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 1: 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

Viewing Device Status

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 4.

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 3.

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 run micro-applications. The VXML pages created by this module are sent to the VXML Gateway to be run. 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

Shutting Down a Server

Starting a Server

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 7.

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 9
- Set Up SIP Service, on page 13

- Set Up IVR Service, on page 14
- Add or Remove Device From Device Pool
- Set Up Infrastructure, on page 27

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 32
View Unified CVP Call Server Statistics, on page 31
View Device Status
Shut Down Server
Start Server

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 7	ICM, IVR, SIP
VRU-Only, on page 8	ICM, IVR
Call Director Using SIP, on page 8	ICM, IVR
Unified CVP VXML Server with ICM Lookup, on page 8	ICM
Unified CVP VXML Server Standalone Call Flow, on page 8	No Service
Basic Video Call Flow, on page 9	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 49.

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 run 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 49.

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 66.

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 run micro-applications. The VXML pages created by this module are sent to the VXML Gateway to be run.
- 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 6. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 29.

Step 2 Fill in the appropriate configuration settings as described in ICM Service Settings, on page 10

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 2: 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 6) or edit a Call Server (Edit Unified CVP Call Server, on page 29), and you use any of these call flow models (Call Services, on page 7):

- 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 6. If you want to change an existing Call Server, see Edit Unified CVP Call Server, on page 29.

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 run. 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 6. If you want to change an existing Call Server, refer to Edit Unified CVP Call Server, on page 29.

Step 2 Fill in the appropriate configuration settings as described in IVR Service Settings, on page 14

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 3: 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 26 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, run 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 26.

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, run 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 26.

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 26 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 26 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 26 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, run 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 26.

Default	Range	Restart Required
None	See Valid Formats for Dialed Numbers, on page 26	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 76 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 26 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, run 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 6. If you want to change infrastructure settings for an existing Call Server, refer to Edit Unified CVP Call Server, on page 29.

Step 2 Fill in the appropriate configuration settings as described in Infrastructure Settings, on page 27.

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 4: 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 6
Shut Down Server
Start Server
Upload Log Messages XML File, on page 65
Download Log Messages XML File, on page 62
View Unified CVP Call Server Statistics, on page 31
View Device Status

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 32.

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 9
- Set Up IVR Service, on page 14
- Set Up SIP Service, on page 13
- Add or Remove Device From Device Pool
- Set Up Infrastructure, on page 27

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 32.

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
IVR Service Call Statistics
Infrastructure Statistics

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 31.

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 5: 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 run.	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 48
Edit Unified CVP Reporting Server, on page 39
General Unified CVP Reporting Server Information Setup, on page 35
Reporting Properties Setup, on page 36
Add or Remove Device From Device Pool
Unified CVP Reporting Server Infrastructure Settings, on page 37
Device Information Field Descriptions, on page 2

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 6: 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 7: 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 8: 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 48
Add Unified CVP Reporting Server, on page 34
Reporting Properties Setup, on page 36
Add or Remove Device From Device Pool
Find Reporting Server, on page 48
Device Information Field Descriptions, on page 2

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 40
Set Up Reporting Database Delete, on page 44
Cancel Reporting Database Backup, on page 44
Reporting User Management, on page 41
View Database Details, on page 46
View Reporting Statistics, on page 47

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 40
Set Up Reporting Database Delete, on page 44
Reporting User Management, on page 41
View Database Details, on page 46
View Reporting Statistics, on page 47

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 43
Cancel Reporting Database Backup, on page 44
Change Reporting Database User Password, on page 40
Reporting User Management, on page 41
View Database Details, on page 46
View Reporting Statistics, on page 47

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 9: 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, stopped, 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 43
Cancel Reporting Database Backup, on page 44
Change Reporting Database User Password, on page 40
Set Up Reporting Database Delete, on page 44
Reporting User Management, on page 41
View Reporting Statistics, on page 47

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 are listed in the Reporting tab.

Related Topics

Run Reporting Database Backup, on page 43
Cancel Reporting Database Backup, on page 44
Change Reporting Database User Password, on page 40
Set Up Reporting Database Delete, on page 44
Reporting User Management, on page 41
View Database Details, on page 46

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 48.

