Configuration Guide for Cisco Unified Customer Voice Portal, Release 12.6(2)

First Published: 2023-04-28

Last Modified: 2023-04-28

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

Preface

Change History

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

Change	See	Date
Initial Release of Document for Release 12.6(2)		April 2023
`DecryptKeystoreUtil.bat` utility added for generating keystore password.	**Unified CVP Security**	
Updated process for generating CVP ECDSA certificate with OpenSSL.	**Unified CVP Security > Generate CVP ECDSA Certificate with OpenSSL**	
Initial Release of Document for Release 12.6(2) ES09		November 2023
Introduced Custom Code isolation feature	Added a new chapter **Remote Custom API Server Configuration**.	

About This Guide

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

- Configuration of Cisco Unified Customer Voice Portal (CVP) components and additional solution components involved in the Unified CVP call path.
- Configuration of high availability and single node for CVP components.

Audience

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

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

Related Documents

- *Compatibility Matrix for Unified CCE*
- *Feature Guide - Writing Scripts for Unified Customer Voice Portal*
- *Operations Guide for Cisco Unified Customer Voice Portal*

Communications, Services, and Additional Information

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

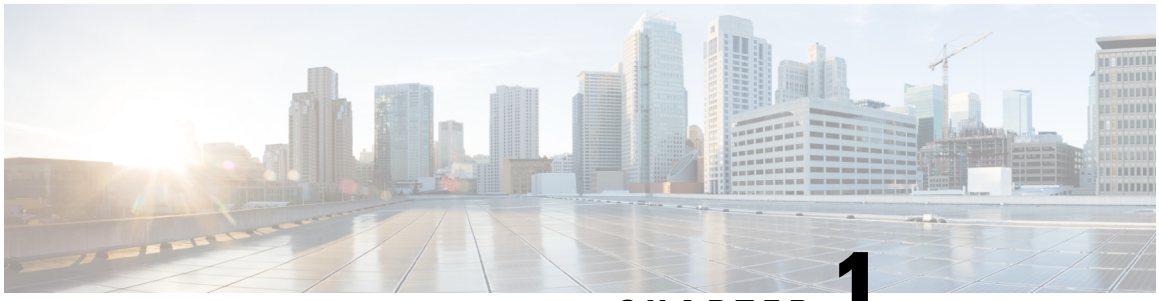
Cisco Bug Search Tool

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

Documentation Feedback

Provide your comments about this document to: mailto:contactcenterproducts_docfeedback@cisco.com.

CONTENTS



CHAPTER 1

Preconfiguration

Prerequisites for Call Flow Model Configuration

This section describes the configuration procedures and information you need before you select a call flow model and implement it.

Design Prerequisites

- Read the *Configuration Guide for Cisco Unified Customer Voice Portal*.
- Understand Cisco Unified Customer Voice Portal (CVP) and the description of call flow models.
- Analyze the design information that is provided in *Configuration Guide for Cisco Unified Customer Voice Portal*, and then choose a call flow model for your desired Unified CVP implementation.
- Create the simplified all-in-one-box step-by-step call model examples.
- Use the troubleshooting information and examples as templates.

Preconfiguration Tasks

Procedure

Step 1 Have network information. See Network Information, on page 2.

Step 2 Perform ring no answer settings with SIP. See Ring No Answer Settings with SIP, on page 93.

Step 3 Install Unified CVP on your computer. For Unified CVP installation, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_installation_guides_list.html and Unified CVP Installation, on page 3.

Step 4 Install Cisco Unified Intelligent Contact Management (ICM), Cisco Unified Communications Manager (CM), VXML and ingress gateways.

Step 5 Ensure that you have login credentials for Operations Console and Reporting Server. To sign in to Operations Console and view its menus, see Operations Console, on page 67.

Step 6 Route calls through the network to the VRU. See Route Calls Through the Network to the VRU, on page 4.

Step 7 Configure ethernet switch/server NIC, gateways, and Call Server settings. See Ethernet Switch/Server NIC, Gateways and Call Server Settings, on page 4.

Step 8 Apply contact center gateway debug settings. Apply Contact Center Gateway Debug Settings, on page 7.

Step 9 Check the network VRU types. See the Network VRU Types, on page 8.

Step 10 Refer to the SIP dialed number pattern matching algorithm. See SIP Dialed Number Pattern Matching Algorithm, on page 9.

Step 11 Default security settings can prevent you from using Operations Console. Check your security policy and, if needed, change the settings to a less restrictive level.

