Cisco Unified Customer Voice Portal

Unified CVP

Unified CVP provides Voice over IP (VoIP) routing services for the Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) product. Unified ICME provides the services necessary to determine where calls should be routed, whether to ACDs, specific agents, or to VRUs, but the routing services themselves must be provided by an external routing client.

Traditionally, ICM routing clients were various Public Switch Telephone Network (PSTN) network switches, or customer-provided ACDs. Unified CVP makes it possible for Unified ICME to use VoIP gateways as routing clients as well. This functionality carries a number of advantages, not the least of which is that call traffic can be handled over the IP network rather than by the PSTN carrier, which reduces costs and provides greater network bandwidth.

Unified CVP supports all the features of existing PSTNs and adds additional features. For example, Unified CVP provides a Voice Response Unit (VRU) platform, which includes the ability to prompt for and collect basic data from the caller before delivering the call. Unified CVP enhances this traditional PSTN feature with the use of its own VXML Interactive Voice Response (IVR) application platform. Also, Unified CVP can

park calls by providing voice prompts or hold music to callers who are waiting in queue for an agent in Unified ICME.

A typical deployment of the Unified CVP solution requires operating, administering, managing, and provisioning multiple servers and IOS components. The Operations Console is a web-based console that enables users to centrally operate, administer, maintain, and provision the Unified CVP solution.

Note This release supports only TLS 1.2. For more information, see *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.

Key Features and Benefits

Unified CVP is a web-based platform that provides carrier-class Interactive Voice Response (IVR) and Internet Protocol (IP) switching services over Voice Over IP (VoIP) networks.

Unified CVP includes these features:

- IP-based services:
  - **Switching** - Unified CVP can transfer calls over an IP network.
  - **Takeback** - Unified CVP can take back a transferred call for further IVR treatment or transfer.
  - **IVR Services** - The classic prompt-and-collect functions: "Press 1 for Sales, 2 for Service," for example.
  - **Queuing** - Calls can be "parked" on Unified CVP for prompting or music on hold, while waiting for a call center agent to be available.
  - **Voice Enabled IVR Services** - Unified CVP provides for sophisticated self-service applications, such as banking, brokerage, or airline reservations.
- **Compatibility with Other Cisco Call Routing and VoIP Products** - Specifically, Cisco Unified Intelligent Contact Management Hosted (Unified ICMH) or Unified ICME, Cisco Gateways, and Cisco IP Contact Center (IPCC).
- **Compatibility with Cisco Unified Communications Manager (Unified CM)** - Unified CM manages and switches VoIP calls among IP phones. When combined with Unified ICME, Unified CM becomes the IPCC product.
- **Compatibility with the PSTN** - Calls can be moved onto an IP-based network for Unified CVP treatment and then moved back out to a PSTN for further call routing to a call center.
- **Carrier-Class Platform** - Unified CVP is a reliable, redundant, and scalable platform, which allows it to work with service provider and large enterprise networks.
- **Reporting** - Unified CVP stores detailed call records in a reporting database using a well-documented schema. You can design and run custom reports using the ODBC-compliant reporting tool of your choice.
- **Operations Console** - A web-based console from which you can centrally operate, administer, maintain, and provision the Unified CVP solution.
- **Call Routing Support** - Unified CVP provides call routing services for SIP (RFC 3261).

- **VXML Services** - Unified CVP provides a platform for developing powerful, speech-driven interactive applications accessible from any phone.

  The VXML platform includes:

  - The Cisco Unified CVP VXML Server, a J2EE- and J2SE-compliant application server that dynamically drives the caller experience.
  - The Cisco Unified Call Studio, a drag-and-drop graphical user interface (GUI) for the rapid creation of advanced voice applications.

Accept Security Certificates

Ensure that the pop-ups are enabled for Operations Console.

After you enter Operations Console URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open Operations Console sign in page. Operations Console sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Note To remove the certificate error from the desktop, you must close and reopen your browser.

Firefox

1. On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

   Note Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On Operations Console sign in page, enter your username and password, and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open Operations Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Note If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certif** **Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to perma accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (not valid)**.

   The **Certificate** dialog box appears.

6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Operations Console. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open Operations Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.

3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter Operations Console URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

Operations Console (OAMP)

The Operations Console is a web-based interface from which you can configure the Unified CVP components in the Unified CVP solution. You can monitor and manage the following Unified CVP components directly from the Operations Console:

- Unified CVP Call Server
- Unified CVP Reporting Server
- Unified CVP VXML Server
- Unified CVP VXML Server (standalone)

The Operations Console manages component configurations. It also provides the ability to distribute Call Studio applications to Unified CVP VXML Servers, perform Reporting DB administration. Finally, the

Operations Console provides basic visual indications as to which managed components are functioning properly and which are having problems.

Use the buttons and menus in the Operations Console to navigate through the web pages. The browser buttons are not supported.

Note Do not use the Back button in your browser to navigate back to the pages that you have visited previously.

The Operations Console provides access to the following operations:

- **Health Monitoring** - You can use any SNMP-standard monitoring tool to get a detailed visual and tabular representation of the health of the solution network. All Unified CVP product components and most Unified CVP solution components also issue SNMP traps and statistics which can be delivered to any standard SNMP management station or monitoring tool.
- **Direct administration of individual IOS-based components** - Administrators can select an individual gateway for direct administration using secure shell (ssh). Configurations which are modified in this way, or which are modified by directly accessing those components without using the Operations Server, can be uploaded to the Operations Server backup for later use.

You can perform the following tasks to get started with the Operations Console:

Log in to Operations Console (OAMP)

To log in to the Operations Console, perform the following procedure.

Before You Begin

If this is the first time you are logging in to the Operations Console after installing the Unified CVP software, you will need the password for the default Administrator account that was created during installation.

The inactivity session timeout for the Operations Console (when no activity is performed in the browser) is set to 60 minutes. If the browser is inactive for more than 60 minutes, you are required to login again.

Procedure

To log in to the Operations Console:

Procedure

Step 1 From the web browser, enter https://*ServerIP*:9443/oamp, where ServerIP is the IP address or hostname of the machine on which the Operations Console is installed.

The main Unified CVP window opens.

Step 2 Enter your user ID in the Username field.

The first time you log in after installing the Unified CVP software, enter **`Administrator`**, the default user account.

Step 3 In the Password field, enter your password.

If you are logging in to the default Administrator account, enter the password that was set for this account during installation.

If the user ID or password is invalid, the Operations server displays the message, "Invalid Username or password." Enter your user ID and password again and click **OK**.

The main Cisco Unified Customer Voice Portal window opens.

Step 4 Default security settings can prevent users from using the Operations Console. Check your security policy and, if needed, change the settings to a less restrictive level.

Related Topics

Log out of Operations Console (OAMP), on page 15

My Account Screen

The My Account screen displays the settings for the account of the user who is currently logged in.

You can view the device pools and user groups to which you are assigned.

Related Topics

User Information, on page 8
User Group Assignment, on page 9
Device Pool Selection, on page 9

User Information

Table 1: User Information Configuration Settings

Field	Description	Default	Range	Restart Required
User Information				
Username	Name of the user account. The user logs in to the Operations Console using this name. After logging in, the username is displayed in the upper right portion of the screen. You cannot change the username when editing a user account.	None	Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.	No
Old Password	Old password for the user account.	None	Any text that follows the guidelines for choosing secure passwords	No
Password	New password for the user account. User must type this password to log into the Operations Console.	None	Any text that follows the guidelines for choosing secure passwords	No

Field	Description	Default	Range	Restart Required
Reconfirm Password	Retype the password for this user account to verify that you typed the password correctly.	None	Text must match the text entered in the Password field.	No
Firstname	(Optional) First name of the user.	None	Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.	No
Lastname	(Optional) Last name of the user.	None	Valid names include uppercase and lowercase letters in the alphabet, the numbers 0 through 9, a dash, and an underscore.	No
E-mail	(Optional) e-mail address of the user.	None	Valid e-mail address	No

User Group Assignment

To add/remove a user to/from a user group:

Procedure

Step 1 To add a user to a group, select the user group from the **Available** pane, and then click the right arrow to move the user group to the **Selected** pane.

Step 2 To remove a user from a group, select the user from the **Selected** pane, and then click the left arrow to move the user group to the **Available** pane.

Step 3 Click **Save**.

Device Pool Selection

To add a user to or remove a user from a device pool:

Procedure

Step 1 Select **User Management** > **User**.

The Find, Add, Delete, Edit Users window opens.

Step 2 Perform one of the following steps:

- Select a user by clicking on the name in the Username list.
- Select the radio button preceding the name.

Step 3 Select **Edit**

The Edit User window opens to the General tab.

Step 4 Select the **Device Pools** tab.

Step 5 Select the device pool from the **Available** pane, and then click the right arrow to move the pool to the **Selected** pane.

Step 6 To remove a user from a device pool, perform the following steps:

a) Select the device pool from the **Selected** pane.

b) Select the left arrow to move the device pool to the **Available** pane.

Note A user must always be associated with at least one device pool.

Step 7 Select **Save**.

Cisco Unified Customer Voice Portal Page

The main Cisco Unified Customer Voice Portal page is displayed when you log in to the Operations Console. Navigation to the entire website is provided with the menu bar at the top of the screen.

Related Topics

Operations Console Menu Options, on page 10
More Information About Unified CVP, on page 14

Window Header

The window header, which displays at the top of each Operations Console window, contains the following fields:

Window header fields:

- Logged in as - User account for the user who is currently logged in.
- My Account- User who is currently logged in. See My Account Screen, on page 8.
- Logout- Logs you out from the console. See Log out of Operations Console (OAMP), on page 15.
- About - Displays the Welcome window.
- Documentation Search - Searches the Ops Console documentation for a keyword.

Operations Console Menu Options

Use the Operations Console menu options to configure Unified CVP components and users.

Note Selecting an item from the menu bar launches the respective page.

Menu	Options	Use To
System	Control Center	View the status of Cisco Unified Customer Voice Portal environment in a network control center. View the status and statistics by Device Type or Device Pools, logical groups of devices in Cisco Unified Customer Voice Portal solution. Initiate Start, Shutdown, or Graceful Shutdown actions on devices in the control center.
	Device Pool	Create, modify, and delete device pool names and descriptions for logical groups of devices (for example, all devices located in a geographical region).
	Import System Configuration	Import a previously-saved Operations Console Server configuration file and apply it to the current system.
	Export System Configuration	Save and export all configuration information for the Operations Console Server to a single file on your local computer. You can later use this file to restore an Operations Console Server during disaster recovery.
	Location	Add, edit, synchronize, and delete Unified CM location information.
	SIP Server Groups	Configure server groups for SIP and view Call Server deployment status.
	Dialed Number Pattern	Configure the Dialed Number Patterns for a destination. You can define the dialed numbers for the Error Tone, Ring Tone, and other destinations.
	Web Services	Configure Diagnostic Portal servlet credentials.
	IOS Configuration	IOS Template Management - Add, Delete, Edit, Copy, and View an IOS template configuration pushed to an IOS gateway. The template contains the IOS commands required for use in a Unified CVP deployment. IOS Template Deployment - Deploy a gateway configuration template to an IOS gateway. The template provisions the gateway and substitutes any variables in the template with the source devices that are chosen when it is deployed.
	VVB Configuration	Configure Virtualized Voice Browser and associate it with device pools.
	Courtesy Callback	Courtesy Callback reduces the time callers have to wait on hold/in queue and allows the system to offer callers who meet certain criteria.
	SIP Error Reason Code Mapping	Configure SIP reason code to ISUP cause code mapping.
	Cloud Services	Configures Proxy Settings .

Menu	Options	Use To
Device Management	Unified CVP Call Server	Configure Unified CVP Call Server general and infrastructure settings; specify call services settings for each deployment model; associate Unified CVP Call Servers with device pools and the SIP Proxy Server.
	Unified CVP Reporting Server	Configure Unified CVP Reporting Server general and infrastructure settings, associate Unified CVP Reporting Servers with Unified CVP Servers, specify reporting properties, and associate Unified CVP Reporting Servers with device pools. Perform Reporting database administration: schedule database backups and purges; manage database and reporting user names and passwords.
	Unified CVP VXML Server	Configure Unified CVP VXML Server general and infrastructure settings; specify primary and backup Unified CVP Call Servers; enable Unified CVP VXML Server reporting and specify VoiceXML data filters; associate Unified CVP VXML Servers with device pools; and transfer scripts to a VXML Server.
	Unified CVP VXML Server (standalone)	Configure Unified CVP VXML Server (standalone) general settings; associate Unified CVP VXML Server (standalone) with device pools; and transfer scripts to a Unified CVP VXML Server (standalone). **Note** A Unified CVP VXML Server (standalone) handles calls that arrive through a VoiceXML gateway. (No statistics are provided when the Unified CVP VXML Server is configured this way.) Also, you cannot configure a database to and capture data from Unified CVP VXML Server (standalone) applications.
	Gateway	Configure Gateway general settings; associate Gateways with device pools; execute a subset of IOS commands; view gateway statistics; and transfer files.
	Virtualized Voice Browser	Configure Virtualized Voice Browser and associate it with device pools.
	Speech Server	Speech Server provides speech recognition and synthesis services. You can add a pre-configured Speech Server to the Operations Console.
	Media Server	Configure Media Server general settings and associate a Media Server with device pools. **Note** Media Server administers the media files that contain messages and prompts callers hear.
	Unified CM	Configure Unified CM general settings; specify the URL to the Unified CM Device Administration page; and associate the Unified CM with device pools.
	Unified ICM	

Menu	Options	Use To
		Configure ICM Server general settings and associate the ICM Server with device pools.
	SIP Proxy Server	Configure SIP Proxy Server general settings; specify the URL to the SIP Proxy Server Device Administration page; and associate the SIP Proxy Server with device pools.
	Unified IC	Configure CUIS Server general settings and associate the CUIS Server with device pools.
	Device Past Configuration	Allows you to view the past 10 saved configurations of a selected device that are currently stored in the Operations Console database.
	Device Versions	View version information for the Unified CVP Call Server, Unified CVP Reporting Server, Unified CVP VXML Server, and Unified CVP VXML Server (standalone).
User Management	User Roles	Create, modify, and delete user roles. Assign SuperUser, Administrator, or Read Only access privileges to roles.
	User Groups	Create, modify, and delete user groups. Assign roles to user groups.
	Users	Manage Unified CVP users, and assign them to groups and roles.
Bulk Administration	File Transfer	Transfer script files and VXML applications to multiple devices at a time.
SNMP	V1/V2c	Configure the SNMP agent that runs on the Unified CVP device to use the V1/V2 SNMP protocol to communicate with an SNMP management station; add and delete SNMP V1/V2c community strings; configure a destination to receive SNMP notifications from an SNMP management station; and associate community strings with the device.
	V3	Configure the SNMP agent that runs on the Unified CVP device to use the V3 SNMP protocol to communicate with an SNMP management station; add and delete SNMP users and set their access privileges; configure a destination to receive SNMP notifications from an SNMP management station; and associate SNMP users with devices.
	System Group	Configure the MIB2 System Group system contact and location settings, and associate the MIB2 System Group with devices.
Tools	SNMP Monitor	Displays the **SNMP Monitor** page.
	Configure	Displays the **Configure Tools** page.
	NOAMP	Logs in to NOAMP automatically.

Menu	Options	Use To
Help	Contents	Displays the table of contents for the help system.
	This Page	Displays help on the current screen.
	About	Displays the Home page.

More Information About Unified CVP

The Operations Console Online Help describes how to use the Operations Console to configure and perform basic monitoring of the components that make up the Unified CVP solution. For design considerations and guidelines for deploying enterprise network solutions that incorporate *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

The following table lists the documents available in the Unified CVP documentation set.

For More Information on...	Refer to...
The versions of software and hardware that are required and compatible with the Unified CVP solution	*Compatibility Matrix for UCCE* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.
System requirements, features of the release, packaging information, limitations and restrictions, and a list of known defects	*Release Notes for Cisco Unified Contact Center Enterprise Solution* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-release-notes-list.html.
Installing Unified CVP software, performing an initial configuration, and upgrading from earlier versions of Unified CVP software	*Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.
Setting up, running, and administering the Unified CVP product, including associated configuration	*Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html
Configuring the Reporting Server and Reporting Database and using report templates to generate reports	*Reporting Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html.
Using the Call Studio environment and deploying applications to the Cisco Unified CVP VXML Server	*User Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.
Configuration options for all Say It Smart plugins	*Say It Smart Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

For More Information on...	Refer to...
Building components that run on the Cisco Unified CVP VXML Server	*Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-programming-reference-guides-list.html.
The ports used by Unified CVP software components.	*Solution Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

Log out of Operations Console (OAMP)

To log out from the Operations Console, perform the following procedure.

Procedure

To log out from the Operations Console:

Procedure

Click **Logout** in the screen header at the top of the screen.

You are logged out and the main Cisco Customer Voice Portal window opens.

Related Topics

Log in to Operations Console (OAMP), on page 7

View System-Level Operation States

The Operations Console provides status information for each device. Each device can be in one of the states listed in the following table.

Table 2: Description of States Displayed in the Status Window

State	Reasons
Success	Indicates that the operation was successful.
Pending	Indicates that the operation has not yet been executed.
In Progress	Indicates that the operation is in progress.

