Administration Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)

First Published: 2020-01-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Preface

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Added steps to connect to the remote desktop of the Reporting Server machine and add a user for the Cisco CVP WebServicesManager in the **Unified CVP Reporting Server Setup** section	Managing Devices	April 2021
Edge Chromium (Microsoft Edge) updates in **Accept Security Certificates** section	Cisco Unified Customer Voice Portal	December 2020
Initial Release of Document for Release 12.5(1)		January 2020
Added section on Operations Console (NOAMP)	Operations Console (NOAMP)	
Added Smart Licensing information	Smart Licensing	

About This Document

The *Administration Guide for Cisco Unified Customer Voice Portal* provides the following information:

- Understand the Operations Console interface and how it is used for configuration, error handling, and Control Center operations.
- Manage devices and Cisco Unified CVP users.
- Perform bulk administration, SNMP agent setup, and launch tools.

Audience

This guide is intended for managers, Unified CVP system managers, Cisco Unified Intelligent Contact Management Enterprise (Unified ICME)/ Cisco Unified Intelligent Management Hosted (Unified ICMH) system managers, VoIP technical experts, and IVR application developers, who are familiar with the following:

- Configuring Cisco Gateways
- Configuring Cisco Unified Communications Manager
- ICM Configuration Manager and ICM Script Editor tools for call center operations and management

Related Documents

- *Solution Design Guide for Cisco Unified Contact Center Enterprise*
- *Configuration Guide for Cisco Unified Customer Voice Portal*
- *Installation and Upgrade Guide for Cisco Virtualized Voice Browser*
- *Developer Guide for Cisco Virtualized Voice Browser*
- *Solution Port Utilization Guide for Cisco Unified Contact Center Solutions*
- *Operations Guide for Cisco Virtualized Voice Browser*

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

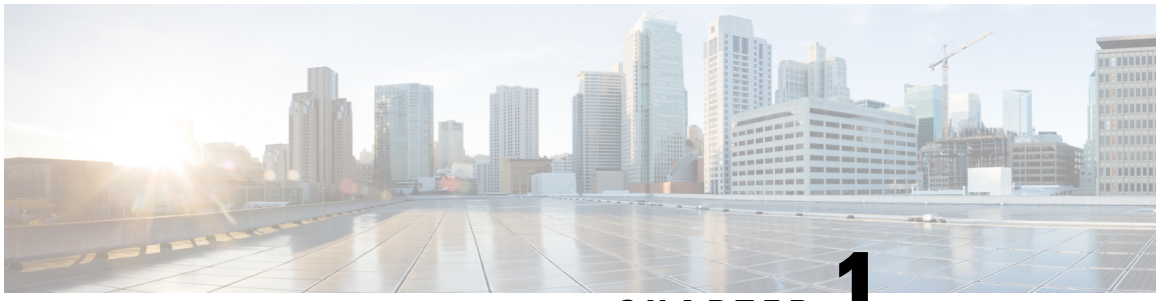
Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

Provide your comments about this document to:

mailto:ccbu_docfeedback@cisco.com

CONTENTS



CHAPTER 1

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 Secure Password Requirements	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 Secure Password Requirements	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, on page 179

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, on page 117
Find Device, on page 119
Past Device Setups in Operations Console Database, on page 230

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

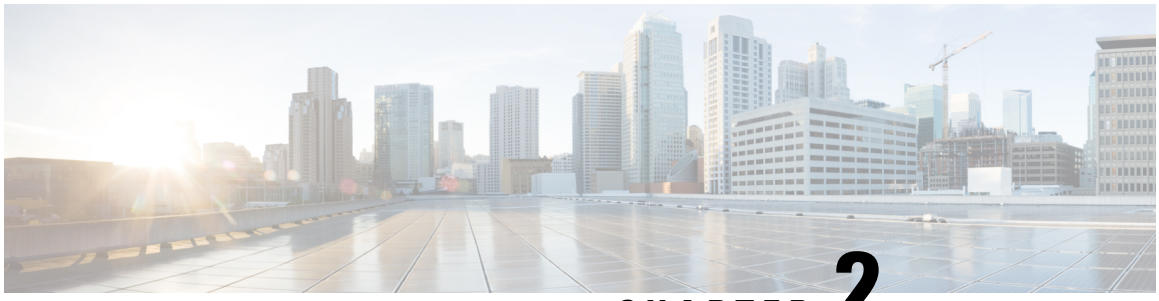
The **Proxy Settings Deployment Status** page displays the last recorded deployment status per configured Unified CVP VXML Server. You can refresh the page, view online help, or go back to the Proxy Settings Configuration page. Display of records can be sorted (in either ascending and descending order) 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.



CHAPTER 2

Managing Devices

Device Properties

The term *device* refers to a configurable application or platform. More than one device can reside on a server. For example, one physical server can contain a Call Server and a Reporting Server. In this case, each device is configured with the same IP address.

The network map is a collection of Unified CVP solution components and their configuration data. When you add a device to the Operations Console, that device becomes visible in the network map and its configuration data is stored in the Operations Console database.

The Operations Console provides two views of the properties of the devices in the network map:

- Offline View of Device Properties
- Online View of Device Properties

For more information, see Device Information Field Descriptions

Offline View of Device Properties

In the Offline view, the Operations Server operates without a running Unified CVP solution, allowing you to build the network map even if the devices do not exist. The configurations are stored locally in the Operations Console database. The Operations Console displays the property values stored in the local database. When you modify a property value in the Offline view and click **Save**, the configuration is stored locally in the Operations Console database *only*. Configurations that are saved while a device is Offline can be applied when the device is ready and available.

By default, Unified CVP devices are displayed in the Offline view. To display the Online device view, select online from the View drop down menu.

Online View of Device Properties

The Online view provides a snapshot of properties used by the running Unified CVP server at the moment. When you modify a property value in the Online view and click **Save**, the configuration is stored locally in the Operations Console database *only*. Clicking **Save & Deploy** saves the change in the Operations Console database and also applies the change to the device. If you change a device property, click **Save**, but do not click **Save & Deploy**, you see the changed value in the Online view, but see the current value in the Offline view.

By default, Unified CVP devices are displayed in the Offline view. To display the Online device view, select online from the View drop-down menu.

Device Information Field Descriptions

When you select a device type from the Device Management menu, information appears about the device that has been added to the Operations Console.

The following table describes the server window fields.

Table 25: Server Window Fields

Field	Description
Hostname	The hostname assigned to the device.
IP Address	IP address of the device.

Field	Description
Device State	The state of the configuration of the device: configured or invalid. The following device types can be in the configured or invalid state: • Unified CVP Call Server • Unified CVP Reporting Server • Unified CVP VXML Server • Unified CVP VXML Server (standalone) • Speech Server A configuration can become invalid if the device is reinstalled or errors occur during device creation. To clear this state, edit the device and click **Save & Deploy**. All other devices in the Operations Console are always in the configured state.
Description	An optional text description for the device.

Related Topics

View Device Status, on page 39

Find Device

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

See also Display Device Statistics, on page 120.

Procedure

To find a device:

Procedure

Step 1 From the **Device Management** menu, select the menu option for the type of device to find from the Device menu.

The Find, Add, Delete, Edit window lists the available devices of the type you selected, sorted by name, 10 per screen.

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 **Hostname**; then selecting a modifier, such as **begins with**; entering your search term; and then clicking **Find**.

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

Display Device Statistics

You can display statistics for any Gateway, Unified CVP VXML Server, Unified CVP Reporting Server, or Unified CVP Call Server, that has been added to the Operations Console.

Procedure

To get device statistics:

Procedure

Step 1 Choose the device from the Device Management menu: For example, if you want to view statistics for the Unified CVP Reporting Server, choose **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Click **Edit**.

Step 3 Find the device using the procedure shown in Find Device, on page 119.

Step 4 From the list of matching records, choose the device for which you want to get statistics.

Step 5 Select **Statistics** from the Configuration menu bar.

The Statistics window opens.

Step 6 If there are multiple statistics options to choose, select the desired option from the Statistics drop-down menu.

The Operations Server displays the statistics in the window.

Unified CVP Licensing

The following Unified CVP licenses are enforced by the software on a per-instance basis:

Unified CVP licenses:

- Call Server - The SIP Service and the IVR Service check at startup time to ensure that it is running on a system with a valid Call Server license.
- Unified CVP VXML Server - The Unified CVP VXML Server checks at startup time to ensure that it is running on a system with a valid Unified CVP VXML Server license.
- Reporting Server - The Reporting Server runs without requiring a license.

The Operations Server runs without requiring a license.

In addition, each Call Server and each Unified CVP VXML Server enforce licenses for a particular number of simultaneous calls. The software does not distinguish between Call Director calls, VRU-only calls, or VRU calls with ASR/TTS or VXML.

Port licensing is enforced as follows:

- The Call Server is licensed for a certain number of ports; SIP and IVR Services share this port pool.
- The SIP Service attempts to allocate one of its licenses whenever it receives an incoming call. Once the last license has been allocated, the SIP Service changes its status and that of its host Call Server (the Call Server on which the SIP Service is running) to Partial status, preventing further calls from being accepted. When a call terminates, the SIP Service releases a license, and if it had been in Partial status due to license depletion, it resumes Up status.

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

- The IVR Service can receive calls transferred from SIP Service or from some other source. The IVR Service can handle both the VRU leg and the switch leg of the same call. The IVR Service keeps a list of active Call IDs, and uses that list to determine whether a particular incoming call has already been counted. Therefore, the IVR Service always accepts an incoming call if its host Call Server (the Call Server on which the IVR Service is running) is in the Up state, and then checks whether the call has been seen before. If the call has not been seen before, the IVR Service allocates a license for that call. If doing so exhausts the available licenses, the IVR Service changes its state and that of its host Call Server to Partial. When a call terminates, the IVR Service releases a license and if it had been in Partial state due to license depletion, it resumes Up status.

Note that this licensing scheme might change in future releases, and should customers order an insufficient number of licenses, they will be impacted in future releases when licensing tracks the number of ports actually ordered.

For more information on licensing, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

Unified CVP Call Server Setup

From the Unified CVP Call Server option on the Device Management menu, you can configure one or more Call Servers. The Unified CVP Call Server provides call control capabilities, using Session Initiation Protocol (SIP) signaling.

The Call Server can be configured to provide the following call control services, which are installed with the Call Server:

- SIP Service - Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks and SIP phones.
- IVR Service - Creates the VXML pages that implement the Unified CVP Micro-applications, based on Run Script instructions received from ICM server. The IVR service functions as the Voice Response

Unit (VRU) leg, and calls must be transferred to it from the SIP Service to execute micro-applications. The VXML pages created by this module are sent to the VXML Gateway to be executed. The IVR Service routes requests from the SIP Service to the ICM Service.

- ICM Service - Enables communication between Unified CVP components and the ICM Server. It sends and receives messages on behalf of the SIP Service, the IVR Service, and the VXML Service.

You can perform the following tasks:

Related Topics

Shut Down Server, on page 59
Start Server, on page 58

Add Unified CVP Call Server

Adding a Unified CVP Call Server creates a configuration for the Unified CVP Call Server in the Operations Console database and adds the Unified CVP Call Server to the list of devices in the Operations Console.

Procedure

To add a Unified CVP Call Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Call Server**.

Call Servers that have been added to the Operations Console are listed.

Note To use an existing Unified CVP Call Server as a template for creating the new Unified CVP Call Server, select the Unified CVP Call Server by clicking the radio button preceding it and then click **Use As Template**.

Step 2 Click **Add New** from the Menu bar or at the bottom of the screen.

The Unified CVP Call Server Configuration window opens to the General tab.

Step 3 Fill in the IP Address and Hostname fields.

Step 4 Optionally, click **Enable secure communications with the Ops Console** to secure communications between the Operations Console and the Unified CVP Call Server.

Step 5 Turn on the Call Services required for the Call Flow you are using by checking the appropriate check boxes, and then click **Next**. See Call Services, on page 123.

The Unified CVP Call Server Configuration page opens to the General tab. Additional tabs for configuring the selected services are displayed.

Step 6 Optionally, click **Change Type** and change your selections of services.

Step 7 Select each tab and verify that the default values are correct or change the values if desired:

Configuration Tabs:

- Set Up ICM Service, on page 125
- Set Up SIP Service, on page 129

- Set Up IVR Service, on page 130
- Add or Remove Device From Device Pool, on page 62
- Set Up Infrastructure, on page 143

Step 8 When you have filled in the configuration settings for all selected Call Services, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save the changes and apply them to the Unified CVP Call Server.

Note You must only deploy to a freshly installed Unified CVP Call Server. Do not deploy to a Unified CVP Call Server that was previously configured.

Step 9 Shut down and start the Unified CVP Call Server to start the newly added services.

Related Topics

Unified CVP Call Server Settings, on page 148
View Unified CVP Call Server Statistics, on page 147
View Device Status, on page 39
Shut Down Server, on page 59
Start Server, on page 58

Call Services

Services Needed for CVP Call Flow Models

Choose the desired call flow model, and then select the required call services in the Call Server Configuration window:

Call Flow Model	Required Call Services
Comprehensive Call Flow Using SIP, on page 123	ICM, IVR, SIP
VRU-Only, on page 124	ICM, IVR
Call Director Using SIP, on page 124	ICM, IVR
Unified CVP VXML Server with ICM Lookup, on page 124	ICM
Unified CVP VXML Server Standalone Call Flow, on page 124	No Service
Basic Video Call Flow, on page 125	ICM, IVR, SIP

Comprehensive Call Flow Using SIP

The Comprehensive call flow model combines the Call Director Using SIP and the VRU-Only scenarios. It provides initial prompt and collect, self-service IVR, queuing, and VoIP routing among all types of UCCE and TDM agents. This scenario is supported at two port licensing levels: Basic and Advanced. The Basic level supports the playing of .wav files and input using DTMF. The Advanced level adds support for ASR, TTS, and Unified CVP VXML Server applications.

VRU-Only

Unified CVP provides ICM with VRU services for calls which are routed in some other manner, such as by a carrier switched network through an ICM NIC interface. VRU services could be for initial prompt and collect, for integrated self service applications, for queuing, or for any combination thereof. This scenario does not use SIP, and requires no Ingress Gateway. It does use VXML Gateways, but the Unified CVP VXML Server is optional, as are ASR and TTS Servers.

Depending on which kind of routing client is in charge of call routing, ICM may transfer the call to the VRU-Only Call Server either by a Translation Route to VRU node, or by a Send To VRU node. In the first case, the Call Server will determine that the arriving call is a VRU leg call by matching the arriving DNIS with its configured list of arriving DNIS numbers. In the second case, it will determine that it is a VRU leg call because the DNIS length is greater than its configured maximum DNIS length. Digits beyond the maximum DNIS length are taken as the Correlation ID.

Call Director Using SIP

In Call Director using SIP, Unified CVP provides ICME with VoIP call routing capabilities only. Use your own Service Control VRU if you are using an ICM Server to queue calls, or queue calls directly on an ACD. Calls can be transferred multiple times, from Ingress, to customer-provided VRU, to either UCCE or customer-provided ACD or agent, and back again. When calls are connected to customer-provided equipment, their voice paths must go to an Egress gateway which is connected by TDM to that equipment. If the signaling is SIP, then Unified CVP will work with customer-provided SIP endpoints which have been tested and certified to interoperate with Unified CVP. Neither Unified CVP VXML Server nor any VXML Gateways are used in this model.

Unified CVP VXML Server with ICM Lookup

In this call flow model, the call server with the ICM Service enabled is required to route calls. The Reporting server is optional. Use a Reporting server if you want to generate reports that include Unified CVP VXML Server events. You can also use the ICM request label from the Unified CVP VXML Server to an ICM Server, if the ICM service is enabled on the Call Server. The Reporting server can be installed on the same physical machine as the Call Server. After you configure the Call Server, you must configure the Unified CVP VXML Server. See Unified CVP VXML Server Setup, on page 165.

The RequestICMLabel is a feature that allows you to make back-end requests to an ICM Server without relinquishing control of the call. The application generally acts on its own, but includes a special step to send a query to the ICM Server and receive a response. The query and the response may contain full call context information, as can the response.

Following are the features of the IVR application :

- An IVR application can request an ICM server to select an available UCCE or ACD agent to which the call should be transferred. Full call context is preserved during the transfer, but queuing is not possible.
- An IVR application can transfer its call to a separate full-blown Unified CVP system for agent selection and queuing. Full call context is preserved throughout.
- An IVR application can request an ICM server to perform a calculation or application gateway transaction that it already knows how to perform, and return the result to the application.
- An IVR application can report intermediate or final call data to an ICM server to be stored in its database.

Unified CVP VXML Server Standalone Call Flow

In this call flow model, the Call Server is used to route messages between the components. Calls arrive through a VXML gateway, and interact directly with a Unified CVP VXML Server to execute VXML applications.

The gateway performs both ingress and VXML functions. This call flow model provides a sophisticated VXML-based VRU, for applications which in many cases do not need to interact with an ICM Server.

For a Unified CVP VXML Server (standalone) with no connection to an ICM Server and no Reporting Server, configure the Call Server with no services enabled. If you need to make requests to an ICM server, without relinquishing control of the call or use Unified CVP reporting, you must configure the VXML Server to use a Call Server with at least the ICM Service enabled. See Unified CVP VXML Server Setup, on page 165.

After you configure the Call Server, you must configure the Unified CVP VXML Server as a Unified CVP VXML Server (standalone). See Unified CVP VXML Server (Standalone) Setup, on page 182.

Basic Video Call Flow

The Basic Video call flow model combines the Call Director and the VRU-Only call flow models, along with video capabilities that are only enabled during the caller-agent conversation. It provides initial prompt and collect, self-service IVR, queuing, and VoIP routing among UCCE and TDM agents.

Note This call flow model is almost identical to the Unified CVP Comprehensive SIP call flow model. The only change between the two call flow models is the addition of video-enabled endpoints for the calling and called parties (Cisco Unified Video Advantage (CUVA), Cisco Unified Personal Communicator (CUPC), and Cisco TelePresence). See the *Configuration Guide for Cisco Unified Customer Voice Portal* for additional information about CUVA and Cisco Telepresence.

Unified CVP Call Server Services Setup

When you are adding a Unified CVP Call Server, you must configure the call services required for the call flow model you are using.

- SIP Service - Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks and SIP phones.
- IVR Service - Creates the VXML pages that implement the Unified CVP Micro-applications, based on Run Script instructions received from an ICM server. The IVR service functions as the Voice Response Unit (VRU) leg, and calls must be transferred to it from the SIP Service in order to execute micro-applications. The VXML pages created by this module are sent to the VXML Gateway to be executed.
- ICM Service - Enables communication between Unified CVP components and the ICM server. It sends and receives messages on behalf of the SIP Service, the IVR Service, and the VXML Service.

Set Up ICM Service

The ICM service enables communication between Unified CVP components and the ICM server. It sends and receives messages on behalf of the SIP Service, the IVR Service, and the VXML Service. The ICM service is installed with the Call Server.

You must configure the ICM service if you are adding or editing a Call Server and you are using any of these call flow models:

Procedure

- Call Director
- VRU-Only
- Comprehensive

What to do next

You must also configure the ICM service if you use a Unified CVP VXML Server (standalone) that makes requests to an ICM server without relinquishing control of the call (Request ICM Label).

Procedure

To configure the ICM Service:

Procedure

Step 1 If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 122. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 145.

Step 2 Fill in the appropriate configuration settings as described in ICM Service Settings, on page 126

Step 3 When you finish configuring all desired Call Server services, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to apply the changes to the Call Server.

ICM Service Settings

The following table describes the property settings that you can change to configure the ICM Service. The first time you configure the ICM Service on a Call Server, you must restart the Call Server. You must also restart the server if you change a configuration setting that has been marked **yes** in the restart required column in the table below.

Table 26: ICM Service Configuration Settings

Property	Description	Default	Range	Restart Required
General Configuration				
VRU Connection Port	The Port Number on which the ICM Service listens for a TCP connection from the ICM PIM.	5000	Any valid TCP/IP connection port	Yes

Property	Description	Default	Range	Restart Required
Maximum Length of DNIS	The maximum length of an incoming Dialed Number Identification Service (DNIS). Valid input for this field is 1 - 99999 characters. Look for this information in your network dial plan. For example, if the Gateway dial pattern is 1800******, the value of Maximum Length of DNIS should be 10. The number of DNIS digits from the PSTN must be less than or equal to the maximum length of DNIS field. **Note** If you are using the Correlation ID method in your ICM script to transfer calls to Unified CVP, the maximum length of DNIS should be the length of the label that is returned from ICM for the VRU leg of the call. When ICM transfers the call, the Correlation ID is appended to the label. Unified CVP then separates the two, assuming that any digits greater than maximum length of DNIS are the Correlation ID. The Correlation ID and label are then passed to ICM.	10	Integer	No
Enable secure communication with VRU PIM	Enables secure communication between ICM and the Unified CVP Server.	No	NA	Yes
Translation Routed DNIS Pool				
Add	Enter a single DNIS number for translation routed calls. DNIS is a phone service that identifies which number the caller dialed. DNIS can be up to 32 characters in length. Validations for DNIS fields are as follows: • The DNIS must be a positive integer; DNIS can begin with a zero (0) • The start and end values for the DNIS range must be the same length • Users cannot add a DNIS or DNIS range that already exists or overlap with (or in) the range of a DNIS added previously	None	Integer	No

Property	Description	Default	Range	Restart Required
Add a Range	List of DNIS numbers for translation routed calls. Add a range of DNIS numbers, select **Add a Range**, enter the first DNIS number in the range, and then enter the last DNIS number in the range in the **to** field. Click **Add DNIS** to add the entered DNIS or DNIS range to the list of Configured DNIS numbers. Select a DNIS or DNIS range in the Configured DNIS box and click **Delete DNIS** to remove it from the list of Configured DNIS numbers. DNIS can be up to 32 characters in length. Valid input for DNIS range requires the first and last DNIS numbers in the range to be the same length. For example, a range from 100 to 900 is valid because each number is three characters in length.	None	Integer	No
Advanced Configuration				
New Call Service ID	Identifies calls to be presented to ICM software as a new call. New Call Service ID calls result in a NEW CALL message being sent to ICM software and the call being treated as a new call, even if it had been pre-routed by ICM software.	1	Integer	Yes
Pre-routed Call Service ID	Identifies calls pre-routed with a translation route or correlation ID. Pre-routed Service ID calls result in a REQUEST_INSTRUCTION message being sent to ICM software, which continues to run the script for the call.	2	Integer	Yes
New Call Trunk Group ID	Calls presented to ICM as new calls are sent with this Trunk Group ID as part of the NEW_CALL message to ICM.	100	Integer	Yes
Pre-routed Call Trunk Group ID	Calls pre-routed with a Translation Route or correlation ID are sent with this Trunk Group ID as part of the REQUEST_INSTRUCTION message to ICM.	200	Integer	Yes
Trunk Utilization				

Property	Description	Default	Range	Restart Required
Enable Gateway Trunk Reporting	Check the check box to enable gateway trunk reporting. **Note** The Add Gateway (when adding or editing a gateway) contains an optional field, **Trunk Group ID**, that can be used to customize the trunk group ID for each gateway.	None	Not applicable	No
Maximum Gateway Ports	The value used for setting the maximum number of ports that a gateway supports in a CVP deployment. This will be used to calculate the number of ports to report to the Unified ICM Server for each gateway.	700	1-1500	Yes
Available	The list of gateways available for trunk reporting.	None	Not applicable	No
Selected	The list of gateways selected for trunk reporting.	All Gateways Selected	Not applicable	No

Set Up SIP Service

You must configure the SIP service if you add a new Call Server (Add Unified CVP Call Server, on page 122) or edit a Call Server (Edit Unified CVP Call Server, on page 145), and you use any of these call flow models (Call Services, on page 123):

- Call Director
- Comprehensive

Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks and SIP phones.

Procedure

The SIP Service is one of the services that can be configured when creating a new Call Server.

Procedure

Step 1 If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 122. If you want to change an existing Call Server, see Edit Unified CVP Call Server, on page 145.

Step 2 Fill in the appropriate configuration settings. For more information, see section SIP Service Settings in the *Managing Devices* chapter.

Step 3 When you finish configuring all desired Call Server services, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to apply the changes to the Call Server.

Set Up IVR Service

The first time you configure the service on a Unified CVP Call Server, you must restart the Call Server.

You must configure the IVR service if you add a new Unified CVP Call Server (Add Unified CVP Call Server) or edit a Unified CVP Call Server (Edit Unified CVP Call Server) and you any of these call flow models (Call Services):

Audio call flow models:

- Call Director, using SIP protocol
- VRU-Only
- Comprehensive, using SIP protocol

The IVR Service creates VXML documents that implement the Micro-Applications based on Run Script instructions received by the ICM. The VXML pages are sent to the VXML Gateway to be executed. The IVR Service can also generate external VXML through the Micro-Applications to engage the Unified CVP VXML Server to generate the VXML documents.

The IVR Service plays a significant role in implementing a failover mechanism: those capabilities that can be achieved without ASR/TTS Servers, and VXML Servers. Up to two of each such servers are supported, and the IVR Service orchestrates retries and failover between them.

Before You Begin

Configure the following servers before configuring the IVR Service:

- ICM Server
- Media Server
- ASR/TTS Server
- Unified CVP VXML Server
- Gateway

Procedure

The IVR Service is one of the services that can be configured when creating a new Call Server.

Procedure

Step 1 If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 122. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 145.

Step 2 Fill in the appropriate configuration settings as described in IVR Service Settings, on page 130

Step 3 When you finish configuring all desired Call Server services, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to apply the changes to the Call Server.