Related Topics

Network Information, on page 2
Ring No Answer Settings with SIP, on page 93
Route Calls Through the Network to the VRU, on page 4
Ethernet Switch/Server NIC, Gateways and Call Server Settings, on page 4
Apply Contact Center Gateway Debug Settings, on page 7
Network VRU Types, on page 8
SIP Dialed Number Pattern Matching Algorithm, on page 9

Network Information

To configure Unified CVP components and additional solution CVP components for a call flow model, ensure that you have the following network information:

- Understanding of which Unified CVP call flow model to implement.

Note For information about call flow models, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.

- Network topology for your system, including addresses and names of the solution components.
- Failover strategy for Gateways, Unified CVP components, and Media Servers.
- Strategy for inbound call routing (that is, dial-peers versus Proxy Server).
- Naming resolution system for Gateways (DNS versus configured on the Gateway).
- Naming schemes to be used for Unified Intelligent Contact Management Enterprise (ICME) peripheral gateways, peripherals, and routing clients.

- If you are using a voice response unit (VRU) other than Unified CVP, have information about VRU trunk group number and number of trunks.
- Know locale values to be used for automatic speech recognition (ASR) and text to speech (TTS) servers.
- Know whether one or multiple VRUs, which refers to the dialed number, are to be used for each customer.

Note If all the dialed numbers use the same VRU, use the default Network VRU instead of configuring multiple Network VRUs. For more information, see Configure Common Unified ICMH for Unified CVP Switch Leg, on page 178.

Related Topics

Configure Common Unified ICMH for Unified CVP Switch Leg, on page 178

Unified CVP Installation

- Install the Unified CVP software. For the installation procedures of Unified CVP components, see the https://www.cisco.com/en/US/products/sw/custcosw/ps1006/prod_installation_guides_list.html.
- Install the solution components.
- If you are using Unified CVP as a Unified ICME queuing platform, ensure that the VRU peripheral gateways use service control with Service Control Reporting enabled. If you are using it as a self-service platform, disable Service Control Reporting. Also, note the VRU Connection Port that is used for each VRU peripheral gateways Peripheral Interface Manager (PIM).

Note

- For information on IVR-related Service Control reporting and queue reporting, see the https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html and the https://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html.
- For Unified CVP reporting, see Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

- Ensure that the NIC cards, voice gateway, and network components have the Ethernet interfaces configured with matching speed and duplex settings.

Note

- For details about the required Ethernet Switch/Server NIC settings, see Ethernet Switch/Server NIC, Gateways and Call Server Settings, on page 4.
- For details on design considerations and guidelines for deploying enterprise network solutions that includes Unified CVP, see the *Configuration Guide for Cisco Unified Customer Voice Portal*.

Related Topics

Ethernet Switch/Server NIC, Gateways and Call Server Settings, on page 4

Route Calls Through the Network to the VRU

Most call flow models involve a step in which the call must be transferred to a VoiceXML gateway. Depending on the specific call flow model in use, one of two techniques is applied to direct that transfer. Both techniques involve one or multiple labels that Unified ICME or Unified Intelligent Contact Management Host (ICMH) provides. Configure these in the other call routing components of the solution to deliver a call to an appropriate VoiceXML gateway. Such labels are part of the overall dialed number plan of the contact center, and must be determined before you configure Unified CVP.

Table 2: Call Flows Using Network VRUs and Customer VRU

Call Flows	Task
Using Network VRUs of Type 7 or 10	Determine the Network Routing Number. This number is the base for routing calls through the network to the VRU. A correlation ID is appended to this number to transfer calls to a Network VRU through the network.
With a Customer VRU in Unified ICMH environments and for NIC Type 8 call flow models	• Determine the translation route pools to use for each VRU. • Determine the labels to be sent to the network to connect the call to the VRU and the corresponding Dialed Number Identification Service (DNIS) that is seen by the VRU. For example, the label for the network might be 18008889999 and the DNIS received by the VRU and sent back to Unified ICME to identify the call might be 9999.

Ethernet Switch/Server NIC, Gateways and Call Server Settings

Ensure to have the following Ethernet Switch/Server NIC, gateways, and Call Server settings:

Caution The **Auto** option is applicable only for matched port/NIC at Gigabit Ethernet (1000 Mbps). If you are unsure of the adjacent station configuration, select 1000/Full on the Gigabit interface. You can use the **Auto** option only if both stations supply Gigabit interfaces.

