Monitoring Cisco Unified Contact Center Enterprise

Cisco: Contact Center Enterprise PowerPack version 103

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Cisco Contact Center Enterprise services in SL1 using the Dynamic Applications in the "Cisco: Contact Center Enterprise" PowerPack.

This chapter covers the following topics:

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 Contact Center Enterprise?

Cisco Unified Contact Center Enterprise software offers solutions that enable inbound and outbound contact centers to improve their business processes and productivity. These solutions include real-time chat capabilities, email and social media messaging, web collaboration, and more.

What Does the Cisco: Contact Center Enterprise PowerPack Monitor?

The "Cisco: Contact Center Enterprise" PowerPack monitors the following Unified Contact Center Enterprise services and components:

- Cisco Unified Contact Center Enterprise
- Cisco Customer Voice Portal (CVP)
- Cisco Unified Intelligence Center (CUIC)
- Cisco Finesse

To monitor these services and components using SL1, you must install the "Cisco: Contact Center Enterprise" PowerPack. This PowerPack includes:

- An example credential you can use to create universal credentials that enable you to collect data from Cisco Unified Contact Center Enterprise (UCCE) using REST API
- Dynamic Applications to discover and monitor the Unity Express voice mailboxes
- Device classes and device categories for each type of UCCE component device monitored by SL1
- Event policies and corresponding alerts that are triggered when UCCE component devices meet certain status criteria
- Device dashboards for each type of discovered device

Installing the Cisco: Contact Center Enterprise PowerPack

Before completing the steps in this manual, you must import and install the latest version of the "Cisco: Contact Center Enterprise" 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 section on *Global Settings*.

IMPORTANT: Ensure that you are running version 12.3.0 or later of SL1 before installing this PowerPack. For details on upgrading SL1, see the relevant *SL1 Platform Release Notes*.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).

3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

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

Chapter 2

Configuration and Credentials

Overview

The following sections describe how to configure Cisco Unified Contact Center Enterprise services for monitoring by SL1 using the "Cisco: Contact Center Enterprise" PowerPack:

This chapter covers the following topics:

Configuring Unified Contact Center Enterprise Monitoring Using SNMP

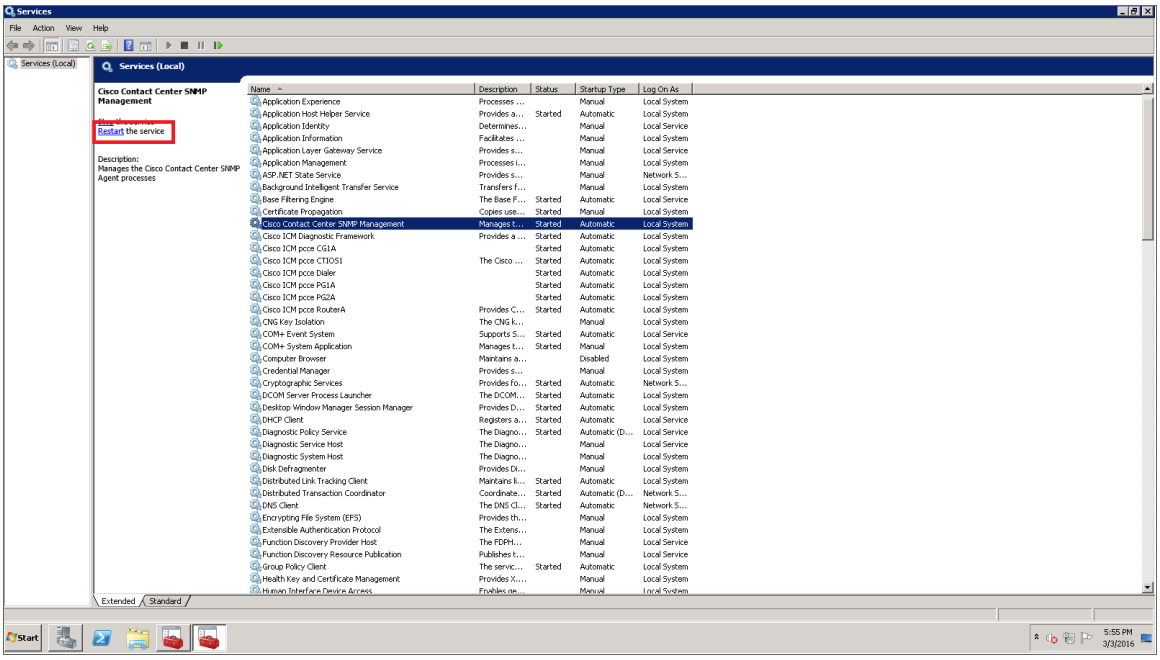
Before you can discover and monitor Cisco Unified Contact Center Enterprise (UCCE) devices in SL1, you must first configure SNMP community strings in each of the UCCE services that you will monitor with SL1. You can then create an SNMP credential in SL1 that enables it to collect data from the UCCE services. Finally, you must compile several Management Information Bases (MIBs) that are required for monitoring UCCE.

Enabling SNMP in Cisco Unified Contact Center Enterprise

To enable SNMP in Cisco Unified Contact Center Enterprise, perform the following steps:

1. Log in to the Cisco Unified Contact Center Enterprise Server as an administrator.
2. Open Microsoft Management Console (32-bit).
3. Click **[File]**, then select *Add/Remove Snap-In*. The **Add or Remove Snap-ins** page appears.
4. In the ***Available snap-ins*** field, select **Cisco SNMP Agent Management**, then click **[Add >]** to move it to the ***Selected snap-ins*** field.

5. Click **[OK]**.
6. In the left panel of the Microsoft Management Console, click **Cisco SNMP Agent Management**. Then, in the right panel, right-click **Community Names (SNMP v1, v2c)** and select *Properties*.
7. In the **Community Names (SNMP v1/v2c) Properties** modal page, click the **[Add New Community]** button to enable the fields on the page.
8. Make entries in the following fields:
    - ***Community Name***. Enter a name for the new community string.
    - ***SNMP Version***. Select *SNMP v2c*.
    - ***Access Rights***. Select *Read Only*.
9. Click **[Save]**, and then click **[OK]**.
10. Close the Microsoft Management Console.
11. Open the Microsoft Windows Services console.
12. In the Microsoft Windows Services console, select **Cisco Contact Center SNMP Management** from the list of local services, then click the **Restart** hyperlink to restart the service.

