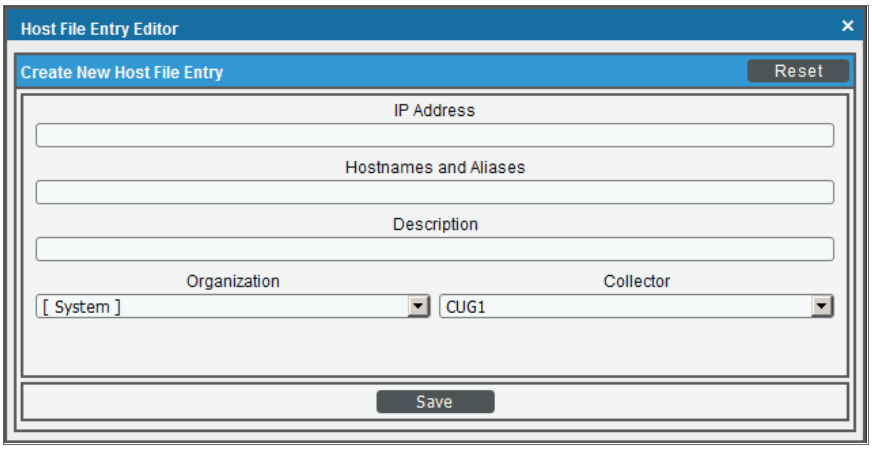
Repeat the following steps for each node in the Cisco Unified CM cluster.

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

Discovering Cisco Unified Communications Manager Clusters

Overview

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

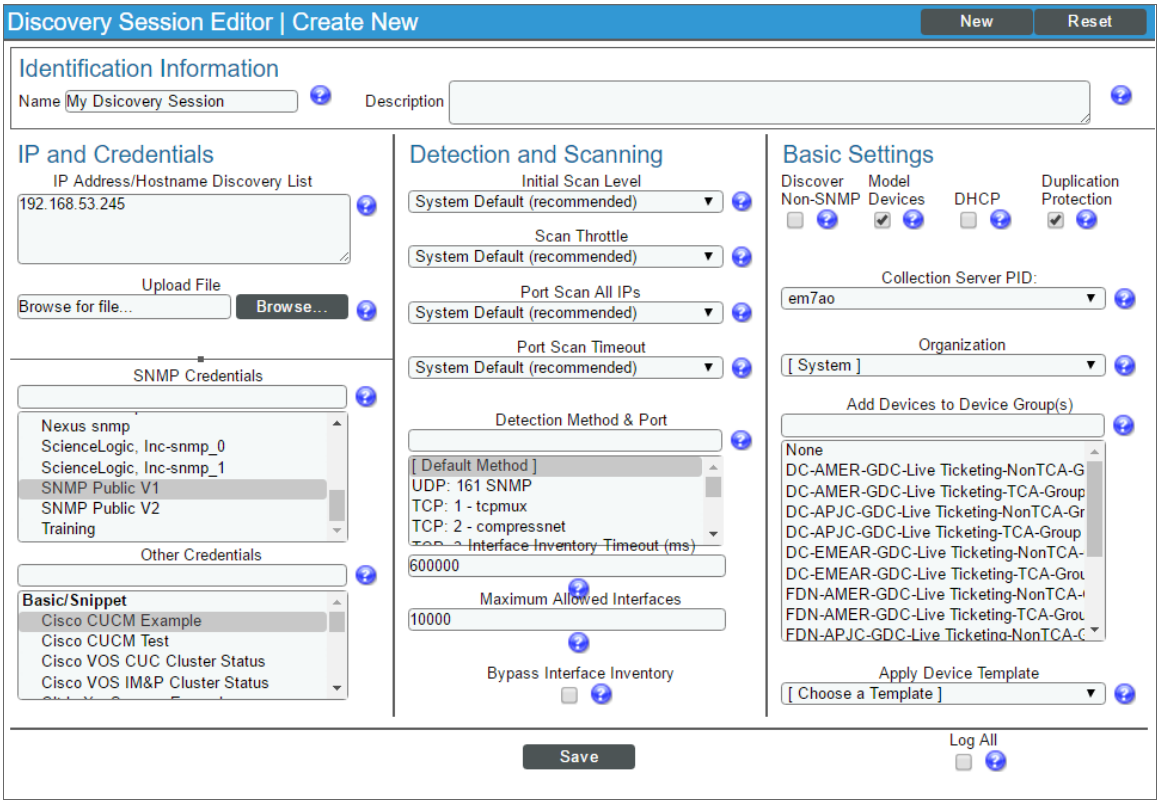
Discovering a Cisco Unified CM Cluster

When you use the *Cisco: CUCM Unified Communications Manager* PowerPack to discover Cisco Unified CM devices, the ScienceLogic platform 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 > Discovery).

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



3. 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.