State	Reasons
Failed	The reasons for a **failed deployment** state are listed below: • Unable to locate IP address in the database • General database failure • The call server was not deployed • Unknown error • Notification error: Contact administrator • Could not write to properties file • The Call Server device is using an unknown version of the Unified CVP software • The Call Server device is using an older version of the Unified CVP software • Configuration not removed from the database This failure has multiple reasons: • Could not write to properties file • Device has not been deployed • General failure • Unable to access the Database
	The reasons for a **failed synchronization** state are listed below: • Device not accessible • Authentication failure • Web service is not available on the device • General database error • General error • Unknown host address • SOAP service error

Note If you make any configuration changes after your initial deployment of any System-level configuration tasks, you must deploy the changed configuration again.

Transfer Script and Media Files

You can transfer a single script or media file at a time from the Operations Console.

Procedure

To transfer a script or media file:

Procedure

Step 1 From the Device Management menu, select the type of server to which to transfer the script file. For example, to transfer a script or media file to a Gateway, select **Device Management** > **Gateway**.

The Find, Add, Delete, Edit window lists any servers that have been added to the Operations Console.

Step 2 Select a server by clicking on the link in its Hostname field or by clicking the radio button preceding it and then clicking **Edit**.

Step 3 Select **File Transfer** in the toolbar and then click **Scripts and Media**.

The Scripts and Media File Transfer page opens, listing the host name and IP address for the selected device. Script and Media files currently stored in the Operations Server database are listed in the Select From available Script Files box.

Step 4 If the script or media file is not listed in the Select From Available Script Files box:

a) Click **Select a Script or Media File from Your Local PC**.

b) Enter the file name in the text box or click **Browse** to search for the script or media file on the local file system.

Step 5 If the script or media file is listed in the Select From Available Script and media Files box, select the script or media file.

Step 6 Click **Transfer** to send the file to the device.

The script or media file is transferred to the selected server.

Operations Console (NOAMP)

Operations Console (NOAMP) is a web-based interface from which you can access and configure the following sections for Unified CVP.

- **Overview**: This is the home page of Cisco Unified Customer Voice Portal.
- **CVA**: This section is used to configure Speech Servers and manage devices settings for CVA.
- **Integration**: This section is used to configure CloudConnect and copy settings to selected devices.
- **License Management**: This section provides licensing information for Unified CVP.
- **CVA Statistics** This section provides CVA-related statistics.
- **Classic OAMP**: Click this to navigate to OAMP (https://ServerIP:9443/oamp).

Log in to Operations Console (NOAMP)

Before you begin

If this is the first time you are logging in to Operations Console after installing the Unified CVP software, you will need the password for the default **Administrator** account that was created during installation.

The inactivity session timeout (when no activity is performed in the browser) for Operations Console is set to 60 minutes. If the browser is inactive for more than 60 minutes, you are required to log in again.

Procedure

Step 1 From the web browser, enter **`https://ServerIP:9443/noamp`**, where ServerIP is the IP address or hostname of the machine on which Operations Console is installed.
The main **Unified CVP** window opens.

Step 2 In the **Username** field, enter your user ID.

Note The first time you log in after installing the Unified CVP software, enter **Administrator** as the default user ID.

Step 3 In the **Password** field, enter your password.

Note
- If you are logging in to the default **Administrator** account, enter the password that was set for this account during installation.
- If the user ID or the password is invalid, the Operations server displays the following message

  `Incorrect Username and/or password.`

Customer Virtual Assistant

Customer Virtual Assistant (CVA) enables the IVR Platform to integrate with cloud-based speech services. CVA provides the following speech services:

- **Text-to-Speech**: Integration with cloud-based TTS services in your application for Speech Synthesis operations. CVA currently supports Google Text-to-Speech service.
- **Speech-to-Text**: Integration with cloud-based ASR services in your application for Speech Recognition operations. CVA currently supports Google Speech-to-Text service.
- **Speech-to-Intent**: CVA provides capability of identifying the intent of customer utterances by processing the text received from Speech-to-Text operations. CVA offers this service by using cloud-based Natural Language Understanding (NLU) services. CVA currently supports Google Dialogflow service.

This section enables you to perform the following tasks.

- Configure VVB devices for speech services.
- View CVA-related statistics for the listed VVB devices.

Configuration

Configure VVB Devices for Speech Services

This procedure configures VVB devices for speech services.

Note If Nuance is configured, it takes precedence over speech services.

Before you begin

1. Import the certificate from Cisco VVB to OAMP Server.

   For more information, see *Secure HTTP Communication between OAMP Server and Cisco VVB* section in *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.
2. Ensure Cisco VVB hostname is DNS resolvable from OAMP Server.
3. Restart **CVP OPSConsoleServer** service.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **CVA** > **Configuration**.

Step 2 From the **Device** drop-down list, select a VVB device.

Step 3 Follow the procedure to configure the selected VVB device(s) for the required speech service.

Text to Speech

Text to Speech (TTS) tab enables you to view, add, edit, or delete TTS service accounts.

Add and Maintain Text to Speech Account

This procedure explains how to add a text to speech account. For more information on maintaining service accounts, see Edit Text to Speech Service Account, on page 20 and Delete Service Account, on page 22.

Procedure

Step 1 Click the **Text to Speech** tab.

Step 2 Click **New** to open the **New Text to Speech Account** pop-up.

Step 3 Complete the fields.

For more information, see Field Details for Text to Speech Service Provider, on page 22.

Step 4 Click **Next** to continue.

Step 5 Complete the fields that are displayed based on the selected service provider.

Step 6 Click **Save**.

Edit Text to Speech Service Account

This procedure explains how to edit configuration details for a Text to Speech account.

Note Any change in configuration takes effect after 5 minutes.

Procedure

Step 1 Click the **Text to Speech** tab.

Step 2 Click the service account for which you want to edit the configuration.

The **Edit** section opens for the selected service account.

Step 3 Edit the required fields.

For more information, see Field Details for Text to Speech Service Provider, on page 22.

Step 4 Click **Save**.

Automatic Speech Recognition

Automatic Speech Recognition (ASR) tab enables you to view, add, edit, or delete ASR service accounts.

Add and Maintain Automatic Speech Recognition Account

This procedure explains how to add an Automatic Speech Recognition account. For more information on maintaining service accounts, see Edit Automatic Speech Recognition Service Account, on page 20 and Delete Service Account, on page 22.

Procedure

Step 1 Click the **Automatic Speech Recognition** tab.

Step 2 Click **New** to open the **New Automatic Speech Recognition** pop-up.

Step 3 Complete the fields.

For more information, see Field Details for Automatic Speech Recognition Service Provider, on page 23.

Step 4 Click **Next** to continue.

Step 5 Complete the fields that are displayed based on the selected service provider.

Step 6 Click **Save**.

Edit Automatic Speech Recognition Service Account

This procedure explains how to edit configuration details for an Automatic Speech Recognition account.

Note Any change in configuration takes effect after 5 minutes.

Procedure

Step 1 Click the **Automatic Speech Recognition** tab.

Step 2 Click the service account for which you want to edit the configuration.

The **Edit** section opens for the selected service account.

Step 3 Edit the required fields.

For more information, see Field Details for Automatic Speech Recognition Service Provider, on page 23.

Step 4 Click **Save**.

Natural Language Understanding

Natural Language Understanding (NLU) tab enables you to view, add, edit, or delete NLU service accounts.

Add and Maintain Natural Language Understanding Account

This procedure explains how to add a Natural Language Understanding (NLU) account. For more information on maintaining service accounts, see Edit Natural Language Understanding Service Account, on page 21 and Delete Service Account, on page 22.

Procedure

Step 1 Click the **Natural Language Understanding** tab.

Step 2 Click **New** to open the **New Natural Language Understanding** pop-up.

Step 3 Complete the fields.

For more information, see Field Details for Natural Language Understanding Service Provider, on page 24.

Step 4 Click **Next** to continue.

Step 5 Complete the fields that are displayed based on the selected service provider.

Step 6 Click **Save**.

Edit Natural Language Understanding Service Account

This procedure explains how to edit configuration details for a Natural Language Understanding account.

Note Any change in configuration takes effect after 5 minutes.

Procedure

Step 1 Click the **Natural Language Understanding** tab.

Step 2 Click the service account for which you want to edit the configuration.

The **Edit** section opens for the selected service account.

Step 3 Edit the required fields.

For more information, see Field Details for Natural Language Understanding Service Provider, on page 24.

Step 4 Click **Save**.

Delete Service Account

Procedure

Step 1 Hover the mouse pointer over the row of the service account to be deleted. Click the **x** icon at the end of the row.

Step 2 Click **Yes** to confirm.

Supported Fields from Service Provider

Field Details for Text to Speech Service Provider

Service Provider	Field	Required?	Editable?	Description
Google	**Service Account**	Yes	Yes (only for adding a service account)	Unique identifier for the service account[1]. This should match the name of the account created in Google.
	Service Provider	Yes	No	Name of the service provider.
	Description	No	Yes	Short description of the service account.
	Set as Default	No	Yes	Makes the service account default. Toggle to turn on/off the **Set as Default**. Only one service account can be set as default for a given service.
	Service Account Key	Yes	Yes	Service account key [2] of the service account.

1 Use the same Service Account name in the Call Studio.
2 Use the key provided in the `.json` file. For more information on how to fetch the `.json` file from the service provider, see https://cloud.google.com/text-to-speech/docs/quickstart-client-libraries. CCAI customers must use the key provided during the onboarding process.

Field Details for Automatic Speech Recognition Service Provider

Service Provider	Field	Required?	Editable?	Description
Google	**Service Account**	Yes	Yes (only for adding a service account)	Unique identifier for the service account[3]. This should match the name of the account created in Google.
	Service Provider	Yes	No	Name of the service provider.
	Description	No	Yes	Short description of the service account.
	Set as Default	No	Yes	Makes the service account default. Toggle to turn on/off the **Set as Default**. Only one service account can be set as default for a given service.
	Service Account Key	Yes	Yes	Service account key[4] of the service account.

[3] Use the same Service Account name in the Call Studio.
[4] Use the key provided in the `.json` file. For more information on how to fetch the `.json` file from the service provider, see https://cloud.google.com/speech-to-text/docs/quickstart-client-libraries. CCAI customers must use the key provided during the onboarding process.

Field Details for Natural Language Understanding Service Provider

Service Provider	Field	Required?	Editable?	Description
Dialogflow	**Service Account**	Yes	Yes (only for adding a service account)	Unique identifier for the service account[5]. This should match the name of the account created for Dialogflow.
	Service Provider	Yes	No	Name of the service provider.
	Description	No	Yes	Short description of the service account.
	Service Account Key	Yes	Yes	Service account key[6] of the service account.

[5] Use the same Service Account name in the Call Studio.
[6] Use the key provided in the `.json` file. For more information on how to fetch the `.json` file from the service provider, see https://dialogflow.com/docs/reference/v2-auth-setup. CCAI customers must use the key provided during the onboarding process.

Copy Settings to Selected Device

This procedure copies the settings from one device to a list of selected devices.

For example, if you have a setup with multiple Cisco VVBs, you can use this procedure to quickly copy the configuration settings from one Cisco VVB to the other Cisco VVBs.

Note The **Copy Settings** option is available only if there are 2 or more VVB devices.

Procedure

Step 1 From the **Device** drop-down list, select the device from which settings are copied.

Step 2 Click **Copy Settings**.
The **Copy Settings to Device** page is displayed.

Step 3 From **Select Devices**, select the devices to which settings are copied.

Note Select the **Select All** check box to select all the devices.

Step 4 Click **Save**.
The settings are copied to the selected devices.

CVA Statistics

This section provides CVA-related statistics for the listed VVB devices.

View CVA Statistics

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **CVA**> **Statistics**.

Step 2 Under the **Statistics** column, click the icon for the required VVB device that is listed under the **Host Name** column.
The **Unified Virtualized Voice Browser Statistics** page is displayed with the CVA statistics for the selected VVB device.

Smart Licensing

Cisco Smart Software Licensing is a flexible software licensing model that streamlines the way you activate and manage Cisco software licenses across your organization. For detailed feature overview on Smart Licensing, see *Administration Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-maintenance-guides-list.html.

License Management

Smart Licensing can be managed by using Cisco SSM and

- **Cisco SSM—**Cisco SSM enables you to manage all your Cisco smart software licenses from a centralized website. With Cisco SSM, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances).

  You can access Cisco SSM from https://software.cisco.com, by clicking the Smart Software Licensing link under the License menu.

- **License Management in CCVP—**In CCVP there are various deployment models:
  - **CVP in Packaged CCE—**When CVP is deployed with Packaged CCE, you can manage the configurations from the Unified CCE Administration Interface.
  - **CVP in Unified CCE or HCS for CC—**When CVP is deployed with Unified CCE or HCS, you can manage the configurations from the NOAMP in CVP.
  - **Standalone CVP—**In the standalone CVP model, you can manage the configurations in the NOAMP in CVP.

  Using the License Management option in the Cisco CVP NOAMP portal or in Unified CCE Administration, you can register or deregister the product instance, select your License Type, set transport settings or view the licensing consumption summary.

Smart Licensing Task Flow

Complete these tasks to set up smart licensing for Unified CVP.

Steps	Action	Description
Step 1	Create your Smart Account	Use the Smart Account to organize licenses according to your needs. To create a Smart Account, go to http://software.cisco.com After the Smart Account is created, Cisco SSM creates a default Virtual Account for this Smart Account. You can use the default account or create other Virtual Accounts.
Step 2	Obtain the Product Instance Registration Token	Generate a product instance registration token for your virtual account. For more information, see Obtain the Product Instance Registration Token.
Step 3	Configure Transport Settings for Smart Licensing	Configure the transport settings through which Unified CVP connects to the Cisco SSM or Cisco SSM On-Prem. For more information, see Configure Transport Settings for Smart Licensing.
Step 4	Select the License Type	Select the License Type before registering the product instance. For more information, see Select License Type.
Step 5	Register with Cisco SSM	Register Unified CVP with Cisco SSM or Cisco SSM On-Prem. For more information, see Register with Cisco Smart Software Manager.

Related Topics

Obtain the Product Instance Registration Token, on page 27
Configure Transport Settings for Smart Licensing, on page 28
Select License Type, on page 29
Register with Cisco Smart Software Manager, on page 30
Registration, Authorization, and Entitlement Status, on page 31

Obtain the Product Instance Registration Token

Obtain the product instance registration token from Cisco SSM or Cisco SSM On-Prem to register the product instance. Generate the registration token with or without enabling the Export-Controlled functionality.

Note The **Allow export-controlled functionality on the products that are registered with this token** check box does not appear for Smart Accounts that are not permitted to use the Export-Controlled functionality.

Procedure

Step 1 Log in to your smart account in either Cisco SSM or Cisco SSM On-Prem.

Step 2 Navigate to the virtual account with which you want to associate the product instance.

Step 3 Generate the Product Instance Registration Token.

Note
- Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for a product instance you want in this smart account. When you select this check box and accept the terms, you enable higher levels of encryption for products that are registered with this registration token. By default, this check box is selected.
- Use this option only if you are compliant with the Export-Controlled functionality.

Step 4 Copy the generated token. This token is required when registering Smart Licensing with Cisco SSM.

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CVP and Cisco SSM.

Note Configure the transport setting individually for all CVP devices installed in the deployment.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, select **License Management**.
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Transport Settings** to set the connection method.

Step 4 Select the connection method to Cisco SSM:

- **Direct**—Unified CVP connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—Unified CVP connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
- **HTTP/HTTPS Proxy**—Unified CVP connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

Step 5 Click **Save** to save the settings.

Select License Type

Note If you select incorrect License Type, the product instance is placed in the Out-of-Compliance state. If this issue is unresolved, the product instance is placed in the Enforcement state where the system operations are impacted.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **License Management**.
The **License Management** page is displayed.

Step 2 Click **License Type**.
The **Select License Type** page is displayed.

Step 3 Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.

The following table lists the license types that CVP Smart Licensing offers and the license name for each license type:

License Type	License Name
Comprehensive Perpetual	• CVP 12.5 Self Service Ports • CVP 12.5 Server Software
Comprehensive Flex	• Flex CVP Self Service Ports
HCS Perpetual	• HCS-CVP 12.5 Self Service Ports
HCS Flex	• HCS-CVP 12.5 Flex Self Service Ports
Standalone	• CVP STD 12.5 Self Service Ports • CVP 12.5 Server Software
Calldirector	• CVP 12.5 Call Director Self Service Ports • CVP 12.5 Call Director
Lab	• CVP 12.5 LAB Self Service Ports • CVP 12.5 LAB Server Software

Note Reported Count is the usage reported by the CVP Server to CSSM.

Comprehensive Perpetual must be selected for standalone deployments. This causes CVP to send comprehensive entitlement in standalone deployments also. Only when standalone specific PIDs are purchased, standalone should be selected.

Step 4 Click **Save**.

Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.

Note After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal** , click **License Management.**
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Register**.

Note
- Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.
- Individually register all CVP devices installed in the deployment.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in Cisco Unified Contact Center Express Features Guide.