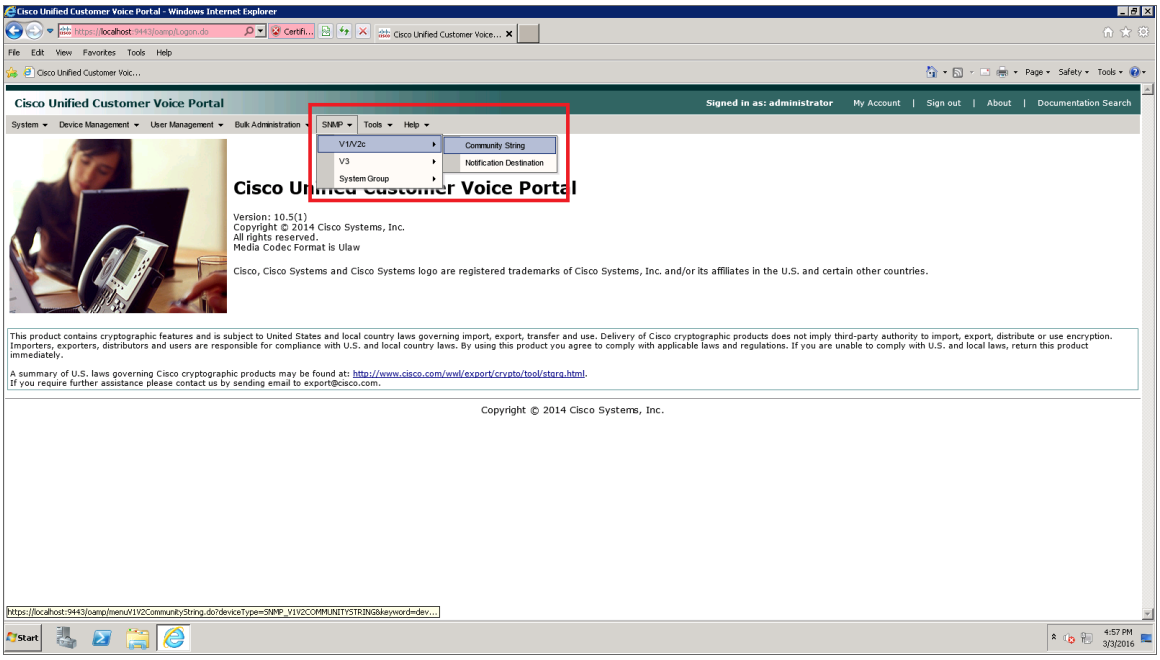


13. Close the Microsoft Windows Services console.
14. Click the Windows **[Start]** menu, then go to Control Panel > System and Security > Windows Firewall.
15. In the left panel, click the **Turn Windows Firewall on or off** hyperlink. The **Customize Settings** page appears.
16. Under **Domain network location settings**, select *Turn off Windows Firewall*, then click **[OK]**.
17. To enable SNMP in Cisco Unified Contact Center Enterprise Data Server, log in to Cisco Unified Contact Center Enterprise Data Server as an administrator and repeat steps 2-16.

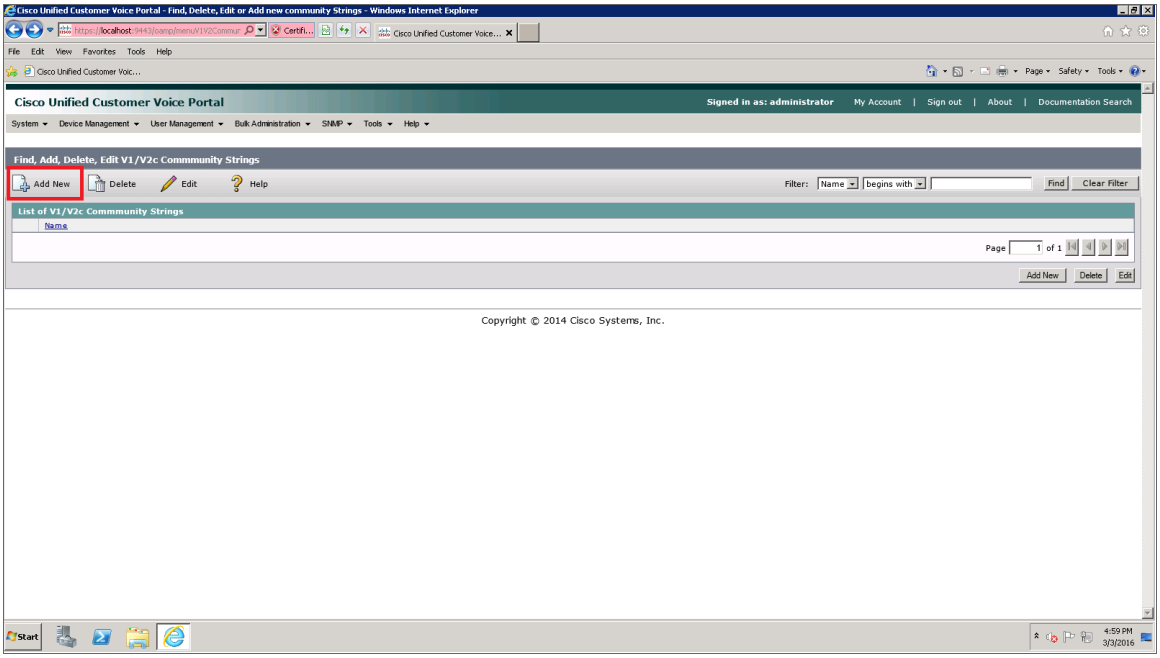
Enabling SNMP in Cisco Unified Customer Voice Portal (CVP)

To enable SNMP in Cisco Unified Customer Voice Portal, perform the following steps:

1. Log in to Cisco Unified Customer Voice Portal as an administrator.
2. Click the **[SNMP]** tab, then select *V1/V2c* > *Community String*.