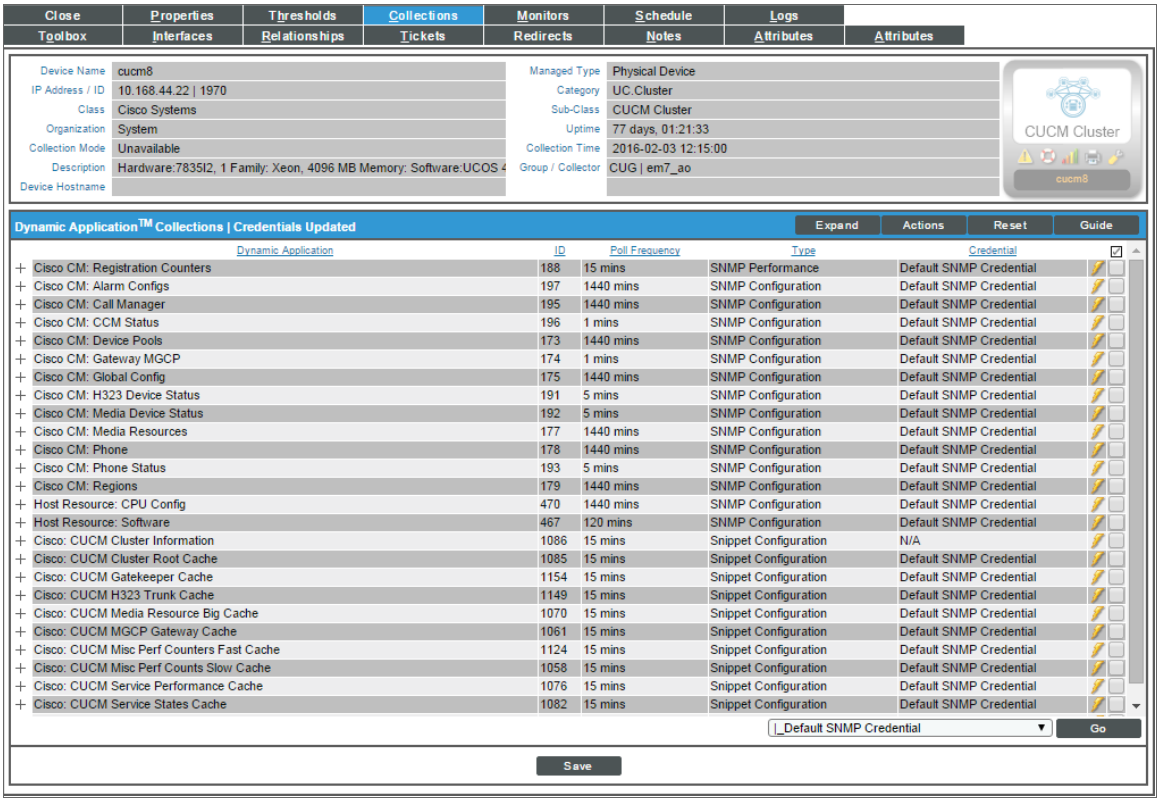
Verifying Discovery and Dynamic Application Alignment

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

To verify that the ScienceLogic platform 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.

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



3. 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

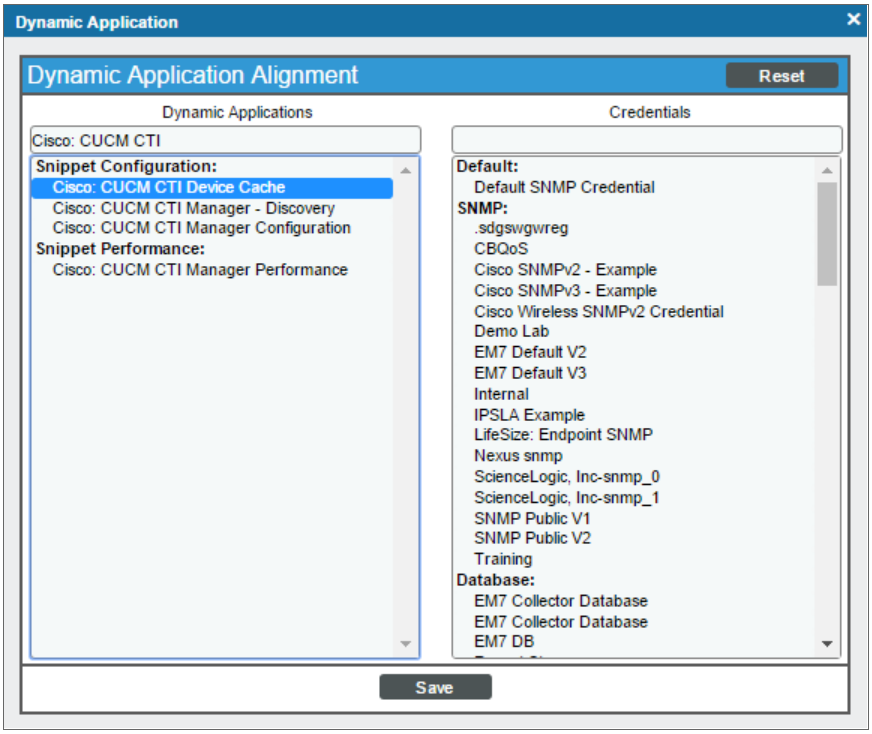
- Cisco: CUCM Partition Cache
- Cisco: CUCM Process Cache
- Cisco: CUCM Service Performance Cache
- Cisco: CUCM Service States Cache
- Cisco: CUCM SIP Trunk Cache