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 34

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
- Viewing 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 54
- Unified CVP VXML Server Infrastructure Settings, on page 56

- Add or Remove Device From Device Pool

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 52
Unified CVP VXML Server Configuration Properties, on page 54
Unified CVP VXML Server Infrastructure Settings, on page 56
Add or Remove Device From Device Pool
Shut Down Server
Start Server

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 52

Add Unified CVP VXML Server, on page 50
Unified CVP VXML Server Configuration Properties, on page 54
Unified CVP VXML Server General Properties, on page 52
Unified CVP VXML Server Infrastructure Settings, on page 56
Find Unified CVP VXML Server, on page 65
Shut Down Server
Start Server
Device Information Field Descriptions, on page 2

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 50
Transfer Script and Media Files
Shut Down Server
Start Server
Find Unified CVP VXML Server, on page 65

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 10: 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 11: 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 60.	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 60.	Yes - Restart VXML Server

Unified CVP VXML Server Infrastructure Settings

Table 12: 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 59
Inclusive and Exclusive VXML Reporting Filter Examples, on page 60

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 13: 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 14: 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 65
Edit Log Messages XML File, on page 63

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 64.

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 63.

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 65
Edit Log Messages XML File, on page 63
Shut Down Server
Start Server

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 run 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 15: 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 68
Edit Standalone Unified VXML Server, on page 68
Find Standalone Unified CVP VXML Server, on page 70
View Device Status

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 70.

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 66
Edit Standalone Unified VXML Server, on page 68

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 16: 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 68
Add Standalone Unified CVP VXML Server, on page 66
Find Standalone Unified CVP VXML Server, on page 70
VXML Application File Transfers, on page 61
View Device Status

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 66
Edit Standalone Unified VXML Server, on page 68
Delete Standalone Unified CVP VXML Server, on page 68

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 run 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
Add or Remove Device From Device Pool

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 17: 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 18: 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 76.

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
Run IOS Commands on Gateway, on page 77
View Gateway Statistics, on page 77
Transfer Script and Media Files

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 76.

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 19: 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 20: 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).

Related Topics

Find Gateway, on page 76
View Gateway Statistics, on page 77
Bulk Administration File Transfer (BAFT)

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.

Related Topics

Find Gateway, on page 76

Run IOS Commands on Gateway

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

Procedure

To run 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 run on the Gateway.

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

Table 21: 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 run 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 22: 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 23: 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 24: 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
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 82.

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 82.

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 25: 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 26: 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 27: 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	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 28: 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 2
Apply Speech Server License, on page 87

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 86.

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 86

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 29: Speech Server Configuration Settings

Field	Description	Default	Range	Reboot/Restart Required
General				

Field	Description	Default	Range	Reboot/Restart Required
IP Address	The IP address of the Speech Server. **Note** This field is not editable.	None	Valid IP address	Yes - Reboot Speech Server
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 86

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 88. 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 30: Media Server Configuration Settings

Field	Description	Default	Range	Restart Required
General				
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.

Field	Description	Default	Range	Restart Required
Confirm Password	Retype password.	None	Enter vaild password.	No Use **Test Sign-in** button to verify the FTP credentials.
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 94.

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 93.

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

Step 4 Restart the Unified CVP VXML Server.

Related Topics

Find Media Server, on page 93

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 Unified CVP VXML Server.

Edit Media Server

Edit 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 31: 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.

Field	Description	Default	Range	Restart Required
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.
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 94.

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

Related Topics

Find Media Server, on page 93

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
- Synchronizing 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 32: 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

Field	Description	Default	Range	Restart Required
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 for more information.)				
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 2
Add or Remove Device From Device Pool
Synchronize Location Information

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 33: 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

Field	Description	Default	Range	Restart Required
Enable Synchronization for Location (See Synchronize Location Information for more information.)				
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.	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 100.

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 2
Find Unified CM Server, on page 100
Add or Remove Device From Device Pool
Synchronize Location Information

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 100.

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 100
Synchronize Location Information

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

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

Device Information Field Descriptions, on page 2

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 34: 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 35: 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
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 104

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 104.

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
Device Information Field Descriptions, on page 2
Find Unified ICM Server, on page 104

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 104.

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 36: 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
Device Information Field Descriptions, on page 2

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 37: 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 38: 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 109.

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 39: 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 40: 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 2

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 109.

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 110
Edit Unified IC Server, on page 112
Delete Unified IC Server, on page 113
Find Unified IC Server, on page 113

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 41: 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 42: 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 110) are also displayed in the edit process.

Related Topics

Unified IC Server Setup, on page 110
Add Unified IC Server, on page 110
Delete Unified IC Server, on page 113
Find Unified IC Server, on page 113

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 113.

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 110 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 110
Add Unified IC Server, on page 110
Edit Unified IC Server, on page 112
Find Unified IC Server, on page 113

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 113.

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 110
Add Unified IC Server, on page 110
Edit Unified IC Server, on page 112
Delete Unified IC Server, on page 113

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.