IVR Service Settings

The following table describes the property settings that you can change to configure the IVR Service.

Table 27: IVR Service Configuration Settings

Property	Description	Default	Range	Restart Required
IOS Voice Browser Configuration				
Last Access Timeout (seconds)	The number of seconds the IVR Service waits for a call request from a non-Unified CVP Voice Browser before removing that Voice Browser from its current client list. This value must be greater than or equal to the call timeout.	7320	0 -2147483647	No
Media Server Timeout	The number of seconds the Gateway should wait to connect to the HTTP Media Server before timing out.	4	0 -2147483647	No
Media Server Retry Attempts	Maximum number of times the non-Unified CVP Voice Browser (IOS Voice Browser) or Unified CVP VXML Server attempts to connect to an HTTP Media Server to retrieve a single prompt. If the Voice Browser or Unified CVP VXML Server fails after the specified number of times, it will try the same number of times to retrieve the media from a backup media server before failing and reporting an error. The backup media server is defined on the gateway as <mediaserver>-backup.	0	0 -2147483647	No
ASR/TTS Server Retry Attempts	Maximum number of times the Gateway tries to connect to an ASR/TTS server. If the Gateway fails to connect this many attempts, it will try the same number of times to connect to a backup ASR/TTS server before failing and reporting an error. (The backup ASR and TTS servers are defined on the gateway as asr-<locale>-backup and tts-<locale>-backup.)	0	0 -2147483647	No

Property	Description	Default	Range	Restart Required
IVR Service Retry Attempts	Maximum number of times the Gateway tries to connect to the IVR Service before failing and reporting an error. This setting controls call results only. The initial NEW_CALL retry count from the Gateway to the IVR Service is controlled from within the bootstrap VXML in flash memory on the Gateway.	0	0 -2147483647	No
Use Backup ASR/TTS Servers	If you select **Yes** (default) and an ASR/TTS Server is unavailable, the Gateway attempts to connect to the backup ASR/TTS server.	Yes	Yes or No	No
Use Backup Media/VXML Servers	If you select **Yes** (default) and a media server is unavailable, the Gateway attempts to connect to the backup Media Server.	Yes	Yes or No	No
Use hostnames for default Media/VXML servers	If you select No (default), the IP address is used for the XML Server and Media Server. If you select Yes, the hostnames are used rather than IP addresses.	No	Yes or No	No
Use Security For Media Fetches	If you select **No** (default), HTTP URLs are generated to media servers. **Note** The default setting is only applicable if the client is SIP Service and the media server is not set to a URL that explicitly specifies an HTTP/HTTPS scheme. Select **Yes** to generate HTTPS URLs to media servers.	No	Yes or No	No
Advanced Configuration				

Property	Description	Default	Range	Restart Required
Call timeout	The number of seconds the IVR Service waits for a response from the SIP Service before timing out. This setting should be longer than the longest prompt, transfer or digit collection at a Voice Browser. If the timeout is reached, the call is cancelled but no other calls are affected. The only downside to making the number arbitrarily large is that if calls are being stranded, they will not be removed from the IVR Service until this timeout is reached.	7200	Must be 6 seconds or greater	No
ASR/TTS use the same MRCP server	Select this option if your ASR and TTS servers are on the same machine. Using this option helps to minimize the number of MRCP connections on the ASR/TTS server.	No	Yes or No	No

SIP Service Settings

The following table describes the properties that you can set to configure the SIP Service. The first time you configure the SIP service on a Call Server, you must restart the Call Server.

Configuration

Enable Outbound Proxy

Select **Yes** to use a use a Cisco Unified SIP proxy server. For more information on configuring the Cisco Unified SIP Proxy Server, consult the CUSP documentation.

Default	Range	Restart Required
No	Yes and No	Yes

Use DNS SRV type query

Select **Yes** to use DNS SRV for outbound proxy lookup. Otherwise, select **No**. See Load-Balancing SIP Calls, on page 142 for information on using DNS SRV for load-balancing SIP calls.

Note If you enable **Resolve SRV records locally**, you must select **Yes** to ensure the feature works properly.

Default	Range	Restart Required
No	Yes and No	Yes

Resolve SRV records locally

Select to resolve the SRV domain name with a local configuration file instead of a DNS Server.

Note If you enable **Resolve SRV records locally**, you must select **Yes** to use DNS SRV type query. Otherwise, this feature will not work.

See the *Configuration Guide for Cisco Unified Custom Voice Portal* for additional information about local SRV configuration.

Default	Range	Restart Required
None	Enabled or Disabled No	Yes

Outbound Proxy Host

If you selected Enable Outbound Proxy, select an Outbound Proxy Server from the drop-down list. These are the SIP Proxy Servers that have been added to the Operations Console. For information on configuring a SIP Outbound Proxy Server, consult the CUSP documentation.

Default	Range	Restart Required
No	Valid IP Address	Yes

Outbound SRV domain name/Server group name (FQDN)

If you use a hostname that is an SRV type record instead of a standard DNS type record, this field contains a fully qualified domain name that is configured on the DNS server. Otherwise, the field contains an SRV configuration file.

For example, outbound calls made from CVP SIP service will be addressed to the URL of sip:<label>@<srvfqdn>. Redundant proxy servers, for example, can route calls using such a configuration.

Default	Range	Restart Required
None	Follows the same validation rules as hostname, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash. 0 - 256 character length.	Yes

DN on the Gateway to Play the Ringtone

Dialed Number (DN) configured on the gateway to play ringtone (dedicated VoIP dial peer).

To learn the DN configured on the gateway to play ringtone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 142.

Default	Range	Restart Required
9191	Any valid label	No

DN on the Gateway to Play the Error Tone

Dialed Number (DN) configured on the gateway to play the error.wav file (dedicated VoIP dial peer).

To learn the DN configured on the gateway to play the error tone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 142.

Default	Range	Restart Required
9292	Any valid label	No

Override System Dialed Number Pattern Configuration

Use the new Dialed Number Pattern system configuration, but maintain the existing Call Server interface.

Default	Range	Restart Required
Unchecked	The override check box's default state differs depending on the device state: • For new devices, override is disabled (unchecked). New Unified CVP Call Server devices will use configured system-level dialed number patterns by default. • For upgraded devices, override is enabled (checked). Upgraded Unified CVP Call Server devices will use device-level dialed number patterns by default.	No

Advanced Configuration

Outbound proxy port

Specify the port to be used.

Default	Range	Restart Required
5060		No

Outgoing transport type

Specifies the outgoing transport, you can set it as TCP or UDP.

Default	Range	Restart Required
TCP	TCP or UDP	Yes

Port number for incoming SIP requests

Specify the port to be used foe incoming SIP requests.

Default	Range	Restart Required
5060		Yes

Incoming transport type

Specifies the incoming transport type.

Default	Range	Restart Required
TCP+UDP	TCP, UDP, TCP+UDP	Yes

Time to wait for ICM instructions

Specifies the wait time in milliseconds for ICM instructions. It is optional value for the list addition.

Default	Range	Restart Required
2000		No

SIP info tone duration

Specifies the wait time in milliseconds for SIP info tone. It is optional value for the list addition.

Default	Range	Restart Required
100		No

SIP info comma duration

Specifies the wait time in milliseconds for SIP info comma. It is optional value for the list addition.

Default	Range	Restart Required
100		Yes

Generic Type Descriptor (GTD) parameter Forwarding

To be added

Default	Range	Restart Required
UUS		No

Prepend digits

Specifies the number of digits to be removed for SIP URI user number.

Default	Range	Restart Required
0	0-20	No

UDP Retransmission Count

Specifies the number of UDP retransmission will be attempted.

Default	Range	Restart Required
3		No

Use Error Refer

Flag for play error tone when call fails to caller.

Default	Range	Restart Required
False	True or False	Yes

IOS Gateway Options Dynamic Routing

Default	Range	Restart Required
	True or False	Yes

IOS Gateway Options Reporting

Reports on resource utilization.

Default	Range	Restart Required
	True or False	Yes

Security Properties

Incoming secure port

Specify the port to be used.

Default	Range	Restart Required
5061		No

Incoming secure protocol

This option is grayed out as it is prepopulated.

Default	Range	Restart Required
TLS		No

Outgoing secure protocol

This option is grayed out as it is prepopulated.

Default	Range	Restart Required
TLS		No

Supported TLS Versions

This allows to select the version of TLS to be supported for securing the SIP signaling on the IVR leg. The TLS version currently supported is TLSv1.2.

Default	Range	Restart Required
TLS v1.2	TLSv1.2	Yes

Note When you select a a given TLS version, Unified CVP supports SIP TLS requests for that version and the higher supported versions.

Supported Ciphers

This field defines the ciphers, which is supported by Unified CVP, with key size lesser than or equal to 1024 bits.

The default cipher is TLS_RSA_WITH_AES_128_CBC_SHA, which is pre-populated and cannot be deleted as it is mandatory for TLSv1.2.

Cipher configuration is available only if TLS is enabled.

Default	Range	Restart Required
TLS_RSA_WITH_AES_128_CBC_SHA		Yes

Note If you are using CUBE version 16.6 and higher, you must manually change the crypto suite to 128 by enabling CLI on the dial-peer towards CVP as shown:

```
voice class srtp-crypto 1
 crypto 1 AES_CM_128_HMAC_SHA1_32

dial-peer voice xxxx voip (Dial-peer to CVP)
    ...
    voice-class sip srtp-crypto 1
```

SIP Header Passing (to ICM)

Header Name

Specify the SIP header name and click **Add** to add it to the list of SIP headers passed to ICM.

Default	Range	Restart Required
None	Maximum length of 210 characters.	No

Parameter

This field is optional for list addition.

Default	Range	Restart Required
None	Maximum length of 210 characters.	No

Local Static Routes

Note Enable "Override System Dialed Number Pattern Configuration" to configure these values.

Dialed Number (DN)

Creates a Static Proxy Route Configuration Table. You must create static routes if you do not use a SIP Proxy Server. Before adding a local static route, you must enter a value into both the Dialed Number (DN) and IP Address fields so that the local static route is complete.

Click **Add** to create a proxy route using the Dialed Number (DN) and the IP address/Hostname entered above the **Add** button. The newly created proxy route is added to the list of proxy routes displayed in the box below the Add button.

Click **Remove** to delete the selected DN from the list box of Dialed Numbers.

Default	Range	Restart Required
None	Dialed number pattern, destination (must be format of NNN.NNN.NNN.NNN or a hostname). See Valid Formats for Dialed Numbers, on page 142 for more information.	No

IP Address/Hostname/Server Group Name

The IP address, hostname, or server group SRV domain name.

Note If you use Server Group Name, you must select **Yes** to use **DNS SRV type query** and you must enable **Resolve SRV records locally** to ensure the feature works properly.

Default	Range	Restart Required
None	Valid IP address, hostname, or SRV domain name	No

Dialed Number (DN) Patterns

Note Enable "Override System Dialed Number Pattern Configuration" to configure these values.

Patterns for sending calls to the originator :

Dialed Number (DN)

Creates a SIP Send Back to Originator Lookup Table. Specify the DN patterns to match for sending the call back to the originating gateway for VXML treatment. For the Unified CVP branch model, use this field to automatically route incoming calls to the Call Server from the gateway back to the originating gateway at the branch. For information on the Unified CVP branch model, see *Planning Guide for Cisco Unified Customer Voice Portal*.

This setting overrides sending the call to the outbound proxy or to any locally configured static routes. It is also limited to calls from the IOS gateway SIP "User Agent" because it checks the incoming invite's User Agent header value to verify this information. If the label returned from ICM for the transfer matches one of the patterns specified in this field, the call is routed to `sip:<label>@<host portion of from header of incoming invite>`.

Three types of DNs work with Send To Originator: VRU label returned from ICM, Agent label returned from ICM, and Ringtone label.

Send To Originator does not work for the error message DN because the inbound error message is played by survivability and the post-route error message is a SIP REFER. (Send To Originator does not work for REFER transfers).

Note For Send To Originator to work properly, the call must be TDM originated and have survivability configured on the pots dial peer.

Default	Range	Restart Required
None	See Valid Formats for Dialed Numbers, on page 142 for more information.	No

Patterns for RNA timeout on outbound SIP calls:

- Dialed Number (DN)

Creates a Dialed Number (DN) pattern outbound invite timeout using the DN and Timeout entered above the Add button. Click **Add** to add the newly created DN pattern outbound invite timeout to the list displayed in the box below the Add button.

Click **Remove** to delete the selected DN pattern outbound invite timeout from the list.

Default	Range	Restart Required
None	See Valid Formats for Dialed Numbers, on page 142 for more information.	No

Timeout (Seconds)

The number of seconds the SIP Service waits for transferee to answer the phone or accept the call.

If a selected termination (for either a new or transferred call) returns a connection failure or busy status, or if the target rings for a period of time that exceeds the Call Server's ring-no-answer (RNA) timeout setting, the Call Server cancels the transfer request and sends a transfer failure indication to Unified ICM. This scenario causes a router requery operation. The Unified ICM routing script then recovers control and has the opportunity to select a different target or take other remedial action.

Default	Range	Restart Required
60 seconds	5 - 60	No

Custom ringtone patterns:

Dialed Number (DN)

Specify a custom Dialed Number (DN) pattern. Click **Add** to add the newly created DN pattern to the list displayed in the box below the Add button.

To learn the DN configured on the gateway to play ringtone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. See Ringtone Dialed Number Learning on Gateway Example, on page 142.

Default	Range	Restart Required
None	See Valid Formats for Dialed Numbers, on page 142	No

Ringtone Media file name

The file name of the ringtone to be played for the respective dialed number.

The ringtone media file must be saved to the VXML Gateway. See Transfer Script and Media File to Gateway, on page 192 for more information.

Default	Range	Restart Required
None	0 - 256 characters. Spaces are not permitted. Provide the URL for the stream name in the following form: `rtsp://<streaming server IP address>/<port>/<foldername>/<filename>.rm`	No

Post Call Survey DNIS Mapping

Note Enable "Override System Dialed Number Pattern Configuration" to configure these values.

Incoming Call Dialed Number (DN)

Click **Add** to add the newly created DN pattern to the list displayed in the box below the Add button. Click **Remove** to delete the selected DN pattern from the list.

Default	Range	Restart Required
None	Dialed Number pattern, destination (must be in the form of NNN.NNN.NNN.NNN or a hostname). See Valid Formats for Dialed Numbers, on page 142 for more information.	No

Survey Dialed Number (DN)

Click **Add** to add the newly created DN to the list displayed in the box below the Add button. Click **Remove** to delete the selected DN from the list.

Default	Range	Restart Required
None	Accepts only alphanumeric characters	No

SIP Transport Setting for UDP

UDP is the default transport in high availability SIP deployments. One of the drawbacks of TCP is the slow response times encountered in transmission failures due to network outages. The slow response times for TCP are caused by slowness in detecting a connection reset in applications running on other SIP devices in the network. This slowness is due to the buffering window of the TCP connection. Higher call loads fill the buffer faster and thus the notification of a connection down with an I/O exception arrives more quickly. Lower call loads or a test with a single call can be affected by as much as a 30-second delay or more. Invite Retry Counts

and Retry Timeout settings are not effective when using TCP transport on SIP calls because of the persistent nature of the TCP connection.

For SIP RFC, use TCP transport in deployments in which packet sizes exceed 1300 bytes, the size of a Maximum Transmission Unit (MTU). Using UDP, if a SIP message exceeds 1300 bytes, then it might fragment and cause problems with delivery and message ordering. See Section 18.1.1 Sending Requests in RFC 3261. A SIP packet can exceed 1 MTU for various reasons; for example, if there are many `Via` headers, or the media portion is very large in bytes.

While the SIP Request For Comments (RFC) mandates the support of both TCP and UDP, not all SIP User Agents support TCP. However, the Unified CVP SIP Service, IOS Gateway, and Cisco Unified Communications Manager use both transport protocols.

Load-Balancing SIP Calls

SIP calls can be load balanced across destinations in several different ways:

- Using the CUSP, define several static routes with the same route pattern and priorities and weights.
- Using DNS, configure SRV records with priorities and weights. A proxy server is not necessary in this method, but both the DNS client and the server settings must be configured and operating successfully for DNS "A" and "SRV" type queries to work. Configure SRV queries to be used wherever outbound SIP calls are made, such as on the IOS Ingress gateway, on the Call Server itself, and on Cisco Unified CM.

Valid Formats for Dialed Numbers

Valid dialed number patterns are the same as for the ICM label sizes and limitations, including:

- Use the period (**.**) or the **X** character for single-digit wildcard matching in any position.

Note Lowercase letter "x" cannot be used as a wildcard.

- Use the greater than (), asterisk (*****), or exclamation (**!**) character as a wildcard for 0 or more digits at the trailing end of a DN.
- Do not use the character **T** for wildcard matching.
- Dialed numbers must not be longer than 24 characters.
- 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 more than one wildcarded pattern, precedence is given from top to bottom of the configured DN list.

Ringtone Dialed Number Learning on Gateway Example

To verify the dialed number configured on the gateway to play ringtone, execute the `sh run` command on the gateway and look for the dial peer that matches the incoming dialed number. For example:

```
sh run

paramspace english index 0

paramspace english language en

paramspace english location flash

service ringtone flash:ringtone.tcl
```

```
paramspace english prefix en

service ringtone

voice-class codec 1

voice-class sip rel1xx disable

incoming called-number 9191T

dtmf-relay rtp-nte h245-signal h245-alphanumeric

no vad
```

Set Up Infrastructure

The Call Server, Unified CVP VXML Server, and Reporting Server offer one or more services. The Call Server provides SIP, IVR, and ICM call services. The Unified CVP VXML Server provides VXML services, and the Reporting Server provides reporting services. Changes to Infrastructure settings affect all services that use threads, publish statistics, send syslog events, or perform logging and tracing. For example, changing the **syslog server** setting applies to all services that write to syslog.

Procedure

Procedure

Step 1 If you are adding a new Call Server, refer to Add Unified CVP Call Server, on page 122. If you want to change infrastructure settings for an existing Call Server, refer to Edit Unified CVP Call Server, on page 145.

Step 2 Fill in the appropriate configuration settings as described in Infrastructure Settings, on page 143.

Step 3 When you finish configuring Call Server services, click **Save** to save the settings in the Operations Console database, or click **Save & Deploy** to save the changes to the Operations Console database and apply them to the Call Server.

Infrastructure Settings

The following table describes the infrastructure configuration settings.

Table 28: Infrastructure Service Configuration Settings

Property	Description	Default	Range	Restart Required
Configuration: Thread Management				
Maximum Threads	Maximum number of threads allocated in the thread pool, that can be shared by all services running as part of a CVP Web Application.	300	100 to 1000	No
Statistics				

Property	Description	Default	Range	Restart Required
Statistics Aggregation Interval	Length of time (in minutes) during which system and service statistics are published to the log file and SNMP events are sent. Once published, the counters will reset and aggregate data for the next interval. Note that this is different than the real time snapshot statistics (for the number of concurrent calls). Realtime statistics are on-demand and have no intervals. Statistics Publishing Interval will be used for attributes like the number of calls in last interval, the number of transfers in last interval, and the number of HTTP sessions in last interval.	30 minutes	10 - 1440 minutes	No
Log File Properties				
Max Log File Size	Maximum size of a log file in Megabytes before a new log file is created.	10 MB	1 through 100 MB	No
Max Log Directory Size	Maximum number of Megabytes to allocate for disk storage for log files. **Note** Modifying the value to a setting that is below the default value might cause logs to be rolled over quickly. Consequently, log entries might be lost, which can affect troubleshooting.	20000 MB	500 - 500000 The log folder size divided by the log file size must be less than 5000.	No
Configuration: Primary Syslog Settings				
Primary Syslog Server	Hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Primary Syslog Server Port Number	Port number of Primary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Primary Backup Syslog Server	Hostname or IP address of the Primary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or host name.	No

Property	Description	Default	Range	Restart Required
Primary Backup Syslog Server Port Number	Port number of Primary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Configuration: Secondary Syslog Settings				
Secondary Syslog Server	Hostname or IP address of Secondary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Secondary Syslog Server Port Number	Port number of Secondary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Secondary Backup Syslog Server	Hostname or IP address of the Secondary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or hostname.	No
Secondary Backup Syslog Server Port Number	Port number of Secondary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No

Edit Unified CVP Call Server

You can change the configuration for a Unified CVP Call Server.

Related Topics

Add Unified CVP Call Server, on page 122
Shut Down Server, on page 59
Start Server, on page 58
Upload Log Messages XML File, on page 181
Download Log Messages XML File, on page 178
View Unified CVP Call Server Statistics, on page 147
View Device Status, on page 39

Procedure

To edit a Unified CVP Call Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Call Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Unified CVP Call Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Unified CVP Call Server Configuration window opens with the current settings displayed.

Step 3 Change the desired configuration settings on the General tab as described in Unified CVP Call Server Settings, on page 148.

You cannot change the IP Address.

Step 4 Optionally, click the **Change Type** button to change the services that are turned on for this Unified CVP Call Server.

Step 5 Select the appropriate tab and change the desired settings:

Configuration Tabs:

- Set Up ICM Service, on page 125
- Set Up IVR Service, on page 130
- Set Up SIP Service, on page 129
- Add or Remove Device From Device Pool, on page 62
- Set Up Infrastructure, on page 143

Step 6 When you finish configuring the Unified CVP Call Server, click **Save** to save the settings, or click **Save & Deploy** to save the changes and apply them to the Unified CVP Call Server.

Step 7 If you changed a configuration setting that requires a restart, shut down and start the Unified CVP Call Server.

Configuration settings that require a restart of the Unified CVP Call Server are identified in Unified CVP Call Server Settings, on page 148.

Delete Unified CVP Call Server

Deleting a Unified CVP Call Server deletes the configuration of the selected Unified CVP Call Server in the Operations Console database and removes the Unified CVP Call Server from the displayed list of Unified CVP Call Servers.

Procedure

To delete a Unified CVP Call Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Call Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Unified CVP Call Server by clicking the radio button preceding it and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

Find Unified CVP Call Server

Use the following procedure to locate a Unified CVP Call Server that has been added in the Operations Console.

Procedure

To find a Unified CVP Call Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Call Server** from the Main menu.

The Find, Add, Delete, Edit window lists the available Unified CVP Call Servers sorted by name, 10 at a time.

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 **Hostname**, selecting a modifier such as **begins with**, entering your search term, and then clicking **Find**.

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

View Unified CVP Call Server Statistics

You can view realtime, interval, and aggregate data for the services enabled on a Unified CVP Call Server.

Related Topics

SIP Service Call Statistics, on page 48
IVR Service Call Statistics, on page 46
Infrastructure Statistics , on page 46

Procedure

To view device statistics:

Procedure

Step 1 Select **Device Management** > **Unified CVP Call Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Find the Unified CVP Call Server by using the procedure in Find Unified CVP Call Server, on page 147.

Step 3 From the list of matching records, select the Unified CVP Call Server that you want to edit.

Step 4 Click **Edit**.

The Edit Unified CVP Call Server Configuration window opens with the current settings displayed.

Step 5 Click the **Statistics** icon in the toolbar.

Statistics are reported for the selected device.

Unified CVP Call Server Settings

If you are adding a Call Server (Add Unified CVP Call Server) or editing a Call Server (Edit Unified CVP Call Server), you can configure the Call Server by filling in or changing values for one or more of these settings.

Table 29: Call Server Configuration Settings

Property	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Call Server	None	Valid IP address	No
Hostname	The hostname of the Call Server	None	A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9,and a dash	No
Description	The description of the Call Server	None	0 - 1024 characters	No

Property	Description	Default	Range	Restart Required
Enable Secure Communication with the Ops Console	Select to enable secure communications between the Operations Console and the Call Server. The device is accessed using SSH and files are transferred using HTTPS. You must configure secure communications *before* you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	None	Enabled or Disabled	Yes
Device Version	Lists the Release and Build Number for this device.	Read Only	Read Only	Read Only
Services				
ICM	Enables the Call Server to communicate with an ICM Server. The ICM Server must be configured in the Operations Console.	None	Not applicable	Yes
IVR	The IVR Service creates VXML pages that implement the Micro-Applications, based on Run Script instructions received from the ICM Server. The VXML pages are sent to the VXML Gateway to be executed.	None	Not applicable	Yes
SIP	Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks and SIP phones. Configure the SIP service if you are adding a new Call Server or editing a Call Server and you are using the Call Director or Comprehensive call flow models.	None	Not applicable	Yes

Unified CVP Reporting Server Setup

From the Unified CVP Reporting Server option in the Device Management menu, you can configure one or more Unified CVP Reporting Servers.

Reporting provides historical reporting to a distributed self-service deployment in a call center. The Unified CVP Reporting Server receives reporting data from one or more Unified CVP Call Servers and Unified CVP VXML Servers, and stores that data in an Informix database. Call data is stored in a relational database, on which you can write custom reports. Administrators can use the Operations Console to schedule data removal

(delete) and database backups. Multiple Unified CVP Call Servers can send data to a single Unified CVP Reporting Server.

You can use third-party reporting tools such as Crystal Reports to generate and view reports on call data. Unified CVP provides four sample Crystal report templates. One of the included templates provides an example of joining Unified CVP and ICM data to create a comprehensive report.

Note Before you start with any of the following tasks, connect to the remote desktop of the Reporting Server machine and add a user for the Cisco CVP WebServicesManager:

1. Open `services.msc`.
2. Right click **Cisco CVP WebServicesManager** and select **Properties**.
3. Select the **Logon** tab and add the Administrator credentials under this account.
4. Restart the Cisco CVP WebServicesManager service.