3. On the **Find, Add, Delete, Edit V1/V2c Community Strings** page, click the **[Add New]** button.



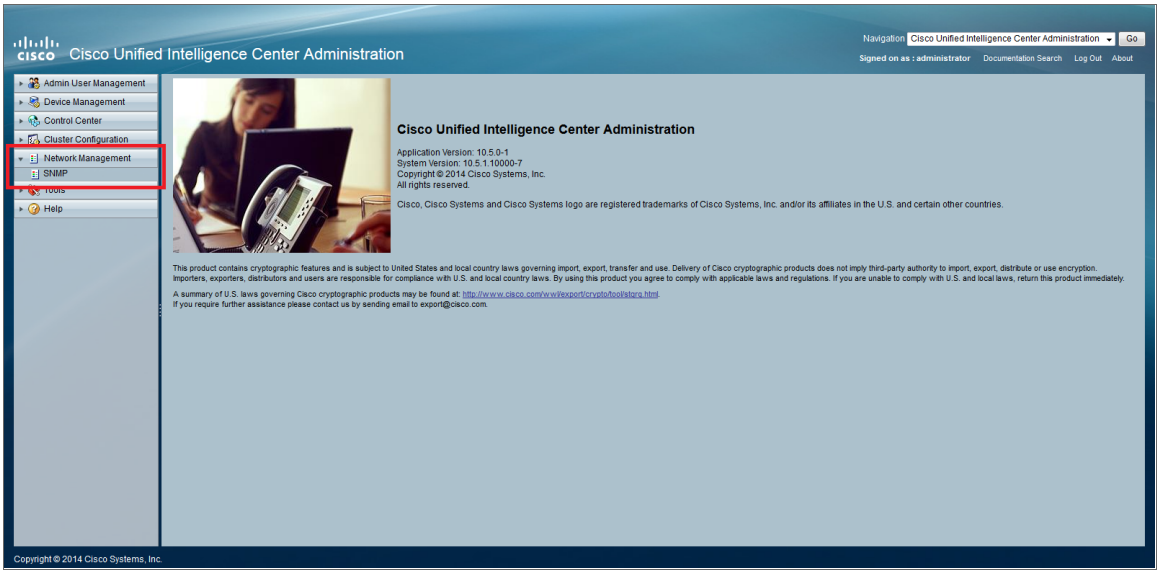
4. The **V1/V2c SNMP Community String Configuration** page appears. Make entries in the following fields:
   - ***Community String Name***. Enter a name for the new community string.
   - ***SNMP Version Information***. Select *V2C*.
   - For the other fields on the page, use the default values.
5. Click the **[Devices]** tab.
6. Select one or more of the devices in the ***Available*** field, then click the right-arrow icon to move the selected device(s) to the ***Selected*** field.
7. Click the **[Save & Deploy]** button. A message confirms that the configuration of the SNMP community string was successfully applied to the selected device(s).

Enabling SNMP in Cisco Unified Intelligence Center (CUIC)

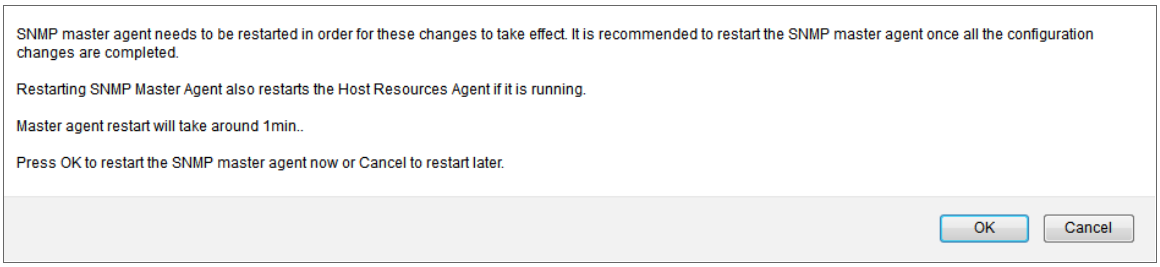
To enable SNMP in Cisco Unified Intelligence Center, perform the following steps:

1. Log in to Cisco Unified Intelligence Center as an administrator.

2. In the left panel, click **[Network Management]**, then select *SNMP*.



3. On the **SNMP Community String Configuration** page, under **Search Options**, click **[Find]**. The **Search Results** section appears.
4. Under **Search Results**, click **[Add New]**.
5. Enter values in the following fields:
    - ***Community String Name***. Enter a name for the new community string.
    - ***Access Privileges***. Select *ReadOnly*.
    - For the other fields on the page, use the default values.
6. Click **[Save]**.
7. Click **[OK]** to restart the SNMP master agent.