Step 5 Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

Table 3: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation
Export-Controlled Functionality	Not Allowed
On Successful Registration	

Smart License Status	Description
Registration Status	Registered (Date and time of registration)
License Authorization Status	Authorized (Date and time of authorization)
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

You can update or purchase entitlements on the Cisco Commerce website. For more information, see https://apps.cisco.com/Commerce/.

Registration, Authorization, and Entitlement Status

Registration Status

This table explains the Unified CVP registration status for Smart Licensing in the Unified CVP Administration portal:

Table 4: Registration Status

Status	Description
Unregistered	Product is unregistered.
Registered	Product is registered. Registration is automatically renewed every six months.
Registration Expired	Product registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months.

Authorization Status

This table describes the possible Unified CVP authorization status for Smart Licensing in the Unified CVP Administration portal:

Table 5: Authorization Status

Status	Description
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
Authorized	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
Authorization Expired	Product authorization has expired. This usually happens when the product has not communicated with Cisco for 90 days. It is in an overage period for 90 days before enforcing restrictions.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Unauthorized	Product is unauthorized.
No License in Use	No Licenses are in use.

License Entitlement Status

This table describes the possible Unified CVP instance license entitlement status for Smart Licensing in the Unified CVP Administration portal:

Table 6: License Entitlement Status

Status	Status Description
Authorization Expired	Product authorization has expired, when the product has not communicated with Cisco for 90 days.
Not Authorized	Product instance is not authorized.
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
In Compliance	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
ReservedInCompliance	Entitlement is in compliance with the installed reservation authorization code.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Not Applicable	Entitlement is not applicable.
Invalid	Error condition state.
Invalid Tag	Entitlement tag is invalid.

Status	Status Description
No License in Use	Entitlement is not in use.
Waiting	Waiting for an entitlement request's response from Cisco SSM or Cisco SSM On-Prem.
Disabled	Product instance is deactivated or disabled.

Smart Licensing Tasks

After you successfully register Smart Licensing, you can perform the following tasks as per the requirement:

- **Renew Authorization**—The license authorization is renewed automatically every 30 days. Use this option to manually renew the authorization.
- **Renew Registration**—The initial registration is valid for one year. Registration is automatically renewed every six months. Use this option to manually renew the registration.
- **Reregister**—Use this option to forcefully register the product instance again.
- **Deregister**—Use this option to release all the licenses from the current virtual account.

Renew Authorization and Renew Registration are automated tasks that take place at regular intervals. If there is a failure in the automated process, you can manually renew authorization and registration.

For more information, see *Smart License Management* section in *Cisco Unified Contact Center Express Admin and Operations Guide*.

Note You have to Deregister and Reregister manually.

Related Topics

Renew Authorization, on page 33
Renew Registration, on page 34
Reregister License, on page 34
Deregister License, on page 35

Renew Authorization

The license authorization is renewed automatically every 30 days. The authorization status expires after 90 days if the product is not connected to Cisco SSM or Cisco SSM On-Prem.

Use this procedure to manually renew the License Authorization Status for all the licenses listed in the License Type.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **License Management.**
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Action** > **Renew Authorization**.

This process takes a few seconds to renew the authorization and close the window.

Renew Registration

Use this procedure to manually renew your certificates.

The initial registration is valid for one year. Renewal of registration is automatically done every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **License Management**.
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Action** > **Renew Registration**.

This process takes a few seconds to renew the authorization and close the window.

Reregister License

Use this procedure to reregister Unified CVP with Cisco SSM or Cisco SSM On-Prem.

Note Product can migrate to a different virtual account when reregistering with the token from a new virtual account.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **License Management.**
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Action** > **Reregister**.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the copied or saved Registration Token Key that you generated using the Cisco SSM or Cisco SSM On-Prem in the Product Instance Registration Token text box.

Step 5 Click **Reregister** to complete the reregistration process.

Step 6 Close the window.

Deregister License

Use this procedure to deregister Unified CVP from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product are released to the virtual account and is available for other product instances to use.

Note If Unified CVP is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product is deregistered, then a confirmation message notifies you to remove the product manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.

Note After deregistering, the product reverts to the Evaluation state if the evaluation period is not expired. All the license entitlements that are used for the product are immediately released to the virtual account and are available for other product instances to use them.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **License Management**.
The **License Management** page is displayed.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Step 3 Click **Action** > **Deregister**.

Step 4 On the **Confirm Deregistration** dialog box, click **Yes** to deregister.

Out-Of-Compliance and Enforcement Rules

Out-of-Compliance

The Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for four consecutive reporting intervals, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state.

All CVPs in a virtual account share the licenses from a pool. If the license consumption exceeds than those available in the pool, all CVPs in the virtual account follow the Out-of-Compliance and Enforcement rules.

Enforcement

The Product Instance is in the Enforcement state in the following scenarios:

- **Out-of-Compliance expiry**: When the Out-of-Compliance period of 90 days has expired.

  Purchase new licenses to exit the Enforcement state.

- **Authorization expiry**: When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.

Renew the license authorizations to exit the authorization expiry state.

- **Evaluation expiry**: When the license evaluation period of 90 days has expired and the Product Instance is not registered with Cisco SSM.

  Register the Product Instance with Cisco SSM to exit the Evaluation expiry state.

In the Enforcement state, the following actions are blocked:

- Uploading VXML applications from OAMP
- Deploying application and updating application scripts in VXML server
- Deploying VXML applications REST call from the Unified CCE Administration interface in Packaged CCE

Integration

This section enables you to perform the following tasks.

- Configure Cloud Connect.
- Copy settings to the selected devices.

In **Cisco Unified Customer Voice Portal**, click **Integration** to access the **Integration** section.

Cloud Connect

Configure CVP Devices for Cloud Connect

This procedure configures CVP devices for Cloud Connect.

Before you begin

1. Import the certificate from Call Server to OAMP Server.

   For more information, see *Secure HTTP Communication between OAMP Server and Call Server* section in *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

2. Ensure Unified CVP hostname is DNS resolvable from OAMP Server.
3. Restart **CVP OPSConsoleServer** service.

Procedure

Step 1 In **Cisco Unified Customer Voice Portal**, click **Integration** > **Cloud Connect**.

Step 2 From the **Device** drop-down list, select a Unified CVP device.

Step 3 In the **Publisher IP Address / Hostname** text box, enter the FQDN / IP address of the publisher.

Step 4 In the **Subscriber IP Address / Hostname** text box, enter the FQDN / IP address of the subscriber.

Step 5 In the **User Name** text box, enter the Cloud Connect administrator username.

Step 6 In the **Password** text box, enter the Cloud Connect administrator password.

Step 7 Click **Save**.

Step 8 Restart **Cisco CVP CallServer** service.

Copy Settings to Selected Device

This procedure copies the settings from one device to a list of selected devices.

For example, if you have a setup with multiple Unified CVPs, you can use this procedure to quickly copy the configuration settings from one Unified CVP to the other Unified CVPs.

Note The **Copy Settings** option is available only if there are 2 or more CVP devices.

Procedure

Step 1 From the **Device** drop-down list, select the device from which settings are copied.

Step 2 Click **Copy Settings**.
The **Copy Settings to Device** page is displayed.

Step 3 From **Select Devices**, select the devices to which settings are copied.

Note Select the **Select All** check box to select all the devices.

Step 4 Click **Save**.
The settings are copied to the selected devices.

Step 5 Restart **Cisco CVP CallServer** service.

Classic OAMP

This section enables you to navigate to Classic OAMP (https://ServerIP:9443/oamp) automatically without having to log in.

1. In **Cisco Unified Customer Voice Portal**, click **Classic OAMP**.

   You are logged in to OAMP automatically.

Log out of Operations Console (NOAMP)

Procedure

Step 1 On the top right-hand corner of the **Cisco Unified Customer Voice Portal** page, click on the username.

Step 2 Select `Sign Out`.
You are logged out of Operations Console.

Error Handling

The Operations Console performs two types of validations:

- **Client Side** - Validations using Javascript, which runs within the web browser. You must enable Javascript in the browser.
- **Server Side** - Validations that are run on the server side. These are extensive validations that include the client side validations and any business validations.

Client side validation errors appear at the top of the page just below the Menu bar.

Control Center Operation

Use the control center to view and manage the devices in the Unified CVP solution from a central place. You can view the status of an individual device or all the devices that belong to a group of devices. You can also shut down and start VXML, Reporting, and Call Servers; and view detailed statistics for each of these devices.

You can perform the following tasks from the Control Center:

View Devices by Type

You can view groups of devices by type (for example, Call Server, or Reporting Server). Devices of the selected device type are listed in the right pane of the Control Center.

Related Topics

Start Server, on page 58
Shut Down Server, on page 59
Edit Device Setup, on page 58
View Device Status, on page 39

Procedure

To view devices by type:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center window opens.

Step 2 Select the Device Type tab.

Devices types are listed in the Device Type tab.

Step 3 Select the type of device to display.

Only devices of the selected type are listed in the Devices tab in the right pane.

View Devices by Device Pool

You can view groups of devices by device pool (for example, the devices in the San Jose pool). If a device belongs to more than one device pool, that device is listed in each device pool.

Related Topics

Start Server, on page 58
Shut Down Server, on page 59
Edit Device Setup, on page 58
View Device Status, on page 39

Procedure

To view devices by device pool:

Procedure

Step 1 Select **System** > **Control Center**.

Step 2 Select the **Device Pool** tab and then select a device pool from the list.

Devices that belong to the selected device pool appear under the **General** tab.

Step 3 Sort the devices by Hostname, IP Address, Device Type, Status, or Active Calls by clicking the desired column header.

Only the devices listed on the current page are sorted. For example, if you select a Call Server device pool and then click the **IP Address** column header, the call servers displayed on the current screen are sorted by the IP address.

Step 4 Select the desired refresh interval from the **Refresh** drop-down menu.

By default, pool statistics are not refreshed.

Step 5 Click individual device in a device pool to display or edit the device configuration.

View Device Status

You can view the devices in a particular device pool by selecting Control Center from the System menu and then selecting the Device Pool tab and selecting a device pool. You can also view a particular type of device by selecting the Device Type tab and selecting a device type.

All CVP devices, Unified CVP Call Servers, Unified CVP Reporting Servers, and Unified CVP VXML Servers, report current operating status. The status of some devices, such as IOS devices, Unified CM, ICM servers, SIP proxy servers display as N/A (Not Applicable) because the Operations Console does not monitor these device types.

The following table describes the fields in the Control Center.

Table 7: Device Status Fields in the Control Center

Field	Description
Hostname	The hostname assigned to the device.
IP Address	IP address for the server.
Device Type	The category of the device, for example: Unified CVP Call Servers, Unified CVP Reporting Servers, or Unified CVP VXML Servers.
Actions	Icons that indicate operations that you can perform on a selected device. Not all actions are available for all devices. Available actions include: • **Statistics** - Data on current activities and activities that occur during an interval. • **Unapplied Changes** - Indicates that configuration changes that have been saved to the Operations Console database have not yet been applied to the device. • **Link to an External Administration Page** - Displays a web-based administration page from which you can administer a server. Available for Unified CM, SIP proxy servers, and ICM Servers.

Field	Description
Status	The current operating status for a selected device. • The Device is up and running. CVP Service Internal States: • **In Service** - The service is running. • **In Service (Warning Threshold Reached)** - The service is running and the warning threshold has been reached. • **In Service (Critical Threshold Reached)** - The service is running and the critical threshold has been reached. • Device is not running or has no communication with local WebServicesManager service. CVP Service Internal States: • **Disabled** - The service has not been configured. • **Stopped** - The service is not running. • **Error Scenario (not an internal state)** - Where local WebServicesManager service has no message bus communication with device. • One or more of the device services are functioning partially. CVP Service Internal States: • **Starting** - The service is starting. • **Partial Service** - The service has been configured and started, but is not running at full service. Partial service may be attributed to waiting on a dependency (such as the IVR and SIP service waiting for ICM to connect to the VRU PIM), not being licensed, or license usage being critical. • **Stopping** - The service is stopping. • **Not Reachable** • The device could not be reached from Operations Console. Common reasons for not reachable status are: • Machine shutdown. • WebServicesManager service on the device is down. • Security is enabled for device but invalid certificate configuration.

Field	Description
Active Calls	The total number of calls currently running in the device. • **<Integer Value>** - The number of calls for devices such as Unified CVP Call Server, Unified CVP Reporting Server, and Unified CVP VXML Server. • **N/A** - Not applicable for device typse such as gateway, Unified CM Server, Virtualized Voice Browser and so on.

Sometimes, the actual device status can be resultant of more than one CVP service state for the corresponding device. For example, the Unified CVP Call Service device status in Control Center is actually an aggregation of SIP, ICM, and IVR service states.

The following table describes device status that is specific to each CVP device type.

Table 8: CVP Device Status

CVP Device	Description
Unified CVP Call Server	• **Up** All configured services (ICM/IVR/SIP) are in the In Service state and report the same to the Operations Console. • **Down** At least one of the configured services (ICM/IVR/SIP) is deemed stopped (or disabled), and none of these services are in the Not Reachable state. • **Partial** At least one of the configured services (ICM/IVR/SIP) is running at Partial Service, and neither of these services are in the Down or Not Reachable state. **Note** If the device status is Partial, the status of the individual services are shown in the Partial state Details. Click the Partial status in Control Center to view the tool tip; it describes each service state. • **Not Reachable** At least one of the configured services (ICM/IVR/SIP) is deemed Not Reachable. If the Unified CVP Call Server is configured with no services (SIP/IVR/ICM) active, its status in Control Center will always be Not Reachable.

CVP Device	Description
Unified CVP Reporting Server	• **Up** The reporting service is running as reported by Central Controller on the Unified CVP Call Server machine. • **Down** If the reporting service is deemed Stopped (or disabled) as reported by Central Controller on the Unified CVP Call Server machine or the WebServicesManager, an associated Unified CVP Call Server machine has no communication with Central Controller. • The WebServicesManager on the Unified CVP Call Server has not received state events from the Controller for the reporting subsystem. • The Unified CVP Reporting Server is unable to communicate with Central Controller on the Unified CVP Call Server machine; Central Controller has no knowledge of state events and, therefore, cannot communicate state events to Operations Console. In either scenario, even if the Unified CVP Reporting Server is up and running and the WebServicesManager on the Unified CVP Reporting Server is up and running, the Operations Console still shows the status of the Unified CVP Reporting Server as Down when there is no communication with Central Controller. • **Partial** The reporting service is not in the Up, Down, or Not Reachable state. Unified CVP Reporting Server indicates a partial status when, for example, the reporting data buffer file is full and all new messages are written in memory in a buffer queue. • **Not Reachable** The Operations Console is unable to communicate to the WebServicesManager co-located with the associated Unified CVP Call Server (for example, the WebServicesManager service on the device is down).

CVP Device	Description
Unified CVP VXML Server and Unified CVP VXML Server (standalone)	In both cases, the Operations Console communicates with the WebServicesManager co-located on the Unified CVP VXML Server (or standalone) server machine. The WebServicesManager on the device runs the Unified CVP VXML Server status script to retrieve device status and the number of active calls. • **Up** If the WebServicesManager gets a valid number for the number of active calls after running the status script. Zero (0) is a valid number. • **Not Reachable** In addition to other reasons for the Not Reachable state, the Unified CVP VXML Server (or standalone) goes into this state if WebServicesManager does not get a valid number for active calls after running the status. There is no Partial or Down status for Unified CVP VXML Servers and Unified CVP VXML Server (standalone).

View Device Statistics

You can view realtime, interval, and aggregate data for Unified CVP devices.

Related Topics

Infrastructure Statistics , on page 46
IVR Service Call Statistics, on page 46
SIP Service Call Statistics, on page 48
View Gateway Statistics, on page 51
Unified CVP VXML Server Statistics, on page 52
Standalone Unified CVP VXML Server Statistics, on page 54
Unified CVP Reporting Server Statistics , on page 55

Procedure

To view device statistics:

Procedure

Step 1 Select **System** > **Control Center**.

Step 2 From the Device Type tab in the left pane, select the type of device for which you want to view statistics.

Step 3 From the Devices tab, select a device by checking the radio button preceding it.

Step 4 Select **Statistics** either in the Actions column or in the toolbar.

Statistics for the selected device are reported in a new statistics result window. All event statistics are sent to an SNMP manager, if one is configured. The log messages XML file, `CVPLogMessages.xml`, defines the

severity, destination (SNMP management station or Syslog server), and possible resolution for Unified CVP log messages.

View Device Associations

The Operations Console supports the association of CVP Call Servers with Unified CVP VXML Servers and/or CVP Reporting Servers.

Procedure

To view devices associated with a Call Server:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center window opens.

Step 2 Click the hostname of a Call Server.

The Edit CVP Call Server Configuration window opens.

Step 3 From the toolbar, click **Device Associations**.

The Device Association page lists the VXML Server, Reporting Server, and Courtesy Callback Reporting Server associated with this Call Server.

View Infrastructure Statistics

You can view realtime, interval, and aggregate data for Unified CVP devices.

Related Topics

Edit Log Messages XML File

Procedure

To view infrastructure statistics:

Procedure

Step 1 Select **System** > **Control Center**.