You can perform the following tasks:

Add Unified CVP Reporting Server

Create a new Unified CVP Reporting Server either by using an existing Unified CVP Reporting Server configuration as a template or by filling in its values from scratch.

Before You Begin

You must configure the Unified CVP Call Server to associate with the Unified CVP Reporting Server *before* configuring the Unified CVP Reporting Server.

Collect the following information about the Unified CVP Reporting Server and Reporting Database during the installation of Unified CVP software:

Procedure

- Hostname of the Call Servers associated with the Unified CVP Reporting Server

Note A Call Server can only be associated with one Unified CVP Reporting Server.

- Hostname and IP address of the server on which the Reporting Database resides
- Password for the Reporting Database user

Procedure

To add a Unified CVP Reporting Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

A window listing Unified CVP Reporting Servers opens.

Note To use an existing Unified CVP Reporting Server as a template for creating the new Unified CVP Reporting Server, select the Unified CVP Reporting Server by clicking the radio button preceding it and then click **Use As Template**.

Step 2 Click **Add New**.

The Unified CVP Reporting Server Configuration window opens to the General Tab.

Step 3 Fill in the IP Address and hostname for the Unified CVP Reporting Server and fill in any other desired information.

Step 4 Optionally, click **Enable secure communications with the Ops Console** to secure communications between the Operations Console and the Unified CVP Call Server.

Step 5 Associate one or more Unified CVP Call Servers to the Unified CVP Reporting Server by selecting a Unified CVP Call Server listed in the Available pane and clicking the right arrow to add it to the Selected pane.

Step 6 Select the **Reporting Properties** tab and configure reporting properties.

Step 7 Optionally, select the **Device Pool** tab and add the Unified CVP Reporting Server to a device pool.

Step 8 Optionally, select the **Infrastructure** tab and configure log file and syslog settings.

Step 9 When you finish configuring the Reporting Server, click **Save** to save the settings in the Operations Server database. Click **Save & Deploy** to deploy the changes to the Unified CVP Reporting Server page.

Related Topics

Delete Reporting Server, on page 164
Edit Unified CVP Reporting Server, on page 155
General Unified CVP Reporting Server Information Setup, on page 151
Reporting Properties Setup, on page 152
Add or Remove Device From Device Pool, on page 62
Unified CVP Reporting Server Infrastructure Settings, on page 153
Device Information Field Descriptions, on page 118

General Unified CVP Reporting Server Information Setup

You can configure settings that identify the Unified CVP Reporting Server, associate it with one or more Unified CVP Call Servers, and enable or disable security on the General Tab.

Table 30: Unified CVP Reporting Server General Tab Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Unified CVP Reporting Server	None	Valid IP address	Yes
Hostname	The host name of the Unified CVP Reporting Server machine	None	Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9	Yes

Field	Description	Default	Range	Restart Required
Description	An optional text description for the Unified CVP Reporting Server	None	Up to 1024 characters	No
Enable Secure Communication with the Ops Console	Select to enable secure communications between the Operations Server and this component. The Unified CVP Reporting Server is accessed using SSH and files are transferred using HTTPS. You must configure secure communications *before* you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	Off	On or Off	No
Device Version	Lists the Release and Build Number for this device.	Read Only	Read Only	Read Only
Associate Unified CVP Call Server(s)	Select one or more Call Servers to associate with the Unified CVP Reporting Server. You must select at least one Unified CVP Call Server. Call data for all SIP, and VXML calls handled by this Unified CVP Call Server are stored in the Reporting Database. Click the right arrow to add a Call Server to the Selected pane. Click the left arrow to remove a Unified CVP Call Server from the Selected pane.	None	A given Unified CVP Call Server can only be associated with one Unified CVP Reporting Server.	No

Reporting Properties Setup

You can configure Reporting Server settings on the Reporting Properties Tab.

Table 31: Reporting Server Reporting Properties Tab Configuration Settings

Field	Description	Default	Range	Restart Required
Configuration				

Field	Description	Default	Range	Restart Required
Enable Reporting	Enables the Reporting Server to receive call data from the associated Call Server(s).	Yes	Yes or No	Yes
Max. File Size (MB):	Defines the maximum size of the file used to record the data feed messages during a database failover. This can be limited by the amount of free disk space.	100	1 through 250 MB	No

Unified CVP Reporting Server Infrastructure Settings

The Unified CVP Reporting Server publishes statistics on the number of reporting events received from the Unified CVP VXML Server, the SIP Service, and the IVR Service. It also publishes the number of times the Reporting Server writes data to the Reporting database. You can configure the interval at which the Reporting Server publishes these statistics, the maximum log file and directory size, and the details for recording syslog messages on the Reporting Server Infrastructure tab.

Table 32: Unified CVP Reporting Server Infrastructure Tab Configuration Settings

Field	Description	Default	Range	Restart Required
Configuration: Thread Management				
Maximum Threads	(Required) The maximum thread pool size in the Reporting Server Java Virtual Machine.	525	100 - 525	Yes
Advanced				
Statistics Aggregation Interval	The Unified CVP Reporting Server publishes statistics at this interval.	30 minutes	10 - 1440	Yes
Log File Properties				

Field	Description	Default	Range	Restart Required
Max Log File Size	(Required) Maximum size of the log file in megabytes. The log file name follows this format: `CVP.DateStamp.SeqNum.log` example: For example: `CVP.2006-07-04.00.log` After midnight each day, a new log file is automatically created with a new date stamp. When a log file exceeds the max log file size, a new one with the next sequence number is created, for example, when `CVP.2006-07-04.00.log` reaches 5 Mb, `CVP.2006-07-04.01.log` is automatically created.	10 MB	1 through 100 MB	Yes
Max Log Directory Size	(Required) Maximum size of the directory containing Unified CVP Reporting Server log files. **Note** Modifying the value to a setting that is below the default value might cause logs to be rolled over quickly. Consequently, log entries might be lost, which can affect troubleshooting.	20000 MB	500 - 500000 MB Max Log File size < Max Log Directory Size Max Log File size > 1 Max Log Dir Size / Max Log File Size cannot be greater than 5000	Yes
Configuration: Primary Syslog Settings				
Primary Syslog Server	Hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Primary Syslog Server Port Number	Port number of Primary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No

Field	Description	Default	Range	Restart Required
Primary Backup Syslog Server	Hostname or IP address of the Primary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or hostname.	No
Primary Backup Syslog Server Port Number	Port number of Primary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Configuration: Secondary Syslog Settings				
Secondary Syslog Server	Hostname or IP address of Secondary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Secondary Syslog Server Port Number	Port number of Secondary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Secondary Backup Syslog Server	Hostname or IP address of the Secondary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or hostname.	No
Secondary Backup Syslog Server Port Number	Port number of Secondary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No

Edit Unified CVP Reporting Server

Procedure

To edit a Unified CVP Reporting Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Unified CVP Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Reporting Server Configuration window opens.

Step 3 On the **General** tab, change the desired general information. You cannot change the IP address of the Reporting Server.

Step 4 Select the **Reporting Properties** tab and edit the reporting properties.

Step 5 Optionally, you can select the **Device Pool** tab and add or remove the Reporting Server from a device pool.

Step 6 Optionally, you can select the **Infrastructure** tab and change log file and syslog settings.

Step 7 When you finish configuring the Unified CVP Reporting Server, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to deploy the changes to the Unified CVP Reporting Server.

Related Topics

Delete Reporting Server, on page 164
Add Unified CVP Reporting Server, on page 150
Reporting Properties Setup, on page 152
Add or Remove Device From Device Pool, on page 62
Find Reporting Server, on page 164
Device Information Field Descriptions, on page 118

Change Reporting Database User Password

The Unified CVP installation procedure creates the following two user accounts and sets an initial password for each account. You can change these passwords from the Reporting Server screen in edit mode, but you can only change one user password at a time.

Procedure

- Unified CVP Database Administrator - Uses the Operations Console to run backups, check database used space, and add and remove Reporting users.
- Unified CVP Database User - Connects, inserts, and updates records in the Informix database. This user cannot modify the Reporting schema.

Procedure

To change a reporting database user password:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select the **Database Administration** menu in the toolbar, then select **Change User Passwords**.

The Reporting Server: Change User Passwords page opens, displaying the IP address and hostname for the currently selected Reporting Server.

Step 4 In the **User** field, use the drop-down menu to select the user whose password you want to change.

Step 5 In the **Old Password** field, enter the existing password for that user.

Step 6 In the **New Password** field, enter the new password.

Note Passwords must follow guidelines for secure passwords.

Step 7 In the **Reconfirm Password** field, retype the new password.

Step 8 Click **Save & Deploy** to save the changes to the Operations Console database and deploy them to the Reporting Server.

Reporting User Management

The cvp_dbadmin should create reporting users to run reports against the Reporting database. Reporting users should have read-only access to the Reporting database, so they cannot accidentally modify the database schema or data.

Add New Reporting Users

To add a new reporting user to the Reporting Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

You can also search for a Reporting Server.

The Edit Reporting Server Configuration window opens.

Step 3 Select the **Database Administration** menu in the toolbar, and then select **Manage Reporting Users**.

The Reporting Server: Manage Users windows opens, listing the IP address and host name for the selected Reporting Server.

Step 4 In the Manage Users pane, click **Add User**.

Step 5 Enter the name for the user in the **Username** field.

Step 6 Enter a password for the new user in the **Password** field.

Step 7 Retype the password in the **Reconfirm Password** field.

Step 8 Click **Add** to add the user.

Change Reporting User Password

To change a reporting user's password:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

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

You can also search for a Reporting Server.

The Edit Reporting Server Configuration window opens.

Step 3 Select the **Database Administration** menu in the toolbar, and then select **Manage Reporting Users**.

The Reporting Server: Manage Users window opens, listing the IP address and hostname for the currently selected Reporting Server.

Step 4 In the Manage Users pane, click **Change Password**.

Step 5 From the Available users list, select the user whose password you want to change and click the left arrow. The user name is displayed in **Username** field.

Step 6 Type the original password in **Old Password** field.

Step 7 In the **New Password** field, type the new password.

Step 8 In the **Reconfirm Password** field, retype the new password.

Step 9 Click **Change** to make the change.

Remove Reporting Users

To remove a reporting user from the Reporting Server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

You can also search for a Reporting Server.

The Edit Reporting Server Configuration window opens.

Step 3 Select **Database Administration** in the toolbar, then select **Manage Reporting Users**.

The Reporting Server: Manage Users window opens, listing the IP address and host name for the currently selected Reporting Server.

Step 4 From the Available users list, select the user to remove and click the left arrow. The user is displayed in the Username field.

Step 5 Enter the Database Administrator password.

Step 6 Click **Delete** to delete the selected user.

Run Reporting Database Backup

By default, Reporting Database backups are disabled. You can choose to schedule backups of the Reporting database or run backups on demand. When you enable backups, files are saved to the Reporting Server's local file system. You are responsible for managing backed-up files. Scheduled backups occur once each day. You can configure the time of day at which backups occur. A maximum of two backups and a minimum of one backup will be available at any time on the local machine.

Procedure

To run a reporting database backup:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

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

The Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select the **Database Administration** menu in the toolbar, then select **Reporting Database Backups**.

The Reporting Server - Database Backup Activities page opens. The IP address and host name for the currently selected Reporting Server are listed.

Step 4 To launch a backup immediately, click **Backup Now**. To schedule a time for daily backups, select **Schedule Daily Backups** and then select the hour and minute of the start time.

Step 5 Enter your cvp_dbadmin password and click **Save & Deploy**.

Related Topics

Change Reporting Database User Password, on page 156
Set Up Reporting Database Delete, on page 160
Cancel Reporting Database Backup, on page 160
Reporting User Management, on page 157
View Database Details, on page 162
View Reporting Statistics, on page 163

Cancel Reporting Database Backup

By default, Reporting Database backups are disabled. You can choose to schedule backups of the Reporting database or run backups on demand. You can cancel daily backups at any time.

Procedure

To cancel a reporting database backup:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

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

The Edit Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select the **Database Administration** menu in the toolbar, and then select **Reporting Database Backups**.

The Reporting Server - Database Backup Activities page displays. The IP address and host name for the currently selected Reporting Server are listed.

Step 4 Click **Cancel Daily Backups**.

Step 5 Enter your cvp_dbadmin Password and **Save & Deploy**.

Related Topics

Change Reporting Database User Password, on page 156
Set Up Reporting Database Delete, on page 160
Reporting User Management, on page 157
View Database Details, on page 162
View Reporting Statistics, on page 163

Set Up Reporting Database Delete

You can delete call data from the Reporting Database. Data Delete is run daily at the time you specify. Each category of call data is retained for a default number of days, before being deleted.

Procedure

To configure Reporting Database Delete settings:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select the **Database Administration** menu in the toolbar, and then select **Data Delete**.

The Reporting Server - Database Delete Settings page opens displaying the IP address and host name for the currently selected Reporting Server.

Step 4 In the Data Delete section of the page, you can change the data retention time for each category of data.

Step 5 Select the hours and minutes to run the delete each day.

Step 6 Enter your cvp_dbadmin password and click **Save & Deploy**.

Related Topics

Run Reporting Database Backup, on page 159
Cancel Reporting Database Backup, on page 160
Change Reporting Database User Password, on page 156
Reporting User Management, on page 157
View Database Details, on page 162
View Reporting Statistics, on page 163

Reporting Data Category Deletion

Using the Operations Console, you can select the time of day to run database delete, and set the number of days that the data is retained by data category. The following table describes each category of data that you can delete from the Reporting Database and lists the default number of days that this data is kept before purging. A high level category, such as Call, cannot have a lower retention time than a dependent category, such as Call Event.

Choosing how much data is to be retained is a sensitive matter. If a database space fills up, then the database is able to continue processing until data is deleted. This is complicated by the fact that when Informix increases its extent for a table within the data file, due to data growth, extension remains even after the data is deleted. This causes space within the file to be reserved even if actual space is no longer needed. The only way to regain the space is to rebuild the table.

Emergency delete is a critical safety mechanism. If used space has grown past the system's threshold, the Reporting Server creates an SNMP trap and the data is deleted. The SNMP notification alerts the user to the loss of data and the data is deleted.

Table 33: Number of Days to Retain Data Before Purging

Data Category	Description	Default
Call	Detailed information about calls received by Unified CVP.	30
Call Event	Call state change event messages published by the Call Server and Unified CVP VXML Server. SIP and IVR services publish call state change event messages when a SIP call changes its state. These states include call initiated, transferred, terminated, aborted, or an error state.	30

Data Category	Description	Default
VXML Session	VXML session data includes application names, session ID, and session variables. Session variables are global to the call session on the Unified CVP VXML Server. Unlike element data, session data can be created and modified by all components (except the global error handler, hotevents, and XML decisions).	30
VXML Element	A VXML element is a distinct component of a voice application call flow whose actions affect the experience of the caller. A VXML element contains detailed script activity to the element level, such as, Call Identifiers, activity time stamp, VXML script name, name and type of the VXML element, and event type.	15
VXML ECC Variable	Expanded Call Context (ECC) variables that are included in VXML data. Unified CVP uses ECC variables to exchange information with Unified ICME.	15
VXML Voice Interact Detail	Application detailed data at the script element level from the Unified CVP VXML Server call services. This data includes input mode, utterance, interpretation, and confidence.	15
VXML Session Variable	VXML session variables are global to the call session on the Unified CVP VXML Server.	15
VXML Element Detail	The names and values of element variables.	15
Callback	Retention days for Courtesy Callback reporting data	15
Trunk Utilization Usage	Retention days for Gateway Trunk Utilization reporting data	15

The data categories are hierarchical. For example, Call data includes Call Event and VXML Session data.

VXML Session Data Categories:

- VXML Element
  - VXML ECC Variable
  - VXML Voice Interact Detail
  - VXML Session Variable
  - VXML Element Detail

Note A high level category, such as Call, cannot have a lower retention time than a dependent category, such as CallEvent.

View Database Details

You can view the size of a Reporting database.

Procedure

To view database details:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select the **Database Administration** menu in the toolbar, and then select **Database Details**.

The Reporting Server - Disk Drives: Housing Database Files page opens, displaying the IP address and host name for the currently selected Reporting Server along with the following database information:

Reporting Database Details:

- Database Name - Name of the database.
- Total Size (MB) - Total data size.

  Note When the usage of the database increases beyond 200 GB, it starts occupying the head room space. In this scenario, the free size is shown as 0(zero) bytes.
- Free size (MB) - Amount of space that has not been taken by extents.
- Used Size (MB) - Data space used.
- Extent size (MB) - Space reserved for tables. This size may be greater than the total size.
- % Free Size - The percent of space that has not been extended (reserved). This might be greater than 100 percent.

Related Topics

Run Reporting Database Backup, on page 159
Cancel Reporting Database Backup, on page 160
Change Reporting Database User Password, on page 156
Set Up Reporting Database Delete, on page 160
Reporting User Management, on page 157
View Reporting Statistics, on page 163

View Reporting Statistics

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

Procedure

To get Reporting Server statistics:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window opens.

Step 2 Select a Unified CVP Reporting Server by clicking the link in the Hostname field or by clicking the radio button preceding it, and then clicking **Edit**.

The Edit Unified CVP Reporting Server Configuration window opens with the current settings displayed.

Step 3 Select **Statistics** in the toolbar.

The Unified CVP Reporting Server Statistics , on page 55 are listed in the Reporting tab.

Related Topics

Run Reporting Database Backup, on page 159
Cancel Reporting Database Backup, on page 160
Change Reporting Database User Password, on page 156
Set Up Reporting Database Delete, on page 160
Reporting User Management, on page 157
View Database Details, on page 162

Delete Reporting Server

You can remove a Reporting server from the Operations Console. Deleting a Reporting Server removes its configuration from the Operations Console database and removes the Reporting Server from the displayed list of Reporting Servers.

Procedure

To delete a reporting server:

Procedure

Step 1 Select **Device Management** > **Unified CVP Reporting Server**.

The Find, Add, Delete, Edit window displays.

Step 2 Find the Reporting Server to delete by using the procedure in Find Reporting Server, on page 164.

Step 3 From the list of matching records, choose the Reporting Server that you want to delete.

Step 4 Click **Delete**.

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

Related Topics

Add Unified CVP Reporting Server, on page 150

Find Reporting Server

The Operations Console lets you locate a Reporting Server on the basis of specific criteria. Use the following procedure to locate a Reporting Server.

Procedure

To find a Reporting Server:

Procedure

Step 1 Choose **Device Management** > **Unified CVP Reporting Server**.

A list of the available Reporting Servers appears, 10 devices per screen, sorted by name.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window 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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Unified CVP VXML Server Setup

The Unified CVP VXML Server is an optional J2EE-compliant application server that provides a solution for rapidly creating and deploying dynamic VXML applications. If you installed a Unified CVP VXML Server, you must configure it before using it to deploy VXML applications or licenses.

If you are using a VXML gateway to route calls from the Unified CVP VXML Server, but want to use the Unified CVP reporting feature, install the Call Server and Reporting Server on the same physical machine. Configure the Call Server with no call services enabled, then configure the Reporting Server and select the Call Server that is installed on the same machine (same IP address) as the primary call server for the Reporting Server.

To make requests to an ICM server, without relinquishing control of the call or use Unified CVP reporting, you must configure the Unified CVP VXML Server to use a Call Server with at least the ICM Service enabled.

You can perform the following tasks:

- Add Unified CVP VXML Server
- Edit Unified CVP VXML Server
- Delete Unified CVP VXML Server
- Upload Log Messages XML File
- Download Log Messages XML File
- VXML Application File Transfers
- Find Unified CVP VXML Server
- View Device Status

Add Unified CVP VXML Server

Before You Begin

Before adding a VXML Server to the Operations Console, ensure that you have done the following:

Procedure

- Collect the hostname or IP address of the Unified CVP VXML Server during the installation of Unified CVP software.
- Install and configure at least one Call Server before configuring the Unified CVP VXML Server.

Note You do not need to install a Call Server if you are adding a Unified CVP VXML Server (standalone).

- Review Call Studio scripts, noting any of the following items you want to include or exclude from Unified CVP VXML Server reporting data:
  a) Application names
  b) Element types
  c) Element names
  d) Element fields
  e) ECC variables

Procedure

To add a Unified CVP VXML Server:

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server**.

The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

Note To use an existing Unified CVP VXML Server as a template for creating the new VXML Server, select the Unified CVP VXML Server by clicking the radio button preceding it and then click **Use As Template**.

Step 2 Click **Add New**.

The Unified CVP VXML Server Configuration window opens to the General Tab.

Step 3 Fill in the IP Address and Hostname fields and a primary Call Server.

Step 4 Optionally, click **Enable secure communications with the Ops Console** to secure communications between the Operations Console and the Call Server.

Step 5 Select each tab and verify that the default values are correct or change the values if desired:

Configuration tabs:

- Unified CVP VXML Server Configuration Properties, on page 170
- Unified CVP VXML Server Infrastructure Settings, on page 172

- Add or Remove Device From Device Pool, on page 62

Step 6 When you finish configuring the Unified CVP VXML Server, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to apply the changes to the Unified CVP VXML Server.

Step 7 Shut down and then start the Unified CVP VXML Server and the primary and backup Call Servers.

Related Topics

Unified CVP VXML Server General Properties, on page 168
Unified CVP VXML Server Configuration Properties, on page 170
Unified CVP VXML Server Infrastructure Settings, on page 172
Add or Remove Device From Device Pool, on page 62
Shut Down Server, on page 59
Start Server, on page 58

Edit Unified CVP VXML Server

You can edit the configuration for a Unified CVP VXML Server that has been added to the Operations Console.

Procedure

To edit a Unified CVP VXML Server configuration:

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server**.

The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

Step 2 You can search for a VXML Server by using the procedure in the Finding a Unified CVP VXML Server topic.

Step 3 From the list of matching records, choose the Unified CVP VXML Server that you want to edit.

Step 4 Click **Edit**.

The Unified CVP VXML Server Configuration window opens to the General Tab.

Step 5 Change any general server information. You cannot change the IP address of the VXML Server.

Step 6 Select the **Configuration Tab**, then edit Unified CVP VXML Server properties.

Step 7 Optionally, you can select the **Device Pool** tab and add or remove the Unified CVP VXML Server from a device pool.

Step 8 Optionally, you can select the **Infrastructure** tab and configure log file and syslog settings.

Step 9 When you finish configuring the Unified CVP VXML Server, click **Save** to save the settings in the Operations Server database. Click **Save & Deploy** to apply the changes to the Unified CVP VXML Server.

Step 10 If instructed, shut down and then start the Unified CVP VXML Server and the primary and backup Call Servers.

Related Topics

Delete Unified CVP VXML Server, on page 168

Add Unified CVP VXML Server, on page 166
Unified CVP VXML Server Configuration Properties, on page 170
Unified CVP VXML Server General Properties, on page 168
Unified CVP VXML Server Infrastructure Settings, on page 172
Find Unified CVP VXML Server, on page 181
Shut Down Server, on page 59
Start Server, on page 58
Device Information Field Descriptions, on page 118

Delete Unified CVP VXML Server

Deleting a Unified CVP VXML Server from the Operations Console deletes the configuration of the selected Unified CVP VXML Server in the Operations Console database and removes the Unified CVP VXML Server from displayed list of Unified CVP VXML Servers.

Procedure

To delete a Unified CVP VXML Server from the Control Center:

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server**.

The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

Step 2 From the list of matching records, select the Unified CVP VXML Server that you want to delete by clicking the radio button preceding it.

Step 3 Click **Delete**.

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

Step 5 Shut down and start the Unified CVP VXML Server and the primary and backup Call Servers.

Related Topics

Add Unified CVP VXML Server, on page 166
Transfer Script and Media Files, on page 17
Shut Down Server, on page 59
Start Server, on page 58
Find Unified CVP VXML Server, on page 181

Unified CVP VXML Server General Properties

You can configure settings that identify the Unified CVP VXML Server and choose a primary, and optionally, a backup Call Server to communicate with the Reporting Server. You can also enable secure communications between the Operations Console and the Unified CVP VXML Server.

Table 34: Unified CVP VXML Server General Configuration Settings

Field	Description	Default	Range	Restart/Reboot Needed
General				
IP Address	The IP address of the Unified CVP VXML Server	None	A valid IP address	No
Hostname	The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.	None	A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The Unified CVP VXML Server description	None	Up to 1,024 characters	No
Enable secure communication with the Ops console	Select to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS. Configure secure communications before you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	None	On or Off	Yes - reboot
Device Version	Lists the Release and Build Number for this device.	Read Only	Read Only	Read Only
Unified CVP Call Servers				
Primary Unified CVP Call Server	The Unified CVP VXML Server uses the message service on this Call Server to communicate with the Reporting Server and to perform an ICM lookup. Select a primary Call Server from the drop-down list. The drop-down list includes all Call Servers added to the Operations Console.	None	Not applicable	Yes - Restart Call Server and Unified CVP VXML Server

Field	Description	Default	Range	Restart/Reboot Needed
Backup Unified CVP Call Server	The Unified CVP VXML Server uses the message service on this Call Server to communicate with the Reporting Server and perform an ICM lookup if the primary Call Server is unreachable. Select a backup Call Server from the drop-down list. The drop-down list includes all Call Servers added to the Operations Console.	None	Not applicable	Yes - Restart Call Server and VXML Server

Important When the primary Call Server is unreachable, the Unified CVP VXML Sever uses the backup Call Server to communicate with the Reporting Server and to perform an ICM lookup. But the VXML Server does not continuously try to re-establish a connection with the primary Call Server. The VXML Server continues to use the backup Call Server until you restart either the Unified CVP VXML Server or the backup Call Server.