Manually Aligning Dynamic Applications

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

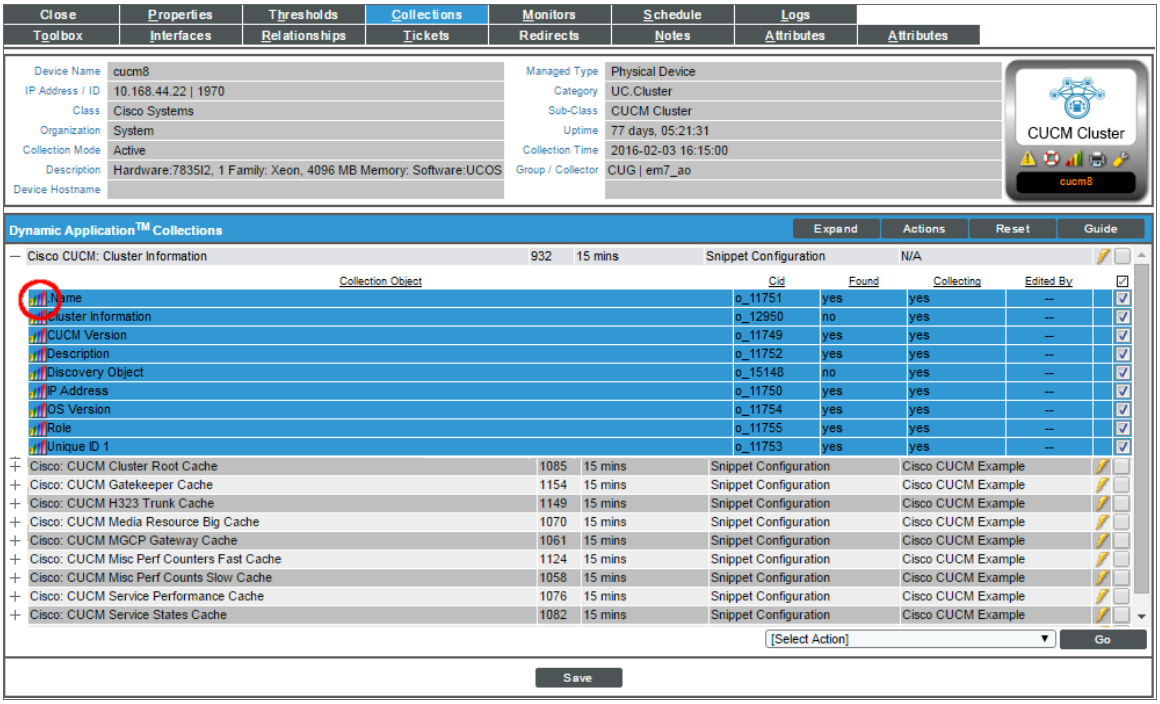
To manually align Dynamic Applications:

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:

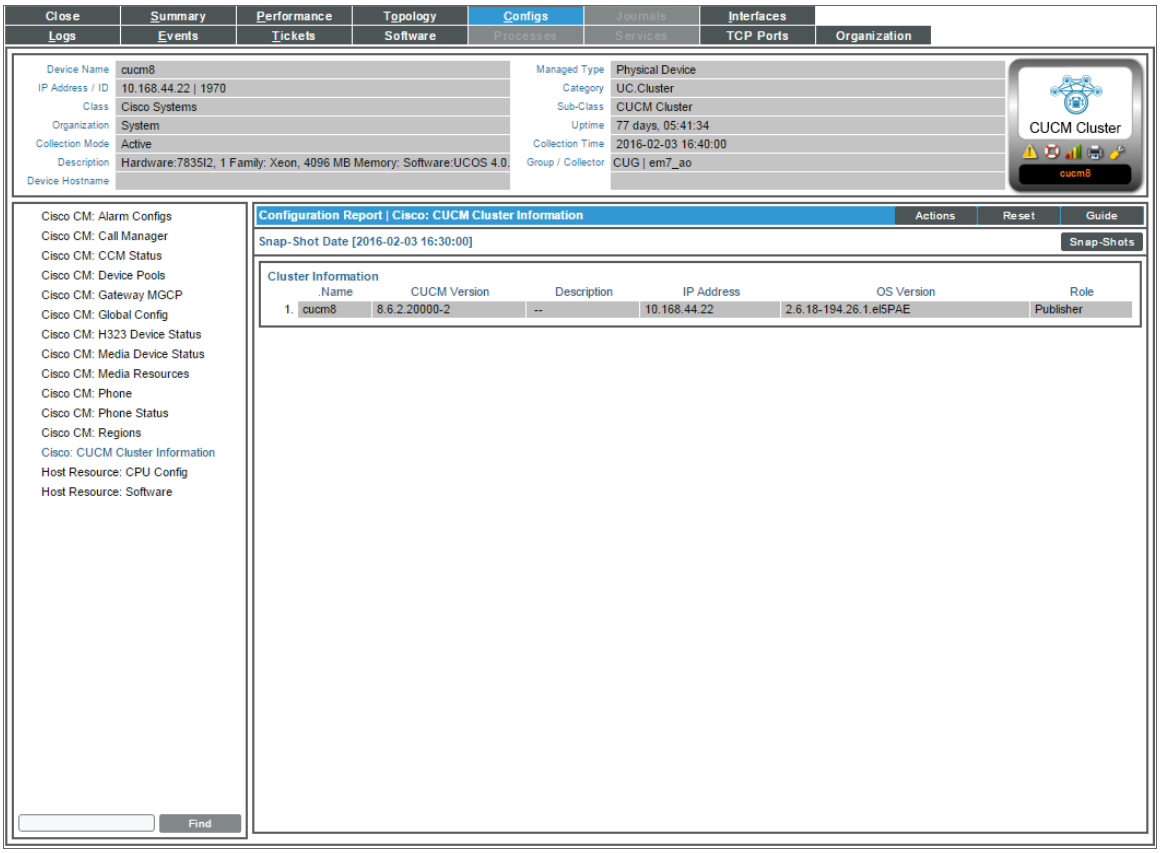


3. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.
4. In the ***Credentials*** field, select the SNMP credential you created for monitor the Cisco Unified CM cluster.
5. Repeat steps 2-4 for the remaining Dynamic Applications to align with the device.

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:



7. 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:

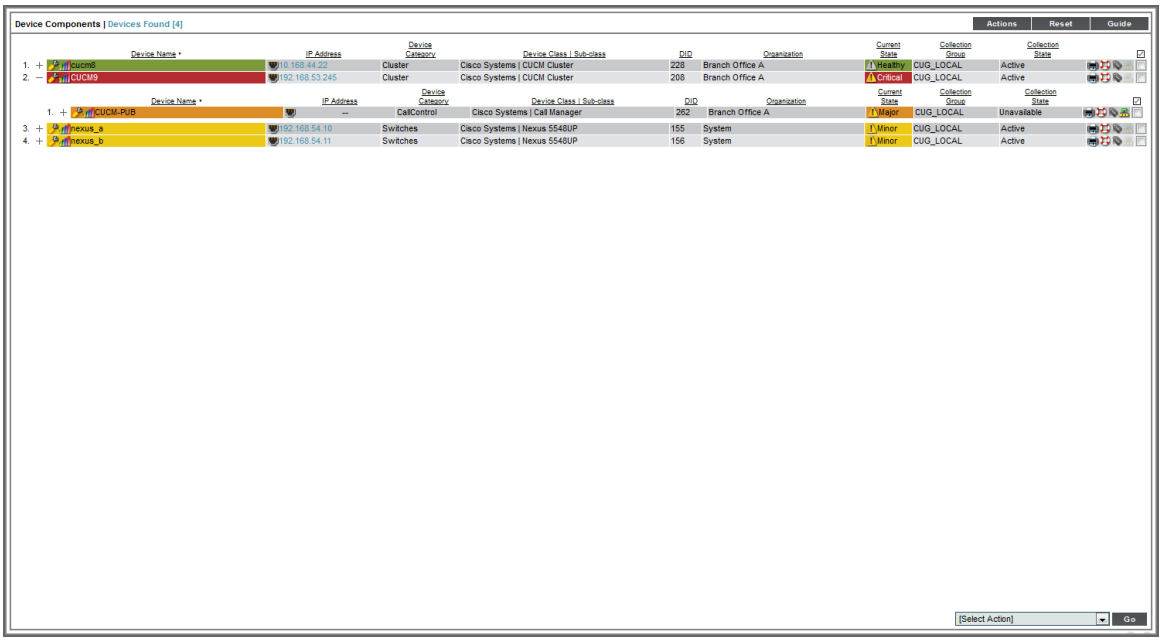


Viewing Component Devices

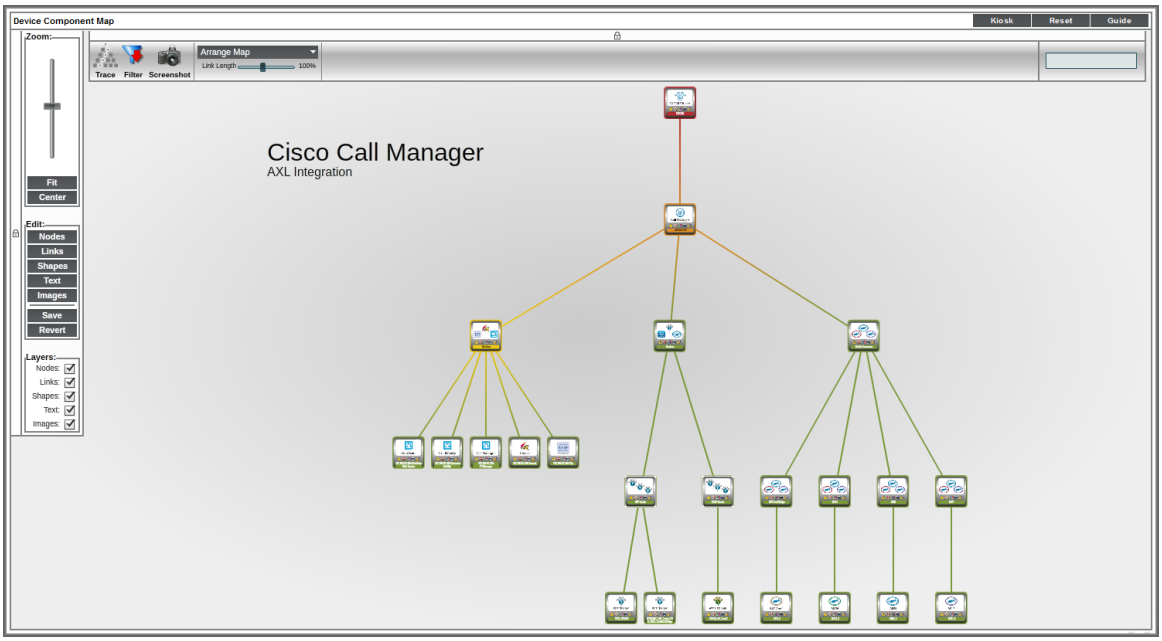
When the ScienceLogic platform performs collection for a Cisco Unified CM cluster, the platform will create component devices for the components in the Cisco Unified CM cluster and align other Dynamic Applications to those component devices. Some of the Dynamic Applications aligned to the component devices 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 (+):



- The **Component Map** page (Views > 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. The ScienceLogic platform 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 Views > 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

Cisco Unified Communications 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.

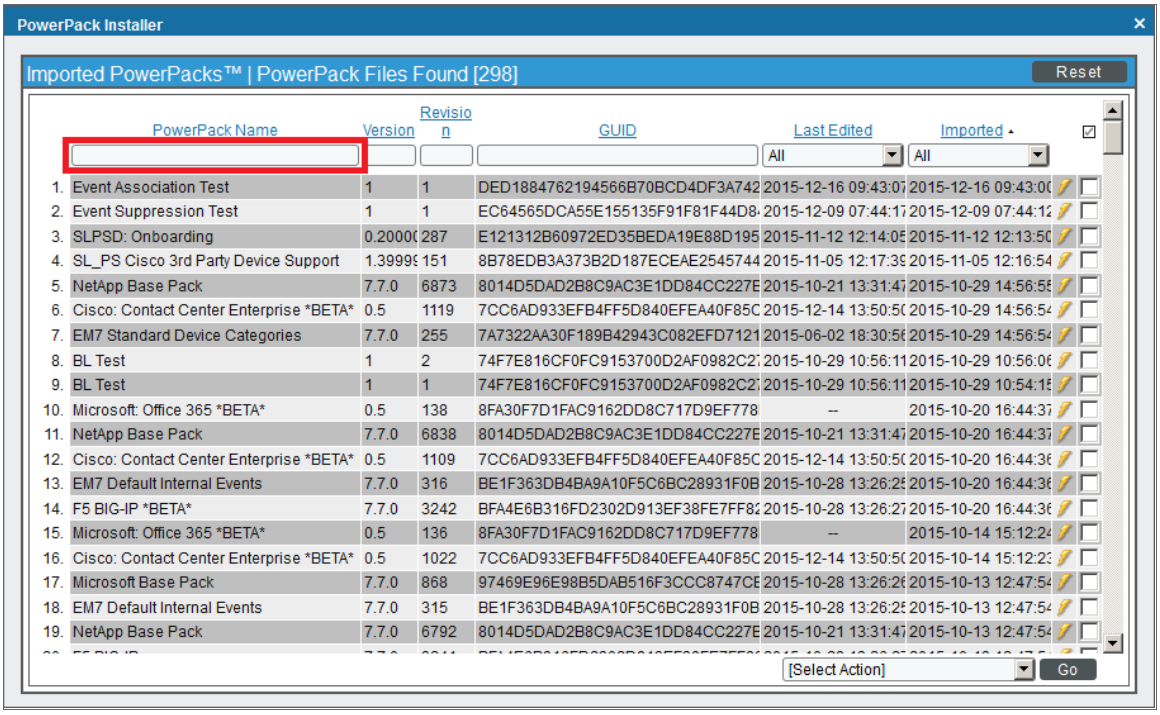
The following sections describe how to install the *Cisco: CUCM Dashboards* PowerPack and provide a description of each dashboard:

Installing the Cisco Unified CM Dashboards

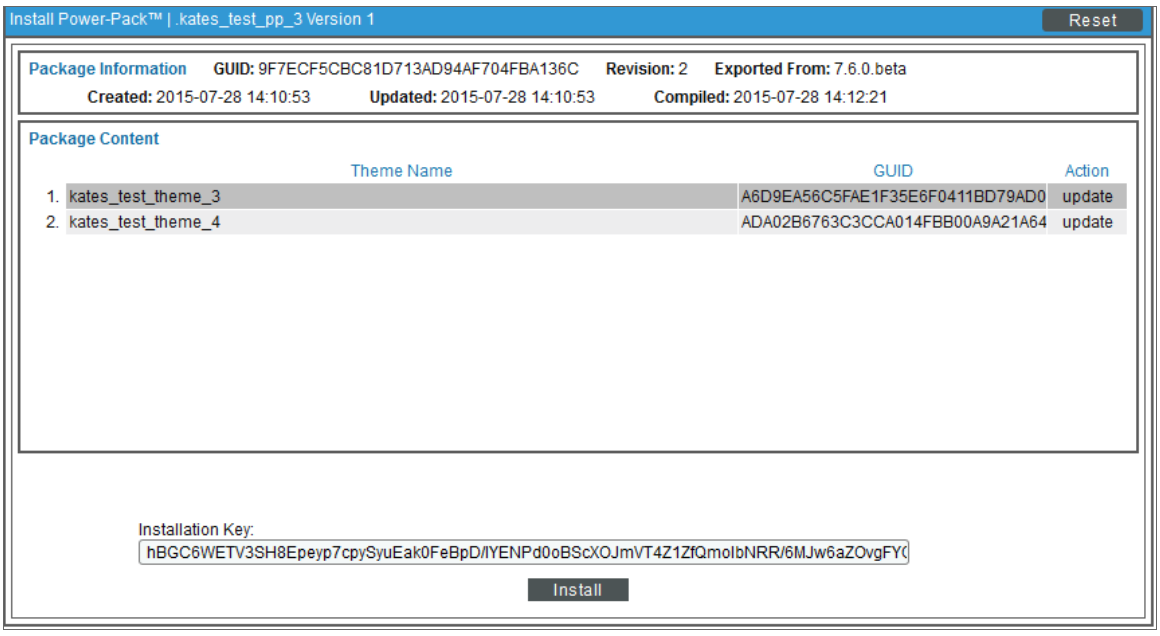
To view the Cisco Unified CM dashboards in the ScienceLogic platform, you must install the *Cisco: CUCM Dashboards* PowerPack. To do so:

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.

3. 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.



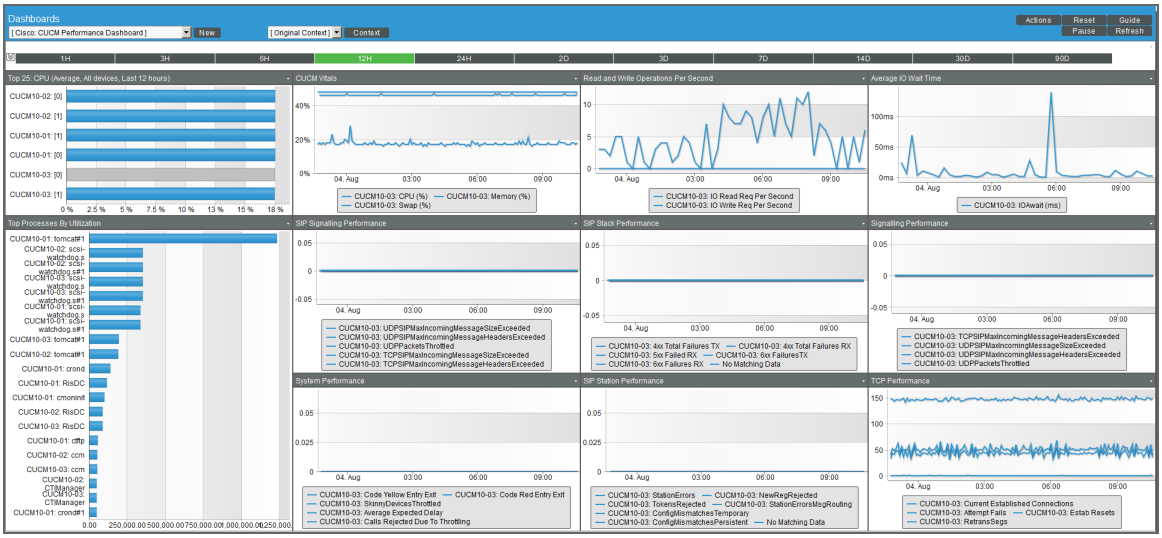
4. Click the lightning-bolt icon ( ) for the PowerPack that you want to install.
5. The **Install PowerPack** modal page appears. To install the PowerPack, click **[Install]**.