Step 2 Select the **Device Type** tab.

Step 3 Select the type of device for which you want infrastructure statistics.

Devices of the selected type display in the Devices tab.

Step 4 Select the device by checking the radio button preceding it.

Step 5 Select **Statistics** in the toolbar.

Step 6 Select the **Infrastructure** tab.

Statistics for the selected device are reported in a new window. All event statistics are sent to an SNMP manager, if one is configured. The log messages XML file, `CVPLogMessages.xml`, defines the severity, destination (SNMP management station or Syslog server), and possible resolution for Unified CVP log messages.

Infrastructure Statistics

IVR Service Call Statistics

The IVR service call statistics include data on calls currently being processed by the IVR service, new calls received during a specified interval, and total calls processed since the IVR service started.

Access IVR Service statistics either by:

- Selecting **System** > **Control Center**, selecting a Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **IVR** tab.
- Selecting **Device Management** > **Unified CVP Call Server**, and selecting a Unified CVP Call Server. Click **Edit** > **Statistics** > **IVR**.

The following table describes the IVR Service call statistics.

Table 9: IVR Service Call Statistics

Statistic	Description
Realtime Call Statistics	
Active Calls	The number of active calls being serviced by the IVR service.
Active HTTP Requests	The number of active HTTP requests being serviced by the IVR service.
Interval Statistics	
Start Time	The time the system started collecting statistics for the current interval.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
Peak Active Calls	Maximum number of active calls handled by the IVR service at the same time during this interval.

Statistic	Description
New Calls	New Calls is a metric that counts the number of New Call requests received from the IOS Gateway Service. A New Call includes the Switch leg of the call and the IVR leg of the call. This metric counts the total number of New Call Requests received by the IVR Service during this interval.
Calls Finished	A Call is a metric that represents the Switch leg of the CVP call and the IVR leg of the CVP call. When both legs of the call are finished, this metric increases. Calls Finished is a metric that counts the number of CVP Calls that have finished during this interval.
Average Call Latency	The average amount of time in milliseconds it took the IVR Service to process a New Call or Call Result Request during this interval.
Maximum Call Latency	The maximum amount of time in milliseconds it has taken for the IVR Service to complete the processing of a New Call Request or a Request Instruction Request during this time interval.
Minimum Call Latency	The minimum amount of time in milliseconds it took for the IVR Service to complete the processing of a New Call Request or a Request Instruction Request during this time interval.
Peak Active HTTP Requests	Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests being processed by the IVR Service. Peak Active Requests is a metric that represents the maximum simultaneous HTTP requests being processed by the IVR Service during this time interval.
Total HTTP Requests	The total number of HTTP Requests received from a client by the IVR Service during this time interval.
Average HTTP Requests/second	The average number of HTTP Requests the IVR Service receives per second during this time interval.
Peak Active HTTP Requests/second	HTTP Requests per Second is a metric that represents the number of HTTP Requests the IVR Service receives each second from all clients. Peak HTTP Requests per Second is the maximum number of HTTP Requests that were processed by the IVR Service in any given second. This is also known as high water marking.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.

Statistic	Description
Total New Calls	New Calls is a metric that counts the number of New Call requests received from the IOS Gateway Service. A New Call includes the Switch leg of the call and the IVR leg of the call. Total New Calls is a metric that represents the total number of new calls received by the IVR Service since system startup.
Peak Active Calls	The maximum number of simultaneous calls processed by the IVR Service since the service started.
Total HTTP Requests	Total HTTP Requests is a metric that represents the total number of HTTP Requests received from all clients. This metric is the total number of HTTP Requests received by the IVR Service since system startup.
Peak Active HTTP Requests	Active HTTP Requests is a metric that indicates the current number of simultaneous HTTP requests processed by the IVR Service. Maximum number of active HTTP requests processed at the same time since the IVR service started. This is also known as high water marking.

SIP Service Call Statistics

The SIP service call statistics include data on calls currently being processed by the SIP service, new calls received during a specified interval, and total calls processed since the SIP service started.

Access SIP service statistics either by:

- Selecting **System** > **Control Center**, selecting a Unified CVP Call Server, clicking the **Statistics** icon in the toolbar, and then selecting the **SIP** tab.
- Selecting **Device Management** > **Unified CVP Call Server** and selecting a Call Server. Click **Edit** > **Statistics** > **SIP**.

The following table describes the SIP Service call statistics.

Table 10: SIP Service Call Statistics

Statistic	Description
Realtime Statistics	
Active Calls	A real time snapshot metric indicating the count of the number of current calls being handled by the SIP service.
Total Call Legs	The total number of SIP call legs being handled by the SIP service. A call leg is also known as a SIP dialog. The metric includes incoming, outgoing, and ringtone type call legs. For each active call in the SIP service, there will be an incoming call leg, and an outgoing call leg to the destination of the transfer label.

Statistic	Description
Active Basic Service Video Calls Offered	The number of basic service video calls in progress where video capability was offered.
Active Basic Service Video Calls Answered	The number of basic service video calls in progress where video capability was answered.
Active Agent Whisper Calls	The number of active whisper call legs.
Active Agent Greeting Calls	The number of active greeting call legs.
Interval Statistics	
Start Time	The time the system started collecting statistics for the current interval.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
New Calls	The number of SIP Invite messages received by Unified CVP in the current interval. It includes the failed calls as well as calls rejected due to the SIP service being out of service.
Connects Received	The number of CONNECT messages received by SIP service in order to perform a call Transfer, in the last statistics aggregation interval. Connects Received includes the regular Unified CVP transfers as well as Refer transfers. Any label coming from the ICM service is considered a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.
Avg Latency Connect to Answer	The period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for all the calls that have been answered in the last statistics aggregation interval.
Failed SIP Transfers (Pre-Dialog)	The total number of failed SIP transfers since system start time. When Unified CVP attempts to make a transfer to the first destination of the call, it sends the initial INVITE request to set up the caller with the ICM routed destination label. The metric does not include rejections due to the SIP Service not running. The metric includes failed transfers that were made after a label was returned from the ICM Server in a CONNECT message.
Failed SIP Transfers (Post-Dialog)	The number of failed re-invite requests on either the inbound or outbound legs of the call during the interval. After a SIP dialog is established, re-INVITE messages are used to perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.

Statistic	Description
Basic Service Video Calls Offered	The number of basic service video calls offered in the current interval.
Basic Service Video Calls Answered	The number of basic service video calls answered in the current interval.
Whisper Announce Answered	The number of calls for which whisper announcement was successful during the interval.
Whisper Announce Failed	The number of calls for which whisper announcement was failed during the interval.
Agent Greeting Answered	The number of calls for which agent greeting was successful during the interval.
Agent Greeting Failed	The number of calls for which agent greeting was failed during the interval.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
Total New Calls	The number of SIP Invite messages received by Unified CVP since system start time. It includes the failed calls as well as calls rejected due to the SIP service being out of service.
Connects Received	The number of CONNECT messages received by SIP service in order to perform a Unified CVP Transfer, since system start time. Connects Received includes the regular Unified CVP transfers as well as Refer transfers. Any label coming from the ICM service is considered a CONNECT message, whether it is a label to send to the VRU or a label to transfer to an agent.
Avg Latency Connect to Answer	The period of time between the CONNECT from ICM and when the call is answered. The metric includes the average latency computation for all the calls that have been answered since system start up time.
Failed SIP Transfers (Pre-Dialog)	The total number of failed transfers on the first CVP transfer since system start time. A SIP dialog is established after the first CVP transfer is completed. The metric does not include rejections due to SIP being out of service. The metric includes failed transfers that were made after a label was returned from the ICM in a CONNECT message.

Statistic	Description
Failed SIP Transfers (Post-Dialog)	The number of failed re-invite requests on either the inbound or outbound legs of the call since start time. After a SIP dialog is established, re-INVITE messages are used to perform transfers. Re-invite requests can originate from the endpoints or else be initiated by a Unified CVP transfer from the Unified ICME script. This counter includes failures for both kinds of re-invite requests.
Total Basic Service Video Calls Offered	The total number of basic service video calls offered since system start time.
Total Basic Service Video Calls Answered	The total number of basic service video calls answered since system start time.
Total Whisper Announce Answered	The total number of call for which whisper announce was successful since the system start time.
Total Whisper Announce Failed	The total number of calls for which whisper announce failed since the system start time.
Total Agent Greeting Answered	The total number of calls for which agent greeting was successful since the system start time.
Total Agent Greeting Failed	The total number of calls for which agent greeting failed since the system start time.

View Gateway Statistics

Gateway statistics include the number of active calls, available memory, and CPU utilization.

Access Gateway statistics either by:

Procedure

- Selecting **System** > **Control Center**, selecting a Gateway, and then clicking the **Statistics** icon in the toolbar.
- Selecting **Device Management** > **Gateway**, selecting a Gateway, and then clicking the **Statistics** icon in the toolbar.

Gateway Statistics

The following table describes Gateway statistics.

Table 11: Gateway Statistics

Statistic	Description
Active Calls	Number of currently active calls handled by the gateway. For example, Total call-legs: 0 no active calls

Statistic	Description

Free Memory	Free memory, for example:
	`Processor memory free: 82%`
	`I/O memory free: 79%`

CPU Utilization	CPU utilization, for example: `CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%`

Unified CVP VXML Server Statistics

The Operations Console displays realtime, interval, and aggregate Unified CVP VXML Server statistics.

- VXML Statistics are not available if the Unified CVP VXML Server is deployed as standalone.
- To view VXML Statistics, at least one deployed Unified CVP VXML Server application must be configured with the CVPDataFeed logger.

Access Unified CVP VXML Server statistics either by:

- Selecting **System** > **Control Center**, selecting a VXML Server, and then clicking the **Statistics** icon in the toolbar.
- Selecting **Device Management** > **Unified CVP VXML Server**, and selecting a Unified CVP VXML Server. Click **Edit** > **Statistics**.

The following table describes the statistics reported by the Unified CVP VXML Server.

Table 12: VXML Server Statistics

Statistic	Description
Port Usage Statistics	
Total Ports	The total number of licensed ports for this Unified CVP VXML standalone server.
Port Usage Expiration Date	The date when the licensed ports expires for this Unified CVP VXML standalone server.
Available Ports	The number of port licenses available for this Unified CVP VXML standalone server.
Total Concurrent Callers	The number of callers currently interacting with this Unified CVP VXML standalone server. **Note** The Total Concurrent Callers statistics is not applicable for applications having only audio elements.
Real Time Statistics	

Statistic	Description
Active Sessions	The number of current sessions being handled by the Unified CVP VXML Server.
Active ICM Lookup Requests	The number of current ICM requests being handled by the Unified CVP VXML Server.
Interval Statistics	
Start Time	The time at which the current interval begins.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
Sessions	The total number of sessions in the Unified CVP VXML Server in the current interval.
Reporting Events	The number of events sent to the Unified CVP Reporting Server from the Unified CVP VXML Server in the current interval.
ICM Lookup Requests	The number of requests from the Unified CVP VXML Server to the ICM Service in the current interval.
ICM Lookup Responses	The number of responses to both failed and successful ICM Lookup Requests that the ICM Service has sent to the Unified CVP VXML Server in the current interval. In the case that multiple response messages are sent back to the Unified CVP VXML Server to a single request, this metric will increment per response message from the ICM Service.
ICM Lookup Successes	The number of successful requests from the Unified CVP VXML Server to the ICM Service in the current interval.
ICM Lookup Failures	The number of requests from the Unified CVP VXML Server to the ICM Service in the current interval. This metric will be incremented in the case an ICM failed message was received or in the case the Unified CVP VXML Server generates the failed message.
Aggregate Statistics	
Start Time	The time at which the current interval has begun.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Total Sessions	The total number of sessions in the Unified CVP VXML Server since startup.
Total Reporting Events	The total number of reporting events sent from the Unified CVP VXML Server since startup.

Statistic	Description
Total ICM Lookup Requests	The total number of requests from the Unified CVP VXML Server to the ICM Service. For each ICM lookup request, whether the request succeeded or failed, this metric will be increased by one.
Total ICM Lookup Responses	The total number of responses the ICM Service has sent to the Unified CVP VXML Server since startup. For each ICM lookup response, whether the response is to a succeeded or failed request, this metric will be increased by one. In the case that multiple response messages are sent back to the Unified CVP VXML Server to a single request, this metric will increment per response message from the ICM Service.
Total ICM Lookup Successes	The total number of requests from the Unified CVP VXML Server to the ICM Service since startup. For each ICM lookup request that succeeded, this metric will be increased by one.
Total ICM Lookup Failures	The total number of requests from the Unified CVP VXML Server to the ICM Service since startup. For each ICM lookup request that failed, this metric will be increased by one. This metric will be incremented if an ICM failed message was received or if the Unified CVP VXML Server generates a failed message.

Standalone Unified CVP VXML Server Statistics

The Operations Console displays realtime, interval, and aggregate Unified CVP VXML (Standalone) Server statistics.

Access Unified CVP VXML (Standalone) Server statistics either by:

- Selecting **System** > **Control Center**, selecting a Unified CVP VXML (Standalone) sever, and then clicking the icon in the toolbar.
- Selecting **Device Management** > **Unified CVP VXML (Standalone) Server**, and selecting a Unified CVP VXML (Standalone) server. Click **Edit** > **Statistics**.

The following table describes the statistics reported by the Unified CVP VXML (Standalone) Server.

Table 13: Unified CVP VXML (Standalone) Server Statistics

Statistic	Description
Port Usage Statistics	
Total Ports	The total number of licensed ports for this Unified CVP VXML standalone server.
Port Usage Expiration Date	The date when the licensed ports expires for this Unified CVP VXML standalone server.
Available Ports	The number of port licenses available for this Unified CVP VXML standalone server.

Statistic	Description
Total Concurrent Callers	The number of callers currently interacting with this VXML standalone server. **Note** The Total Concurrent Callers statistics is not applicable for applications having only audio elements.

View Pool Statistics

Device Pool statistics summarize the statistics for the devices that belong to the currently selected device pool.

Procedure

To view device pool statistics:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center Network Map window opens.

Step 2 Select **Pool Statistics**.

Step 3 Select **Refresh** to update the data on the Pool Statistics tab.

Related Topics

Pool Statistics Tab, on page 57

Unified CVP Reporting Server Statistics

Unified CVP Reporting Server statistics include the total number of events received from the IVR, SIP, and VXML services.

Access Reporting Server statistics either by:

- Choosing **System** > **Control Center**, selecting a Unified CVP Reporting Server, and then clicking the **Statistics** icon in the toolbar.
- Choosing **Device Management** > **Unified CVP Reporting Server**, and selecting a Unified CVP Reporting Server. Click **Edit** > **Statistics**.

The following table describes the Unified CVP Reporting Server statistics.

Table 14: Unified CVP Reporting Server Statistics

Statistic	Description
Interval Statistics	

Statistic	Description
Start Time	The time the system started collecting statistics for the current interval.
Duration Elapsed	The amount of time that has elapsed since the start time in the current interval.
Interval Duration	The interval at which statistics are collected. The default value is 30 minutes.
VXML Events Received	The total number of reporting events received from the VXML Service during this interval. For each reporting event received from the VXML Service, this metric will be increased by one.
SIP Events Received	The total number of reporting events received from the SIP Service during this interval. For each reporting event received from the SIP Service, this metric will be increased by one.
IVR Events Received	The total number of reporting events received from the IVR service in the interval. For each reporting event received from the IVR service, this metric will be increased by one.
Database Writes	The total number of writes to the database made by the Unified CVP Reporting Server during the interval. For each write to the database by the Unified CVP Reporting Server, this metric will be increased by one.
Aggregate Statistics	
Start Time	The time the service started collecting statistics.
Duration Elapsed	The amount of time that has elapsed since the service start time.
VXML Events Received	The total number of reporting events received from the VXML Service since the service started. For each reporting event received from the VXML Service, this metric will be increased by one.
SIP Events Received	The total number of reporting events received from the SIP Service since the service started. For each reporting event received from the SIP Service, this metric will be increased by one.
IVR Events Received	The total number of reporting events received from the IVR Service since the service started. For each reporting event received from the IVR Service, this metric will be increased by one.
Database Writes	The total number of writes to the database made by the Unified CVP Reporting Server since startup. For each write to the database by the Unified CVP Reporting Server, this metric will be increased by one.

Pool Statistics Tab

Device pool statistics report data on the devices contained within a device pool as described in the following table.

Table 15: Pool Statistics

Field	Description
Number of Servers in Different States	
Server Type	Unified CVP servers include: Call Servers, Unified CVP VXML Servers, Unified CVP VXML Servers (standalone), and Reporting Servers.
Total Devices	Total number of devices for each server type.
Up	Number of servers of each type that are up and running.
Down	Number of servers of each type that have down status.
Partial	Number of servers of each type that have partial status.
Not Reachable	Number of servers of each type that have a Not Reachable status.
Percentage of Servers in Different States	
Server Type	Unified CVP servers include: Call Servers, Unified CVP VXML Servers, Unified CVP VXML Servers (standalone), and Reporting Servers.
Total Devices	Total number of devices for each server type.
Up	Percentage of servers of each type that are up and running.
Down	Percentage of servers of each type that have down status.
Partial	Percentage of servers of each type that have partial status.
Not Reachable	Percentage of servers of each type that have an Unreachable status.