Unified CVP VXML Server Configuration Properties

From the Unified CVP VXML Server Configuration tab, you can enable the reporting of Unified CVP VXML Server and call activities to the Reporting Server. When enabled, the Unified CVP VXML Server reports on call and application session summary data. Call summary data includes call identifier, start and end timestamp of calls, ANI, and DNIS. Application session data includes application names, session ID, and session timestamps.

If you choose detailed reporting, Unified CVP VXML Server application details are reported, including element access history, activities within the element, element variables and element exit state. Customized values added in the **Add to Log** element configuration area in Call Studio applications are also included in reporting data. You can also create report filters that define which data are included and excluded from being reported.

Table 35: Unified CVP VXML Server Configuration Settings

Field	Description	Default	Range	Restart/Reboot Needed
Configuration				
Enable Reporting for this Unified CVP VXML Server	Indicates whether or not the Unified CVP VXML Server sends data to the Reporting Server. If disabled, no data is sent to the Reporting Server, and reports do not contain any VXML application data.	Enabled	Enabled (the default) or Disabled.	No

Field	Description	Default	Range	Restart/Reboot Needed
Enable Reporting for VXML Application Details	Indicates whether VXML application details are reported.	Disabled	Enabled or Disabled (the default).	No
Max. Number of Messages	Define the maximum number of reporting messages that will be saved in a file if failover occurs. (Limited by amount of free disk space.)	100,000	Not applicable	Not applicable
VXML Applications Details: Filters				
Inclusive Filters	List of applications, element types, element names, and element fields, and ECC variables to include in reporting data.	None	A semicolon-separated list of text strings. A wildcard character (*) is allowed within each element in the list. **Note** For information about filter syntax and rules, see Inclusive and Exclusive VXML Reporting Filter Examples, on page 176.	Yes - Restart VXML Server

Field	Description	Default	Range	Restart/Reboot Needed
Exclusive Filters	List of applications, element types, element names, and element fields, and ECC variables to exclude from reporting data.	None	A semicolon-separated list of text strings. A wildcard character (*) is allowed within each element in the list. **Note** For information about filter syntax and rules, see Inclusive and Exclusive VXML Reporting Filter Examples, on page 176.	Yes - Restart VXML Server

Unified CVP VXML Server Infrastructure Settings

Table 36: VXML Server Infrastructure Tab Configuration Settings

Field	Description	Default	Range	Restart Required
Configuration: Thread Management				
Maximum Threads	(Required) The maximum thread pool size in the VXML Server Java Virtual Machine.	525	100 - 1000	Yes
Advanced				
Statistics Aggregation Interval	The VXML Server publishes statistics at this interval.	30 minutes	10 - 1440	Yes
Log File Properties				

Field	Description	Default	Range	Restart Required
Max Log File Size	(Required) Maximum size of the log file in Megabytes. The log file name follows this format: `CVP.DateStamp.SeqNum.log` example: For example: `CVP.2006-07-04.00.log` After midnight each day, a new log file is automatically created with a new date stamp. Also, when a log file exceeds the max log file size, a new one with the next sequence number is created, for example, when `CVP.2006-07-04.00.log` reaches 5 Mb, `CVP.2006-07-04.01.log` is automatically created.	10 MB	1 through 100 MB	Yes
Max Log Directory Size	(Required) Maximum size of the directory containing VXML Server log files. **Note** Modifying the value to a setting that is below the default value might cause logs to be rolled over quickly. Consequently, log entries might be lost, which can affect troubleshooting.	20,000 MB	500 - 500000 MB Max Log File size < Max Log Directory Size Max Log File size > 1 Max Log Dir Size / Max Log File Size cannot be greater than 5.000	Yes
Configuration: Primary Syslog Settings				
Primary Syslog Server	Hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Primary Syslog Server Port Number	Port number of Primary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No

Field	Description	Default	Range	Restart Required
Primary Backup Syslog Server	Hostname or IP address of the Primary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or hostname.	No
Primary Backup Syslog Server Port Number	Port number of Primary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Configuration: Secondary Syslog Settings				
Secondary Syslog Server	Hostname or IP address of Secondary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No
Secondary Syslog Server Port Number	Port number of Secondary Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
Secondary Backup Syslog Server	Hostname or IP address of the Secondary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server cannot be reached.	None	Valid IP address or hostname.	No
Secondary Backup Syslog Server Port Number	Port number of Secondary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No

Inclusive and Exclusive VXML Reporting Filters

You use Inclusive and Exclusive VXML filters to control the data that the Unified CVP VXML Server feeds to the Reporting Server.

Data feed control is crucial for:

- Saving space in the reporting database.
- Preserving messaging communication bandwidth.

Procedure

To configure inclusive and exclusive filters for a Reporting Server:

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server**.

The Find, Add, Delete, Edit Unified CVP VXML Servers window opens.

Step 2 You can search for a Unified CVP VXML Server by using the procedure in the Finding a Unified CVP VXML Server topic.

Step 3 From the list of matching records, choose the Unified CVP VXML Server that you want to edit.

Step 4 Click **Edit**.

The Unified CVP VXML Server Configuration window opens to the General Tab.

Step 5 Select the **Configuration Tab**, then configure Unified CVP VXML Server properties.

Step 6 In the **VXML Applications Details: Filters** pane, enter an inclusive filter that defines the VXML elements to include in data sent to the Reporting Server.

Step 7 Optionally, enter an exclusive filter that excludes some of the data specified by the inclusive filter.

Step 8 When you finish configuring filters, click **Save** to save the settings in the Operations Console database or click **Save & Deploy** to save and apply the changes to the Unified CVP VXML Server.

Step 9 Shut down and then start the Unified CVP VXML Server and the primary and backup Call Servers.

Related Topics

VXML Inclusive and Exclusive Filter Rules, on page 175
Inclusive and Exclusive VXML Reporting Filter Examples, on page 176

VXML Inclusive and Exclusive Filter Rules

Inclusive and exclusive filters operate using the following rules:

- Filters are case sensitive.
- By default, all items except the Start, End, Subdialog_Start and Subdialog_End elements are filtered from reporting data unless they are added to an Inclusive Filter. The Subdialog_Start and Subdialog_End elements are never filtered from reporting data unless Reporting is disabled on the Unified CVP VXML Server.
- The Exclusive Filter takes precedence over the Inclusive Filter. For example, if an application name is in the Exclusive Filter, then the items of that applications are excluded from reporting data even if a particular field or element is listed in the Inclusive filter.
- The syntax for Inclusive/Exclusive filters is:

```
Appname.ElementType.ElementName.FieldName
```

or

```
AppName.*.*.SESSION:Varname
```

Note This syntax indicates session variables.

- Use a semicolon (;) to separate each item in a filter. For example, `ElementA ; ElementB` is valid.
- Use a single wildcard (*) anywhere within the application name, element type, element name, or field name.
- Element types, element names, and field names can contain alphanumeric characters, underscores, and a space character.
- An application name can contain alphanumeric characters and underscores, but the space character is not allowed. For example, `A_aa.B_bb.*C_cc_DD.E_ee_F*` is valid.

VXML Filter Wildcard Matching Examples

The table below provides examples of VXML filter wildcard matching.

Table 37: Examples of VXML Filter Wildcard Matching

Filter	What It Matches
MyApplication.voice.*.*	Matches all voice elements in MyApplication
.voice..*	Matches all Voice elements in all applications
MyApplication.*.*.var*	Matches all fields in MyApplication that start with the string `var`
MyApplication.*.*.*3	Matches all fields in MyApplication that end with `3`
MyApplication.*.*.SESSION:Company	Matches the Company session variable in MyApplication

Inclusive and Exclusive VXML Reporting Filter Examples

The table below provides examples of some different combinations of Inclusive and Exclusive filters and the resulting data that the Unified CVP VXML Server feeds to the Reporting Server.

Table 38: Examples of Inclusive and Exclusive VXML Filters for Reporting

Inclusive Filter	Exclusive Filter	Data the Unified CVP VXML Server Feeds To the Reporting Server
`Application1.*.*.*`	None	All Application1 data
`Application1.*.*.*`	`*.*.Element1.*;` `*.*.Element2.*`	All Application1 data, except Element1 and Element2

Inclusive Filter	Exclusive Filter	Data the Unified CVP VXML Server Feeds To the Reporting Server

`Application1.*.*.*`	`*.*.Element1.*;`
	`*.*.Element2.*;`
	`*.*.*.Field1`
		All Application1 data, except Element1, Element2, and Field1

`Application1.*.*.*`	`*.voice.*.*` which matches Element3 and Element4	All Application1 data, except Element3 and Element4

`*.*.Element1.*;`
`*.*.Element2.*;`
`*.*.*.Field1`
	`Application1.*.*.*`	No data for Application1. Other Data for other applications, such as Application2, which contain Element1, Element2 and Field1, will be fed.

`*.voice.*.*` which matches Element1, Element2, Element3, and Element4	`*.*.Element3.*;` `*.*.Element4.*`	Only Element1 and Element2 and all applications.
`*.voice.*.*` which matches Element1 and Element2	`*.*.*.Field1`	Element1 and Element2, except for Field1, if it exists in those elements
`*.*.Element1.*`	None	Element1
`*.*.Element1.*`	`*.*.*.Field1`	Element1, except for Field1 if it exists in Element1
`*.*.*.Field1`	`*.*.Element3.*;` `*.*.Element4.*`	Field1 in any elements except Element3 and Element4

A good strategy for using filters is to create an Inclusive filter that includes the data you want to save in the Reporting database and then create an Exclusive filter to *exclude* portions of the data, for example, sensitive security information such as Social Security Numbers. For example, you

- First, create an inclusive filter to include all information:

  ```
  MyApp.voice.*.*
  ```

- Then, create an exclusive filter to remove credit card and social security numbers information:

  ```
  MyApp.voice.*.CreditCard; MyApp.voice.*.SSN
  ```

VXML Application File Transfers

Applications transferred to a Unified CVP VXML Server or Unified CVP VXML Server (standalone) must be stored in the `.zip` archive format, otherwise the Operations Console returns an invalid format error message and the file is not transferred. Use the Call Studio archive feature to create `.zip` application files to be transferred to a Unified CVP VXML Server or Unified CVP VXML Server (standalone).

To create an Archive file using Call Studio:

1. Right-click on a project in the Navigator view, and choose **Deploy**.

2. Under Deploy Destination, choose **Archive File**.
3. Enter the location and filename of the destination file in the **Archive File text** field.

Note The filename must end with a ".zip" extension.

4. Click **Finish**.

Transferring a file is a two-step process:

1. Upload the file to the Operations Console.
2. Select one or more servers to transfer the uploaded file to.

To transfer VXML application files to the Unified CVP VXML Server (standalone):

1. From the main menu, select **Device Management** > **Unified CVP VXML Server (standalone)**.

   The Find, Add, Delete, Edit window lists any servers that have been added to the Operations Console.
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**.
3. Select **File Transfer** > **VXML Applications** in the toolbar and then click **Applications**.

   The VXML Application File Transfer page opens, listing the host name and IP address for the selected device. VXML applications currently stored in the Operations Server database are listed in the Select From available VXML applications box.
4. If the VXML application is not listed in the Select From available VXML application files box: Click **Select a VXML application file from Your Local PC**. Click **Browse** to search for the VXML application on the local file system.
5. If the VXML application is listed in the **Select From available VXML applications** box, select the VXML application.
6. Click **Transfer** to send the file to the device.

   The VXML application is transferred to the selected server.

Download Log Messages XML File

You can download a Log Messages XML file, `CVPLogMessages.xml`, to your local machine from any Unified CVP server. After downloading the file, you can edit it to configure the way Unified CVP event notifications are handled. Then after you edit the file, you can upload the customized file to any Unified CVP server.

Procedure

To download a Log Messages XML file from the Operations Console to a Unified CVP Server:

Procedure

Step 1 From the Device Management menu, choose the type of server from which you want to download a syslog XML file. For example, to download a file to a Unified CVP VXML Server, choose **Device Management** > **Unified CVP VXML Server**.

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

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 **Log Messages XML File Download**.

The Log Messages XML Download dialog box opens.

Step 4 Click **Download** to transfer the XML file to the server.

A message indicates that this operation takes time. Click **OK** to continue with the download or click **Cancel**.

Related Topics

Upload Log Messages XML File, on page 181
Edit Log Messages XML File, on page 179

Edit Log Messages XML File

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. This file also identifies an event type identifier and message text identifier for each event. The text for these identifiers is stored in the resource properties file, `LogMessagesRes.properties`.

Each Unified CVP Call Server, Unified CVP VXML Server, and Reporting Server has a log messages XML file and log message file. You can edit the `CVPLogMessages.xml` file on a particular Unified CVP server to customize the severity, destination and possible resolution for each event that the server generates. You can also edit the `LogMessagesRes.properties` file to change the text of the message that is generated when an event occurs on that server.

Use any plain-text editor (one that does not create any markup) or XML editor to edit the `CVPLogMessages.xml` file. Use a resource file editor, to edit the `LogMessagesRes.properties` file. If a resource file editor is not available, use a text editor.

Message Element	Possible Values	What it Means
Name	Resource="identifier"	Identifies the event type described in the `LogMessagesRes.properties` file.
Body	Resource="identifier"	Identifies the message text described in the `LogMessagesRes.properties` file.
Severity	0 to 6	Identifies the severity level of the event. See Unified CVP Event Severity Levels, on page 180.

Message Element	Possible Values	What it Means
SendToSNMP	True or false	Set to true, to send this message, when logged, to an SNMP manager, if one is configured.
SendToSyslog	True or false	Set to true to send this message, when logged, to a Syslog server, if one is configured.
SNMPRaise	True or false	Set to true to identify this message, when logged, as an SNMP raise event, which the SNMP management station can use to initiate a task or automatically take an action. Set to false to identify this message as an SNMP clear when sent to an SNMP management station. An SNMP clear event usually corresponds to an SNMP raise event, indicating that the problem causing the raise has been corrected. An administrator on an SNMP management station can correlate SNMP raise events with SNMP clear events.

Unified CVP Event Severity Levels

The following table describes the available severity levels for Unified CVP events. You can set the severity level for an event by editing the log messages XML file, CVPLogMessages.xml, on the server that generates events. For instructions on editing this file, see Edit Log Messages XML File, on page 179.

Level	Severity	Purpose
EMERGENCY	0	System or service is unusable
ALERT	1	Action must be taken immediately
CRITICAL	2	Critical condition, similar to ALERT, but not necessarily requiring an immediate action
ERROR	3	An error condition that does not necessarily impact the ability of the service to continue to function
WARN	4	A warning about a bad condition, which is not necessarily an error
NOTICE	5	Notification about interesting system-level conditions, which are not errors
INFO	6	Information about internal flows or application or per-request information, not system-wide information

Upload Log Messages XML File

You can download a Log Messages XML file, `CVPLogMessages.xml`, to your local machine from any Unified CVP server. After downloading the file, you can edit it to configure the way Unified CVP event notifications are handled. Then after you edit the file, you can upload the customized file to any Unified CVP server.

Procedure

To upload a Log Messages XML file from a Unified CVP Server to the Operations Console:

Procedure

Step 1 From the Device Management menu, select the type of server to which you want to upload a syslog XML file. For example, to upload a file to a Unified CVP VXML Server, select **Device Management** > **Unified CVP VXML Server**.

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

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 **Log Messages XML File Upload**.

The Log Messages XML Upload page opens.

Step 4 In the **Select a Log Messages XML file from your local PC** text box, enter a file name or click **Browse** and search for the file on your local system.

Step 5 Click **Upload** to transfer the selected file to the Unified CVP VXML Server.

Step 6 Shut down and then start the corresponding Unified CVP VXML Server.

Related Topics

Upload Log Messages XML File, on page 181
Edit Log Messages XML File, on page 179
Shut Down Server, on page 59
Start Server, on page 58

Find Unified CVP VXML Server

The Operations Console lets you locate a Unified CVP VXML Server on the basis of specific criteria.

Procedure

To find a Unified CVP VXML Server:

Procedure

Step 1 Select **Device Management** > **Unified VXML Server**.

The Find, Add, Delete, Edit Unified CVP VXML Servers window lists the available Unified CVP VXML Servers, 10 at a time, sorted by name.

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

Step 3 You can also filter the list by selecting an attribute such as **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Unified CVP VXML Server (Standalone) Setup

In the Unified CVP VXML Server (standalone) call flow model, the Call Server routes messages between the components. Calls arrive through a VXML gateway and interact directly with a Unified CVP VXML Server to execute VXML applications. The gateway performs both ingress and VXML functions. This call flow model provides a sophisticated VXML-based VRU, for applications which in many cases do not need to interact with an ICM Server.

You can perform the following tasks:

Add Standalone Unified CVP VXML Server

Procedure

To add a Unified CVP VXML Server (standalone):

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server (Standalone)**.

The Find, Add, Delete, Edit Unified CVP VXML Server (standalone) window opens.

Note To use an existing Unified CVP VXML Server as a template for creating the new Unified CVP VXML Server, select the Unified CVP VXML Server by clicking the radio button preceding it, and then click **Use As Template**.

Step 2 Click **Add New**.

The Unified VXML Server (standalone) Configuration window opens to the General Tab.

Step 3 Fill in the IP address and hostname and an optional description for the Unified CVP VXML Server.

Table 39: Unified CVP VXML Server General Configuration Settings

Field	Description	Default	Range	Restart/Reboot Needed
General				

Field	Description	Default	Range	Restart/Reboot Needed
IP Address	The IP address of the Unified CVP VXML Server	None	A valid IP address	No
Hostname	The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.	None	A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash	No
Description	The description of the Unified CVP VXML Server	None	Up to 1,024 characters	No
Enable secure communication with the Ops console	Select to enable secure communications between the Operations Server and this component. The device is accessed using SSH and the files are transferred using HTTPS. You must configure secure communications before you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	None	On or Off	Yes - reboot
Device Version	Lists the Release and Build Number for this device.	Read Only	Read Only	Read Only

Step 4 Optionally, click **Enable secure communications with the Ops Console** to secure communications between the Operations Console and the Call Server.

Step 5 Optionally, you can select the **Device Pool Tab** and add the server to an additional device pool.

Step 6 When you finish configuring Unified CVP VXML Server (standalone), click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the changes to the Unified CVP VXML Server (standalone).

Related Topics

Delete Standalone Unified CVP VXML Server, on page 184
Edit Standalone Unified VXML Server, on page 184
Find Standalone Unified CVP VXML Server, on page 186
View Device Status, on page 39

Delete Standalone Unified CVP VXML Server

Deleting a Unified CVP VXML Server (standalone) from the Operations Console deletes its configuration data in the Operations Console database and removes the Unified CVP VXML Server from the displayed list of VXML Servers.

Procedure

To delete a Unified CVP VXML Server (standalone):

Procedure

Step 1 Select **Device Management** > **Unified CVP VXML Server (Standalone)**.

The Find, Add, Delete, Edit Unified CVP VXML Servers (standalone) window opens.

Step 2 Select the Unified CVP VXML Server (standalone) by clicking the radio button preceding it and then clicking **Delete**. To narrow the list of servers see Find Standalone Unified CVP VXML Server, on page 186.

Step 3 Click **Delete**.

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

Related Topics

Add Standalone Unified CVP VXML Server, on page 182
Edit Standalone Unified VXML Server, on page 184

Edit Standalone Unified VXML Server

Procedure

To edit a Unified CVP VXML Server (standalone):

Procedure

Step 1 Choose **Device Management** > **Unified CVP VXML Server (Standalone)**.

The Find, Add, Delete, Edit Unified CVP VXML Servers (standalone) window opens.

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**.

the Unified CVP VXML Server (standalone) Configuration window opens to the General Tab.

Step 3 Make the desired changes to the settings. You cannot change the IP address.

Table 40: Unified CVP VXML Server General Configuration Settings

Field	Description	Default	Range	Restart/Reboot Needed
General				
IP Address	The IP address of the Unified CVP VXML Server. **Note** This field is not editable.	None	A valid IP address	No
Hostname	The host name of the Unified CVP VXML Server. Host names must be valid DNS names, which can include letters in the alphabet, the numbers 0 through 9, and a dash.	None	A valid DNS name, which includes uppercase and lowercase letters in the alphabet, the numbers 0 through 9, and a dash	No
Description	The description of the Unified CVP VXML Server	None	Up to 1,024 characters	No
Enable secure communication with the Ops console	Select to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS. You must configure secure communications *before* you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	None	On or Off	Yes - reboot
Device Version	Lists the Release and Build Number for this device.	Read Only	Read Only	Read Only

Step 4 When you finish editing Unified CVP VXML Server (standalone), click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the changes to the Unified CVP VXML Server (standalone).

Related Topics

Delete Standalone Unified CVP VXML Server, on page 184
Add Standalone Unified CVP VXML Server, on page 182
Find Standalone Unified CVP VXML Server, on page 186
VXML Application File Transfers, on page 177
View Device Status, on page 39

Find Standalone Unified CVP VXML Server

The Operations Console lets you locate a Unified CVP VXML Server on the basis of specific criteria. Use the following procedure to locate a Unified CVP VXML Server (standalone).

Related Topics

Add Standalone Unified CVP VXML Server, on page 182
Edit Standalone Unified VXML Server, on page 184
Delete Standalone Unified CVP VXML Server, on page 184

Procedure

To find a Unified CVP VXML Server (standalone):

Procedure

Step 1 Select **Device Management** > **Unified CVP VXML Server (Standalone)**.

The Find, Add, Delete, Edit Unified CVP VXML Server (standalone) window lists the available Unified CVP VXML Server (standalone) sorted by name, 10 at a time.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list. Or, 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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Gateway Setup

From the Device Management menu, Gateway option, you can add an IOS Gateway to the Operations Console. Once added, you can execute a subset of IOS Gateway commands on the Gateway from the Operations Console.

The Ingress Gateway is the point at which an incoming call enters the Unified CVP solution. It terminates TDM phone lines on one side and implements VoIP on the other side. It also provides for sophisticated call routing capabilities at the command of other Unified solution components. It works with SIP protocols, and also supports MGCP for use with Unified CM.

The VXML Gateway hosts the IOS voice browser, the component which interprets VXML pages from either the Unified CVP IVR service or the VXML Server, plays .wav files and Text-to-Speech (TTS), inputs voice and DTMF, and sends results back to the VXML requestor. It also mediates between Media Servers, Unified CVP VXML Servers, ASR and TTS Servers, and the IVR service.

The Ingress Gateway may be deployed separately from the VXML Gateway, but in most implementations they are the same: one Gateway performs both functions. Gateways are often deployed in farms, for centralized deployment models. In Branch deployment models, one combined Gateway is usually located at each branch office.

An Egress Gateway is typically used in Call Director Model to provide access to a call center ACD or third-party IVR.

See Also:

Add Gateway

You can add a an IOS Gateway to the Operations Console.

In Unified CVP there are fields for **Trunk Group ID**. If the Call Server associated with this Gateway has **Enable Gateway Trunk Reporting** checked on the ICM tab, then the Trunk Group ID is used for Gateway trunk reporting. The default value is 300, however the value can be from 1 to 65535.

Related Topics

IOS Setup, on page 95
Add or Remove Device From Device Pool, on page 62

Procedure

To add a Gateway:

Procedure

Step 1 Select **Device Management** > **Gateway**.

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

Step 2 Click **Add New**.

The Gateway Configuration window opens.

Note In the **Username and Passwords** panel there is a button labeled **Test Sign In**. Clicking **Test Sign In** attempts to verify the credentials by connecting to the Gateway. A message appears with the test result.

Step 3 Fill in the IP address, hostname, Trunk Group ID, user password, and enable password for the Gateway:

Table 41: Gateway Configuration General Settings

Field	Description	Default	Range
IP Address	The IP address of the Gateway	None	Valid IP address
Hostname	The name of the Gateway	None	Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9, and a dash
Device Type	The type of Gateway device	None	Valid Gateway devices listed in the drop-down menu
Description	The description of the Gateway	None	Up to 1,024 characters

Field	Description	Default	Range
Trunk Group ID	If the Call Server associated with this Gateway has **Enable Gateway Trunk Reporting** checked on the ICM tab, then the Trunk Group ID is used for Gateway trunk reporting.	300	1 to 65535
Location ID	Read only. The location ID for this Gateway.	Blank if not assigned to a system-level configuration location.	Not editable
Enable Secure Communication with the Ops console	Select **On** to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS. Select only if security is enabled and configured on Gateway. **Note** • You must configure secure communications before you enable this option. For more information, see the *Configuration Guide for Unified Customer Voice Portal*. • Ops console supports only *diffie-hellman-group1-sha1* algorithm for secure communication with gateway.	None	Enabled or disabled

Table 42: Gateway Configuration Username and Password Settings

Field	Description	Default	Range
Username	(Optional) Username to access the device (Telnet or SSH Username). If specified, the user name must be configured on the device.	None	None

Field	Description	Default	Range
User Password	Password to access the device (Telnet or SSH password), needs to be configured on device.	None	None
Enable Password	Password to change to exec mode on device.	None	None
Port	The port over which to connect to the gateway CLI.	23	Valid IP Port

Note To use an existing Gateway as a template for creating the new Gateway, select the Gateway by clicking the radio button preceding it, and then click **Use As Template**.

Step 4 Optionally, you can select the **Device Pool** tab and add the Gateway to a device pool.

Step 5 When you finish configuring the Gateway, click **Save** to save the configuration.

Delete Gateway

Procedure

To delete a Gateway:

Procedure

Step 1 Select **Device Management** > **Gateway**.

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

Step 2 Find the Gateway using the procedure in Find Gateway, on page 192.