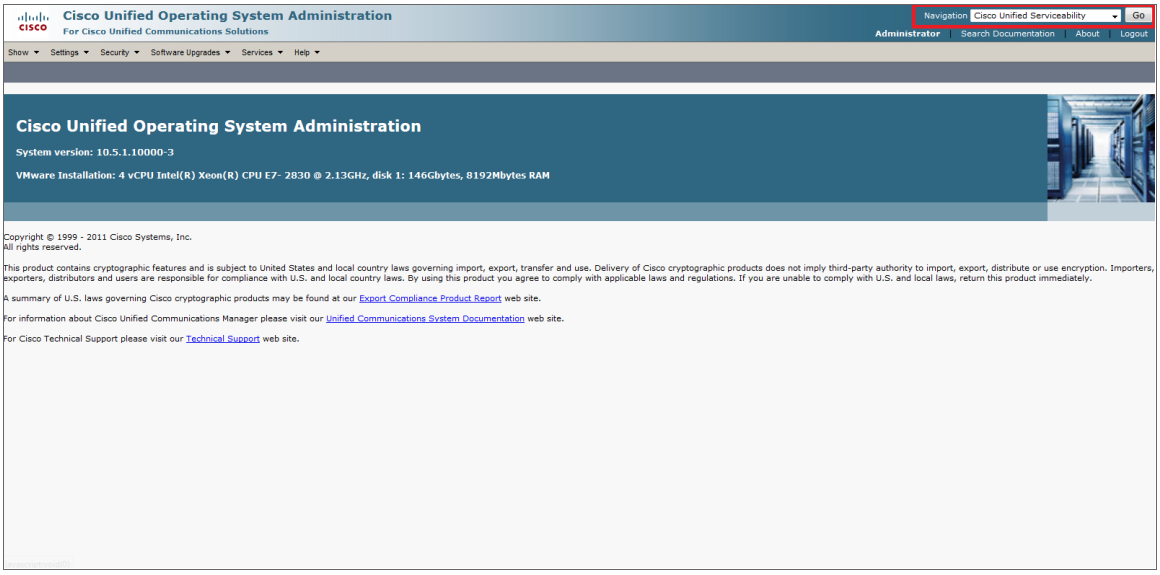


Enabling SNMP in Cisco Finesse Server

To enable SNMP in Cisco Finesse Server, perform the following steps:

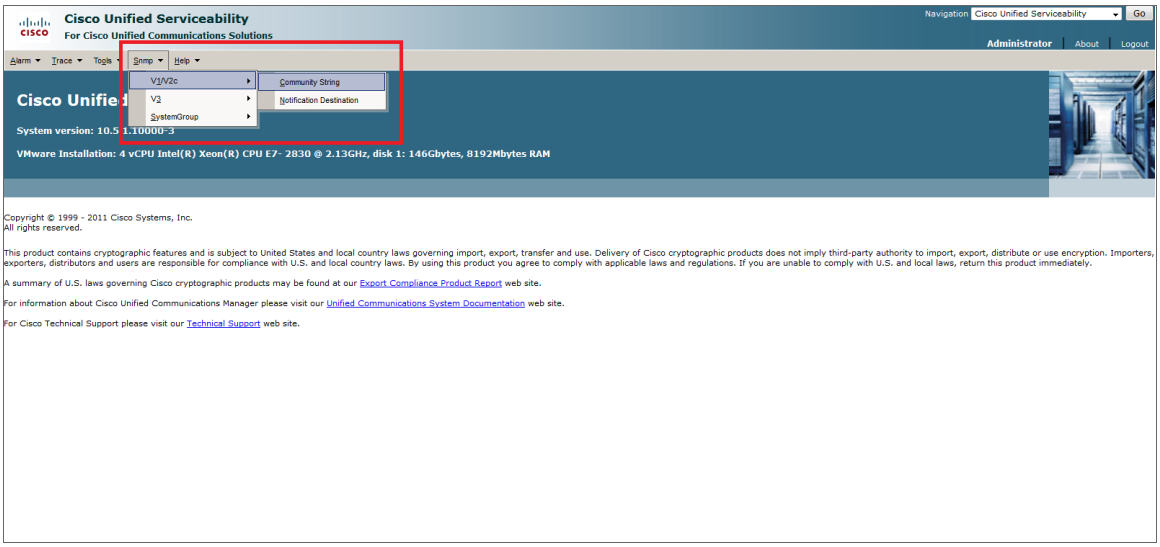
1. Log in to Cisco Unified Operating System Administration as an administrator.

2. In the top-right corner of the page, in the ***Navigation*** field, select *Cisco Unified Serviceability* and then click **[Go]**.



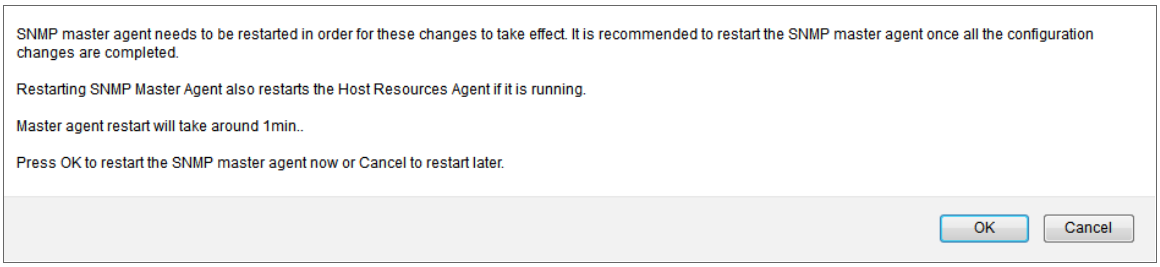
NOTE: You might be required to enter your login credentials again before proceeding.

3. Click the **[SNMP]** tab, then select *V1/V2c* > *Community String*.



4. On the **SNMP Community String Configuration** page, under **Search Options**, click **[Find]**. The **Search Results** section appears.
5. Under **Search Results**, click **[Add New]**.

6. Enter values in the following fields:
    - ***Community String Name***. Enter a name for the new community string.
    - ***Access Privileges***. Select *ReadOnly*.
    - For the other fields on the page, use the default values.
7. Click **[Save]**.
8. Click **[OK]** to restart the SNMP master agent.



Creating an SNMP Credential for Unified Contact Center Enterprise

To configure SL1 to monitor Cisco Unified Contact Center Enterprise (UCCE), you must create an SNMP credential. This credential allows the Dynamic Applications in the "Cisco: Contact Center Enterprise" PowerPack to communicate with your UCCE account.

To configure an SNMP credential for UCCE:

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

Compiling SNMP MIBs for Unified Contact Center Enterprise

You must manually compile some of the Management Information Base (MIB) files that are required for monitoring Cisco Unified Contact Center Enterprise in SL1. To compile these MIBs, perform the following steps:

1. Go to the **MIB Compiler** page (System > Tools > MIB Compiler).
2. Locate the CISCO-CONTACT-CENTER-APPS-MIB and then click its lightning bolt icon ( ).
3. Repeat step 2 for the CISCO-CUICAPPS-MIB and the CISCO-CVP-MIB.