6. The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your ScienceLogic 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

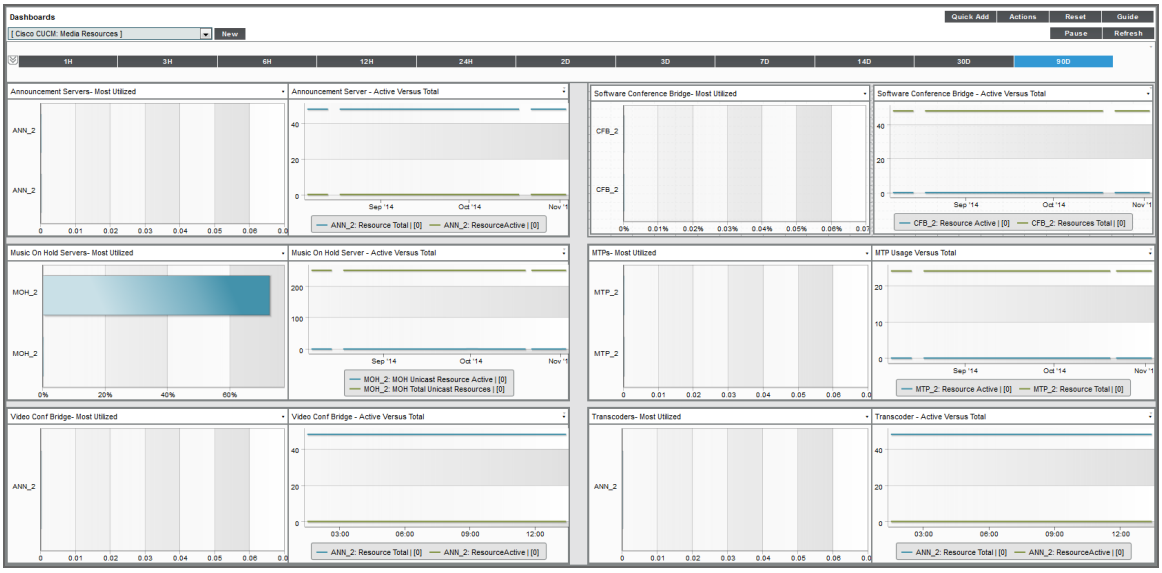
The Cisco: CUCM Locations LBM (Location Bandwidth Manager) dashboard displays eight widgets.

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.



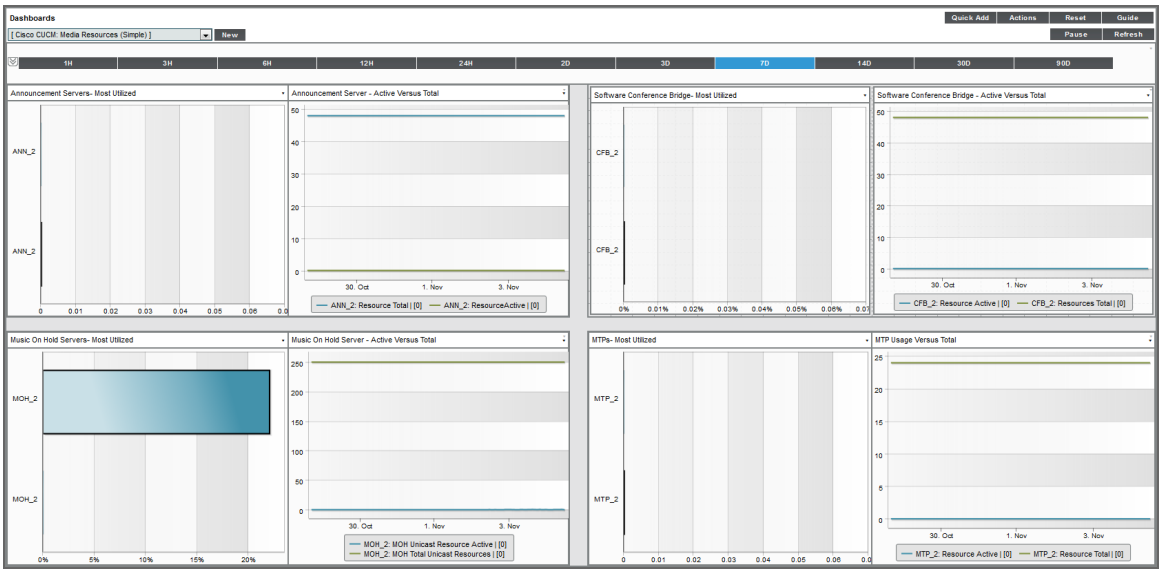
The dashboard includes the following widgets:

- ***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

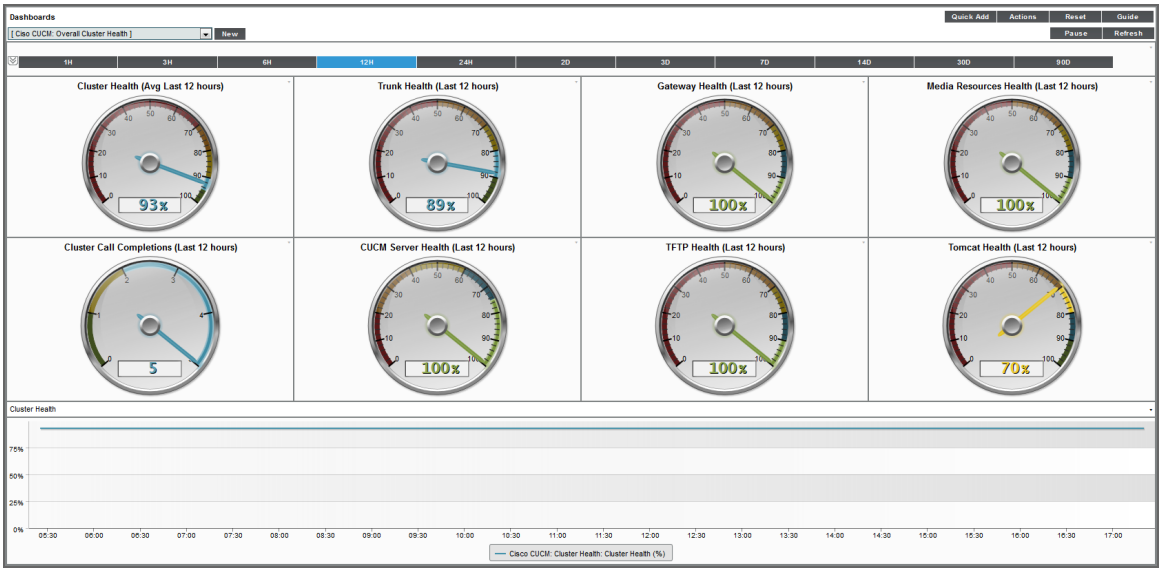
The Cisco: CUCM Tomcat dashboard displays 12 widgets that monitor servers and services that use the Tomcat Java Webserver.

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.

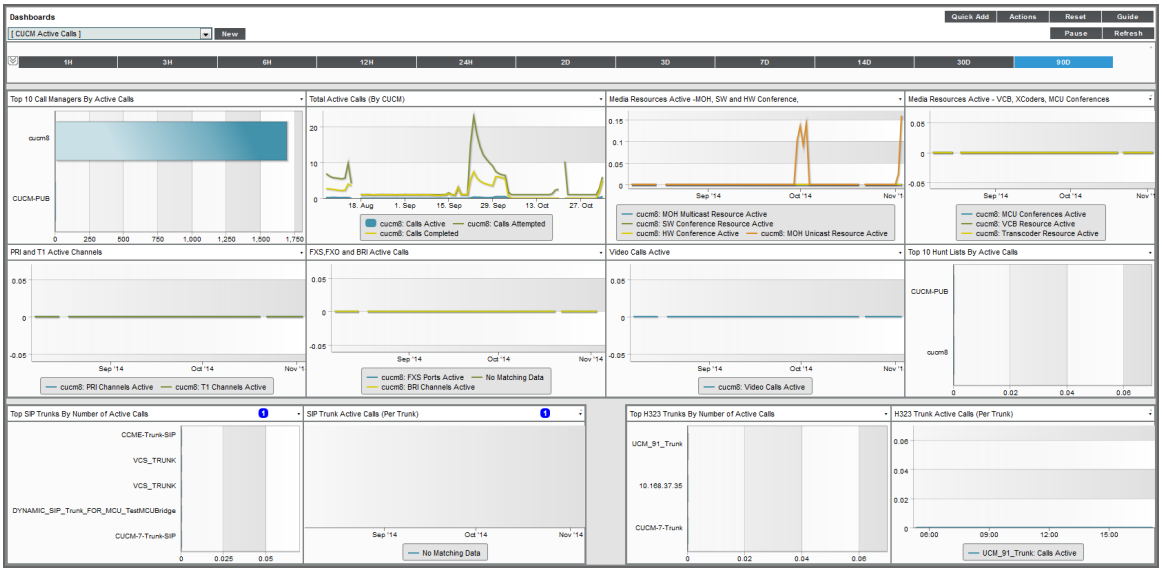


The dashboard includes the following widgets:

- 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:

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 ScienceLogicDatabase Server.
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 -1 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.)`"	The ScienceLogic platform 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 *Manually Creating Host File Entries for CUCM Nodes* 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>
```

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010