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

If this Gateway is assigned to a system-level configuration location or trunk utilization, then the association must be removed prior to deleting this Gateway.

Edit Gateway

Related Topics

Add or Remove Device From Device Pool, on page 62
Execute IOS Commands on Gateway, on page 193
View Gateway Statistics, on page 193
Transfer Script and Media Files, on page 17

Procedure

To edit a Gateway:

Procedure

Step 1 Select **Device Management** > **Gateway**.

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

Step 2 Find the Gateway using the procedure in Find Gateway, on page 192.

Step 3 From the list of matching records, select the Gateway that you want to edit.

Step 4 Click the Gateway name to edit it.

The **Gateway Configuration** window opens with the current settings displayed on the **General** tab.

Step 5 Change the appropriate configuration settings.

Table 43: Gateway Configuration General Settings

Field	Description	Default	Range
IP Address	The IP address of the Gateway. **Note** This field is not editable.	None	Not editable
Hostname	The name of the Gateway	None	Valid DNS name, which can include letters in the alphabet, the numbers 0 through 9, and a dash
Device Type	The type of Gateway device	None	Valid Gateway devices are listed in the drop-down menu.
Description	The description of the Gateway	None	Up to 1,024 characters
Trunk Group ID	If the Call Server associated with this Gateway has **Enable Gateway Trunk Reporting** checked on the ICM tab, then the Trunk Group ID is used for Gateway trunk reporting.	300	1 to 65535
Location ID	Read only. The location ID for this Gateway.	Blank if not assigned to a system-level configuration location.	Not editable

Field	Description	Default	Range
Enable Secure Communication with the Ops console	Select **On** to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS. Select only if security is enabled and configured on Gateway. You must configure secure communications before you enable this option. For more information, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.	None	Enabled or disabled

Table 44: Gateway Configuration Username and Password Settings

Field	Description	Default	Range
Username	(Optional) Username to access the device (telnet or ssh Username). If specified, the user name must be configured on the device.	None	None
User Password	Password to access the device (Telnet or SSH password) needs to be configured on device.	None	None
Enable Password	Password to change to exec mode on device.	None	None
Port	The port over which to connect to the gateway CLI.	23	Valid IP Port

Note To use an existing Gateway as a template for creating the new Gateway, select the Gateway by clicking the radio button preceding it, and then click **Use As Template**.

Step 6 Optionally, you can select the **Device Pool** tab and add edit the device pool setting.

Step 7 When you finish editing the Gateway configuration, click **Save**.

Find Gateway

Because you probably have several Gateways in your network, the Operations Console lets you locate specific Gateways on the basis of specific criteria. Use the following procedure to locate a Gateway.

Procedure

To find a Gateway:

Procedure

Step 1 Select **Device Management** > **Gateway**.

The Find, Add, Delete, Edit Window lists the available Gateways, 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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Transfer Script and Media File to Gateway

You can transfer a single script at a time from the Operations Console to one or more Gateways. If you want to **transfer multiple scripts** at a time, use the Bulk Administration File Transfer menu option. See Bulk Administration File Transfer (BAFT), on page 247.

Related Topics

Find Gateway, on page 192
View Gateway Statistics, on page 193
Bulk Administration File Transfer (BAFT), on page 247

Procedure

To transfer scripts between the Operations Console and a Gateway:

Procedure

Step 1 Select **Device Management** > **Gateway**.

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

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

The Edit Gateway Configuration window opens.

Step 3 Select **File Transfer** > **Scripts and Media** from the Gateway configuration toolbar.

The File Transfer window opens.

Step 4 Select a script and media file to transfer to the Gateway.

a) If the script and media file is located on your local machine, click **Select a script and media file from your local PC**, then click **Browse** and select the script and media file to transfer to the Operations Console.

b) If the script and media is located on the Operations Console, click **Select from available script and media files**.

Step 5 When you have selected the script and media file to transfer, click **Transfer** to copy the selected script and media file to the Operations Console and the Gateway.

View Gateway Statistics

You can display statistics for any Gateway that has been added to the Operations Console.

Procedure

To get Gateway statistics:

Procedure

Step 1 Choose **Device Management** > **Gateway**.

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

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

The Edit Gateway Configuration window opens to the General tab.

Step 3 Click **Statistics** in the toolbar and then select the type of statistics to view from the drop-down menu.

The Gateway Statistics Results window opens, displaying the selected statistics. If the statistics fill the display area, use the scroll bar to move forward and backward or up and down in the display. See View Gateway Statistics, on page 51.

Related Topics

Find Gateway, on page 192

Execute IOS Commands on Gateway

You can use a drop-down menu to select and execute a subset of available Gateway IOS commands when you are editing a Gateway configuration.

Procedure

To execute a Gateway commands:

Procedure

Step 1 Select **Device Management** > **Gateway**.

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

Step 2 If you are editing an existing Gateway configuration, click **Edit**.

Step 3 Select **IOS Commands** from the Gateway Configuration toolbar.

Step 4 From the IOS Commands drop-down menu, select an IOS command to execute on the Gateway.

You can execute the following IOS Gateway commands from the IOS Commands drop-down menu on the Gateway Configuration window.

Table 45: IOS Gateway Commands

Command	Description
Show version	Displays IOS version
Show startup-config	Displays startup-config
Show running-config	Displays running-config

If the command fails, the error will be displayed in an error web page.

Virtualized Voice Browser

From the Device Management menu, you can add Virtualized Voice Browser (VVB) server. You can also execute a subset of VVB commands on the VVB from the Operations Console.

The VVB component interprets VXML pages from either the Unified CVP IVR service or the VXML Server, plays .wav files and Text-to-Speech (TTS), inputs voice and DTMF, and sends results back to the VXML requestor. It also mediates between Media Servers, Unified CVP VXML Servers, ASR and TTS Servers, and the IVR service.

Add VVB

You can add a new VVB from the Operations Console.

Procedure

Procedure

Step 1 Select **Device Management** > **Virtualized Voice Browser**.

Step 2 Click **Add New**.

Step 3 Enter the following fields:

Table 46: General Settings

Field	Description	Default	Range
IP Address	The IP address of the VVB.	None	Valid IP address
Hostname	The name of the VVB.	None	Valid DNS name, which can include letters in the alphabet, the numbers 0 to 9, and a hyphen
Description	The description of the VVB.	None	Up to 1024 characters
Enable secure communication with the Ops console	Select to enable secure communications between the Operations Console and VVB.	Off	On or Off

Table 47: Administration Credentials Settings

Field	Description
Username	Username to access the device (VVB Operations Console password). If specified, the username must be configured on the device.
User Password	Password to access the device (VVB Operations Console password). The password must be configured on the device.

Table 48: Cisco VVB Serviceability Fields

Field	Description	Default	Data Range
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for VVB.	Not Selected	Not Applicable
Username	The username (ssh or system CLI credentials) required to sign in as system CLI credentials. For Cisco VVB, the username is typically a VVB CLI Platform credentials.	Not Applicable	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.

Field	Description	Default	Data Range
Password/Confirm Password	The password required to sign in (VVB CLI Platform credentials).	Not Applicable	Any text that follows the requirements for choosing secure passwords. See General User Information Settings, on page 240
Port	The port on which Serviceability is configured on Cisco VVB.	8443	Not Applicable

Note
- In the **Username and Passwords** panel there is a button labeled **Test Sign-In**. Clicking **Test Sign In** attempts to verify the operations console credentials by connecting to the Cisco VVB. A message appears with the test result.
- To use an existing VVB as a template for creating the new VVB, select the VVB by clicking the radio button preceding it, and then click **Use As Template**.

Step 4 Optionally, you can select the **Device Pool** tab and add the VVB to a device pool.

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

Delete VVB

Procedure

Procedure

Step 1 Select **Device Management** > **Virtualized Voice Browser**.

Step 2 Find the VVB using the procedure in Procedure, on page 198.

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

Edit VVB

Procedure

Procedure

Step 1 Select **Device Management** > **Virtualized Voice Browser**.

Step 2 Find the VVB using the procedure in Procedure, on page 198.

Step 3 From the list of matching records, select the VVB that you want to edit.

Step 4 Click the VVB name to edit it.

Step 5 Change the appropriate configuration settings.

Table 49: Virtualized Voice Browser Configuration General Settings

Field	Description	Default	Range
IP Address	The IP address of the VVB. **Note** This field is not editable.	None	Not editable
Hostname	The name of the VVB.	None	Valid DNS name, which can include letters in the alphabet, the numbers 0 to 9, and a hyphen.
Description	The description of the VVB .	None	Up to 1024 characters
Enable secure communication with the Ops console	Select to enable secure communications between the Operations Console and VVB.	Off	On or Off

Table 50: Administration Credentials Settings

Field	Description
Username	Username to access the device (VVB Operations Console password). If specified, the username must be configured on the device.
User Password	Password to access the device (VVB Operations Console password). The password must be configured on the device.

Table 51: Cisco VVB Serviceability Fields

Field	Description	Data Range	Default
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for VVB.	Not Selected	Not Applicable

Field	Description	Data Range	Default
Username	The username (ssh or system CLI credentials) required to sign in as system CLI credentials. For Cisco VVB, the username is typically a VVB CLI Platform credentials.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable
Password/Confirm Password	The password required to sign in (VVB CLI Platform credentials).	Any text that follows the requirements for choosing secure passwords. See General User Information Settings, on page 240	Not Applicable
Port	The port on which Serviceability is configured on Cisco VVB.	N/A	8443

Note To use an existing VVB as a template for creating the new VVB, select the VVB by clicking the radio button preceding it, and then click **Use As Template** .

Step 6 Optionally, you can select the **Device Pool** tab and add edit the device pool setting.

Step 7 Click **Save** to save the changes.

Find VVB

If you have several Gateways in your network, the Operations Console lets you locate specific VVB on the basis of specific criteria. Use the following procedure to locate a VVB.

Procedure

Procedure

Step 1 Select **Device Management** > **Virtualized Voice Browser**.

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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Speech Server Setup

A Speech Server provides speech recognition and synthesis services. You can add a pre-configured Speech Server to the Operations Console. Once added to the Operations Console, you can add a Speech Server to one or more device pools.

A Speech Server provides speech recognition services and text-to-speech services for a VXML Gateway.

Note The Operations Console can only manage Speech Servers installed on Microsoft Windows.

You can perform the following tasks:

Add Speech Server

Procedure

Before you begin

Install the Remote Operations in the Speech Server before you add the Speech Server to the Operations console.

Procedure

Step 1 Select **Device Management** > **Speech Server**.

The Find, Add, Delete, Edit Speech Server window opens.

Note To use an existing Speech Server as a template for creating the new Speech Server, select the Speech Server by clicking the radio button preceding it, and then click **Use As Template**.

Step 2 Click **Add New**.

The Speech Server Configuration window opens.

Step 3 Fill in the appropriate configuration settings on the General tab as described in Speech Server Configuration Settings.

You can change the settings described in the following table to configure a Speech Server.

Table 52: Speech Server Configuration Settings

Field	Description	Default	Range	Reboot/Restart Required
General				
IP Address	The IP address of the Speech Server	None	Valid IP address	Yes - Reboot Speech Server

Field	Description	Default	Range	Reboot/Restart Required
Hostname	The host name of the Speech Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash	Yes - Reboot Speech Server
Description	The description of the Speech Server	None	Up to 1,024 characters	No
License File Location	The path of the license file on the Speech Server. The Operations Console transfers the license file to this location. **Note** The license file is the license file for the respective Speech Server. The location must be the absolute path to where the license file exists on the Speech Server. The license file must exist at that path before you can successfully save and deploy.	None	Any text	Yes - Restart
Enable secure communication with the Ops console	Select **On** to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS.	None	On or Off	No

Step 4 Select the **Device Pool** tab to optionally add the Speech Server to additional device pools.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to deploy the changes to the Speech Server.

Related Topics

Device Information Field Descriptions, on page 118
Apply Speech Server License, on page 203

Delete Speech Server

You can delete a Speech Server that has been added to the Operations Console. Deleting a Speech Server removes its configuration from the Operations Console database.

Procedure

To delete a Speech Server:

Procedure

Step 1 Select **Device Management** > **Speech Server**.

The Find, Add, Delete, Edit Speech Server window opens.

Step 2 Select the Speech Server by clicking the radio button preceding it and then clicking **Delete**. To narrow the list of servers see Find Speech Server, on page 202.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

Edit Speech Server

You can edit a Speech Server that has been added to the Operations Console. Editing a Speech Server changes its configuration from the Operations Console database.

Related Topics

Find Speech Server, on page 202

Procedure

To edit a Speech Server:

Procedure

Step 1 Select **Device Management** > **Speech Server**.

The Find, Add, Delete, Edit Speech Server window opens.

Step 2 Select the radio button next to the Speech Server that you want to edit, and click **Edit**.

Step 3 Change the appropriate configuration settings on the General tab.

You can change the settings described in the following table to configure a Speech Server.

Table 53: Speech Server Configuration Settings

Field	Description	Default	Range	Reboot/Restart Required
General				
IP Address	The IP address of the Speech Server. **Note** This field is not editable.	None	Valid IP address	Yes - Reboot Speech Server

Field	Description	Default	Range	Reboot/Restart Required
Hostname	The host name of the Speech Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash	Yes - Reboot Speech Server
Description	The description of the Speech Server	None	Up to 1,024 characters	No
License File Location	The path of the license file on the Speech Server. The Operations Console transfers the license file to this location.	None	Any text	Yes - Restart
Enable secure communication with the Ops console	Select **On** to enable secure communications between the Operations Server and this component. The device is accessed using SSH and files are transferred using HTTPS.	None	On or Off	No

Step 4 Select the **Device Pool** tab to optionally add or remove the Speech Server to or from device pools.

Step 5 When you finish configuring the Speech Server, click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to deploy the changes to the Speech Server.

Find Speech Server

The Operations Console lets you locate a Speech Server on the basis of specific criteria. Use the following procedure to locate a Speech Server.

Procedure

To find a Speech Server:

Procedure

Step 1 Select **Device Management** > **Speech Server**.

The Find, Add, Delete, Edit Speech Servers window lists the available Call Servers sorted by name, 10 at a time.

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 window 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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Apply Speech Server License

When you are creating a new Speech Server, you must apply a valid license file before using the server. You can browse for and upload the license file to the Operations Console, and then transfer the license to the Speech Server. Select either an existing license file in the Operations Console database or a new license file from your local desktop.

Procedure

To apply a license file:

Procedure

Step 1 Select **Device Management** > **Speech Server**.

The Find, Add, Delete, Edit Speech Server window opens.

Step 2 Select the radio button next to the Speech Server that you want to edit and click **Edit**.

Step 3 Make sure the **License File Location** lists the correct path of the license file on the Speech Server. The Operations Console transfers the license file to this location.

Step 4 Select **File Transfer** in the toolbar and then click **Licenses**.

The License File Transfer page displays, listing the host name and IP address for the currently selected Speech Server.

Step 5 If the license is listed in the **Select From Available License Files** text box, select the license file.

Step 6 If the license file is not listed in the **Select From Available License Files** text box:

a) Click **Select a License File from Your Local PC**.

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

Step 7 Click **Transfer** to transfer the selected license file to the selected device.

The license is applied to the selected server.

Related Topics

Find Speech Server, on page 202

Media Server Setup

A Media Server administers the media files that contain messages and prompts callers hear. You can add a pre-configured Media Server to the Operations Console. Once added, you can add a Media Server to one or more device pools.

When you add and deploy Media Server(s) to the Operations Console, that information gets pushed to all the Callservers. It is similar to how WebServices information gets added to the CVP devices. This automatically

populates the media servers in the FTP element of the Studio application. You can designate a default media server.

The Media Server is a simple web server/FTP server (if FTP enabled) with the sole purpose within Unified CVP to store and serve `.wav` files to the VXML gateway, as required in order to render VXML pages. The VXML gateway caches the `.wav` files it retrieves from the Media Server. In most deployments, the Media Server encounters extremely low traffic from Unified CVP.

The Media Server must be an IIS web server on a separate machine, with FTP enabled. The Agent Greeting recording script requires the Media Server to have FTP enabled. This is done automatically with Unified CVP as long as the Media Server is configured with Add Media Server, on page 204. If it is not enabled, then make sure that Microsoft FTP Service Startup Type is set to Automatic and the status is Running. Using Tomcat on the Unified CVP VXML server is not a supported configuration as a Media Server, and the FTP element in the recording application fails if the FTP operation fails.

SFTP is also supported with Media Servers. Refer to the Port settings in the *Media Server Configuration Settings* table for more details.

Add Media Server

Procedure

To add a Media Server:

Note Whenever you add, edit, or delete a Media Server, you must click the **Deploy** button to make the change effective.

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit window opens.

Note To use an existing Media Server as a template for creating the new Media Server, select the Media Server by clicking the radio button preceding it, and then click **Use As Template**.

Step 2 Click **Add New**.

The Media Server Configuration window opens.

Step 3 Fill in the appropriate configuration settings on the General tab.

The following table describes the fields that can be configured for a Media Server:

Table 54: Media Server Configuration Settings

Field	Description	Default	Range	Restart Required
General				

Field	Description	Default	Range	Restart Required
IP Address	The IP address of Media Server	None	Valid IP address.	No
Hostname	The name of the Media Server	None	Follow *RFC 1123 Section 2.1* naming conventions for hostnames.	No
Description	The description of the Media Server	None	Up to 1,024 characters.	No
FTP Enabled	Indicates that this media server has FTP Enabled. A media server that has FTP enabled is automatically populated as a session variable to the Unified CVP VXML Server. The default agent greeting recording application automatically uses the media servers defined in CVP OAMP that have FTP enabled to FTP the agent greeting recording.	Disabled	Select the check box to enable this feature.	No Use **Test Sign-in** button to verify the FTP credentials.
Anonymous Access	Indicates that this media server uses anonymous FTP access. In this case, the username is specified by default as anonymous. The password field is not specified for anonymous access. The user can specify the port number or select the default port number (21).	Disabled	Select the check box to enable this feature. **Note** You must enable FTP to enable Anonymous Access.	No Use Test Sign-in button to verify the FTP credentials.
Username and Password	These fields apply if FTP is enabled and Anonymous Access is disabled. In this case, enter the username and password.	None	Enter a valid username and password.	No Use Test Sign-in button to verify the FTP credentials.
Confirm Password	Retype password.	None	Enter vaild password.	No Use **Test Sign-in** button to verify the FTP credentials.

Field	Description	Default	Range	Restart Required
Port	Enter a new port number or use the default port number (21). For SFTP, use port 22 or any other custom port that you may have configured.	21	Valid ports are 1 to 65535.	No Use Test Sign-in button to verify the FTP credentials.

Step 4 Optionally, you can select the Device Pool tab and add the Media Server to a device pool. See Add and Remove Media Server From Device Pool, on page 209.

Step 5 When you finish configuring the Media Server, click **Save**.

Delete Media Server

Procedure

To delete a Media Server:

Warning You will receive a special prompt if you attempt to delete the default Media Server.

Note Whenever you add, edit, or delete a Media Server, click the **Deploy** button to make the change effective.

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit Media Server window opens.

Step 2 Select the Media Server by clicking the radio button preceding it and then clicking **Delete**. To narrow the list of servers see Find Media Server, on page 209.

Step 3 When prompted to confirm the delete operation, click **OK** to delete or click **Cancel** to cancel the delete operation.

Related Topics

Find Media Server, on page 209

Deploy Media Server

Use the **Deploy** button to update the Media Server device list that is sent to all Call Servers

A default media server device may be specified in the Operations Console. If specified, micro-applications use that default media server if the ECC variable for the media server is not defined in the UCCE ICM script.

Procedure

To deploy a Media Server to all Call Servers:

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit window opens.

Step 2 From the **Default Media Server** drop-down menu, select the default Media Server.

Step 3 Click the **Set** button next to the Media Server you want to set as the default Media Server.

Step 4 Click the **Deploy** button to have the default Media Server sent to the Call Servers and VXML Servers.

You must select the Deploy button to have the Media Server sent to the Call Servers and VXML Servers.

Note Configuration information for all Media Servers, and the default Media Server is updated on each Call Server in the property file `CVP_HOME\conf\mediaServer.properties`.

Step 5 Restart the VXML Server.

Edit Media Server

Procedure

To edit a Media Server:

Note Whenever you add, edit, or delete a Media Server, click the **Deploy** button to make the change effective.

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit Media Server window opens.

Step 2 From the list of matching records, select the Media Server that you want to edit.

Step 3 Select the radio button next to the Media Server you want to Edit, and then click **Edit**.

Step 4 Change appropriate configuration settings on the General tab. You cannot change the IP address of the Media Server.

The following table describes the fields that can be configured for a Media Server:

Table 55: Media Server Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of Media Server. **Note** This field is not editable.	None	Valid IP address	No
Hostname	The name of the Media Server	None	Follow *RFC 1123 Section 2.1* naming conventions for hostnames.	No
Description	The description of the Media Server	None	Up to 1,024 characters	No
FTP Enabled	Indicates that this media server has FTP Enabled. A media server(s) that has FTP enabled is automatically populated as a session variable to the Unified CVP VXML Server. The default agent greeting recording application automatically uses the media servers defined in CVP OAMP that have FTP enabled for FTPing the agent greeting recording.	Disabled	Select the check box to enable this feature.	No Use Test Sign-in button to verify the FTP credentials.
Anonymous Access	Indicates that this media server uses anonymous FTP access. In this case, the username is specified by default as anonymous. The password field is not specified for anonymous access. The user can specify the port number or select the default port number (21).	Disabled	Select the check box to enable this feature. **Note** You must enable FTP to enable Anonymous Access.	No Use Test Sign-in button to verify the FTP credentials.
Username and Password	These fields apply if FTP is enabled and Anonymous Access is disabled. In this case, enter the username and password.	None	Enter a valid username and password.	No Use Test Sign-in button to verify the FTP credentials.

Field	Description	Default	Range	Restart Required
Port	Enter a new port number or use the default port number (21).	21	Valid ports are 1 to 65535.	No Use **Test Sign-in** button to verify the FTP credentials.

Step 5 Optionally, you can select the **Device Pool** tab and edit the Media Server's association with a device pool. See Add and Remove Media Server From Device Pool, on page 209.

Step 6 When you finish configuring the Media Server, click **Save**.

Related Topics

Find Media Server, on page 209

Find Media Server

The Operations Console lets you locate a Media Server on the basis of specific criteria. Use the following procedure to locate a Media Server.

Procedure

To find a Media Server:

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit Call Servers window lists the available Media Servers sorted by name, 10 at a time.

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

Step 3 You can filter the list by selecting an attribute such as **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Add and Remove Media Server From Device Pool

Procedure

To add or remove a Media Server from a device pool:

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit Media Server window opens.

Step 2 From the list of matching records, select the Media Server that you want to edit.

Step 3 Click **Edit**.

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

Step 5 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 6 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 7 Click **Save**.

View Deployment Status

Use the **Deployment Status** button to view the status of the Media Server device list.

Procedure

To view the status of the Media Server device list:

Procedure

Step 1 Select **Device Management** > **Media Server**.

The Find, Add, Delete, Edit Media Server window opens.

Step 2 Click the **Deployment Status** button to view the status of the deployment of the default Media Server to each Call Server.

You must select the **Deploy** button to have the Media Server sent to the Call Servers.

Unified Communications Manager Server Setup

From the Device Management menu, Communications Manager option, you can add a Unified CM Server to the Operations Console. Once added, you can add the Unified CM Server to a device pool and access a Unified CM administration web page, from which you can configure the Unified CM Server.

Unified CM manages and switches VoIP calls among IP phones. Unified CVP interacts with Unified CM to send PSTN-originated calls to UCCE agents.

Note If the Unified CM was synchronized for its configured locations, and the Unified CM synchronization is disabled or the Unified CM device is deleted, then the previously configured synchronization locations are marked as invalid.

You can perform the following tasks:

- Add Unified CM Server
- Edit Unified CM Server
- Delete Unified CM Server
- Find Unified CM Server
- Synchronize Location Information

Add Unified CM Server

Procedure

Use this procedure to add a Unified CM Server. See the following table for the Unified CM field descriptions.

Table 56: Unified CM Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Unified CM Server.	None	Valid IP address	No
Hostname	The name of the Unified CM Server	None	Valid DNS names, includes letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The description of the Unified CM Server	None	Any text	No
Device Admin URL	The Administration URL for the Unified CM Server	None	A valid URL. The Operations Console validates the URL for syntax errors but does not check that the site exists.	No
Enable Synchronization (See Synchronize Location Information, on page 71 for more information.)				

Field	Description	Default	Range	Restart Required
Enable synchronization	Select to enable synchronization for location. If enabled, the Operations Console extracts (synchronizes) the Unified CM location information from the Unified CM server.	Disabled When you enable this service, the Port field defaults to 8443.	Enabled or Disabled	No
Username	User name to access the Unified CM AXL interface.	None	Valid Unified CM AXL username.	No
Password	Password to access the Unified CM AXL interface	None	Valid Unified CM AXL password.	No
Confirm Password	Retype the password to verify that you typed the password correctly	None	Text must match the text entered in the Password field	No
Port	The port to which the Unified CM server connects when establishing initial contact	8443	1 through 65535	No

Procedure

Step 1 Select **Device Management** > **Unified CM**.

The Find, Add, Delete, Edit Unified ICM Servers window opens.

Step 2 Click **Add New**.

The Unified ICM Server Configuration window opens to the General tab.

Step 3 Fill in the appropriate configuration settings.

See the Unified CM configuration settings field descriptions table for details.

Note Cisco AXL Web Service must be enabled on the Unified CM for synchronization to work.