NOTE: The MIB Compiler page displays "Yes" in the Compiled column for the MIBs before these steps are completed. However, you must still compile the MIBs manually using the lightning bolt icon ( ).

If the message "MIB File Missing" appears when you click the lightning bolt icon ( ), you must download and import the MIB(s) before compiling them. To do so:

1. Download the MIB(s) you need:
    - CISCO-CONTACT-CENTER-APPS-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CONTACT-CENTER-APPS-MIB.my
    - CISCO-CUICAPPS-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CUICAPPS-MIB.my
    - CISCO-CVP-MIB: ftp://ftp.cisco.com/pub/mibs/v2/CISCO-CVP-MIB.my
2. Go to the **MIB Compiler** page (System > Tools > MIB Compiler).
3. Click the **[Import]** button.
4. Click the **[Browse]** button to locate the downloaded MIB. Select the MIB, and then click the **[Import]** button.
5. Click **[OK]** to confirm.
6. On the **MIB Compiler** page, locate the imported MIB and click its lightning bolt icon ( ) to compile it.
7. If you downloaded more than one MIB, repeat steps 2-6 for the additional MIB(s) that need to be imported and compiled.

Configuring Unified Contact Center Enterprise Monitoring Using REST API

Some Dynamic Applications in the "Cisco: Contact Center Enterprise" PowerPack collect data from Cisco Unified Contact Center Enterprise (UCCE) using the UCCE REST API. The following Dynamic Applications require a Cisco Unified Contact Center Enterpreise universal credential to enable SL1 to communicate with your UCCE account:

- Cisco: CCE Administration and Data Server Enhanced Performance
- Cisco: CCE Call Router Enhanced Performance
- Cisco: CCE Campaign Manager Enhanced Performance
- Cisco: CCE CTI Gateway Enhanced Performance
- Cisco: CCE CTI Object Server Enhanced Performance
- Cisco: CCE Dialer Enhanced Performance
- Cisco: CCE Enhanced Performance Caching
- Cisco: CCE ICM Distributor Enhanced Performance
- Cisco: CCE Logger Enhanced Performance
- Cisco: CCE PG OPC Enhanced Performance

- Cisco: CCE PG PIM Enhanced Performance
- Cisco: CCE PG VRU PIM Enhanced Performance

To use these Dynamic Applications, you will need credentials for a UCCE user with either a local account in the Windows security group "ICMDiagnosticFrameworkUsers" or a domain user in the "CONFIG" domain security group of the UCCE instance.

An example universal credential that you can edit for your own use is included in the "Cisco: Contact Center Enterprise" PowerPack. To create a universal credential to monitor UCCE:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select *Cisco: cce Credential*. The **Create Credential** modal page appears.
3. Supply values in the following fields:
    - ***Name***. Type a name for your credential.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
    - ***Timeout (ms)***. Keep the default value of 1500.
    - ***Authentication type***. Keep the default value (Basic Authentication).
    - ***Username***. Type the Cisco: Contact Center Enterprise account username.
    - ***Password***. Type the Cisco: Contact Center Enterprise account password.
    - ***URL***. Type the URL and port for the Cisco: Contact Center Enterprise system, using the following format: *https://Host:Port/Path*.

    Proxy Settings

    Toggle on this field if you are using a proxy server to communicate with your Cisco: Contact Center Enterprise account, enter the values in the fields listed below:

    - ***Proxy scheme type***. Select *http* or *https* from the drop-down field.
    - ***Proxy Hostname/IP***. Enter the hostname or the IP address associated with your device.
    - ***Proxy Port***. Enter the port number for the proxy server.
    - ***Proxy User***. Enter the username for the proxy server.
    - ***Proxy Password***. Enter the password for the proxy server.
4. Click **[Save & Close]**.

Chapter 3

Discovery

Overview

The following sections describe how to discover Cisco Unified Contact Center Enterprise devices for monitoring by SL1 using the "Cisco: Contact Center Enterprise" PowerPack:

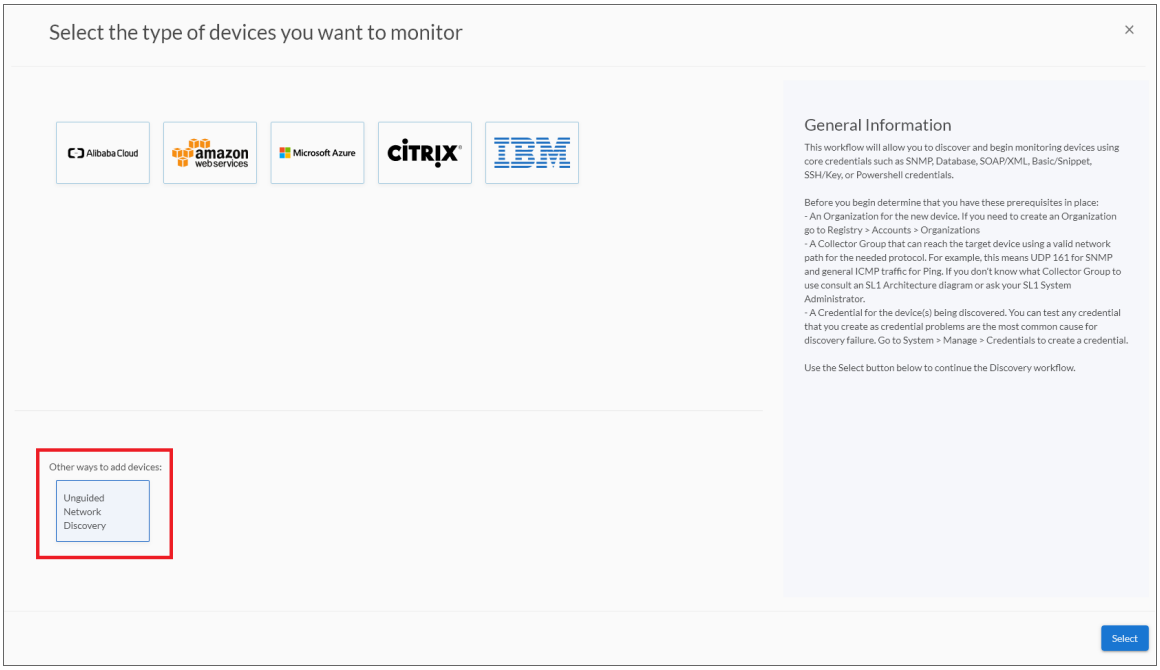
This chapter covers the following topics:

Discovering Component Devices in Cisco Unified Contact Center Enterprise

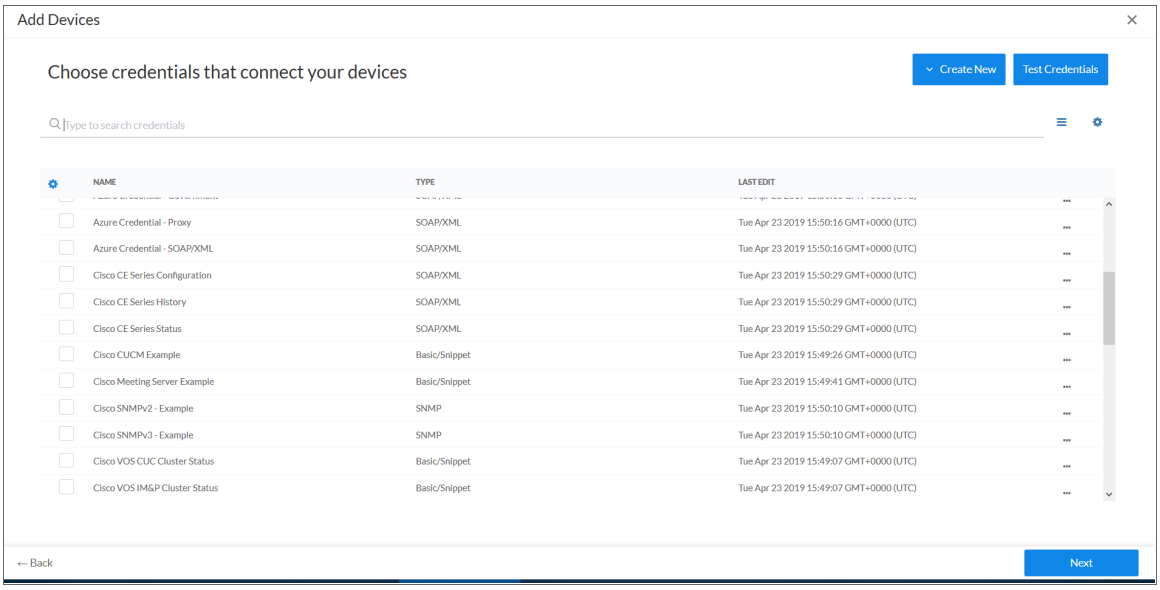
When you discover your Cisco Unified Contact Center Enterprise (UCCE) instance with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor UCCE, Customer Voice Portal (CVP), Cisco Unified Intelligence Center (CUIC), and/or Finesse services, and all the associated component devices.

To discover your UCCE instance, perform the following steps:

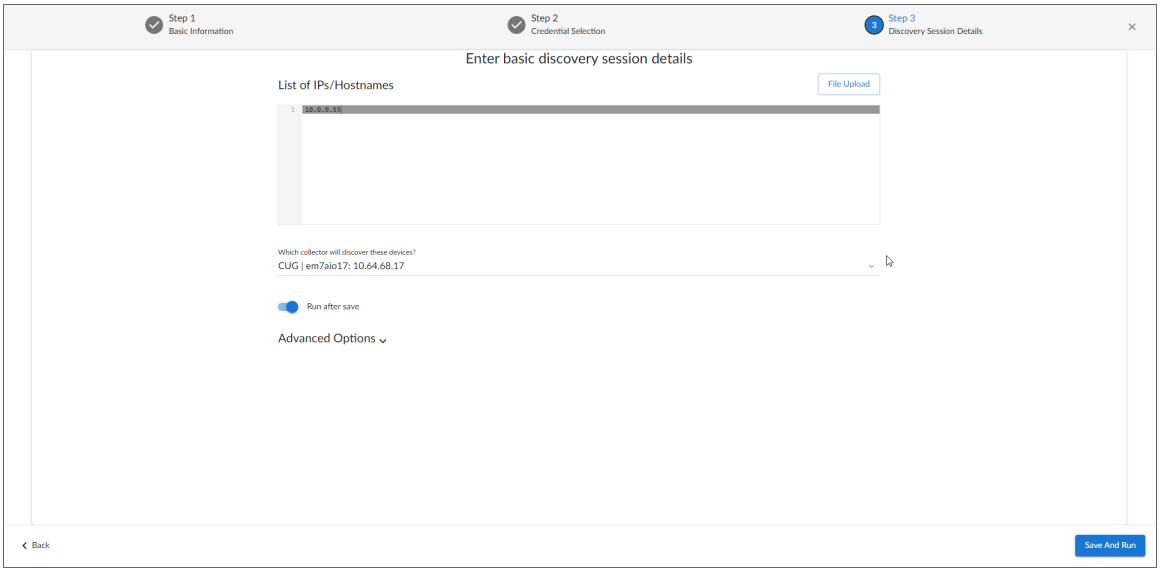
1. On the **Devices** page ( ) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



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, locate and select:
    - The *SNMP credential you created*.
    - The *universal credential you created*.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



8. Complete the following fields:
    - ***List of IPs/Hostnames***. Enter the IP address(es) or the range of IP addresses for the UCCE, CVP, CUIC, and/or Finesse services you want to discover.
    - ***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.

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

Discovering Component Devices in Cisco Unified Contact Center Enterprise in the SL1 Classic User Interface

When you discover your Cisco Unified Contact Center Enterprise (UCCE) instance with SL1, SL1 auto-aligns a series of Dynamic Applications to discover, configure, and monitor UCCE, Customer Voice Portal (CVP), Cisco Unified Intelligence Center (CUIC), and/or Finesse services, and all the associated component devices.