Related Topics

View Pool Statistics, on page 55

Sort Servers

You can choose to sort the servers in ascending and descending sort sequences: by their network status (up, down, partial, unreachable), hostname, IP address, device type, and by the number of active calls.

Procedure

To sort servers:

Procedure

Step 1 Select **System** > **Control Center**.

Step 2 Select **Device Pool** and then select a device pool from the list.

Devices that belong to the selected device pool display on the General tab.

Step 3 To sort the list of servers, click the heading for the column you want to sort by. After you sort the column, up/down arrows appear in the column headings. Click the arrows to specify the sort order for the column.

Edit Device Setup

You can edit the configuration of a device that has been added to the Operations Console.

Procedure

To edit the configuration of a device:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center Network Map window opens to the General tab.

Step 2 Click on the device hostname or select the radio button preceding the hostname and then click **Edit** on the toolbar.

The Edit Configuration window for the selected device opens.

Related Topics

Device Properties
Find Device
Past Device Setups in Operations Console Database

Start Server

You can start a Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server from the Control Center.

Related Topics

View Device Status, on page 39
View Devices by Type, on page 38
Shut Down Server, on page 59

Procedure

To start a server:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center window opens to the General tab.

Step 2 Select the Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server to restart by clicking the radio button next to the server.

Step 3 Select **Start**.

The server starts; its state displays in the Status column on the General tab.

Note By default, the device status is not refreshed. To set a refresh interval, select the desired interval from the Refresh drop-down menu.

Shut Down Server

You can shut down a Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server from the Control Center. A server instance enters the shutdown state as a result of a graceful shutdown or forced shutdown process.

During a graceful shutdown, running processes complete before the server is shut down. For example, if you want to stop the Unified CVP Call Server but want to complete the processing of calls in progress, you must choose Graceful Shutdown.

In a forceful shutdown, all processes are suspended immediately. If you were to shut down the Unified CVP Call Server forcefully, calls in progress will be immediately dropped.

Related Topics

Start Server, on page 58

Procedure

To shut down a server:

Procedure

Step 1 Select **System** > **Control Center**.

The Control Center window opens to the General tab.

Step 2 Select the Unified CVP Call Server, Unified CVP Reporting Server, or Unified CVP VXML Server to shut down by clicking the radio button next to the server.

Step 3 To shut down a server immediately, select **Shutdown**. To shut down a server gracefully, select **Graceful Shutdown**.

The selected server shuts down, and its status shows as Down in the Devices tab in the right pane of the Control Center window.

Note Graceful Shutdown is not supported by Unified CVP VXML Server.

Device Pools

A device pool is a logical group of devices. Device pools provide a convenient way to define a set of common characteristics that can be assigned to devices, for example, the region in which the devices are located. You can create device pools and assign devices to the device pools you created.

Every device you create is automatically assigned to a default device pool, which you can never remove from the selected device pool list. The Administrator account is also automatically assigned to the default device pool, which ensures that the Administrator can view and manage all devices. You cannot remove the Administrator from the default device pool.

When you create a user account, you can assign the user to one or more device pools, which allows the user to view the devices in that pool from the Control Center. Subsequently, you can remove the user from any associated device pools, which prevents that user from viewing the pool devices in the Control Center. Removing a user from the default device pool prevents the user from viewing all devices.

You can perform the following tasks using device pools:

Add Device Pool to Operations Console

This section describes how to add a device pool to the Operations Console.

Procedure

To add a device pool to the Operations Console:

Procedure

Step 1 Select **System** > **Device Pool**.

The Find, Add, Edit, Delete Device Pools window opens.

Step 2 Select **Add New**.

Step 3 In the General tab, fill in a unique name for the device pool and add a description.

Note Device pool names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.

Step 4 Select **Save** to save the device pool.

Related Topics

Device Pools, on page 60
Delete Device Pool, on page 61
Edit Device Pool, on page 61
Add or Remove Device From Device Pool, on page 62

Find Device Pool, on page 62

Edit Device Pool

You can change the name and description of any device pool, except the default device pool.

Procedure

To edit a device pool:

Procedure

Step 1 Select **System** > **Device Pool**.

The Find, Add, Delete, Edit Device Pools window opens.

Step 2 Select the device pool by clicking on its name in the device pool list or selecting the radio button preceding it and clicking **Edit**.

The Edit Device Pool Configuration window opens to the General tab.

Step 3 You can change the description. You cannot change the name of a device pool.

Step 4 Select **Save**.

Related Topics

Device Pools, on page 60
Delete Device Pool, on page 61
Add Device Pool to Operations Console, on page 60
Add or Remove Device From Device Pool, on page 62
Find Device Pool, on page 62

Delete Device Pool

This section describes how to delete a device pool from the Operations Console.

Procedure

To delete a device pool:

Procedure

Step 1 Select **System** > **Device Pool**.

The Find, Add, Edit, Delete Device Pools window opens.

Step 2 Find the device pool by using the procedure in the Finding a Device Pool topic.

Step 3 From the list of matching records, select the device pool that you want to delete.

Step 4 Select **Delete**.

Step 5 When prompted to confirm the delete operation, Select **OK** to delete or select **Cancel** to cancel the delete operation.

Related Topics

Device Pools, on page 60
Edit Device Pool, on page 61
Add Device Pool to Operations Console, on page 60
Add or Remove Device From Device Pool, on page 62
Find Device Pool, on page 62

Add or Remove Device From Device Pool

This section describes how to delete a device pool from the device pool.

Procedure

To add or remove a device from a device pool:

Procedure

Step 1 From the Device Management menu, select the type of device you want to add to a device pool. For example, to add a Call Server to a device pool, select Unified CVP Call Server from the menu.

A window listing known devices of the type you selected appears. For example, if you selected Call Server, known Unified CVP Call Servers are listed.

Step 2 Select the device pool by clicking on its name in the device pool list or by selecting the radio button preceding it and clicking **Edit**.

Step 3 Select the **Device Pool** tab.

Step 4 To add a device to a device pool, select the device pool from the **Available** pane, and then click the right arrow to move the pool to the **Selected** pane.

Step 5 To remove a device from a device pool, select the device pool from the **Selected** pane, and then click the left arrow to move the device pool to the **Available** pane.

Step 6 Click **Save** to save the changes to the Operations Console database. Some edit device screens have an Apply button. Click **Apply** to copy the configuration to the device.

Find Device Pool

Because you might have several device pools in your network, the Operations Console lets you locate specific device pools on the basis of specific criteria. Use the following procedure to locate device pools.

Procedure

To find a device pool:

Procedure

Step 1 Select **System** > **Device Pool**.

The Find, Add, Delete, Edit Device Pools window lists the available device pools 10 at a time, sorted by name.

Step 2 If the list is long, you can click the first page, previous page, next page, and last page icons on the bottom right of the screen to page through the list. Or, you can enter a page number in the **Page** field and press **enter** to go directly to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **Name**; selecting a modifier such as **begins with**; entering your search term; and clicking **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Import System Configuration

In the event of disaster recovery, you can import a system configuration and apply a previously saved configuration.

The Unified CVP Operations Console supports the import of system-level configuration data.

When you import a database which was exported from an older version, the imported database is automatically upgraded to the latest version as indicated in the confirmation message.

Note The Unified CVP import operation does not back up or restore the CVP configuration of the VoiceBrowser or the sip.properties files. If a complete restore of Unified CVP server is required, you will need to manually restore some of the content of the sip.properties file as well as the VoiceBrowser configuration in addition to importing the system configuration using the Operations Console.

Procedure

To import a system configuration:

Procedure

Step 1 Stop the Cisco CVP WebServicesManager Service:

a) Select **Start** > **All Programs** > **Administrative Tools** > **Services**.
b) Select **Cisco CVP WebServicesManager**.
c) Select **Stop**.

Step 2 Select **System** > **Import System Configuration**.

The Import System Configuration window opens.

Step 3 If you know the file name, enter it in the Enter Configuration File text box. Otherwise, select **Browse to** and search for the configuration to import.

Step 4 Select **Import**.

Step 5 Restart the Cisco CVP OPSConsoleServer and Cisco CVP WebServicesManager Services on the machine and then log in to the Operations Console again:

a) Select **Start** > **All Programs** > **Administrative Tools** > **Services**.
b) Select **Cisco CVP OPSConsoleServer**.
c) Select **Restart**.
d) Select **Cisco CVP WebServicesManager**.
e) Select **Restart**

Note All data in the Operations Console that is importing the configuration will be lost and replaced with the imported data.

Related Topics

Export System Configuration, on page 64

Export System Configuration

Using Export System Configuration on the System menu, you can save and export all the configurations of the Operations Console to a single file on your local computer. This is particularly useful in a back up scenario. For example, if the Operations Console configuration file were to become corrupt, you can import the file and restore the Operations Console configuration without having to individually reconfigure each module. Consider exporting the database on a regular basis and also when you make major configuration changes to a device.

All Operations Console configuration data is exported, except for any files you have uploaded, including application scripts. The Operations Console supports the export of system-level configuration data.

Note The Unified CVP import and export operations do not back up or restore the CVP configuration of VoiceBrowser `sip.properties` files. If you must do a complete backup and record of the Unified CVP configuration, then you must manually back up the sip.properties file and the result of the VoiceBrowser **sall** command in addition to exporting the system configuration using the Operations Console.

Procedure

To export a system configuration:

Procedure

Step 1 Select **System** > **Export System Configuration**.

The Export System Configuration window displays.

Step 2 Select **Export**.

Step 3 In the Save As dialog box, select the location to store the file.

Note You will probably save the configuration multiple times. Choose a naming convention that helps you identify the configuration, for example, include the current date and time in the file name.

Related Topics

Import System Configuration, on page 63

Location Feature

Use the Location feature to route calls locally to the agent available in the branch office, rather than routing calls to centralized or non-geographical numbers. This system-level feature allows you to select a Unified CM server and extract the Unified CM location information (location provider). Once the administrator initiates the synchronization, the system retrieves the location information for all available Unified CM servers which have been identified as sources for location information.

After you have enabled synchronization for a Unified CM server, information can be retrieved from any of the Unified CM servers that have been identified as sources for location information.

Prerequisites:

- Ensure that the device type (Gateway / Virtualized Voice Browser) is already configured.
- The device Location ID information, if configured in the Location configuration page, is displayed as a read-only field.
- Any configurable fields remain empty if they were not configured by the user.

Note If a location is associated with more than one Gateway / Virtualized Voice Browser, the system displays multiple rows of the same location information for each associated device.

Note All Unified CM servers enabled for synchronization are used during the synchronization task. If you do not want a particular Unified CM to be used when the synchronization task is performed, then disable synchronization for that Unified CM.

The following table describes the settings used to configure the Location feature.

You can perform the following tasks:

View Location Information

Procedure

To view location-based information:

Procedure

Step 1 Select **System** > **Location**.

Location information is listed on the Location tab. The Location tab displays the retrieved location information where you can edit and configure additional information.

If a location is associated with more than one Gateway / Virtualized Voice Browser, the same location information is presented in multiple rows. Only the associated device column differs.

Step 2 Click the required device to launch the device configuration window.

Related Topics

Location Feature, on page 65
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Edit Location Information, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Insert Site Identifiers

The Site Identifier insert applies to all selected call servers using the Location configuration.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Edit Location Information, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To insert site identifiers:

Procedure

Select **System** > **Location**.

Site identifier information is listed on the General tab.

Three options are available to identify the site information:

- Insert site identifier between the Network VRU label and the correlation ID
- Insert site identifier at the beginning of the Network VRU label
- Do not insert site identifier

Deploy Location Information

By default, location information is deployed to all associated Call Servers. You can choose to deploy location information to one or more Call Servers.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Add Locations, on page 69
Edit Location Information, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To deploy location information:

Procedure

Step 1 Selects **System** > **Location**.

Step 2 After making the required configuration changes, you have two options to save the configuration:

- Selects **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save the location information and initiate a deployment request to the selected Call Servers.

  See View Location Deployment or Synchronization Status, on page 72 for details on viewing the status information.

- Selects **Save** to save three components to the database: the location information, information in the General tab, and the associated Call Servers.

Caution In the following cases, the Deployment Status displays a warning message:

- If you have only saved the configuration details and have not deployed them.
- If you have edited or deleted an existing configuration and have not deployed the changes.
- If you changed the call server association.

Error Scenario Deployment

The following table provides the status, and workaround for the deployment error scenarios.

Status	Workaround
Unable to access the database.	Restart the Operations Console service. Try again. Contact your administrator.
General failure.	There is an unknown error in deployment. Contact your administrator.
The device was not deployed.	Deploy the device first. Try again.
The device was not deployed.	Cannot remove from the database.
The device could not be reached.	Check the network connection by pinging the device. Check the firewall setting. Turn off the firewall if the firewall is on. If it is available, check if WebServicesManager service is on. Try again later.
The device is using an unknown version of the Unified CVP software.	Upgrade to the compatible version, then deploy again.
The device is using an unknown version of the Unified CVP software.	Cannot remove.
Device has no SIP Subsystem	If OAMP has deployed SIP Server Group to the call server, delete the call server, and re-create the call server with a SIP Subsystem; or, do not select Call Servers with No SIP when deploying SIP Server Group configuration.

Add Locations

You can manually add location information for locations that do not exist in the Unified CM database.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Edit Location Information, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To add locations:

Procedure

Step 1 Select **System** > **Location**.

Step 2 On the **Location** tab, select **Add New**.

The Location Configuration window opens.

Step 3 Assign the Location, Site ID, Location ID, and the Unified CM IP Address as applicable to your configuration.

Step 4 Optionally, select the required Gateway / Voice Browser by moving it/them to the Selected column.

Step 5 Select **Save** or **Cancel**.

Edit Location Information

You can only select a single location for this operation.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To edit the required location:

Procedure

Step 1 Select **System** > **Location**.

Step 2 On the **Location** tab, select the required location in one of two ways:

- Select the check box for the required location and click **Edit**.
- Select the required location in the Location tab.

Step 3 Make the required changes and click **Save** or **Cancel** as applicable.

Delete Location

You can delete one or more locations at the same time.

Only manually-configured and invalid locations can be deleted.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Edit Location Information, on page 69
Synchronize Location Information, on page 71
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To delete a location:

Procedure

Step 1 Select **System** > **Location**.

Step 2 Select the required locations.

Step 3 On the **Location** tab, select **Delete**.

A prompt window appears to confirm your intention.

Step 4 Respond to the prompt (Proceed with Delete? OK | Cancel).

This prompt may differ if you select a location which cannot be deleted.

When you make your selection, the Location tab refreshes to display the results of your deletion in the message bar.

Synchronize Location Information

Location synchronization is a user-initiated task in the Operations Console. A single synchronization task runs in the background when initiated. When initiated, the system synchronizes and merges the location information for all Unified CM servers selected during the configuration. There are two sub-tasks to complete a synchronizing operation:

Procedure

- Synchronization: The system retrieves the location data from Unified CM database.
- Merge: The system merges the retrieved data with existing location data in the Operations Console database.

What to do next

Note The Location synchronization feature in the Operations Console only works with Unified CM.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Edit Location Information, on page 69
Delete Location, on page 70
View Location Deployment or Synchronization Status, on page 72
Find Location, on page 73

Procedure

To synchronize and refresh the location information with the Unified CM server and merge the information with the Operations Console database:

Procedure

Step 1 Configure and save one or more Unified CM devices with synchronization enabled.

Step 2 Select **System** > **Location**.

Step 3 Select **Synchronize**.

The synchronization process is initiated.

Note Only one synchronization or deployment process can run at any given time. If one process is already running, you receive an error message stating the same.

Step 4 Click **Refresh** to view the retrieved location information after the synchronization process is completed.

Synchronize Error Scenarios

The following table provides the status, cause, and workaround for the synchronization error scenarios.

Status	Workaround
Not able to connect with the device.	Check the network connection by pinging the device. If the device is connected, try again.
User credentials are not correct. User can't be authenticated.	Check the user credentials.
Host name is unknown. Check the host name.	The host name is not correct. Verify the host name.
Web Service is not available on the device.	Determine if the AXL Web Service is available on the device. Enable the AXL Web Service on the device.
General database failure.	Restart your Operations Console service. Try again. If the problem persists, contact your administrator.
General failure.	There is an unknown error in synchronization. Contact your administrator.

View Location Deployment or Synchronization Status

Deployment and Synchronization operations can be time consuming depending on the number of Call Servers or Unified CMs. When either process is running, you can select a status report to view the progress of the last initialized deployment or synchronization request.

Note The Deployment and Synchronization operations are mutually exclusive. Only one synchronization or deployment process can run at any given time. If one process is already running, you cannot initiate another process and you receive an error message.

The following information applies to the Status window:

Procedure

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one call server can be deployed at any given time. The other call servers are either in the queue or in an already successful/failed state.

Related Topics

Location Feature, on page 65
View Location Information, on page 66
Insert Site Identifiers, on page 66
Deploy Location Information, on page 67
Add Locations, on page 69
Edit Location Information, on page 69
Delete Location, on page 70
Synchronize Location Information, on page 71
Find Location, on page 73

Procedure

To show deployment or synchronization results:

Procedure

Step 1 Select **System** > **Location**.