To enable Cisco AXL Web Service on the Unified CM, perform the following steps:

a) Log on to Unified CM.
b) Open the Cisco Unified Serviceability dashboard and select **Tools** > **Service Activation**.
c) In the drop down menu, select the Unified CM server that is configured in this Operations Console, and click **Go**.
d) In the Database and Admin Services section, check the box next to Cisco AXL Web Service.
e) Click **Save**.

Step 4 (Optional) Select the **Device Pool** tab and add the Unified CM Server to a device pool.

Step 5 When you finish configuring the Unified CM, click **Save**.

Related Topics

Device Information Field Descriptions, on page 118
Add or Remove Device From Device Pool, on page 62
Synchronize Location Information, on page 71

Edit Unified CM Server

Procedure

Use this procedure to edit a Unified CM Server.

See the following table for the Unified CM field descriptions

Table 57: Unified CM Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Unified CM Server. **Note** This field is not editable.	None	Valid IP address	No
Hostname	The name of the Unified CM Server	None	Valid DNS names, includes letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The description of the Unified CM Server	None	Any text	No
Device Admin URL	The Administration URL for the Unified CM Server	None	A valid URL. The Operations Console validates the URL for syntax errors, but does not check that the site exists.	No
Enable Synchronization for Location (See Synchronize Location Information, on page 71 for more information.)				

Field	Description	Default	Range	Restart Required
Enable synchronization	Select to enable synchronization for location. If enabled, the Operations Console extracts (synchronizes) the Unified CM location information from the Unified CM server.	Disabled When you enable this service, the Port field defaults to 8443.	Enabled or Disabled	No
Username	User name to access the Unified CM AXL interface.	None	Valid names include uppercase and lowercase alphabetical letters, the numbers 0 through 9, a dash, and an underscore.	No
Password	Password to access the Unified CM AXL interface	None	Any text that follows the requirements for choosing secuire passwords. See General User Information Settings, on page 240.	No
Confirm Password	Retype the password to verify that you typed the password correctly	None	Text must match the text entered in the Password field	No
Port	The port to which the Unified CM server connects when establishing initial contact	8443	1 through 65535	No

Procedure

Step 1 Select **Device Management** > **Unified CM**.

The Find, Add, Delete, Edit Unified ICM Servers window opens.

Step 2 Select the Unified CM Server that you want to edit. To narrow down the list of servers see Find Unified CM Server, on page 215.

Step 3 Click **Edit**.

The Edit Unified CM Server Configuration window opens to the General tab with the current settings displayed.

Step 4 Update the configuration settings as required.

See the Unified CM configuration settings field descriptions table for details.

Note Cisco AXL Web Service must be enabled on the Unified CM for synchronization to work.

To enable Cisco AXL Web Service on the Unified CM, perform the following steps:

a) Log on to Unified CM .
b) Open the Cisco Unified Serviceability dashboard and select **Tools** > **Service Activation**.
c) In the drop down, select the Unified CM server that is configured in this Operations Console, and click **Go**.
d) In the Database and Admin Services section, check the box next to "Cisco AXL Web Service".
e) Click **Save**.

Step 5 (Optional) Select the **Device Pool** tab and add the server to a device pool.

Step 6 When you finish configuring the server, click **Save** to save the configuration.

Related Topics

Device Information Field Descriptions, on page 118
Find Unified CM Server, on page 215
Add or Remove Device From Device Pool, on page 62
Synchronize Location Information, on page 71

Delete Unified CM Server

Deleting a Unified CM Server deletes the configuration of the selected server from the Operations Console database and removes the server from the displayed list of Unified CM Servers.

Procedure

To delete a Unified CM Server:

Procedure

Step 1 Select **Device Management** > **Unified CM**.

The Find, Add, Delete, Edit Unified ICM Servers window opens.

Step 2 Select the Unified CM Server that you want to delete. To narrow down the list of servers, see Find Unified CM Server, on page 215.

Step 3 Click **Delete**.

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

Related Topics

Find Unified CM Server, on page 215
Synchronize Location Information, on page 71

Find Unified CM Server

You can locate a Unified CM Server on the basis of specific criteria. Use the following procedure to locate a Unified CM Server.

Related Topics

Synchronize Location Information, on page 71

Procedure

To find a Unified CM Server:

Procedure

Step 1 Select **Device Management** > **Unified CM**.

The Find, Add, Delete, Edit Unified ICM Servers window lists the available Unified ICM Servers, sorted by name, 10 at a time.

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

Step 3 You can also filter the list by selecting an attribute such as Hostname. Then select a modifier, such as **begins with**, enter your search term, and then click**Find**.

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

Unified ICM Server Setup

Unified CVP provides VoIP routing services for the Unified CCE and Unified CCX products. Unified ICM provides the services 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.

A Unified ICM Server is required in Unified CVP Comprehensive, Call Director, and VRU-Only call flow models.

Add Unified ICM Server

From the Device Management menu, ICM Server option, you can add a pre-configured ICM Server to the Operations Console. Once added, you can add the ICM Server to a device pool.

Related Topics

Add or Remove Device From Device Pool, on page 62
Device Information Field Descriptions, on page 118

Procedure

To add an ICM Server:

Procedure

Step 1 Select **Device Management** > **Unified ICM**.

The Find, Add, Delete, Edit ICM Server window opens.

Note To use an existing ICM Server as a template for creating the new ICM Server, select the ICM Server by clicking the radio button preceding it, and then clicking **Use As Template**.

Step 2 Click **Add New**.

The Unified ICM Server Configuration window opens.

Step 3 Fill in the appropriate Unified ICM configuration settings on the General tab.

Table 58: Unified ICM General Tab Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Unified ICM Server	None	Valid IP address	No
Hostname	The name of the Unified ICM Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The description of the Unified ICM Server	None	Up to 1,024 characters	No
Device Admin URL	The URL for the Unified ICM web configuration application.	None	Valid URL	No

Step 4 In the Unified ICM server, enter the information in the Enable Serviceability panel so that Serviceability information for this Unified ICM server is distributed using the web services manager feature of Unified CVP.

Table 59: Unified ICM Serviceability Fields

Field	Description	Default	Range
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for Unified ICM.	Not Selected	Not Applicable

Field	Description	Default	Range
Username	The username required to sign in to Unified ICM Serviceability. For Unified ICM, the Username is typically a `domain\username` combination.	Not Applicable	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.
Password/Confirm Password	The password required to sign in to Unified ICM Serviceability.	Not Applicable	Any text that follows the requirements for choosing secure passwords. See General User Information Settings, on page 240
Port	The port on which Serviceability is configured on Unified ICM.	7890	1 - 65535

Step 5 (Optional) Select the Device Pool tab and add the Unified ICM Server to a device pool.

Step 6 When you finish configuring the Unified ICM Server, click **Save**.

Delete Unified ICM Server

Deleting a Unified ICM Server deletes the configuration of the selected Unified ICM Server in the Operations Console database and removes the Unified ICM Server from the list of Unified ICM Servers displayed in the Operations Console.

Related Topics

Find Unified ICM Server, on page 220

Procedure

To delete a Unified ICM Server:

Procedure

Step 1 Select **Device Management** > **Unified ICM**.

The Find, Add, Delete, Edit window opens.

Step 2 Select the Unified ICM Server that you want to delete. To narrow the list of servers see Find Unified ICM Server, on page 220.

Step 3 Click **Delete**.

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

Edit Unified ICM Server

Related Topics

Add or Remove Device From Device Pool, on page 62
Device Information Field Descriptions, on page 118
Find Unified ICM Server, on page 220

Procedure

To edit a Unified ICM Server:

Procedure

Step 1 Select **Device Management** > **Unified ICM**.

The Find, Add, Delete, Edit Unified ICM Server window opens.

Step 2 Select the Unified ICM Server that you want to edit. To narrow the list of servers see Find Unified ICM Server, on page 220.

Step 3 Click **Edit**.

The Unified ICM Server Configuration window opens and displays the current settings.

Step 4 Change the appropriate Unified ICM Server configuration settings on the General tab as required.

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of the Unified ICM Server. **Note** This field is not editable.	None	Valid IP address	No
Hostname	The name of the Unified ICM Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The description of the Unified ICM Server	None	Up to 1,024 characters	No
Device Admin URL	The URL for the Unified ICM web configuration application.	None	Valid URL	No

Step 5 In the Unified ICM server, you can change the information in Enable Serviceability panel.

Table 60: Unified ICM Serviceability Fields

Field	Description	Data Range	Default
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for Unified ICM.	Not Selected	Not Applicable
Username	The username required to sign in to Unified ICM Serviceability. For Unified ICM, the Username is typically a `domain\username` combination.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable
Password/Confirm Password	The password required to sign in to Unified ICM Serviceability (for example, the web admin password).	Must match password on Unified ICM	Not Applicable
Port	The port on which Serviceability is configured on Unified ICM.	1 - 65535	7890

Step 6 Update the **Device Pool** tab settings.

Step 7 When you are finished configuring the Unified ICM Server, click **Save**.

Find Unified ICM Server

You can locate a Unified ICM Server on the basis of specific criteria. Use the following procedure to locate a Unified ICM Server.

Procedure

To find a Unified ICM Server:

Procedure

Step 1 Select **Device Management** > **Unified ICM**.

The Find, Add, Delete, Edit Unified ICM Servers window lists the available Unified ICM Servers.

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

Step 3 You can also filter the list by selecting an attribute such as **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

SIP Proxy Server Setup

From **Device Management** > **SIP Proxy Server**, add a SIP Proxy Server to the Operations Console. Once added, you can add the SIP Proxy Server to a device pool. You can also configure a link to the administration web page for the SIP Proxy Server so that you can access that page from the Operations Console.

A SIP Proxy Server is a device that routes individual SIP transport messages among SIP endpoints. It plays a key role in high availability in a Unified CVP deployment for call switching. It is designed to support multiple SIP endpoints of various types, and implements load balancing and failover among those endpoints. SIP Proxy Servers are deployed alone or as a pair. Also, smaller Unified CVP deployments run without a SIP Proxy Server. In such cases, the Unified CVP SIP service assumes some of those functions because it configures a static table to look up destinations.

Unified CVP works with RFC-3261-compliant SIP Proxy Servers and has been qualified with the following:

- Cisco Unified SIP Proxy

Add SIP Proxy Server

Related Topics

Add or Remove Device From Device Pool, on page 62
Device Information Field Descriptions, on page 118

Procedure

To add SIP Proxy Server:

Procedure

Step 1 Select **Device Management** > **SIP Proxy Server**.

The Find, Add, Delete, Edit window opens.

Note To use an existing SIP Proxy Server as a template for creating the new SIP Proxy Server, select the SIP Proxy Server by clicking the radio button preceding it, and then click **Use As Template**.

Step 2 Click **Add New**.

The SIP Server Configuration window opens.

Step 3 Fill in the appropriate SIP Proxy Server configuration settings on the **General** tab.

Table 61: SIP Proxy Server Configuration Settings

Field	Description	Default	Range	Restart Required
IP Address	The IP address of the SIP Proxy Server	None	Valid IP address	Not Applicable
Hostname	The host name of the SIP Proxy Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash	Not Applicable
Device Type	The type of proxy server.	Cisco Unified SIP Proxy	Cisco Unified SIP Proxy	Not Applicable
Description	The description of the SIP Proxy Server	None	Up to 1,024 characters	Not Applicable
Device Admin URL	The Administration URL of SIP Proxy Server.	None	A valid URL. The UI validates the URL for URL syntax errors, but no validation for site existence.	Not Applicable

Table 62: SIP Proxy Server Serviceability Fields

Field	Description	Default	Data Range
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for SIP Proxy Server.	Not Selected	Not Applicable
Username	The username required to sign in to the proxy server's serviceability.	Not Applicable	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.
Password	For Unified SIP Proxy Only. The password that matches the user password.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.

Field	Description	Default	Data Range
Confirm Password	Retype password.	Not Applicable	Must match password on the SIP Proxy.
Port	The port on which Serviceability is configured on the SIP Proxy.	8443	1 - 65535

Step 4 Optionally, select the **Device Pool** tab and add the SIP Proxy Server to a device pool.

Step 5 When you finish configuring the SIP Proxy Server, click **Save**.

Edit SIP Proxy Server

You can change an existing SIP Proxy Server configuration.

Procedure

To edit SIP Proxy Server:

Procedure

Step 1 Select **Device Management** > **SIP Proxy Server**.

The Find, Add, Delete, Edit SIP Servers window opens.

Step 2 Select the SIP Proxy Server that you want to edit. If the list is too long, see Find SIP Proxy Server, on page 225.

Step 3 Click **Edit**.

The SIP Proxy Server Configuration window opens and displays the current settings.

Step 4 Fill in the appropriate configuration settings on the General tab.

Table 63: SIP Proxy Server Configuration Settings

Field	Description	Default	Range	Restart Required
IP Address	The IP address of the SIP Proxy Server **Note** This field is not editable	None	Valid IP address	Not Applicable
Hostname	The host name of the SIP Proxy Server	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash	Not Applicable

Field	Description	Default	Range	Restart Required
Device Type	The type of proxy server	Cisco Unified SIP Proxy	Cisco Unified SIP Proxy	Not Applicable
Description	The description of the SIP Proxy Server	None	Up to 1,024 characters	Not Applicable
Device Admin URL	The Administration URL of SIP Proxy Server	None	A valid URL. The UI validates the URL for URL syntax errors, but no validation for site existence	Not Applicable

Table 64: SIP Proxy Server Serviceability Fields

Field	Description	Data Range	Default
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for SIP Proxy Server.	Not Selected	Not Applicable
Username	The username required to sign in to Unified ICM Serviceability.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable
User Password/Enable Password	The password required to sign in to SIP Proxy Serviceability.	Must match password on Unified ICM	Not Applicable
Port	The port on which Serviceability is configured on the SIP Proxy.	1 - 65535	8443

Step 5 (Optional) Select the **Device Pool** tab and update the device pool settings.

Step 6 When you finish configuring the SIP Proxy Server, click **Save**.

Related Topics

Device Information Field Descriptions, on page 118

Delete SIP Proxy Server

Deleting a SIP Proxy Server deletes the configuration of the selected Proxy Server in the Operations Console database and removes the server from displayed list of SIP Proxy Servers.

Procedure

To delete a SIP Proxy Server:

Procedure

Step 1 Select **Device Management** > **SIP Proxy Server**.

The Find, Add, Delete, Edit SIP Proxy Server window opens.

Step 2 Select the radio button next to the SIP Proxy Server that you want to delete. If the list is too long, see Find SIP Proxy Server, on page 225.

Step 3 Click **Delete**.

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

Find SIP Proxy Server

You can locate a SIP Proxy Server on the basis of specific criteria. Use the following procedure to locate a SIP Proxy Server.

Procedure

To find a SIP Proxy Server:

Procedure

Step 1 Select **Device Management** > **SIP Proxy Server**.

The Find, Add, Delete, Edit SIP Proxy Servers window lists the available proxy servers of the type you selected, sorted by name, 10 at a time.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window 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 **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Unified IC Server Setup

The Unified Intelligence Center (Unified IC) Server is a device type in Operations Console for Unified CVP.

To support a Unified CVP reporting solution, install and configure a Unified IC Server with the Unified CVP Reporting Server.

Note To use an existing Unified IC Server as a template for creating the new Unified IC Server, select the Unified IC Server by clicking the radio button preceding it, and then click **Use As Template**.

- Configured Unified IC Servers are listed in the Device Past Configurations table listing. Unified IC Server devices are only saved to the Operations Console database--they are not saved and deployed. Consequently, each Unified IC Server is listed as one past configuration entry.
- The Unified IC Server is a standalone device and is not integrated with Unified CVP. Therefore, the Unified IC Server is not displayed in the Device Versions table.
- A Unified IC Server device is not included as a selectable device in the SNMP menu option windows.
- If you select a Unified CVP Reporting Server for deletion and this server has a Unified IC Server association, a warning message prompts you to remove the association.

Add Unified IC Server

You can create a new Unified IC Server by using an existing Unified IC Server configuration as a template or by filling in its values from scratch.

Related Topics

Unified IC Server Setup, on page 226
Edit Unified IC Server, on page 228
Delete Unified IC Server, on page 229
Find Unified IC Server, on page 229

Procedure

To add a Unified IC Server to the Operations Console database and associate it with a Unified CVP Reporting Server:

Procedure

Step 1 Select **Device Management** > **Unified IC**.

All Unified IC Servers that have been added to the Operations Console are listed in the Find, Add, Delete, Edit Unified IC Servers list.

Step 2 Click **Add New**.

The Unified IC Server Configuration window opens to the General tab.

Step 3 Fill in the appropriate Unified IC Server configuration settings on the **General** tab.

Table 65: General Settings

Field	Description	Default	Range	Restart Required
IP Address	The IP address of the Unified IC	None	Valid IP address	Not Applicable
Hostname	The host name of the Unified IC	None	Valid DNS name, includes letters in the alphabet, the numbers 0 through 9, and a dash	Not Applicable
Description	The description of the Unified IC	None	Up to 1,024 characters	Not Applicable
Device Admin URL	The Administration URL of Unified IC	None	A valid URL. The UI validates the URL for URL syntax errors, but no validation for site existence	Not Applicable

Table 66: Unified IC Server Serviceability Fields

Field	Description	Default	Data Range
Enable Serviceability	Select this check box to enable serviceability. This option allows you to use system CLI to collect diagnostic (health and status) and device-specific information for Unified IC.	Not Selected	Not Applicable
Username	The username required to sign in to the proxy server's serviceability.	Not Applicable	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.
Password	For Unified SIP Proxy Only. The password that matches the user password.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.	Valid names contain uppercase and lowercase alphanumeric characters, period, dash and underscore.
Confirm Password	Retype password.	Not Applicable	Must match password on the SIP Proxy.

Field	Description	Default	Data Range
Port	The port on which Serviceability is configured on the SIP Proxy.	8443	1 - 65535

Step 4 Assigning Unified CVP Reporting Servers is optional. One Unified CVP Reporting Server can be assigned to multiple Unified IC Server devices. By associating a Reporting Server, you are tracking that this Reporting Server is being set up as a data source for Unified IC.

Step 5 Click **Device Pool** to associate the Unified IC Server to a device pool.

The default device pool is automatically assigned to the newly-configured Unified IC Server. You can specifically assign the Unified IC Server to required device pool.

Step 6 When you finish configuring the Unified IC Server, click **Save** to save the settings in the Operations Console database.

Edit Unified IC Server

While you can edit any existing Unified IC Server device, you cannot change the IP address of a Unified IC Server. The same fields present when adding a Unified IC Server (see Add Unified IC Server, on page 226) are also displayed in the edit process.

Related Topics

Unified IC Server Setup, on page 226
Add Unified IC Server, on page 226
Delete Unified IC Server, on page 229
Find Unified IC Server, on page 229

Procedure

To edit an existing Unified IC Server:

Procedure

Step 1 Select **Device Management** > **Unified IC**.

The Find, Add, Delete, Edit Unified IC Server window opens.

Step 2 Select a Unified IC Server by clicking on the link in its name field or by clicking the radio button preceding it, and then clicking **Edit**. To narrow the list of servers see Find Unified IC Server, on page 229.

All fields are pre-populated with existing configuration information if available: IP Address (read-only, required), Hostname (required), Description, Device Admin URL, and Reporting Server Assignment. Serviceability information is also present if configured. See Add Unified IC Server, on page 226 for details on the fields.

Step 3 (Optional) Select the **Device Pool** tab to add/remove devices the device pool.

Step 4 When you finish configuring the Unified IC Server, click **Save** to save the settings in the Operations Console database.

Delete Unified IC Server

One Unified CVP Reporting Server can be assigned to several Unified IC Servers. Before the assigned Unified CVP Reporting Server can be deleted, these associated references in the Unified IC devices must also be removed. When you select a Unified CVP Reporting Server for deletion and that server has a Unified IC Server association, you receive a warning message prompting you to delete all Unified IC Server associations.

You can delete existing Unified IC Servers using the procedure specified in this section.

Related Topics

Unified IC Server Setup, on page 226
Add Unified IC Server, on page 226
Edit Unified IC Server, on page 228
Find Unified IC Server, on page 229

Procedure

To delete a Unified IC Server:

Procedure

Step 1 Select **Device Management** > **Unified IC**.

The Find, Add, Delete, Edit Unified IC Server window opens.

Step 2 Select the required Unified IC Server by clicking the radio button preceding it, and then clicking **Delete**. To narrow the list of servers see Find Unified IC Server, on page 229.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Find Unified IC Server

Use the following procedure to locate a Unified IC Server that has been added in the Operations Console.

Related Topics

Unified IC Server Setup, on page 226
Add Unified IC Server, on page 226
Edit Unified IC Server, on page 228
Delete Unified IC Server, on page 229

Procedure

To find a Unified IC Server:

Procedure

Step 1 Select **Device Management** > **Unified IC**.

The Find, Add, Delete, Edit Unified IC Servers window lists the available Unified IC Servers, 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 window to page through the list. Or, you can enter a page number in the **Page** field and press **enter** to go to the numbered page.

Step 3 You can also filter the list by selecting an attribute such as **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Past Device Setups in Operations Console Database

You can view the past 10 saved configurations of a selected device that are currently stored in the Operations Console database.

Find Past Device Setup

To find a past configuration for a device, first find the device. As you probably have several devices in your network, the Operations Console lets you locate specific devices on the basis of specific criteria. Use the following procedure to locate a device.

Procedure

To find a past configuration for a device:

Procedure

Step 1 Select **Device Management** > **Device Past Configurations**.

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

Step 3 You can also filter the list by selecting an attribute such as **Hostname**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

View Past Device Setup

Procedure

To view the details of a past configuration for a device:

Procedure

Step 1 Select **Device Management** > **Device Past Configurations**.

Step 2 Select the device configuration by clicking the radio button preceding it and then clicking **Past Configurations**.

The List of Past Configurations window lists the configurations that have been saved for the selected device.

Step 3 Select a device past configuration to view by clicking the link in the description field or by clicking the radio button preceding it, and then clicking **View**.

Configuration details for the selected past configuration are displayed.

Apply Past Device Setup

The Operations Console stores configurations for a device. You can select a previous device configuration and apply it to a device.

Procedure

To apply a past configuration to a device:

Procedure

Step 1 Select **Device Management** > **Device Past Configurations** from the Main menu.

Step 2 Select the device configuration by clicking the radio button preceding it, and then clicking **Past Configurations**.

The List of Past Configurations window lists the configurations that have been saved for the selected device.

Step 3 Select a device past configuration to view by clicking the link in the description field or by clicking the radio button preceding it, and then clicking **View**.

Configuration details for the selected past configuration are displayed.

Step 4 Click **Save** to save the selected configuration to the database.

Note If this is a Reporting Server, Call Server, VXML Server, Unified CVP VXML Server (standalone), or Speech Server, you must click **Save & Deploy**.

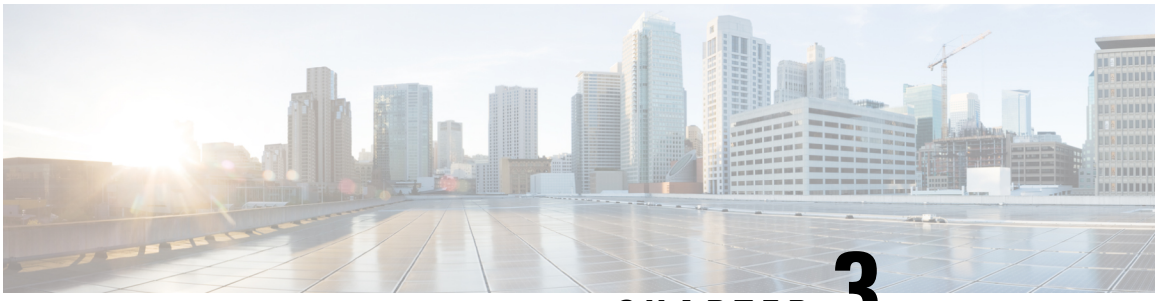
Device Versions

From the Device Management menu, Device Version option, you can view version information for the Call Server, Reporting Server, Unified CVP VXML Server, and Unified CVP VXML Server (standalone). Device version information is available for CVP specific devices only.

To view version information for CVP device types:

1. Select **Device Management** > **Device Versions**.
2. From the **Select Device Type** drop-down menu, select the CVP device type that you want version information about.

   The table refreshes to display devices of the selected type and corresponding version data.



CHAPTER 3

Managing Unified CVP Users

From the User Management menu, Users option, you can create one user account at a time. Unified CVP includes the Super User, Administrator, Read Only, and Serviceability Administration roles. You can assign users to any of these roles. The Unified CVP installation creates an Administrator account, which is assigned to the Super User role and a "wsmadmin" account which is assigned a Serviceability Administration role.

User groups are provided so that you can group users together. Assigning users to groups limits the operations users can perform from the Operations Console menus. For example, administrators for San Jose devices can belong to a user group called SanJose_Admins with Administrator privilege.

Device pools are logical groupings of devices, for example, SanJose-Gateways. If a user is configured with SanJose-Gateways as the device pool, then that user can operate only on devices in this device pool. The types of allowed operations also depends on which user group the user belongs to. For example, if a user belongs to SanJose_Admins, a group with Administrator privilege, then this user has Administrator privilege for devices in the SanJose-Gateways device pool.