To discover your UCCE instance, perform the following steps:

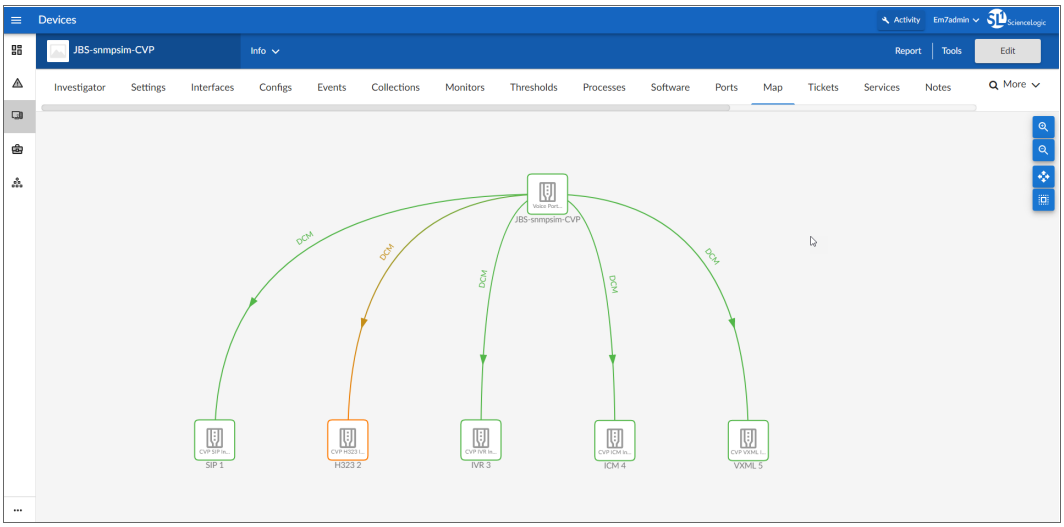
1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery or System > Manage > Discovery in the classic user interface).
2. Click the **[Create]** button. The **Discovery Session Editor** page appears.
3. Supply values in the following fields:
   - ***IP Address/Hostname Discovery List***. Enter the IP address(es) or the range of IP addresses for the UCCE, CVP, CUIC, and/or Finesse services you want to discover.
   - ***SNMP Credentials***. Select the *SNMP credential you created*.
   - ***Other Credentials***. Select the *universal credential you created*.
4. Optionally, supply values in the other fields in this page. For a description of the fields in this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button.
6. The **Discovery Control Panel** page refreshes. Click the lightning bolt icon (⚡) for the discovery session you created.
7. In the pop-up window that appears, click the **[OK]** button. The **Discovery Session** page displays the progress of the discovery session.

Viewing Cisco Unified Contact Center Enterprise Component Devices

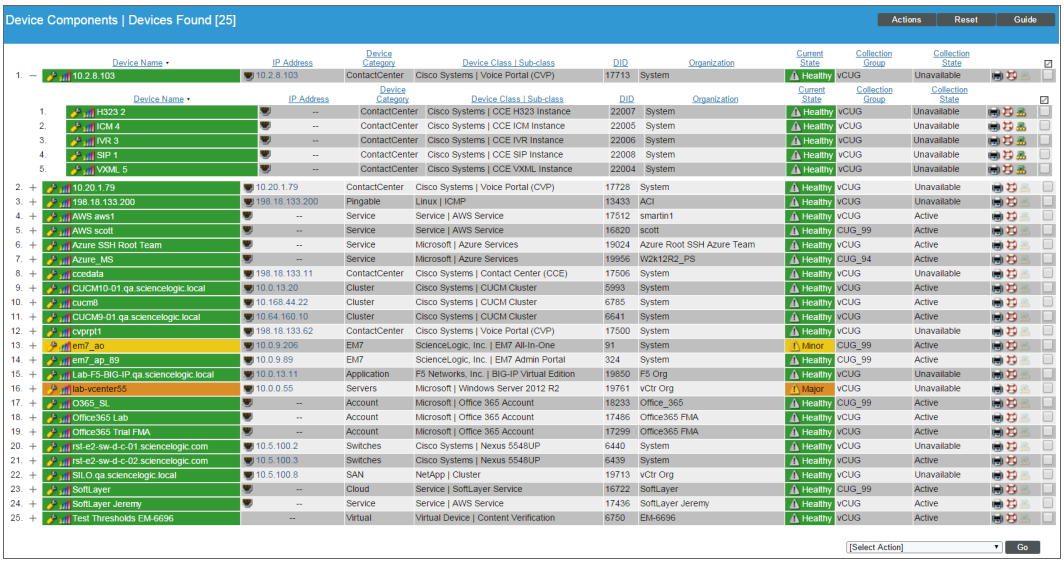
When SL1 discovers your Cisco Unified Contact Center Enterprise (UCCE), Customer Voice Portal (CVP), Cisco Unified Intelligence Center (CUIC), or Finesse services, SL1 creates component devices that represent each component in those services.

You can view all associated component devices in the following places in the user interface:

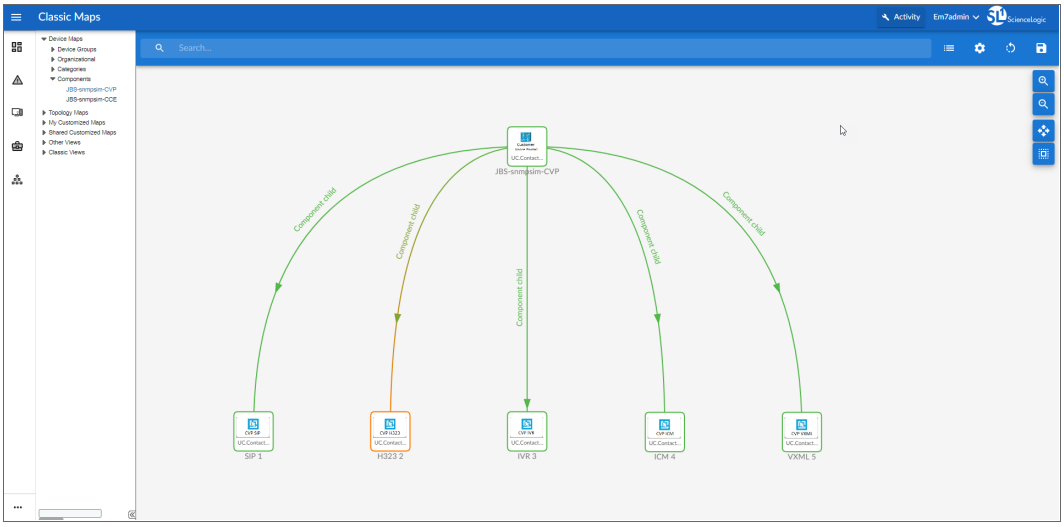
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device:



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



- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This view makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for your UCCE, CVP, CUIC, or Finesse service, 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.