Step 2 From the toolbar, select **Status**.

- To view synchronization results, select **Synchronization Status**.
- To view deployment results, select **Deployment Status**.

Step 3 Select **Refresh** to view the updated status information.

See View System-Level Operation States, on page 15 for more details on each state.

Find Location

Procedure

To show deployment and/or synchronization results:

Procedure

Step 1 Select **System** > **Location**.

Step 2 To scroll through multiple pages of the list, select the first, previous, next, and last page icons on the bottom left to view the next group of available notification destinations.

Step 3 You can filter the list by using the filter at the top right of the list. Select a field to search, a modifier (such as *Starts with*), and then select **Find**. The filter is not case-sensitive and wildcards are not allowed.

SIP Server Groups

In Unified CVP, you can add server groups at the system level to perform SIP dynamic routing.

A Server Group consists of one or more destination addresses (endpoints) and is identified by a Server Group domain name. This domain name is also known as the SRV cluster name, or Fully Qualified Domain Name (FQDN). Server Groups contain Server Group Elements.

View SIP Server Groups

SIP Server Groups

- General tab
- Heartbeat Properties tab
- Call Server Deployment tab

General tab

The General tab displays the list of SIP Server Groups and SIP Server Group Elements

Table 16: General Tab

Column	Description
Name	The name of the SIP Server Group. Nested under the SIP Server Group are the SIP Server Group Elements. Clicking the +/- icon next to the SIP Server Group name expands and collapses the elements within the group. Additionally, you can use **Collapse all** and **Expand all** to collapse/expand all the elements within the server groups listed on the page.
Number of Elements	The number of elements contained in the group.
Port	Port number of the element in the server group.
Secure Port	The listening port for secure connection.
Priority	Priority of the element in relation to the other elements in the server group. Specifies whether the server is a primary or backup server. Primary servers are specified as 1.
Weight	Weight of the element in relation to the other elements in the server group. Specifies the frequency with which requests are sent to servers in that priority group.

Note Clicking any of the column headers on this list sorts the list.

Heartbeat Properties tab

Note The Up and Down Endpoint Heartbeat Interval is between any two heartbeats; however, it is not between heartbeats to the same endpoint. The SIP Server Group does not wake up at specific interval and send a heartbeat for all elements since this approach can result in CPU utilization issues. It also takes more resources to track heartbeats for many endpoints. For example, for 3 total elements across all SIP Server Groups, to proactively send a heartbeat to each element at 30000ms (30 seconds) intervals, you have to set the Endpoint Heartbeat Interval to 10000ms (10 seconds). It is less deterministic for reactive mode since elements that are currently down can fluctuate so the heartbeat interval fluctuates with it. To turn off pinging when the element is UP, set the UP interval to zero (reactive pinging). To turn off pinging when the element is down, set the DOWN interval to zero (proactive pinging). To ping when the element is either UP or DOWN, set both the intervals to greater than zero (adaptive pinging).

Table 17: Heartbeat Properties Tab

Property	Description	Default	Value
Use Heartbeats to Endpoints	Select to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled. **Note** Endpoints that are not in a Server Group can not use the heartbeat mechanism.	Disabled (unchecked)	Enabled or Disabled
Number of failed Heartbeats for unreachable status	The number of failed heartbeats before marking the destination as unreachable.	3	1 through 5
Heartbeat Timeout (ms)	The amount of time, in milliseconds, before timing out the heartbeat.	800 milliseconds	100 through 3000

Property	Description	Default	Value
Up Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is up.	5000 milliseconds	5000 through 3600000
Down Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is down.	5000 milliseconds	5000 through 3600000
Heartbeat Local Listen Port	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067	0 through 65000
Heartbeat SIP Method	The heartbeat SIP method. **Note** PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS	OPTIONS or PING

Property	Description	Default	Value
Heartbeat Transport Type	During transportation, Server Group heartbeats are performed with a UDP or TCP socket connection. If the Operations Console encounters unreachable or overloaded callbacks invoked in the Server Group, that element is marked as being down for both UDP and TCP transports. When the element is up again, it is routable for both UDP and TCP. **Note** TLS transport is not supported.	UDP	UDP or TCP
Overloaded Response Codes	The response codes are used to mark an element as *overloaded* when received. If more than one code is present, it is presented as a comma delimited list. An OPTIONS message is sent to an element and if it receives any of those response codes, then this element is marked as overloaded.	503,480,600	1 through 128 characters. Accepts numbers 0 through 9 and/or commas (,).

Property	Description	Default	Value
Options Override Host	The contact header hostname to be used for a heartbeat request (SIP OPTIONS). The given value is added to the name of the contact header of a heartbeat message. Thus, a response to a heartbeat would contain gateway trunk utilization information.	cvp.cisco.com	Valid hostname, limited to 128 characters.

The **Heartbeats Estimation** section displays the Total Server Groups and Elements, and the Estimated Heartbeat interval for the current configuration.

The **Call Server Deployment** tab allows you to select to which Unified CVP Call Servers to deploy the SIP Server Groups.

You can perform the following tasks:

- Add SIP Server Group, on page 78
- Delete SIP Server Group, on page 80
- Edit SIP Server Group, on page 80 (including adding, deleting, or editing SIP Server Group Elements)
- Find SIP Server Groups, on page 81
- Deploy SIP Server Group Configurations, on page 82
- View SIP Server Groups Deployment Status, on page 83

Add SIP Server Group

Procedure

To add a SIP Server Group:

Procedure

Step 1 In the Operations Console, select **System** > **SIP Server Groups**.

The SIP Server Groups window opens.

Step 2 Select **Add New**.

Step 3 Fill in the appropriate configuration settings:

Table 18: SIP Server Group Configuration Settings

Property	Description	Default	Value
SIP Server Group Configuration			
Server Domain Name FQDN	The Server Group Fully Qualified Domain Name (FQDN).	None	Up to 128 characters Must be unique. Must be a Fully Qualified Domain Name.
SIP Server Group Elements Enter the properties below and click **Add** to add the element to the SIP Server Group. Highlight any of the configured SIP Server Group Elements in the box below the property fields and; • To remove the element from the group, highlight the element and click **Remove** • To replace a selected element with the new element, edit the SIP Server Group Elements properties, highlight an existing element in the text box, and then click **Replace**.			
IP Address/Hostname	IP address or hostname of the Server Group Element.	None	Valid IP address or hostname
Port	Port number of the element.	5060	1 through 65535
Secure Port	The listening port for secure connection.	None	5061
Priority	Priority of the element in relation to the other elements in the server group. Specifies whether the server is a primary or backup server. Primary servers are specified as 1.	10	1 through 2147483647
Weight	Weight of the element in relation to the other elements in the server group. Specifies the frequency with which requests are sent to servers in that priority group.	10	10 through 2147483647

Step 4 Select **Save** to save the SIP Server Group.

You are returned to the **SIP Server Groups** page. To deploy the SIP Server Groups, you must associate a Unified CVP Call Server. Select the **Call Server Deployment** tab, select a Unified CVP Call Server and then click **Save & Deploy**. See Deploy SIP Server Group Configurations, on page 82.

Related Topics

View SIP Server Groups

Delete SIP Server Group

Note If you only want to delete elements within the group, see Edit SIP Server Group, on page 80.

To delete a SIP Server Group:

Procedure

Step 1 Select **System** > **SIP Server Groups**.

The SIP Server Group page opens.

Step 2 Find the SIP Server Group by using the procedure in Find SIP Server Groups, on page 81.

Step 3 Select the radio button next to the SIP Server Group that you want to delete and click **Delete**.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

Edit SIP Server Group

To configure a SIP Server Group, you must first define a FQDN and add it to the list.

Procedure

To edit a SIP Server Group:

Procedure

Step 1 In the Operations Console, select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window opens.

Step 2 On the **Server Groups Configuration** tab, define a FQDN for the server and select **Add** to add it to the list box.

Step 3 Fill in the appropriate configuration settings, as shown in the following table:

Table 19: SIP Server Group Configuration Settings

Property	Description	Default	Value
SIP Server Group Configuration			

Property	Description	Default	Value
Server Domain Name FQDN	The Server Group Fully Qualified Domain Name (FQDN). **Note** This field is not editable	None	Up to 128 characters Must be unique. Must be a Fully Qualified Domain Name.
SIP Server Group Elements Enter the properties below and click **Add** too add the element to the SIP Server Group. Highlight any of the configured SIP Server Group Elements in the box below the property fields and; • To remove the element from the group, highlight the element and click **Remove**, or • To replace a selected element with the new element, edit the SIP Server Group Elements properties, highlight an existing element in the text box, and then click **Replace**.			
IP Address/Hostname	IP address or hostname of the Server Group Element.	None	Valid IP address or hostname
Port	Port number of the element.	5060	1 through 65535
Secure Port	The listening port for secure connection.	None	5061
Priority	Priority of the element in relation to the other elements in the server group. Specifies whether the server is a primary or backup server. Primary servers are specified as 1.	1	1 through 2147483647
Weight	Weight of the element in relation to the other elements in the server group. Specifies the frequency with which requests are sent to servers in that priority group.	10	10 through 2147483647

Step 4 Click **Save** to save the SIP Server Group.

You are returned to the **SIP Server Groups** page. To deploy the SIP Server Groups, click **Save & Deploy** to save and deploy the edited configuration.

Find SIP Server Groups

To find a SIP Server Group:

Procedure

Step 1 Select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window displays.

Step 2 If the list is long, you can click the first page, previous page, next page, and last page icons on the bottom right of the screen to page through the list. Or, you can enter a page number in the **Page** field and press *enter* to go directly to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **SIP Server Group Name** then selecting a modifier, such as **begins with**, and entering your search term then clicking **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Deploy SIP Server Group Configurations

The Operations Console displays all configured SIP Server Groups. This section identifies the procedure to deploy a SIP Server Group.

Procedure

To deploy SIP Server Group configurations:

Procedure

Step 1 In the Operations Console, select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window opens.

Step 2 Click the **Call Server Deployment** tab.

Step 3 From the **Available** list box, select one or more Call Servers and use the arrow button to move your selection to the **Selected** list box.

Step 4 After making the required configuration changes, you have two options to save the configuration:

- Click **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save the SIP server information and initiate a deployment request to the selected devices.

  See View SIP Server Groups Deployment Status, on page 83 for details on viewing the status information.

- Click **Save** to save the configuration to the Operations Console database.

Note In the following cases, the Deployment Status displays a warning message:

- If you have only saved the SIP server details and have not deployed them.
- If you have edited or deleted an existing configuration and have not deployed the changes.
- If you changed the call server association.

Note

- Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you receive an error message stating the same.

  A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

- The SIP Server Group configuration is not specific to a single CVP. It is global and applied to all CVPs. Therefore, every time the selected Call Servers are configured, the de-selected server configurations are erased.

See View System-Level Operation States, on page 15 for more details on each state.

View SIP Server Groups Deployment Status

The Operations Console displays all configured SIP Server Groups. If a deployment fails because the call server is not accessible (either not deployed or off line) or is not upgraded to the current version, the Operations Console issues a descriptive message.

Deployment operations can be time consuming, depending on the number of Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

Note The Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message stating the same.

The following information applies to the Status window:

Procedure

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one call server can be deployed at any given time. The other call servers are either in the queue or in an already successful/failed state.

Procedure

To view Call Server deployment status:

Procedure

Step 1 In the Operations Console, select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window opens.

Step 2 From the toolbar, click **Deployment Status**.

Step 3 Optionally, instead of Step 2, you can also click **Deployment Status** at the bottom right corner of the window.

The Operations Console provides status information for SIP Server Group (including the Operation Console's server time stamp). In case of a failure, the Operations Console provides a reason for the failure.

See View System-Level Operation States, on page 15 for more details on each state.

Dialed Number Pattern

You can perform the following tasks on Dialed Number Patterns:

- Add Dialed Number Pattern
- Delete Dialed Number Pattern
- Edit Dialed Number Pattern
- **Collapse All** - Collapse all hierarchical table entries to display root entries only.
- **Expand All** - Expand all hierarchical table entries to display all entries.
- **Pagination** - The bottom of the list display contains pagination fields to go to a specific page, go to the first page, go to the previous page, go to the next page, and go to the last page in the table list.
- View Dialed Number Pattern Deployment Status The Call Server(s) do not require a restart for the changes to take affect after clicking the **Deploy** button.
- View Dialed Number Pattern Deployment Status Display the deployment status for the previous deployment to configured Call Servers.

You can select the **Display Pattern Type** to display all configured Dialed Number Patterns in a tree-hierarchy view. Available selections are:

- Display All (default)
- Local Static Route
- Send Calls to Originator
- RNA Timeout for Outbound Calls
- Custom Ringtone
- Post Call Survey for Incoming Calls

Once the view is selected, a table containing the Dialed Number Patterns for the respective, selected type displays. The current view for the dialed number system-level configuration list page is maintained until the user session expires, either by timeout or by signing out from the Operations Console, or until the dialed number pattern view type selection changes.

Each dialed number pattern is displayed as a row. Each dialed number pattern column type can be sorted alphabetically in ascending or descending order. The Dialed Number list is in hierarchical format which lets you collapse or expand individual entries. One or more root hierarchical rows can be selected using the check-boxes. All table entries are expanded by default or after certain operations like sorting, filtering, or pagination.

The column types are as follows:

Dialed Number Pattern - The actual dialed number pattern.

Description - The dialed number pattern description.

You may also use the filtering function to filter for specific Dialed Number Patterns. Only the Dialed Number Pattern itself is filterable by the standard constraint criteria (that is, begins with, contains, ends with, is exactly, is empty). The Dialed Number Pattern list also has sortable columns.

Add Dialed Number Pattern

Procedure

To add a new Dialed Number Pattern:

Procedure

Step 1 In the Operations Console, select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern window opens.

Step 2 Select **Add New**.

Step 3 Fill in the appropriate configuration settings:

Table 20: Dialed Number Pattern Configuration Settings

Property	Description	Default	Value
General Configuration			

Property	Description	Default	Value
Dialed Number Pattern	The actual Dialed Number Pattern.	None	Must be unique. Maximum length of 24 characters. Can contain alphanumeric characters, wildcard characters such as exclamation mark (!) or asterisk (*), or single digit matches such as the uppercase letter X or period (.). **Note** Lowercase letter x cannot be used as a wildcard. Can end with an optional greater than (>) wildcard character.
Description	Information about the Dialed Number Pattern.	None	Maximum length of 1024 characters.
Dialed Number Pattern Types			

Property	Description	Default	Value
Enable Local Static Route	Enable local static routes on this Dialed Number Pattern. If Local Static Routes are enabled: • **Route to Device -** Select the device from the drop-down list which contains a list of configured, supported devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **Route to SIP Server Group -** Select the device from the drop-down list which contains a list of configured, support devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **IP Address/Hostname/Server Group Name -** If you have not selected a **Route to Device** or **Route to SIP Server Group**, enter the IP address, hostname, or the server group name of the route. **Note** The hostname or IP address of a static route is validated at startup and configuration deployment time with a DNS lookup resolution. If the hostname does not resolve to an A record or SRV (static route validation) record, then the route is disabled and a notice is printed in the Unified CVP error log. The calls cannot pass to this route in this state. If the host is in the local SRV Server Groups configuration as an SRV name, then the host is not checked, because it resolves to a local SRV name. IP addresses pass the validation	Disabled	Maximum length of 128 characters. Must be a valid IP address, hostname, or fully qualified domain name.
Enable Send Calls to Originator	Enables calls to be sent to originator.	Disabled	n/a
Enable RNA Timeout for Outbound Calls	Enables Ring No Answer (RNA) timer for outbound calls. • **Timeout -** Enter the timeout value in seconds.	Disabled none	n/a Valid integer in the inclusive range from 5 to 60.

Property	Description	Default	Value
Enable Custom Ringtone	Enables customized ring tone. • **Ringtone media filename -** Enter the name of the file that contains the ringtone.	Disabled none	Maximum length of 256 characters. Cannot contain whitespace characters.
Enable Post Call Survey for Incoming Calls	Enables post call survey for incoming calls. • **Survey Dialed Number Pattern -** Enter the survey dialed number pattern.	Disabled none	n/a Maximum length of 24 characters Accepts only alphanumeric characters

Step 4 Click **Save** to save the Dialed Number Pattern.

You are returned to the **Dialed Number Pattern** page. To deploy the Dialed Number Pattern configuration, click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

Delete Dialed Number Pattern

Procedure

Deleting a dialed number pattern deletes the entire dialed number pattern and all dialed number pattern types associated with that dialed number pattern. You can check one or more dialed number pattern check boxes and select **Delete**.

To delete a Dialed Number Pattern:

Procedure

Step 1 Select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern window opens.

Step 2 Find the Dialed Number Pattern.

Step 3 Select the radio button next to the Dialed Number Pattern that you want to delete and click **Delete**.

Step 4 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation. If confirmed, the delete operation proceeds and a message displays the results. If canceled, no

operation will occur. The end-user will be presented with an error message if the delete button is selected and no check boxes are checked.