Unified CVP includes four categories of access criteria:

- Super User - Allows any operation in the Operations Console. Only the Super User can create and delete Administrator accounts and assign device pools to any user. The Super User can view all devices because this account is associated with the "default" device pool.
- Administrator - Allows any operation in the Operations Console except deleting Administrator accounts. Administrators can only view devices in the device pools to which they have been associated. Administrators can disassociate themselves from a device pool, but cannot associate themselves to a device pool.
- Read Only- Allows read-only access to the Operation Console.
- Serviceability Administration - Allows Web Services authentication through the Unified System CLI tool and does not provide any privileges for the Operations Console. Only the Administrator can create and delete Web Services users. Whenever Web Services user information is changed or whenever a Unified CVP device is deployed successfully, the configured Web Services users are pushed to all deployed Unified CVP devices (see Web Services, on page 93).

  Users roles that have Serviceability Administration applied cannot have any roles assigned that contain Super User, Administrator, or Read Only privileges.

User Role Management

A user role is a logical group of privileges, also called access criteria, that determine the operations a user can perform. For example, you might create a role that grants an operator read-only access to the Reporting Server, but grants write access to the Unified CVP VXML Servers. You can do this by creating an operator user group and assigning that group the default Administrator privilege, which allows any operation except deleting accounts with superuser privilege. Then, create a device pool that contains all Unified CVP VXML Servers. Finally, assign the Unified CVP VXML Server device pool to the operator user group.

Add User Role

Related Topics

Edit User Role, on page 234
Delete User Roles, on page 236
Assign Role to User Group, on page 238
Assign User Role Access Criteria, on page 235
Find User Role, on page 236

Procedure

To add a user role:

Procedure

Step 1 Select **User Management** > **User Roles** from the Main menu.

The Find, Add, Delete, Edit window opens.

Step 2 Select **Add New**.

Step 3 On the General tab, fill in the name of the role in the Role Name field.

Step 4 Fill in descriptive text in the Description field, if desired.

Step 5 Select the **Access Criteria** tab and assign access criteria to the user role. See Assign User Role Access Criteria, on page 235.

A default Access Criteria of Administrator is applied to every new user role you create.

Step 6 When you finish configuring the user role, click **Save** to save the configuration.

Edit User Role

Related Topics

Add User Role, on page 234
Delete User Roles, on page 236
Find User Role, on page 236
Assign User Role Access Criteria, on page 235

Procedure

You can change the access criteria, which are privileges, assigned to a user role that has been added to the Operations Console.

Procedure

Step 1 Select **User Management** > **User Roles** from the Main menu.

The Find, Add, Delete, Edit Application User Roles window opens.

Step 2 Select the desired Role Name link or select the user role from the list and click **Edit**. If you have a long list of user roles, see Find User Role, on page 236.

The Edit Application User Role window opens to the General tab.

Step 3 Change the description for the user role, if desired.

Step 4 Select the **Access Criteria** tab and change the access criteria assigned to the user role. See Assign User Role Access Criteria, on page 235.

Step 5 When you finish configuring the user role, select **Save**.

Assign User Role Access Criteria

Access criteria are privileges that let users perform one or more operations using the Operations Console. Assign access criteria to a user role when:

Procedure

- Add User Role, on page 234
- Edit User Role, on page 234

Related Topics

Find User Role, on page 236
Delete User Roles, on page 236
Assign Role to User Group, on page 238

Procedure

To assign access criteria to a user role:

Procedure

Step 1 Select **Access Criteria** tab.

Step 2 Select the desired access criteria.

Step 3 Click **Save** to save the user role with assigned access criteria to the Operations Console database.

Find User Role

The Operations Console lets you locate specific user roles on the basis of specific criteria. Use the following procedure to locate a user role:

Procedure

To find a user role:

Procedure

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

The Find, Add, Delete, Edit 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 window to page through the list. Or, you can enter a page number in the **Page** field and press Enter to go to the numbered page.

Step 3 Filter the list by selecting an attribute such as **Role Name**. Select a modifier, such as **begins with**. Enter your search term and click **Find**.

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

Delete User Roles

Deleting a user role deletes the configuration of the selected user role in the Operations Console database and removes the user role from the displayed list of user roles.

Related Topics

Add User Role, on page 234
Edit User Role, on page 234
Find User Role, on page 236

Procedure

To delete a user role:

Procedure

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

The Find, Add, Delete, Edit Application User Roles window opens.

Step 2 Find the user roles using the procedure shown in Find User Role, on page 236.

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

Step 4 Select **Delete**.

Step 5 When prompted to confirm the delete operation, perform one of the following steps:.

- Select **OK** to delete the operation.
- Select **Cancel** to cancel the operation.

Service Types User Roles and User Group Associations

In Unified CVP, the Operations Console allows you to add a new type of user role: a Web Services (Serviceability Administration) user role.

The Operation Console does not support a mix-and-match of various user roles. The existing Operations Console service type user roles (Super User, Administrator, and Read-only users) cannot co-exist with the Web service type user roles (Web Services users) within a single user group.

Whenever you add/modify/delete a Web Services user role, a current list of Web Services users is pushed to all deployed Unified CVP devices.

The end user receives a validation error in the following situations:

- When you edit any user role, the list of user groups associated with this user role are retrieved. If the user role changes and causes a mismatch of user role service types within any of its associated user groups.
- A role changes and causes a mismatch of user role service types within any of its associated users.

Users assigned a Web Services user role cannot log into the Operations Console.

User Group Management

A user group is a collection of users to which you can assign one or more user roles. These groups limit the operations that users can perform to the Operations Console.

Add User Group

Related Topics

Edit User Groups, on page 238
Assign Role to User Group, on page 238
Delete User Group, on page 239
Find User Group, on page 240

Procedure

To add a User Group:

Procedure

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

The Find, Add, Delete, Edit Application User Groups window opens.

Step 2 Select **Add New**.

Step 3 Fill in the name of the group in the Group Name field.

Step 4 Fill in descriptive text in the Description field, if desired.

Step 5 Select the **User Roles** tab and assign a user role to the user group. See Assign Role to User Group, on page 238 for details.

You must assign at least one user role to each user group you create.

Note You cannot add a Web Service Role and an Operations Console user role to the same user group.

Note Users assigned a Web Service Role cannot log in to the Operations Console.

Step 6 When you finish configuring the user group, select **Save**.

Edit User Groups

You can change one or more settings for a user group that has been added to the Operations Console.

Related Topics

Add User Group, on page 237
Delete User Group, on page 239
Find User Group, on page 240
Assign Role to User Group, on page 238

Procedure

To edit a User Group:

Procedure

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

The Find, Add, Delete, Edit User Groups window opens.

Step 2 If you have a long list of user groups, see Find User Group, on page 240 to narrow the list of choices.

Step 3 Select the radio button next to the User Group name and click **Edit** or click the Group Name. See Assign Role to User Group, on page 238 for details.

The User Group Configuration window opens to the General tab.

Step 4 You can change the description for the group by editing the Description field.

Step 5 Select the **User Roles** tab and edit the assigned roles for this user group.

Step 6 When you finish configuring the user group, click **Save**.

Assign Role to User Group

A user role is a named collection of privileges that can be assigned to a user group. You can assign one or more user roles to a user group on the User Role tab. Assign a user role to a user group when you:

Procedure

- Add User Group, on page 237
- Edit User Groups, on page 238

Related Topics

Find User Group, on page 240
Delete User Group, on page 239
Edit User Groups, on page 238
User Role Management, on page 234

Procedure

To assign a user role to a user group:

Procedure

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

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

Step 3 Click **Save**.

Delete User Group

Deleting a user group from the Operations Console deletes the configuration of the selected user group in the Operations Console database and removes the user group from the displayed list of user groups.

Related Topics

Add User Group, on page 237
Find User Group, on page 240
Edit User Groups, on page 238

Procedure

To delete a user group from the Operations Console:

Procedure

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

The Find, Add, Delete, Edit Application User Groups window opens.

Step 2 Find the groups by using the procedure in Find User Group, on page 240.

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

Step 4 Select **Delete**.

Step 5 When prompted to confirm the delete operation, perform one of the following steps:

- Select **OK** to delete the operation
- Select **Cancel** to cancel the delete operation

Find User Group

The Operations Console lets you locate specific user groups on the basis of specific criteria. Use the following procedure to locate a user group.

Procedure

To find a user group:

Procedure

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

The Find, Add, Delete, Edit Application User Groups Window lists the available user groups.

Step 2 If the list is long, you can perform one of the following steps:

- Select the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list, or
- Enter a page number in the **Page** field and press Enter to go to the numbered page.

Step 3 To filter the list, perform the following steps:

a) Select an attribute, such as **Group Name**
b) Select a modified, such as **begins with**
c) Enter your search term
d) Select **Find**

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

Unified CVP User Setup

From the User Management menu, Users option, you can create one user account at a time. Unified CVP includes four roles: Super User, Administrator, and Read Only in the Operations Console Server type of role, and Serviceability Administration in the Web Services type of role. You can assign users to any of these roles; however, you cannot assign users to roles that include both the Operations Console type and the web services type. See Assign User Role Access Criteria, on page 235 for information about this restriction.

General User Information Settings

Configure general information about a Unified CVP user when you:

- Add User Account

- Edit User Account

Table 67: 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
Password	New password for the user account. User must type this password to log into the Operations Console.	None	Any text that follows the Secure Password Requirements	No
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
Signed in User Password	The password used to log into the user account.	None	Valid e-mail address	No

Secure Password Requirements

Note Passwords must meet all the following criteria.

Passwords must only contain the following ASCII characters:

- Maximum password length is 80 characters.

- Minimum password length is 12 characters
- The password must contain characters from at least three of the following classes: lowercase characters, uppercase characters, digits, and special characters.
  - Lowercase letters (abcdefghijklmnopqrstuvwxyz)
  - Uppercase letters (ABCDEFGHIJKLMNOPQRSTUVWXYZ)
  - Digits (012345689)
  - Special characters: !"#$%&'()*+,-./ :;<=>?@ [\]^_` {|}~
- No character in the password can be repeated more than three (3) times consecutively.
- Password must not repeat or reverse username. Password is not **`cisco`**, **`ocsic`**, or any variant obtained by changing the capitalization of letters therein.

Add User Account

Related Topics

General User Information Settings, on page 240
Add or Remove User From Device Pool, on page 245
Edit User Account, on page 243
Delete User Account, on page 243
Find User Account, on page 244
Add User Role, on page 234
Add User Group, on page 237

Procedure

Before You Begin

When you are adding a new user for the first time after installing Unified CVP software, you must create at least one user role and user group before creating the user account. For information on performing these tasks, see Add User Role, on page 234, Add User Group, on page 237.

Note You must create Device Pools to further limit access to devices. See Add Device Pool to Operations Console, on page 60.

To add a user account:

Procedure

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

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

Step 2 Select **Add New**.

Step 3 Fill in the appropriate configuration settings on the General tab.

Step 4 Select the **Device Pools** tab and assign a Device Pool to the user. Each user must be assigned to at least one device pool. See Add or Remove User From Device Pool, on page 245.

Step 5 Select the **User Group** tab and add the user to one or more user groups. See Add User Group, on page 237.

Step 6 When you finish configuring the user, click **Save**.

Edit User Account

Related Topics

Add User Account, on page 242
Delete User Account, on page 243
Find User Account, on page 244
General User Information Settings, on page 240
Add or Remove User From Device Pool, on page 245

Procedure

You can change one or more settings for a user account that has been added to the Operations Console.

Procedure

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

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

Step 2 Select the desired Username link or select radio button next to the username from and select **Edit**. You can reduce the list of users displayed. See Find User Account, on page 244.

The Edit User page opens to the General tab.

Step 3 Fill in the appropriate configuration settings on the General tab as described in General User Information Settings, on page 240.

Step 4 Select the Device Pools tab and assign a device pool to the user. See Add or Remove User From Device Pool, on page 245.

Step 5 Select the User Groups tab and add/remove the user to/from one or more user groups. See Add User Group, on page 237.

Step 6 When you finish configuring the user, select **Save**.

Delete User Account

You can delete one or more user accounts from the Operations Console. Deleting a user account from the Operations Console removes the user account data from the Operations Console database and from the displayed list of user accounts.

Related Topics

Add User Account, on page 242

Find User Account, on page 244
Edit User Account, on page 243

Procedure

To delete a user account:

Procedure

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

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

Step 2 From the list of users, select the user that you want to delete. You can reduce the list of users displayed. See Find User Account, on page 244

Step 3 Select **Delete**.

Step 4 When prompted to confirm the delete operation, perform one of the following steps:

- Select **OK** to delete.
- Select **Cancel** to cancel the delete operation.

Find User Account

The Operations Console lets you locate users on the basis of specific criteria. Use the following procedure to locate an Operations Console user account.

Related Topics

Add User Account, on page 242
Delete User Account, on page 243
Edit User Account, on page 243

Procedure

To find a user:

Procedure

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

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

Step 2 Perform one of the following steps:

- If the list is long, select the first page, previous page, next page, and last page icons on the bottom right of the window to page through the list.
- Enter a page number in the **Page** field and press Enter to go directly to the numbered page.

Step 3 Filter the list by performing the following steps:

a) Select an attribute, such as **Username**.

b) Select a modifier, such as **begins with**.
c) Enter your search term.
d) Select **Find**.

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

Add or Remove User From Device Pool

A device pool is a named collection of devices. You must add each user to at least one device pool. Users can be added to or removed from one or more device pools.

Related Topics

Add User Account, on page 242
Find User Account, on page 244
Edit User Account, on page 243
Device Pools, on page 60

Procedure

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**.

Assign User to User Group

Assigning users to groups can limit the operations users can perform from the Operations Console menus. You must assign each user to at least one user group. Unified CVP includes four roles:

- Super User - a role with superuser privileges that allow any operation in the Operations Console.
- Administrator - can perform any operation in the Operations Console except deleting user accounts.
- Serviceability Administration - Allows Web Services authentication through the "Unified System CLI" tool and does not allow any privileges for the Operations Console.
- Read Only - Has Read-only access to the Operations console.

You add/remove a user to/from a user group when you:

- Add User Account, on page 242
- Edit User Account, on page 243

Related Topics

Find User Account, on page 244
Delete User Account, on page 243
Add User Role, on page 234

Procedure

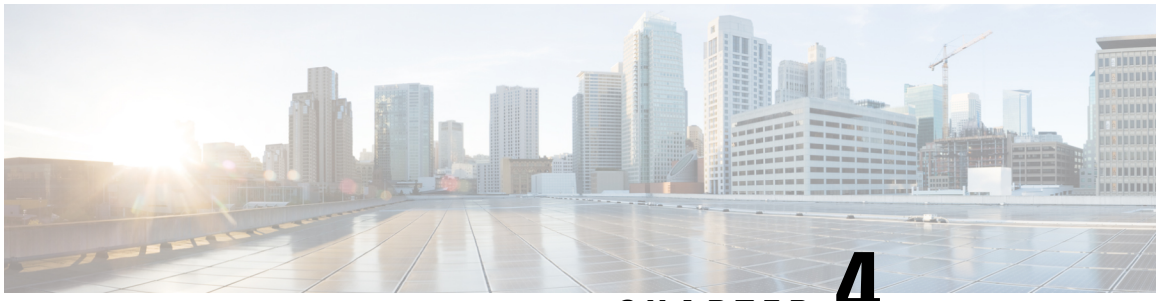
To add/remove a user to/from a user group:

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**.



CHAPTER 4

Bulk Administration

Bulk Administration File Transfer (BAFT)

You can transfer multiple VXML application files and Script and Media files from the Operations Console to one or more devices in a single operation. Some types of files can only be transferred to certain types of devices. Script and Media files can be transferred to Gateways. VXML Application files can be transferred to Unified CVP VXML Servers.

See also:

Transfer Scripts and Media Files Using BAFT

To transfer one or more script or media files:

Procedure

Step 1 Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.

The **File Transfer - Scripts and Media** window opens.

Step 2 In the **Device Association** panel, use the **Select Device Type** drop-down menu and select the type of device to which you want to transfer scripts and/or media files.

Step 3 Select a device from the **Available** box and click the right arrow to move the device to the **Selected** box.

Step 4 To remove a device from the **Selected Devices** box, select the device and click the left arrow to move the device to the **Available** box.

Step 5 In the **Script and Media Files** panel, select the radio button for the action you want to perform, then select or browse for the files you want to transfer.

There are three choices:

- Default Gateway files - the default gateway files are displayed in the list box. By default, all default files are selected. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click transfer.

- Managed files - Managed files are non-default files that have already been transferred to a device from this Operations Console server. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click transfer. You can optionally highlight files and then click **Delete Managed file** to remove the file from this Operations Console server and the managed files list.
- Select new files - You can click browse to select a new file to upload from your local computer. After you browse and select a file, another slot is made available to browse and upload, up to a limit of 10 files. After transfer, these files are displayed in the Managed Files section.

Step 6 When you finish selecting devices and files, select **Transfer**.

The selected file(s) is transferred to each selected device. You can view the status of the transfer by clicking File Transfer Status. See View File Transfer Status, on page 249.

Transfer VXML Applications Using BAFT

To transfer one or more VXML applications:

Procedure

Step 1 Select **Bulk Administration** > **File Transfer** > **VXML Applications**.

The **File Transfer - VXML Application window opens.**

Step 2 Select one or more Unified CVP VXML Servers and click the appropriate arrow to move them into the **Selected** panel.

The list of available Unified CVP VXML Servers to which you can transfer a VXML application is listed in the Associated Unified CVP VXML Server(s)Available panel.

Step 3 In the **VXML Application Files** panel, select the radio button for the action that you want to perform, then select or browse for the files that you want to transfer.

There are two choices:

- Select new files - You can click browse to select a new VXML application to upload from your local computer. After you browse and select a VXML application, another slot is made available to browse and upload, up to a limit of 10 VXML applications. After the transfer finishes, these files are displayed in the Managed Files section.
- Managed files - Managed files are files that have already been transferred to a device from this Operations Console server. You can select or deselect one or more files using CTRL-click. Highlighted files are sent to the device(s) after you click **Transfer**. You can also highlight files and then click **Delete Managed file** to remove the file from this Operations Console server and the managed files list.

  Note During the Enforcement state, uploading of VXML application from OAMP is blocked. Refer the NOAMP Help to understand the Enforcement Rules.

Step 4 When you finish selecting devices, click **Transfer**.

The selected file(s) is transferred to each selected device. You can view the status of the transfer by clicking File Transfer Status. See View File Transfer Status, on page 249.

View File Transfer Status

To view the status of a bulk administration file transfer:

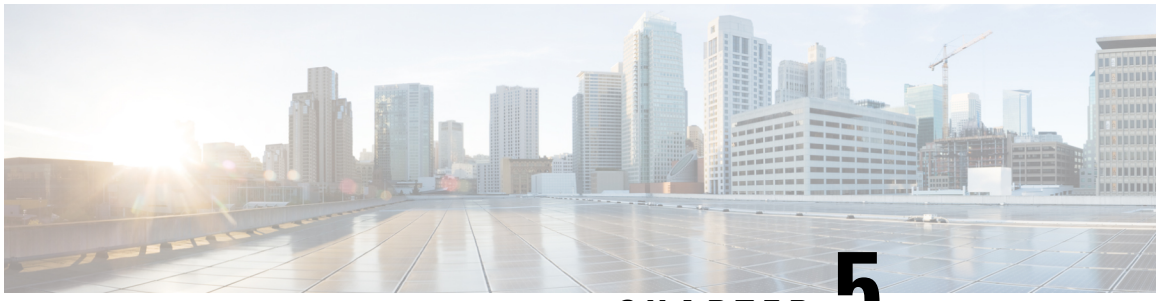
Procedure

Step 1 Select **Bulk Administration** > **File Transfer** then **Scripts and Media Files** or **VXML Application**.

Step 2 Select the **File Transfer Status** button on the resulting page.

The status for the transfer is listed in the table.

Select **Refresh** to refresh the list of statuses.



CHAPTER 5

SNMP Agent Setup

Simple Network Management Protocol Support

Simple Network Management Protocol (SNMP), an application layer protocol, facilitates the exchange of management information among network devices, such as nodes, routers, and so on. As part of the TCP/IP protocol suite, SNMP enables administrators to remotely manage network performance, find and solve network problems, and plan for network growth. The Unified CVP SNMP agent lets customers and partners to integrate with their existing SNMP network management system to provide instantaneous feedback on the health of their Unified CVP system.

The Call server, Unified CVP VXML Server, and Reporting server can send SNMP traps and statistics to any standard SNMP management station. You can configure a link to the administration web page for an SNMP monitoring tool and then access it by selecting SNMP Monitor from the Tools menu.

The SNMP menus from the Operations Console enable you to configure SNMP-associated settings, such as community strings, users, and notification destinations for V1, V2c, and V3. SNMP V3 offers improved security features.

SNMP Basics

An SNMP-managed network is comprised of managed devices, agents, and network management systems.

Key SNMP Components

- Managed device - A network node that contains an SNMP agent and resides on a managed network. Managed devices collect and store management information and make it available by using SNMP.

- Agent - A network-managed software module that resides on a managed device. An agent contains local knowledge of management information and translates it into a form that is compatible with SNMP. Unified CVP uses a primary agent and subagent components to support SNMP. The primary agent acts as the agent protocol engine and performs the authentication, authorization, access control, and privacy functions that relate to SNMP requests. Likewise, the primary agent contains a few MIB variables that relate to MIB-II. The SNMP primary agent listens on port 161 and forwards SNMP packets for Vendor MIBs. The Unified CVP subagent interacts with the local Unified CVP only. The Unified CVP subagent sends notifications and SNMP response messages to the primary agent for forwarding to a Network Management Station. The SNMP primary agent communicates with the SNMP trap receiver (notification destination).
- Network Management System (NMS) - A SNMP management application (together with the PC on which it runs) that provides the bulk of the processing and memory resources that are required for network management. An NMS executes applications that monitor and control managed devices. Unified CVP works with any standard SNMP-based NMS.

SNMP Management Information Base (MIB)

SNMP allows access to Management Information Base (MIB), which is a collection of information that is organized hierarchically. MIBs comprise managed objects, which are identified by object identifiers. A MIB object, which contains specific characteristics of a managed device, comprises one or more object instances (variables). The Unified CVP Simple Network Management Protocol (SNMP) agent resides in each component and exposes the CISCO-CVP-MIB that provides detailed information about devices that are known to the Unified CVP subagent. The CISCO-CVP-MIB provides device information such as device registration status, IP address, description, and model type for the component.

The AIX Native agent by default listens on port 161 for Network Management Station requests. Upon installation of CVP, the AIX Native agent is reconfigured to listen on port 8161. The CVP SNMP Agent takes over listening on port 161. The CVP SNMP Agent acts as a proxy to the Native AIX Agent. The CVP SNMP Agent handles the forwarding of traps and statistics. SNMP Traps generated by the Native AIX Agent are sent to the CVP SNMP Agent and forwarded to all SNMP Notification targets that are configured using the Operations Console.

Unified CVP supports the following MIBs:

Supported MIBs:

- CISCO-CVP-MIB - Provides general information; server name and version number; and status and statistics for each component.
- HOST-RESOURCES-MIB - The Host Resources MIB found in Cisco SNMP is an implementation of the Host Resources MIB document, proposed standard RFC 1514 (https://www.ietf.org/rfc/rfc1514.txt). It is also compliant with Host Resources MIB, draft standard RFC 2790 (https://www.ietf.org/rfc/rfc2790.txt). This MIB defines objects that are useful for managing host systems and allows SNMP access to useful host information, such as the storage resources, process table, device information, and the installed software base.
- The System-level Managed Objects for Applications (SYSAPPL) MIB, RFC 2287 (https://www.ietf.org/rfc/rfc2287.txt), supports configuration, fault detection, performance monitoring, and control of application software. It provides for tables that define an application as a series of processes and services. This includes objects for applications installed on the system, elements and processes that are included in an application, and current and previously run applications.

Set Up SNMP

Table 68: SNMP Configuration Checklist

Configuration Steps	Related Procedures and Topics
Install and configure the SNMP NMS.	SNMP product documentation that supports the NMS.
Import all previous SNMP configurations to the Operations Console.	Import Previously Configured Windows SNMP v1 Community Strings
If you are using SNMP v1/v2c, configure the community string.	SNMP v1/v2c Community String Setup
If you are using SNMP v3, configure the SNMP user.	SNMP v3 User Setup
Configure the notification destinations.	SNMP v1/v2 Notification Destination Setup
Configure the system contact and location for the MIB2 system group.	SNMP MIB2 System Group Setup

Import Previously Configured Windows SNMP v1 Community Strings

To import previously configured Windows SNMP V1 Community Strings:

Procedure

Step 1 View the list of previously configured Windows SNMP V1 community strings by performing the following:

a) Open the Windows Services viewer.
b) Right-click **SNMP Service** and select **Properties**.
c) Select the **Security** tab. This tab lists the accepted V1 community strings and the access granted for each string, and also lists the hosts from which SNMP packets are accepted.

Note The accepted hosts apply to all community strings, whereas the Operations Console provides more granularity, allowing you to specify accepted hosts on a per-community string basis.

Step 2 Configure these community strings using the Operations Console:

a) Open the Operations Console and select **SNMP | V1/V2C | Community String**.
b) For each community string discovered above that has not already been configured in the Operations Console, add it by clicking **Add New**.

Perform the following actions:

- Enter the community string exactly as it appeared in step 1 above.

- Select **V1** as the version.
- For Windows community strings with permission other than "Read Only," select **Read Write** in the Operations Console.
- Select the device(s) on which this community string was seen in step 1.

SNMP v1/v2c Agent Setup

SNMP version 1 (SNMPv1), the initial implementation of SNMP that functions within the specifications of the Structure of Management Information (SMI), operates over protocols, such as User Datagram Protocol (UDP) and Internet Protocol (IP). The SNMPv1 SMI defines highly structured management information base tables (MIBs) that are used to group the instances of a tabular object (that is, an object that contains multiple variables). Tables contain zero or more rows, which are indexed to allow SNMP to retrieve or alter an entire row with a supported command. With SNMPv1, the NMS issues a request, and managed devices return responses. Agents use the Trap operation to asynchronously inform the NMS of a significant event.