Chapter 4

Dashboards

Overview

The following sections describe the device dashboards that are included in the "Cisco: Contact Center Enterprise" PowerPack.

This chapter covers the following topics:

Device Dashboards

The "Cisco: Contact Center Enterprise" PowerPack includes device dashboards that provide summary information for Contact Center Enterprise component devices. The following device dashboards in the "Cisco: Contact Center Enterprise" PowerPack are aligned as the default device dashboard for the equivalent device class.

Cisco: CCE Admin and Data Server

The ***Cisco: CCE Admin and Data Server*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Four instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - DB Write Average Time
    - DB Write Records Processed

- Queue Depth
- Write Average Time

Cisco: CCE Call Router

The ***Cisco: CCE Call Router*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Number of Logged In Agents
  - Router Calls Per Sec
  - Calls In Router and Calls In Queue
  - Router Calls In Progress
  - Pending PQA Agent Count
  - Peripheral Gateway and NIC Counts
  - Pending PQ Count

Cisco: CCE Campaign

The ***Cisco: CCE Campaign*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Five instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Active Dialers
  - Average Queue Time
  - Queue Depth
  - Database Utilization
  - Do Not Call Number Count

Cisco: CCE CTI Gateway

The ***Cisco: CCE CTI Gateway*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Four instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Talking Agents
    - Ready Agent Count and Logged In Agent Count
    - Session Counts - Open and Total Sessions
    - Session Counts - Failed, Closed and Unknown Sessions

Cisco: CCE CTI Object Server

The ***Cisco: CCE CTI Object Server*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Active Clients and Call Count
    - Active Monitors
    - Configured Agents
    - Client and CTI Message Rate
    - Configured Teams and Skill Group
    - Queue Sizes
    - Transfer Count and Call Failed Count

Cisco: CCE Dialer

The ***Cisco: CCE Dialer*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device

- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Ports Used and Ports Blocked
    - Port Counts
    - Call Attempts
    - Agents Talking
    - Ports Actively Dialing
    - Call Counts
    - Queue Depth

Cisco: CCE Logger

The ***Cisco: CCE Logger*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Three instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Average DB Write Time
    - Number of Database Records Written/Second
    - Number of Database Records Processed

Cisco: CCE Peripheral Gateway

The ***Cisco: CCE Peripheral Gateway*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Agent Counts
    - Call Counters
    - PIM Count

- Communications Manager PIM Counts (Agent and Call Counts)
- Communications Manager PIM Counts (Messages/sec and Calls/Second)
- VRU PIM - Calls at VRU and VRU TCP Connection Resets
- VRU PIM - New Calls/Second and Pre-Routed Calls/Second

Cisco: CUIC

The ***Cisco: CUIC*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Vitals
  - Database Performance
  - Security Performance - Users
  - Reporting Engine Performance - Real Time Reports
  - Security Performance - Login Failed Attempts
  - Reporting Engine Performance - Historical Reports
  - Scheduler Performance

Cisco: CVP H323

The ***Cisco: CVP H323*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Vitals
  - H323 CPU Usage
  - H323 Memory Usage
  - H323 Call Arrival Rate and Call Transfer Rate
  - Prompts Not Found and Critical Media

- H323 Call Transfers and Redirects
- Average New Call Latency

Cisco: CVP ICM

The ***Cisco: CVP ICM*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Six instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Active Calls
  - Total Calls
  - Video Calls
  - Active ICM Lookup Requests
  - SIP and H323 Call Legs
  - Active VRU Call Legs

Cisco: CVP IVR

The ***Cisco: CVP IVR*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
  - Active Calls
  - New Call Requests and HTTP Requests
  - Agent VCR Control Invocations
  - HTTP Requests
  - Agent Initiated Recording
  - Max Full Video Calls
  - Agent Pushed Video

Cisco: CVP Reporting

The ***Cisco: CVP Reporting*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Four instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Database Writes
    - VXML Events
    - IVR Events
    - SIP Events

Cisco: CVP SIP

The ***Cisco: CVP SIP*** device dashboard displays the following information:

- The basic information about the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Seven instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Active Calls
    - Total Calls
    - Total Call Legs
    - Video Calls
    - Average Latency
    - Failed Transfer Calls - Pre Dialog Calls
    - Failed Transfer Calls - Post Dialog Calls

Cisco: CVP VXML

The ***Cisco: CVP VXM***L device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device

- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Six instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Sessions
    - Reported Events
    - ICM Look Up Requests
    - ICM Look Up Responses
    - ICM Look Up Success
    - ICM Look Up Fails

Host Resource and IF MIBS+Topology

The ***Host Resource and IF MIBS*** device dashboard displays the following information:

- The basic information about the device
- The current health, availability, and latency for the device
- A list of active events and open tickets associated with the device
- A count of, and links to, the elements associated with the device
- Two instances of the Multi-series Performance Widget that display the following metrics trended over the last 12 hours:
    - Vitals
    - Storage Utilization
- Two additional widgets that display the following information:
    - Top 10 Interfaces by Bit Rate (Average Last Hour)

Copyrights and Trademarks

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

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

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

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

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

Other

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

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

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

International: +1-703-354-1010