Edit Dialed Number Pattern

To edit a Dialed Number Pattern, you must first define a Dialed Number Pattern.

Procedure

To edit a Dialed Number Pattern:

Procedure

Step 1 In the Operations Console, select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern Configuration window opens.

Step 2 Select the Dialed Number Pattern and click **Edit**.

Step 3 Modify the appropriate configuration settings:

Table 21: Dialed Number Pattern Configuration Settings

Property	Description	Default	Value
General Configuration			
Dialed Number Pattern	The actual Dialed Number Pattern. This field is read-only.	n/a	n/a
Description	Information about the Dialed Number Pattern.	None	Maximum length of 1024 characters

Property	Description	Default	Value
Enable Local Static Route	Enable local static routes on this Dialed Number Pattern. If Local Static Routes are enabled: • **Route to Device -** Select the device from the drop down list which contains a list of configured, supported devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **Route to SIP Server Group -** Select the device from the drop down list which contains a list of configured, support devices. Once a selection is made, the IP Address/Hostname/Server Group Name field is automatically updated with the IP Address of the selected device. • **IP Address/Hostname/Server Group Name -** If you have not selected a **Route to Device** or **Route to SIP Server Group**, enter the IP address, hostname, or the server group name of the route.	Disabled	Maximum length of 128 characters Must be a valid IP address, hostname, or fully qualified domain name
Enable Send Calls to Originator	Enables calls to be sent to originator.	Disabled	n/a
Enable RNA Timeout for Outbound Calls	Enables Ring No Answer (RNA) timer for outbound calls. • **Timeout -** Enter the timeout value in seconds.	Disabled none	n/a Valid integer in the inclusive range from 5 to 60.
Enable Custom Ringtone	Enables customized ring tone. • **Ringtone media filename -** Enter the name of the file that contains the ringtone.	Disabled none	Maximum length of 256 characters Cannot contain whitespace characters
Enable Post Call Survey for Incoming Calls	Enables post call survey for incoming calls. • **Survey Dialed Number Pattern -** Enter the survey dialed number pattern.	Disabled none	n/a Maximum length of 24 characters Accepts only alphanumeric characters

Step 4 Click **Save** to save changes to the Dialed Number Pattern.

You are returned to the **Dialed Number Pattern** page. To deploy the Dialed Number Pattern configuration, click **Deploy** to deploy the configuration to all Unified CVP Call Server devices.

Find Dialed Number Patterns

Procedure

To find a Dialed Number Pattern:

Procedure

Step 1 Select **System** > **Dialed Number Pattern** from the Main menu.

The Dialed Number Pattern Configuration window opens.

Step 2 If the list is long, you can click the first page, previous page, next page, and last page icons on the bottom right of the screen to page through the list. Or, you can enter a page number in the **Page** field and press **enter** to go directly to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **Dialed Number Pattern Name** then selecting a modifier, such as **begins with**, and entering your search term then clicking **Find**.

Note The filter is not case-sensitive, and wildcard characters are not allowed.

Deploy Dialed Number Pattern

You can deploy all configured dialed number patterns to all configured Unified CVP Call Server devices.

Procedure

To deploy Dialed Number Pattern configurations:

Procedure

Step 1 In the Operations Console select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern Configuration window opens.

Step 2 Select one or more Dialed Number Patterns. Use the check box to the left of the Dialed Number Pattern column header to select all Dialed Number Patterns.

Step 3 Click **Deploy** in the in the bottom right corner of this page to initiate a deployment request to the Unified CVP Call Servers.

Note In the following cases, the Deployment Status displays a warning message:

- No Unified CVP Call Server devices are configured
- A Dialed Number Pattern deployment is already in progress

You will receive a success message if at least one Unified CVP Call Server is configured, using the system-level configuration, and no dialed number pattern deployment task is currently in progress. No restart is required on a successful deployment to each Unified CVP Call Server device.

Note Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message.

A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

View Dialed Number Pattern Deployment Status

The Operations Console displays all configured Dialed Number Patterns. If a deployment fails because the Unified CVP Call Server is not accessible (either not deployed or off line) or is not upgraded to the current version, the Operations Console issues a descriptive message.

The Dialed Number Pattern Deployment Status page displays the last recorded deployment status per configured Unified CVP Call Server. You may refresh the page, view online help, or go back to the dialed number pattern list page. You may also sort (in alternating ascending and descending order) the Deployment Status table contents by the following column fields: Hostname, IP Address, Device Type Status, or Last Updated.

Deployment operations can be time consuming, depending on the number of Unified CVP Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

Note The Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If one process is already running, you will not be able to initiate another process and you will receive an error message.

The following information applies to the Status window:

Procedure

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP Call Server can be deployed at any given time. The other call servers are either in the queue or in an already successful/failed state.

Procedure

To view Call Server deployment status:

Procedure

Step 1 In the Operations Console, select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern Configuration window opens.

Step 2 Select **Deployment Status** at the bottom right corner of the window.

The Operations Console provides status information for Dialed Number Pattern. In case of a failure, the Operations Console provides a reason for the failure.

Web Services

Unified CVP offers a Web Services-based framework to deliver a common user experience across all Cisco Unified Communications applications for features such as setting preferences, directories, and communication logs; setting serviceability parameters; and collecting, analyzing, and reporting on information necessary to manage and troubleshoot Cisco Unified Communications solution. This centralized framework enables consistency between Cisco Unified Communications applications and ensures a unified view of common serviceability operations.

The Web Services application handles API queries from external clients for CVP diagnostic information.

The Operations Console interfaces with the Web Services application in two ways:

- **Web Services User Management:** The Operation Console administrator can configure new Web Services users (users with the Web Services user role type). The Operations Console administrator can also manually push any configured Web Services users using the procedure identified in Set Up Web Services, on page 94.

  When you make Web Services user information changes and when you successfully deploy a device, all Web Services users are *automatically* pushed to the deployed Unified CVP devices listed below:

  - Unified CVP Call Server
  - Unified CVP Reporting Server
  - Unified CVP VXML Server
  - Unified CVP VXML Server (standalone)
  - CVP Remote Operations device

  External clients may connect to the Web Services application and authenticate themselves with these credentials.

- **List Application Servers:** The Operations Console currently stores configuration details for all devices in the database. The Operations Console writes this information to a device file which the Web Services application uses to reply to queries from external clients.

To configure Web Services, see Set Up Web Services, on page 94.

To view deployed Web Services configuration, see View Web Services Deployment Status, on page 94.

Set Up Web Services

You can manually deploy configured Web Services users to Unified CVP devices.

Procedure

To manually deploy Web Services configurations:

Procedure

Step 1 Select **System** > **Web Services**.

The Web Services Configuration window opens.

Step 2 There is no configuration on the general tab. Optionally, select the **Remote Operations Deployment** tab to configure remote operations deployment.

Step 3 To associate Unified CVP Remote Operations with a third-party device, on the remote applications deployment tab:

Provide the IP Address and Hostname, and optionally a description, of the third-party device.

Click **Add** to add the device to the list of devices associated with this Unified CVP deployment's web services.

Note The third-party device must have CVP Remote Operations installed.

Step 4 Click **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save and deploy the configuration to the impacted devices in the Operations Console database.

See View Web Services Deployment Status, on page 94 for details on viewing the status information.

View Web Services Deployment Status

You can verify the latest deployment status of the Web Services configuration. The deployment status is listed for each Unified CVP device.

Procedure

To view the deployment status of Web Services configurations:

Procedure

Step 1 Select **System** > **Web Services**.

The Web Services Configuration window opens.

Step 2 From the toolbar, click **Deployment Status**.

The Web Services Deployment Status window displays the device IP address and current status.

See View System-Level Operation States, on page 15 for more details on each state.

IOS Setup

The Operations Console supports the ability to configure IOS gateways using templates. Templates are text files that contain the IOS commands required for use in a Unified CVP deployment. You can deploy the configuration defined in the template to a gateway right from the Operations Console. You can also rollback the configuration on the gateway to the point immediately before the template was deployed.

Note There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

You can use the included default templates or create custom templates. The templates are text files that can be edited locally and then uploaded to the Operations Console.

The templates contain variables that are placeholders for configuration data. The variables can reference data that is in the Operations Console database as well as reference data that is outside of the Operations Console database, if it is accessible to the Operations Console (such as some portions of the Unified ICM database). The variables are replaced with the actual values of the data when the template is sent to the IOS Gateway.

Templates are located in the following directories on the Operations Console server:

- **Default Templates** - %CVP_HOME%\OpsConsoleServer\IOSTemplates\default
- **Custom Templates** - %CVP_HOME%\OpsConsoleServer\IOSTemplates\custom

IOS Configuration consists of :

- Template Management - Add, Delete, Edit, Copy, and View details about templates.
- Template Deployment - preview & deploy, view deployment status, and rollback template deployments.

See Also :

IOS Template Format

The IOS template must have a specific format to be accepted by the Operations Console:

- The second should be a configure terminal command, such as:

  conf t

See View Template Details for examples of the remaining configuration. With the exception of variables, all of the commands use standard IOS syntax.

The variables that can be used are detailed below:

Component	Variables
Unified CVP Call Server	• %CVP.Device.CallServer.General.IP Address% • %CVP.Device.CallServer.ICM.Maximum Length of DNIS% • %CVP.Device.CallServer.ICM.New Call Trunk Group ID% • %CVP.Device.CallServer.ICM.Pre-routed Call Trunk Group ID% • %CVP.Device.CallServer.SIP.Outbound SRV Domain Name/Server Group Domain Name (FQDN)% • %CVP.Device.CallServer.SIP.Outbound Proxy Port% • %CVP.Device.CallServer.SIP.Port number for Incoming SIP Requests% • %CVP.Device.CallServer.SIP.DN on the Gateway to play the ringtone% • %CVP.Device.CallServer.SIP.DN on the Gateway to play the error tone% • %CVP.Device.CallServer.SIP.Generic Type Descriptor (GTD) Parameter Forwarding% • %CVP.Device.CallServer.SIP.PrependDigits - Number of Digits to Strip and Prepend% • %CVP.Device.CallServer.SIP.UDP Retransmission Count% • %CVP.Device.CallServer.IVR.Media Server Retry Attempts% • %CVP.Device.CallServer.IVR.IVR Service Timeout% • %CVP.Device.CallServer.IVR.Call Timeout% • %CVP.Device.CallServer.IVR.Media Server Timeout% • %CVP.Device.CallServer.IVR.ASR/TTS Server Retry Attempts% • %CVP.Device.CallServer.IVR.IVR Service Retry Attempts%
Unified CVP Reporting Server	%CVP.Device.ReportingServer.General.IP Address%
Unified CVP VXML Server	%CVP.Device.VXMLServer.General.IP Address%
Gateway	• %CVP.Device.Gateway.Target.IP Address% • %CVP.Device.Gateway.Target.Trunk Group ID% • %CVP.Device.Gateway.Target.Location ID%
SIP Proxy Server	%CVP.Device.SIPProxyServer.General.IP Address%

Component	Variables
Speech Server	`%CVP.Device.Speech Server.General.IP Address%`
Unified Communications Manager	`%CVP.Device.Unified CM.General.IP Address%`
Media Server	`%CVP.Device.Media Server.General.IP Address%`

IOS Template Management

You use this page to manage IOS templates.

You can perform the following tasks:

Add New Template

To add a new template:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management page opens.

Step 2 From the toolbar, select **Add New**.

The IOS Template Configuration page opens.

Step 3 Click **Browse** to browse to a template file on your local computer. Provide a name for the template and an optional description. Click **Save** to upload the template file to the Operations Console.

Note The file you select to upload must be of a valid file format or the upload fails. See IOS Template Format, on page 95 for details on the format required and the variables that you can use in your template.

A message is displayed confirming successful upload if the file is valid.

Delete Templates

Note You cannot delete default templates. Only custom templates can be deleted.

To delete templates:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management page opens.

Step 2 Select the checkboxes next to the templates you want to delete.

Step 3 From the toolbar, select **Delete**.

A confirmation appears. Select **OK** to proceed and delete any custom templates selected.

Edit Templates

You can edit templates. You can change the description of any template. You can edit the body of custom templates from within the browser. You cannot edit the body of default templates.

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management window opens.

Step 2 Select the check box next to the template you want to Edit.

Step 3 From the toolbar, select **Edit**.

The IOS Template Configuration page appears.

Step 4 Optionally, edit the description field.

Step 5 If this is a custom template, then you can check the *Enable template modification* check box to allow for editing of the template body. See IOS Template Format, on page 95 for details about template syntax. You can undo any unsaved changes you made to the body by clicking **Undo Template Body Changes**.

Step 6 Select **Save** to save the template when you complete your changes.

Copy Templates

You can copy templates to create a new template to which you can make modifications. For instance, it is not possible to edit the body of a default template, however, you can copy a default template and then edit the body of the copy.

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management window opens.

Step 2 Select the checkbox next to the template that you want to copy

Step 3 From the toolbar, select **Copy**.

The Copy IOS Template screen opens.

Step 4 Edit the Name and Description for the copy.

Step 5 Optionally, check the box entitled *Enable template modification* and make changes to the copy. You can also make changes later. See Edit Templates, on page 98.

Step 6 Select **Save** to create the copy with the changes you made.

View Template Details

To view the details of a template:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Management**.

The IOS Template Management page opens.

Step 2 Select **Details** in the details column for the template you want to view.

The IOS Template Details page opens.

The name and the template body of the template is displayed. See IOS Template Format, on page 95 for details about template syntax.

IOS Template Deployment

The IOS Template Deployment pages allow you to deploy a gateway configuration template to a gateway. The template provisions the gateway and substitutes any variables in the template with source devices that you choose when you deploy.

From this page you can:

Preview and Deploy Template

To preview (validate) and deploy a template:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Deployment**.

The IOS Template Deployment page opens.

Step 2 In the **Select Template** panel, select the template that you want to deploy.

Step 3 In the **Associate Source Device(s)** panel, select the devices to be replaced with device variables in the template.

Step 4 In the **Associated Gateways** panel, deselect any of the gateways that will not receive the template deployment. By default, all gateways are selected.

Step 5 Click **Preview and Deploy** to validate and preview the template to the selected gateways with the selected settings.

After clicking **Preview and Deploy**, the script is validated. If there is an error in the script, or there is a variable in the script for which a device is required, but no device was selected from the **Associate Source Device(s)** panel, then errors are listed on the IOS Template Preview Page. Even if you click **Deploy** at this point, the template is not deployed, and the status page shows a failure due to an invalid template.

Once the preview screen appears, you can perform one of three actions:

- If the template is valid or invalid, click **enable template modification** and edit the template on this screen. Click **Verify** to verify your changes as valid, or click **Undo All Changes** to revert the template to the way it was before you began editing.
- If the template is valid, click **Deploy** to deploy the template to the selected gateways,
- If the template is valid, click **Save and Deploy** to save the template and deploy the template to the selected gateways. If this is an existing custom template, then any changes you made are saved to this custom template. If this is a default template, then the template is copied to a new custom template and saved.

Check Deployment Status

To check the status of a template deployment:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Deployment**.

The IOS Template Deployment window opens.

Step 2 From the toolbar, select **Deployment Status**.

The IOS Template Deployment - Deployment Status window opens.

The status page lists information about the attempted deployment. Click on the status message for any deployment for additional details.

Roll Back Deployment

Note There is only one level of rollback. If you deploy a template (Template A) and then deploy another template (Template B), you can only roll back to Template A.

To Rollback a deployment:

Procedure

Step 1 Select **System** > **IOS Configuration** > **IOS Template Deployment**.

The IOS Template Deployment window opens.

Step 2 From the toolbar, click **Deployment Status**.

The IOS Template Deployment - Deployment Status window opens.

Step 3 Check the check box next to the deployment you want to rollback and click **Rollback**.

A confirmation dialog opens. Read the warning and click **OK** to continue the rollback.

A status message is displayed stating that the rollback is in progress. You can refresh the status page by clicking **Refresh** to see the status of the rollback.

Cisco VVB Setup

The Operations Console supports the ability to configure Cisco Virtualized Voice Browser using templates. Templates are text files that contain the VVB settings required for deployment. You can deploy the configurations defined in the template to a VVB from the Operations Console.

You can use the included default templates or create custom templates. The templates are text files that can be copied and edited on the Operations Console.

You can use this page to manage VVB templates.

Add New Template

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 From the toolbar, click **Add New**.

Step 3 In the **General** tab, enter a unique template name and description.

Step 4 Select the **ASR Servers** tab and configure server, port.

For configuration details, see ASR and TTS Servers Setup, on page 102.

Note All ASR Servers selected must have the same port number to access.

Step 5 Select the **TTS Servers** tab and configure server, port.

For configuration details, see ASR and TTS Servers Setup, on page 102.

Note All TTS Servers selected must have the same port number to access.

Step 6 Select the **Applications** tab and add new applications.

For configuration details, see Application Setup, on page 102.

Step 7 Select the **Triggers** tab and associate triggers for newly created applications.

For configuration details, see Triggers Setup, on page 106.

Step 8 Click **Save** to save the template file to the Operations Console.

ASR and TTS Servers Setup

You can configure ASR and TTS Servers using the following settings.