As with SNMPv1, SNMPv2c functions within the specifications of the Structure of Management Information (SMI). MIB modules contain definitions of interrelated managed objects. The operations that are used in SNMPv1 are similar to those that are used in SNMPv2. The SNMPv2 Trap operation, for example, serves the same function as that used in SNMPv1, but it uses a different message format and replaces the SNMPv1 Trap.

You need to compile the Cisco CVP MIB with your SNMP network management application. The CVP MIB is located in the %CVP_HOME%\conf folder. You can also find the current list of supported MIBS at: https://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Note The CVP MIB is defined using version 2 of the Structure of Management Information (SMI) and contains "Counter64" (64-bit integer) object types. While the CVP SNMP infrastructure supports version 1 of the SNMP protocol, SNMP v1 cannot query Counter64 object values. Hence, you must use SNMP v3 or SNMP v2c.

You can configure SNMP v1 support from the SNMP V1/V2c menu.

You can perform the following tasks:

- SNMP v1/v2c Community String Setup, on page 254
- SNMP v1/v2 Notification Destination Setup, on page 259

SNMP v1/v2c Community String Setup

Although SNMP community strings provide no security, they authenticate access to MIB objects and function as embedded passwords. Typically, one community string is used for read-only access to a network element.

You configure SNMP community strings for SNMP v1 and v2c only. SNMP v3 does not use community strings. Instead, version 3 uses SNMP users. These users serve the same purpose as community strings, but users provide security because you can configure encryption or authentication for them.

Add SNMP v1/v2C Community String

Related Topics

SNMP v1/v2c Community String Settings, on page 256
Find SNMP v1/v2c Community String, on page 258

Procedure

To add an SNMP v1/v2c community string:

Procedure

Step 1 Select **SNMPV1/V2cCommunity String**.

The Find, Add, Delete, Edit window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select **Add New**.

The V1/V2c SNMP Community String Configuration window opens to the General tab.

Step 3 Fill in the community string and verify that the default values for other fields are correct.

Step 4 Select the **Devices** tab and assign an SNMP community string to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or select **Save & Deploy** to save the changes and apply the changes to the selected devices.

Edit SNMP v1/v2C Community String

Related Topics

SNMP v1/v2c Community String Settings, on page 256
Find SNMP v1/v2c Community String, on page 258

Procedure

You can change the name, the hosts to accept SNMP packets from, and the access privileges for an SNMP V1/V2C community string.

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 Select the SNMP community string to edit by checking the check box preceding it and selecting **Edit**.

The Community String Configuration window opens to the General tab.

Step 3 Make the desired changes to the community string settings. You cannot change the name of the SNMP community string.

Step 4 Select the **Devices** tab and make desired changes to the assignment of the SNMP community string to a device.

Step 5 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply the changes to the selected devices.

SNMP v1/v2c Community String Settings

The following table describes the fields that you can change to configure an SNMP v1/v2c community string.

Table 69: SNMP v1/v2c Community String Configuration

Field	Description	Default	Range	Restart Required
Community String Information				
Community String Name	You cannot change this name if you are editing a Community String.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
SNMP Version Information				
V1 or V2c	Select SNMP Version 1 or 2c agent	V1	V1 or 2c	No
Host IP Addresses Information				
Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts	Select hosts that are allowed to query or access the configured devices using this community string.	Accept SNMP Packets From Any Host	From any host or from only these hosts	No
Host IP Address	Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click **Add** to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click **Remove**.	None	Valid IP address	No
Access Privileges				

Field	Description	Default	Range	Restart Required
Access Privileges	Choose the appropriate access level from the following list: Access Privileges: • **ReadOnly** - The community string can only read the values of MIB objects. • **ReadWrite** - The community string can read and write the values of MIB objects.	ReadOnly	ReadOnly, ReadWrite	No

Assign SNMP Entity to Device

Procedure

While you add or edit any of the following SNMP entities, you can add them to or remove them from one or more devices:

SNMP Entities:

- SNMP V1/V2C community strings
- SNMP V1/V2C or V3 notification destinations
- SNMP MIB-2 user groups
- SNMP V3 users

Procedure

Step 1 Select the **Devices** tab.

Step 2 To add an SNMP V1/V2 community string to a device, perform the following steps:

a) Select the device from the **Available** pane.
b) Select the right arrow to move the device to the **Selected** pane.

Step 3 To remove an SNMP V1/V2 community string from a device, perform the following steps:.

a) Select the device from the **Selected** pane.
b) Select the left arrow to move the device to the **Available** pane.

Step 4 Select **Save** to save the configuration to the Operations Console database. Select **Save & Deploy** to save the changes and apply the changes to the selected devices.

Find SNMP v1/v2c Community String

If you have several SNMP community strings in your network, the Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP community string.

Procedure

To find an SNMP V1/V2c community string:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 To scroll through the list, select **Next** to view the next group of available community strings.

Step 3 Select **Previous** to view the previous group of available community strings.

Step 4 To filter the list:

a) Using the filter at the top right of the list, select a field to search.
b) Select a modified (such as Starts with).
c) Select **Find**.

Note The filter is not case-sensitive and wildcards are not allowed.

Step 5 From the second window drop-down list box, select one of the following search criteria:

- begins with
- contains
- ends with
- is exactly

Step 6 Specify the appropriate search text, if applicable, and select **Find**.

Delete SNMP v1/v2c Community String

Procedure

To delete one or more SNMP V1/V2c community strings:

Procedure

Step 1 Selec **SNMP** > **V1/V2c** > **Community String**.

The Find, Add, Delete, Edit Window lists the available SNMP community strings, sorted by name, 10 at a time.

Step 2 To select the SNMP community string to delete, perform the following steps:

a) Select the check box preceding the string.

b) Select **Delete**.

Step 3 When prompted to confirm the delete operation, perform one of the following steps:

- Select **OK** to delete the operation.
- Select **Cancel** to cancel the delete operation.

Related Topics

Find SNMP v1/v2c Community String, on page 258

SNMP v1/v2 Notification Destination Setup

You can configure different community strings for SNMP v1 and v2c depending on which protocol they wish to use on their network. If you use both SNMP v1 and v2c, you can configure one community string for v1 and another for v2.

You might have one management station (using SNMP v1) collecting notifications from one part of the network and another management station (using SNMP v2) collecting notifications from another part. In this case, when configuring a destination, you must specify the community string that correlates the SNMP version used to send the notification.

SNMP v1/v2 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

Table 70: Notification Destination Configuration Settings

Field	Description	Default	Range	Restart Required
Host IP Address Information				
Host IP Address	IP address of host to receive SNMP notifications.	None	Valid IP address	No
Port Number	Port number to receive SNMP notifications.	162	Any available port number. Valid port numbers are integers between 1 and 65535	No
Notification Destination Information				

Field	Description	Default	Range	Restart Required
Notification Destination Name	When you are adding a notification destination, assign a name. You cannot change the Notification Destination Name.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
Community String Information				
Community String	Select the community string from the drop-down list.	None	Not applicable	No

Add SNMP v1/v2c Notification Destination

Procedure

To add an SNMP v1/v2c notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2c Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The V1/V2c Notification Destination Configuration window opens to the Configuration tab.

Step 3 Fill in the fields on the configuration tab.

Step 4 Select the **Devices** tab and assign the SNMP notification destination to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save and apply the changes to the selected devices.

Related Topics

SNMP v1/v2 Notification Destination Settings, on page 259

Edit SNMP v1/v2C Notification Destination

Related Topics

SNMP v1/v2 Notification Destination Settings, on page 259
Assign SNMP Entity to Device, on page 257
Find SNMP v1/v2C Notification Destination, on page 261

Procedure

To change an SNMP V1/V2C notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To select the SNMP notification destination to edit, perform the following steps:

a) Select the check box preceding the destination.
b) Select **Edit**.

The Notification Destination Configuration window opens to the Configuration tab.

Step 3 Make the desired changes to the fields on the Configuration tab.

Note You cannot change the name of the notification destination.

Step 4 Select the **Devices** tab and assign an SNMP entity to a device.

Step 5 Select **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save and apply the changes to the selected devices.

Delete SNMP v1/v2C Notification Destination

Procedure

To delete one or more SNMP V1/V2c notification destinations:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2C Notification Destinations Window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To select the SNMP notification destination to delete, perform the following steps:

a) Select the check box preceding the destination.
b) Select **Delete**.

Step 3 When prompted to confirm the delete operation, select **OK** to delete or select **Cancel** to cancel the delete operation.

Find SNMP v1/v2C Notification Destination, on page 261

Find SNMP v1/v2C Notification Destination

The Operations Console lets you locate specific community strings on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

Procedure

To find an SNMP V1/V2c notification destination:

Procedure

Step 1 Select **SNMP** > **V1/V2c** > **Notification Destination**.

The Find, Add, Delete, Edit V1/V2c Notification Destinations window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 To scroll through many pages of the list, click 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 performing the following steps:

a) Using the filter at the top right of the list, select a field to search.
b) Select a modifier (such as Starts With).
c) Select **Find**.

Note The filter is not case-sensitive and wildcards are not allowed.

SNMP v3 Agent Setup

SNMP version 3 provides security features such as authentication (verifying that the request comes from a genuine source), privacy (encryption of data), authorization (verifying that the user allows the requested operation), and access control (verifying that the user has access to the objects requested.) To prevent SNMP packets from being exposed on the network, you can configure encryption with SNMPv3. Instead of using community strings like SNMP v1 and v2, SNMP v3 uses SNMP users, as described in the SNMP Community Strings and Users topic.

Configure SNMP v3 support from the SNMP V3 menu.

You can perform the following tasks:

- SNMP v3 User Setup, on page 262
- SNMP v3 Notification Destination Setup, on page 267

SNMP v3 User Setup

When you create SNMP users, match their SNMP user names to the user names you have already configured for the NMS.

You can perform the following tasks:

- Find SNMP v3 User, on page 263
- Add SNMP v3 User, on page 263
- Edit SNMP v3 User, on page 264

Find SNMP v3 User

Procedure

To find an SNMP user:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit Users window lists the available SNMP v3 users, sorted by name, 10 at a time.

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 window to page through the list. Or, you can enter a page number in the **Page** field and press **enter** to go to the numbered page.

Step 3 You can filter the list by selecting an attribute such as **V3 Username**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Add SNMP v3 User

Related Topics

SNMP v3 User Settings, on page 264
Assign SNMP Entity to Device, on page 257

Procedure

To add an SNMP v3 user:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit V3 Users window lists the available SNMP users, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The SNMP V3 User Configuration window opens to the Configuration tab.

Step 3 Fill in the username and verify that the default values for other fields are correct.

Step 4 Select the **Devices** tab and assign the user to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the change to the selected devices.

Edit SNMP v3 User

Related Topics

SNMP v3 User Settings, on page 264
Assign SNMP Entity to Device, on page 257
Find SNMP v3 User, on page 263

Procedure

You can change the access privileges, authentication and privacy information for an SNMP V3 user.

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit Users window lists the available SNMP users, sorted by name, 10 at a time.

Step 2 Select the SNMP user name to edit by selecting the check box preceding it or highlighting the user name and then clicking **Edit**.

The SNMP User Configuration window opens to the Configuration tab.

Step 3 Make the desired changes to SNMP V3 users settings. You cannot change the username for the SNMP V3 user.

Step 4 Select the **Devices** tab and change the assignment of the user to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save and apply the change to the selected devices.

SNMP v3 User Settings

The following table describes the fields that you can change to configure an SNMP v3 user.

Field	Description	Default	Range	Restart Required
User Information				
Username	Enter the SNMP v3 user name. You cannot change this name when editing an SNMP v3 user.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No

Field	Description	Default	Range	Restart Required
Access Privileges	Select the appropriate access level from the following list: Access Privileges: • **ReadOnly** - The community string can only read the values of MIB objects. • **ReadWrite** - The community string can read and write the values of MIB objects.	ReadOnly	ReadOnly, ReadWrite	No
Host IP Addresses Information				
Accept SNMP Packets From any Host or Accept SNMP Packets Only from these Hosts	Select hosts that are allowed to query or access the configured devices using this community string.	Accept SNMP Packets From Any Host	From any host or from only these hosts	No
Host IP Address	Enter the IP address of an SNMP management station from which SNMP agents accept SNMP packets. Enter the IP address and click **Add** to include the IP address in the list of Host IP Addresses. To remove an IP address from the list, select the IP address and click **Remove**.	None	Valid IP address	No
Authentication Information				
Authentication Required	Select to require authentication for this user. This offers an additional level of security not provided with SNMP v1 and v2c. The SNMP user only gains access to the device when using both a valid user name and password. If authentication is not required, security is no better with v3 than it would be for SNMP v1/v2c using community strings.	Disabled	Enabled or Disabled	No
Password	Password for the SNMP Version 3 user. This password is required to accept incoming SNMP v3 packets.	None	Any text that follows the Secure Password Requirements.	No

Field	Description	Default	Range	Restart Required
Re-enter Password	Retype the password for this user account to verify that you typed the password correctly.	None	The same text that was entered in the Password field.	No
Protocol	Choose MD5 or SHA-1 protocols to encrypt the password.	None	MD5 or SHA-1	No
Privacy Information				
Privacy Required	Select to require privacy for the SNMP user. Enabling privacy causes the SNMP message data to be encrypted during transmission. This provides an additional level of security over authentication (only) in that it protects the data, rendering it unreadable by would-be snoopers while traveling over the wire.	Disabled	Enabled or disabled.	No
Password	Password the SNMP user must enter.	None	Any text that follows the Secure Password Requirements.	No
Re-enter Password	Re-type the same text entered in the Password field.	None	The same text entered in the Password field.	No
Protocol	Select the protocol to encrypt the user password.	None	3DES, AES-192 , AES-256	No

Delete SNMP v3 User

Procedure

To delete one or more SNMP users:

Procedure

Step 1 Select **SNMP** > **V3** > **User**.

The Find, Add, Delete, Edit window lists the available users, sorted by name, 10 at a time.

Step 2 Select the SNMP users to delete by selecting the check box preceding it or highlighting the user name, and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP v3 User, on page 263

SNMP v3 Notification Destination Setup

A notification destination identifies the target host and port to receive SNMP notifications sent by the Unified CVP SNMP agent on the devices you specify. You can specify an SNMP v3 user and associated authorization for an SNMP v3 notification destination.

Add SNMP v3 Notification Destination

Related Topics

SNMP v3 Notification Destination Settings, on page 268
Assign SNMP Entity to Device, on page 257

Procedure

To add an SNMP V3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Add New**.

The SNMP Notification Destination Configuration window opens to the Configuration tab.

Step 3 Fill in the name of the SNMP V3 notification destination.

Step 4 Select the **Devices** tab and assign the SNMP notification destination to a device.

Step 5 Click **Save** to save the settings in the Operations Console database. Click **Save & Deploy** to save the change and apply them to the selected devices.

Edit SNMP v3 Notification Destination

Related Topics

SNMP v3 Notification Destination Settings, on page 268
Assign SNMP Entity to Device, on page 257

Procedure

To change an SNMP v3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Click **Edit**.

The SNMP Notification Destination Configuration window opens to the Configuration tab.

Step 3 Change the desired notification destination configuration settings. You cannot change the name of the notification destination.

Step 4 Select the **Devices** tab and add or remove devices to this notification destination.

Step 5 Click **Save** to save the settings in the Operations Console database, or click **Save & Deploy** to save the change and apply them to the selected devices.

SNMP v3 Notification Destination Settings

The following table describes the fields that you can change to configure the host and port to receive SNMP notifications.

Field	Description	Default	Range	Restart Required
Notification Destination Information				
Notification Destination Name	Name for the notification destination. You cannot change this name when editing a notification destination.	None	Letters in the alphabet, the numbers 0 through 9, and a dash	No
Host IP Addresses Information				
Host IP Address	IP address of host to receive SNMP notifications.	None	Valid IP address	No
Port Number	Port number to receive SNMP notifications.	162	Any available port number. Valid port numbers are integers between 1 and 65535	No
User Information				
User	Select a user from the drop-down list.	None	None	No

Find SNMP v3 Notification Destination

As you probably have several SNMP notification destinations in your network, the Operations Console lets you locate specific destination notifications on the basis of specific criteria. Use the following procedure to locate an SNMP notification destination.

Procedure

To find an SNMP V3 notification destination:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, 10 at a time, sorted by name.

Step 2 If the list is long, click the first page, previous page, next page, and last page icons on the bottom right of the window 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**. Then select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Delete SNMP v3 Notification Destination

Procedure

To delete one or more SNMP V3 notification destinations:

Procedure

Step 1 Select **SNMP** > **V3** > **Notification Destination**.

The Find, Add, Delete, Edit window lists the available SNMP notification destinations, sorted by name, 10 at a time.

Step 2 Select the SNMP notification destination to delete by selecting the check box preceding it or highlighting the notification destination and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP v1/v2C Notification Destination, on page 261

SNMP MIB2 System Group Setup

The Operations Console allows you to change the system contact and system location information in the SNMP MIB-II system group, and to assign that system group to a device. For example, you could enter Administrator, 555-121-6633, for the system contact and San Jose, Bldg 23, 2nd floor, for the system location.

You can perform the following tasks:

Add SNMP MIB2 System Group

Procedure

To add an SNMP MIB2 system group:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit MIB2 System Groups window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time. Each device can only be associated with one system group. Only devices that are not associated with other system groups are displayed in the available system groups.

Step 2 Click **Add New**.

The MIB2 System Group Configuration window opens to the Configuration tab.

Step 3 In the **System Contact** field, enter a person to notify when problems occur.

Step 4 In the **System Location** field, enter the location of the person that is identified as the system contact.

Step 5 Select the **Devices** tab and assign the devices to this system group.

Step 6 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

Edit SNMP MIB2 System Group

Procedure

To change SNMP MIB2 system group information:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

Step 2 Click **Edit**.

The MIB2 System Group Configuration window opens to the Configuration tab.

Step 3 In the **System Contact** field, change the name of the person to notify when problems occur.

Step 4 Select the **Devices** tab and add or remove devices to this system group.

Step 5 Click **Save** to save the configuration to the Operations Console database, or click **Save & Deploy** to save the changes and apply them to the selected devices.

Delete SNMP MIB2 System Group

Procedure

To delete one or more SNMP MIB2 system groups:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

Step 2 Select the SNMP MIB2 system group to delete by selecting the check box preceding it and then clicking **Delete**.

Step 3 When prompted to confirm the delete operation, click **OK** or click **Cancel**.

Related Topics

Find SNMP MIB2 System Group, on page 271

Find SNMP MIB2 System Group

Procedure

To find an SNMP MIB2 system group:

Procedure

Step 1 Select **SNMP** > **System Group** > **MIB2 System Group**.

The Find, Add, Delete, Edit window lists the available SNMP MIB2 system groups, sorted by name, 10 at a time.

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

Step 3 You can also filter the list by selecting an attribute such as **System Location**. Select a modifier, such as **begins with**, enter your search term, and then click **Find**.

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

Syslog

Set Up Syslog Server

The instructions below describe how to adjust syslog settings for a Unified CVP Call Server, Unified CVP VXML Server, and/or Unified CVP Reporting Server using the Operations Console.

Procedure

Step 1 Open the Operations Console.

Step 2 Select the server where you want to configure syslog.

Step 3 Click **Edit**.

Step 4 Click **Infrastructure** tab.

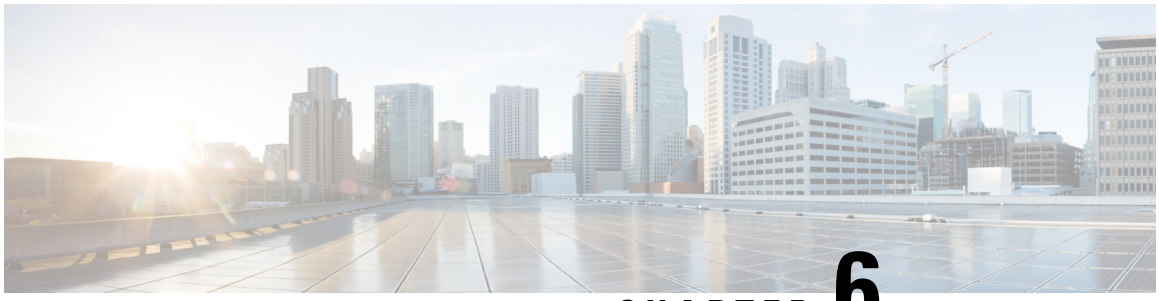
Step 5 Edit the fields for backup severs and port numbers for secondary syslog server.

Step 6 Click **Save**.

Unified CVP allows you to configure primary and backup syslog servers. However, it is important to note that failover from primary to backup server is not guaranteed. When the primary syslog server goes down (the entire machine not just the syslog receiver application), Unified CVP relies on the host operating system and the Java Runtime Environment for notification that the destination is not reachable. As this notification does not guarantee delivery, Unified CVP cannot guarantee failover.

Unified CVP allows you to configure secondary set of syslog and backup servers. CVP sends the syslog messages to both primary syslog and secondary syslog server on the ports specified.

See the *Configuration Guide for Cisco Unified Customer Voice Portal* for additional information about Syslog Server settings.



CHAPTER 6

Launch Tools

Launch SNMP Monitor

You can use any standard SNMP-based monitoring tool to view details of the health of the Unified CVP solution network. All Unified CVP product components issue SNMP events, which can be delivered to the network monitoring tool. To specify a SNMP-based monitoring tool as the destination for SNMP traps and statistics, you must edit the Log Messages XML file on the Unified CVP Server for each event that the server generates. For information on editing the Log Message XML file to send SNMP events to an SNMP monitoring tool, see Edit Log Messages XML File, on page 179.

You can launch the administration web page for an external SNMP monitoring tool from the Tools menu in the Operations Console.

Before you begin

Before you can launch an SNMP monitor, you must first specify the URL of the SNMP monitor web page to launch. For information on configuring the URL external tools, see the Links to Tools, on page 273 topic.

Procedure

To Launch SNMP Monitor, choose **Tools** > **SNMP Monitor** from the Operations Console.

Links to Tools

You can store URLs for the tools available from the Tools menu. Once configured, you can launch the administrative web page for each tool by selecting the tool from the Operations Console Tools menu bar.

Add URL to Tools Menu

Procedure

To add a URL link to a tool:

Procedure

Step 1 Select **Tools** > **Configure** from the Operations Console.

The Configure Tools window opens, listing the current URL configured for each tool listed on the Tools menu.

Step 2 In the Enter New URL text box for the tool you want to configure, enter the URL for each tool to launch.

The web page indicated by this URL is launched when you select the tool from the Tools menu.

Step 3 Click **Save** to save the URLs.

Remove URL From Tools Menu

Procedure

To remove a URL link for a tool:

Procedure

Step 1 Choose **Tools** > **Configure** from the Operations Console.

The Configure Tools window opens, listing the current URL for each tool.

Step 2 In the Enter New URL text box for the tool you want to configure, delete the URL from the text box, and click **Save**.

The URL for that tool is removed from the Operations Console, which means that no URL is configured for that tool.

Modify URL on Tools Menu

Procedure

To modify a URL link for a tool:

Procedure

Step 1 Select **Tools** > **Configure** from the Operations Console.

The Configure Tools window opens, listing the current URL for each tool.

Step 2 In the Enter New URL text box for the tool you want to configure, modify the URL and click **Save**.

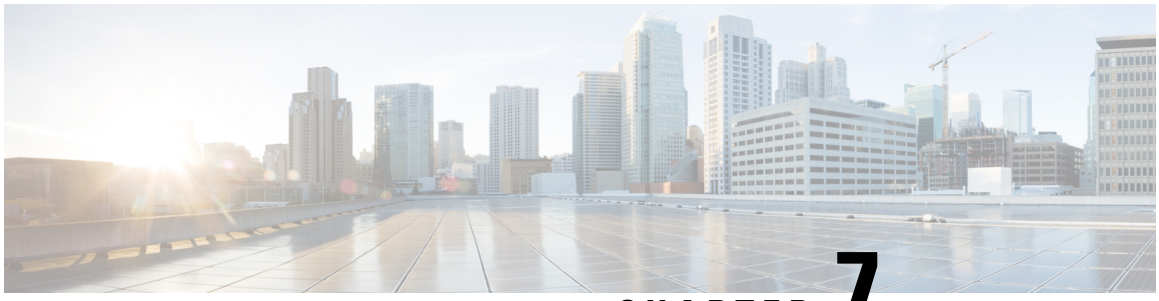
This modifies the URL for the selected tool. The web page indicated by this URL is launched when you select the tool from the Tools menu.

Launch NOAMP

This procedure explains how to navigate automatically to NOAMP (NOAMP) using the credentials of Operations Console (OAMP).

Procedure

Go to **Tools** > **NOAMP**.
You are logged in to NOAMP automatically.



CHAPTER 7

Documentation Search

Documentation Search

The Documentation search feature searches for a term in the Unified CVP documents hosted on cisco.com. You can refine your search results by clicking on the tabs at the top of the page (for example, *Configuration* or *Troubleshooting*).

Note The Operations Console must be able to access both *google.com* and *cisco.com* for the documentation search to function. If the Operations Console is firewalled for port 80, then you cannot use the documentation search feature.

To use the search documentation feature from within the Operations Console, click the **Documentation Search** link on the top right of the page.

Documentation Search

INDEX

D

E

F

G

H

I

L

M

T

U

V