Table 22: ASR Servers Tab Configuration Settings

Field	Description	Default	Range
ASR / TTS Server Selection	Servers configured in Speech Servers page are listed in the Available Servers drop-down menu. Select the server from the drop-down list and click **Add** to select the server. To add a custom server which is not listed in the Speech Servers, you can type the hostname (FQDN) in the drop-down field and click **Add** to select the server. Cisco VVB uses the hostname to connect to these servers and VVB should be able to perform a DNS resolution for the hostname.	None	None
Port Number	Provide the port number that is configured for communication.		1 to 65535

Application Setup

You can configure Applications using these settings.

Table 23: Application Tab Configuration Settings

Field	Description	Default	Range	Base Type
Application Name	Provide an application name.	None	None	Alphanumeric .
Application Type	Select the application script type from the drop-down menu.	SelfService	SelfService, Comprehensive, VRUComprehensive, Error, Ringtone	None

Script	Description	Parameters	Default	Base Type
SelfService	The standalone call flow runs this scripting application.	*VXML Application Name*—Application name that is present on the VXML server. Mandatory field to enter.	None	Alphanumeric
		Port—Port on which the VXML server or load balancer is running.	7000	Numeric
		Primary VXML Server—VXML server or load balancer IP address. Mandatory field.	None	IP Address or Domain Name
		Backup VXML Server—VXML server backup server IP address.	None	IP Address or Domain Name
		Maximum Sessions—Provide number of sessions you like to associate with this application. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.	25	Numeric
		Secured—Select the check box to encrypt the communication between Cisco VVB and VXML server. **Note** If you have enabled secure communication, then ensure to: **1.** Change the port number in the above field to *7443*. **2.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide*. **3.** Restart Tomcat server and Engine from command line.	None	Boolean

Script	Description	Parameters	Default	Base Type
Comprehensive	The comprehensive call flow runs this scripting application.	*Sigdigit*—Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the CVP comprehensive service is configured to strip the digits, so that when the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.	None	Numeric
		Maximum Sessions—Provide number of sessions you like to associate with this application. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.	25	Numeric
		Secured—Select the check box to encrypt the communication between Cisco VVB and VXML server. By default it is disabled. **Note** If you have enabled secure communication, then ensure to: **1.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide* **2.** Restart Tomcat server and Engine from command line. If you are using a coresident VXML and Call Server, use CA-signed certificate.	None	Boolean

Script	Description	Parameters	Default	Base Type
VRUComprehensive	The non-reference VRU call flow and VRU-only call flow runs this scripting application.	*PrimaryVXMLServer*—VXML server or load balancer IP address.	""	Alphanumeric
		BackupVXMLServer—VXML backup server or load balancer IP address.	""	Alphanumeric
		Port—Port on which VXML server or load balancer is running. **Note** Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later. For earlier versions of CVP, configure ports 8000/8443.	"7000"	Numeric
		Secured—Select the check box to encrypt the communication between Cisco VVB and VXML server. **Note** If you have enabled secure communication, then ensure to: **1.** Change the port number in the above field to *7443*. **2.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide*. **3.** Restart Tomcat server and Engine from command line.	false	Boolean
		Sigdigit—Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the CVP comprehensive service is configured to strip the digits, so that when the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.	0	Numeric

Script	Description	Parameters	Default	Base Type
Error	This script is used to play error tone.	*Maximum Sessions*—Provide number of sessions you like to associate with this application. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.	25	Numeric
		Custom Error Prompt—Provide the custom error .wav file to play. **Note** Prompt name field is case-sensitive. The prompt file must be uploaded to Cisco VVB. If custom prompts are not uploaded or found, the default prompt is played.	None	Numeric
Ringtone	This script is used to play ringtone.	*Maximum Sessions*—Provide number of sessions you like to associate with this application. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.	25	Numeric

Triggers Setup

You can associate trigger with the applications added in Applications tab.

Table 24: Trigger Tab Configuration Settings

Field	Description	Default
Dial Number Pattern	A unique phone number. The value includes numeric characters, preceded or followed by the special character: * Examples of **valid** Directory Numbers: *12* or 12*23 Examples of **invalid** Directory Numbers: 91X+, 91X?, 91!, 813510[^0-5] because this number contains a character other than numerical and allowed special characters, or 8]90[-, because this number does not conform with the rule that the square bracket ([ ]) characters enclose a range of values. **Note** For more information, see *Wildcards and Special Characters in Route Patterns and Hunt Pilots* section in the *Cisco Unified Communications Manager System Guide*.	None
Application Name	Select the application from the drop-down menu to associate trigger with the application and click **Add**.	None

Delete Template

Note You cannot delete default templates. Only custom templates can be deleted.

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 Select the templates you want to delete.

Step 3 From the toolbar, select **Delete**.

A confirmation appears. Select **OK** to proceed and delete any custom templates selected.

Edit Templates

You can edit and change description of any template. You can also edit custom templates within a browser, but you cannot edit the default templates.

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 Select the check box next to the template you want to edit and click **Edit**.

Step 3 For details on other tabs, see Add New Template, on page 101.

Step 4 Select **Save** to save the template when you complete your changes.

Copy Templates

You can copy templates to create a new template to which you can modify. For instance, it is not possible to edit the body of a default template, however, you can copy a default template and then edit the body of the copy.

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 Select the check box next to the template that you want to copy

Step 3 From the toolbar, select **Copy**.

The Copy VVB Template screen is displayed.

Step 4 Edit the Name and Description, and for modifying other settings, see Add New Template, on page 101.

Step 5 Select **Save** to create the copy with the changes you made.

Deploy Template

To preview and deploy a template:

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 From the **List of Template**, select the template that you want to deploy.

Step 3 Click **Deploy** to deploy the selected template. You can verify the template body of the selected template.

Step 4 In the **Associated Virtualized Voice Browsers** panel, move VVBs to **Selected** pane to deploy.

Step 5 Click **Deploy** to deploy the template to the selected Voice Browsers.

If there is an error in the script, or there is a variable in the script for which a device is required, but no device was selected from the **Associate Source Device(s)** panel, then errors are listed on the VVB Template Preview page.

At this point, even if you attempt to deploy the template by clicking the **Deploy** button, the template will not be deployed, and the status page displays “Failure due to an invalid template”.

Check Deployment Status

Procedure

Step 1 Select **System** > **VVB Configuration**.

Step 2 From the toolbar, select **Deployment Status**.

The VVB Template Deployment - Deployment Status page is displayed.

The status page lists information about the attempted deployment. Click the status message for more details on deployment status.

Perform Courtesy Callback

The Courtesy Callback feature is available in Unified CVP. Courtesy Callback reduces the time callers have to wait on hold/in queue. The feature allows the system to offer callers who meet certain criteria, for example, callers with the possibility of being in queue for more than X minutes, the option to be called back by the system when the wait time would be considerably shorter.

If the caller decides to be called back by the system, then they leave their name and phone number. When the system determines that an agent is available (or will be available soon), then a call is placed back to the caller. The caller must answer the call and indicate that they are the caller. The caller is connected to the agent after a short wait.

Procedure

To configure Courtesy Callback:

Procedure

Step 1 Select **System** > **Courtesy Callback**.

The Courtesy Callback Configuration window opens.

Step 2 Select the required Unified CVP Reporting Server (if configured) from the drop-down list.

Note If you leave the selection blank, no Reporting Server is associated with the Courtesy Callback deployment.

Step 3 Optionally, enable the check box (default is disabled) next to the label *Enable secure communication with the Courtesy Callback database* to secure the communication between the Unified CVP Call Server and Unified CVP Reporting Server used for Courtesy Callback.

Step 4 In the **Dialed Number Configuration** section:

The Dialed Number Configuration of Courtesy Callback allows you to restrict the dialed numbers that callers can enter when they are requesting a callback. For example, it can stop a malicious caller from having Courtesy Callback dial *911*. The table below lists the configuration options for the **Dialed Number Configuration**:

Field	Description	Default
Allow Unmatched Dialed Numbers	This checkbox controls whether or not dialed numbers that do not exist in the **Allowed Dialed Numbers** field can be used for a callback. By default, this is unchecked. If no dialed numbers are present in the **Allowed Dialed Numbers** list box, then **Courtesy Callback does not allow any callbacks**.	Unchecked - Callbacks can only be sent to dialed numbers listed in the **Allowed Dialed Numbers** list.
Allowed Dialed Numbers	The list of allowed dialed numbers to which callbacks can be sent. You can use dialed number patterns; for example, `978>` allows callbacks to all phone numbers in the area code *978*. To Add/Remove Dialed Numbers: • To Add a number to the list of allowed dialed numbers - Enter the dialed number pattern in the **Dialed Number (DN):** field and click **Add**. • To remove a number from the list - Highlight the number and click **Remove**.	Empty - If **Allow Unmatched Dialed Numbers** is *not* checked, and this list remained empty, then no callbacks can be made.

Field	Description	Default
Denied Dialed Numbers	The list of denied dialed numbers to which callbacks are never sent. You can use dialed number patterns; for example, `555>` allows callbacks to all phone numbers in the area code *555*. To Add/Remove Dialed Numbers: • To Add a number to the list of denied dialed numbers - Enter the dialed number pattern in the **Dialed Number (DN):** field and click **Add**. • To remove a number from the list - Highlight the number and click **Remove**. Denied numbers takes precedence over allowed numbers. • Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character. **Note** Small letter "x" cannot be used as a wildcard. • Any of the wildcard characters in the set ">*!T" match multiple characters but can only be used as trailing values because they always match all remaining characters in the string. • The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. • When the number of characters are matched equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.	The Denied Dialed Numbers window is prepopulated if your local language is "en-us"(United States, English). Be sure to add any additional numbers you want to deny.
Maximum Callbacks Per Calling Number	The default value is 0, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000. This setting allows you to limit the number of calls, from the same calling number that are eligible to receive a callback. If this field is set to a positive number (X), then the courtesy callback “Validate” element only allows X callbacks per calling number to go through the “preemptive” exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the “none” exit state of the “Validate” element. In addition, if no calling number is available for a call, the call always goes through the “none” exit state of the “Validate” element.	*0*

Step 5 Click the **Call Server Deployment** tab to view a list of available call servers and to select a Unified CVP Call Server to associated with Courtesy Callback.

Step 6 After making the required configuration changes, you have two options to save the configuration:

- Click **Save & Deploy** in the bottom right corner of this page (or the **Save & Deploy** button in the toolbar above) to save the Call Server information and initiate a deployment request to the selected devices.

  See the View Courtesy Callback Deployment Status section for details on viewing the status information.

- Click **Save** to save the configuration to the Operations Console database

  .

View Courtesy Callback Deployment Status

You can verify the latest deployment status of the Courtesy Callback configuration using the Unified CVP Operations console. The deployment status is listed for each Unified CVP Call Server.

Procedure

To view the deployment status of Courtesy Callback configurations:

Procedure

Step 1 Select **System** > **Courtesy Callback**.

The configuration window opens.

Step 2 From the toolbar, click **Deployment Status**.

The Courtesy Callback Deployment Status window displays the device IP address and current status. Note that you can click **Refresh** to view the latest status.

In the following cases, the Deployment Status displays a warning message:

- If you have only saved the configuration details and have not deployed them.
- If you have edited or deleted an existing configuration and have not deployed the changes.
- If you changed the call server association.

SIP Error Reason Code Mapping

In a REFER label transfer scenario, a call comes from the network to Cisco Unified Border Element (CUBE). The CUBE receives a REFER from Cisco Unified Customer Voice Portal (CVP) and starts a new INVITE toward refer-to number. If the call fails, CUBE receives a status message with q.850 Reason header which includes ISDN User Part (ISUP) cause codes. CUBE then starts a NOTIFY to Unified CVP with the Session Initiation Protocol(SIP) error string. Unified CVP maps the SIP code to ISUP cause code and sends back to CUBE in a BYE message and in-turn to network. This result is achieved by configuring the SIP reason code to ISUP cause code mapping under SIP Error Reason Code Mapping menu.

Configure SIP Error Reason Code Mapping

Before you begin

- Install Call Server 12.0(1).
- Ensure that the Call server is up and running.
- Check the **SIP Subsystem** check box to enable this service in the Call Server.

Procedure

Step 1 In the Operations console, select **System** > **SIP Error Reason Code Mapping**.

Step 2 Enter the value of the error reason code in the **Error Reason Code(SIP)** field.

Note
- The value of Error Reason Code (SIP) must be unique and it can be a three-digit positive integer.
- The SIP Error Reason Code field must not be blank.

Step 3 Enter the value of ISUP cause code in the **Cause Code (ISUP)** field.

Note
- The ISUP cause code value must be two or three digit positive integers.
- The ISUP cause code field must not be blank.

Step 4 Perform one of the following options:

- Click **Add** to add the entries to the **Reason to Cause Code Mapping** list.

  Note A maximum of ten mapping entries are allowed.

- Click **Remove** to remove an entry from the **Reason to Cause Code Mapping** list. Click **OK**.

Step 5 After changing the Error Reason Code Mapping configurations, you have two options to save the configuration:

- Click **Save** to save the configuration to the Operations Console derby database.
- Click **Save & Deploy** to deploy the configurations to all the Call Servers.

Step 6 Click **Deployment Status** to view the deployment status.
The SIP Error Reason Code Mapping - Deployment Status window displays the device IP address and the deployment status.

Step 7 Click **Refresh** to view the latest status.

Caution The Deployment Status page displays a warning message, in the following cases:

- If you have saved the configuration details and have not deployed them.
- If you have edited or deleted an existing configuration detail, and have not deployed the changes.

View SIP Error Reason Code Mapping Deployment Status

The Operations Console displays the Unified CVP Call Server IP address and the deployment status. If a deployment fails because the Unified CVP Call Server is not accessible (either not deployed or off line) or is not upgraded to the current version, the Operations Console issues a descriptive message.

The **SIP Error Reason Code Mapping Deployment Status** page displays the last recorded deployment status per configured Unified CVP Call Server. You can refresh the page, view online help, or go back to the **SIP Error Reason Code Mapping Configuration** page. You can also sort (in either ascending and descending order) the Deployment Status table contents by the following column fields: **Hostname**, **IP Address**, **Device Type**, **Status**, or **Last Updated**.

Deployment operations can be time-consuming, depending on the number of Unified CVP Call Servers. When either process is running, you can select a status report to view the progress of the last initialized deployment request.

Note Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If a process is already running, you cannot start another process. You will receive an error message.

The following information applies to the Status window:

Procedure

- Unapplied changes (deployment status only) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP Call Server can be deployed at any given time. The other call servers are either in queue or in a successful or failed state.

Procedure

To view the SIP error code mapping deployment status:

Procedure

Step 1 From the Operations Console, select **System** > **SIP Error Reason Code Mapping**.

The Operations Console displays the **SIP Error Reason Code Mapping Configuration** page.

Step 2 Click **Deployment Status** at the bottom right corner of the window.

The Operations Console displays the Call Server IP address and the deployment status. If there is a failure, the Operations Console provides a reason for the failure.

Cloud Services

Proxy Settings

Prerequisite

- Install CVP 11.6(1) or above.
- Ensure that the VXML servers are up and running.

Enabling Proxy Settings

Procedure

Step 1 From the Operations Console, select **System** > **Cloud Services** > **Proxy Settings**.

Step 2 Enter the value of the Proxy.

- The proxy hostname must be in the format: *hostname:port* or *IP_address:port*.
- Leave the proxy setting column blank for a deployment that does not require a proxy for access.

Step 3 After changing the proxy configurations, save it. There are two options to save the configuration:

- Click **Save** to save the configuration to the Operations Console derby database.

  -OR-

- Click **Save & Deploy** to save and deploy the configurations to all the VXML servers.

Step 4 Click **Deployment Status** to view the current deployment status. The **Proxy Settings - Deployment Status** window displays the device IP address and the deployment status.

Step 5 Click **Refresh** to view the latest status.

Note The **Deployment Status** page displays a warning message, in the following cases:

- If you have saved the configuration details and not deployed the changes.
- If you have edited or deleted an existing configuration and not deployed the changes.

What to do next

Restart VXML service and Ops Console service.

View Proxy Settings Deployment Status

The Operations Console displays the Unified CVP VXML Server IP address and the deployment status. If a deployment fails because of any of the following reasons, then a descriptive message is displayed.

- Unified CVP VXML Server is not accessible (either not deployed or offline)

- Unified CVP VXML Server is not upgraded to the current version

The **Proxy Settings Deployment Status** page displays the last recorded deployment status per configured Unified CVP VXML Server. You can refresh the page, view online help, or go back to the Proxy Settings Configuration page. Display of records can be sorted (in either ascending and descending order) by column fields: **Hostname**, **IP Address**, **Device Type**, **Status**, or **Last Updated**.

Deployment operations can be time-consuming, depending on the number of Unified CVP VXML Servers. When a deployment process is running, you can select the status report.

Note Deployment operations are mutually exclusive. Only one deployment process can run at any given time. If a process is already running, you cannot start another process. You will receive an error message.

The following information applies to the Status window:

- Unapplied changes (only deployment status) indicate that a Save operation took place since the last deployment operation.
- Only one Unified CVP VXML server can be deployed at any given time. The other VXML servers are either in queue or in a successful or failed deployment state.