Table 3: Ethernet Switch/Server NIC, Gateways and Call Server Settings

Ethernet Switch Speed	Server/Gateway NIC Speed	Speed/Duplex Setting for Switch Port	Speed/Duplex Setting for Server/GW NIC
1000 Mb	1000 Mb	1000/Full	1000/Full
1000 Mb	1000 Mb	Auto/Auto	Auto/Auto
1000 Mb	100 Mb	100 Mb/Full	100 Mb/Full

Ethernet Switch Speed	Server/Gateway NIC Speed	Speed/Duplex Setting for Switch Port	Speed/Duplex Setting for Server/GW NIC
100 Mb	100 Mb	100 Mb/Full	100 Mb/Full
100 Mb	1000 Mb	100 Mb/Full	100 Mb/Full

Call Server and VXML Gateway in Different Subnets

Unified CVP shows one to two seconds delay in the Call Server when VXML gateway bootstraps the call. The delay is caused if the Call Server and VXML gateway are in different subnets.

To avoid the delay:

Procedure

Step 1 Open the registry of the machine.

Step 2 Navigate to the following path: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<Interface GUID.`

Step 3 Set **TcpAckFrequency** parameter to 1.

Step 4 Restart the windows machine.

Trunk Utilization and Reporting

DS0 Trunk Information

Through Unified CVP, Unified ICM passes the gateway trunk and DS0 information from the arriving SIP call.

PSTN gateway trunk and DS0 information received at ICM has the following purposes:

- Reporting
- Routing in the Unified CCE Script Editor where TrunkGroupID and TrunkGroupChannelNum information is available for routing decisions.

Following message is used in the examples:

The PSTN trunk group data comes from the PSTN Gateway in the SIP INVITE as shown:

```
Via: SIP/2.0/UDP
192.168.1.79:5060;x-route-tag="tgrp:2811-b-000";x-ds0num="ISDN 0/0/0:15
0/0/0:DS1 1:DS0";branch
```

The following logic is used in Unified CVP to parse and pass the PSTN trunk group information to Unified ICM:

- For TrunkGroupID, look for **tgrp:** in the **x-route-tag** field.

- If **tgrp:** found **TrunkGroupID=value after tgrp:**> + <**data between ISDN and :DS1 tags**>· Using the above example: **TrunkGroupID = 2811-b-000<space>0/0/0:15 0/0/0.**
- TrunkGroupID = <I**P addr of originating device in Via header**> + <**data between ISDN and:DS1 tags**>

  Using the above example: **TrunkGroupID=192.168.1.79<space>0/0/0:15 0/0/0.**

- For TrunkGroupChannelNum, look for **DS0** in **x-ds0nun** field.
  - If found, **TrunkGroupChannelNum** = <**value before the :DS0**>· Using the above example: **TrunkGroupChannelNum = 1**
  - **TrunkGroupChannelNum** = <**max int value**> to indicate we did not find the DS0 value.

    Using the above example: **TrunkGroupChannelNum = Integer.MAX_VALUE (2^31 - 1)**

Trunk Utilization Routing and Reporting

Through the Trunk Utilization feature, a gateway is used for real-time Unified CVP routing and Unified ICM reporting and scripting. A gateway pushes the status of memory, DS0, DSP, and CPU to Unified CVP. Because this feature uses a push method to send resource data to Unified CVP, resources are monitored more closely and failover can occur faster when a device goes down or is out of resources.

This feature has the following characteristics:

- Each gateway can publish an SIP OPTIONS message with CPU, Memory, DS0, and DSP information to Unified CVP every three minutes when operation conditions are usual on the gateway.
- The push interval is configurable through the Cisco IOS CLI on the gateway.
- If a high watermark level is reached, the gateway sends the SIP OPTIONS message immediately with an **Out-Of-Service = true** indication, and does not send another OPTIONS message until the low watermark level is reached with an **Out-Of-Service = false** indication.
- Up to five Resource Availability Indication (RAI) targets can be set up on the gateway.

Trunk Utilization Routing can also be used to update trunk group status in the Unified CCE router. A PSTN call (through the ICM script) can query the router with a preroute from a NIC to use the available ingress gateway for the post route to Unified CVP.

Note DS0 is the data line that provides utilization information about the number of trunks free on a gateway.

Gateway Trunk Utilization with Server Group Pinging Combination

When you combine the Server Group element polling feature with the Cisco IOS Gateway trunk utilization feature, your solution has faster failover for high availability call signaling.

Deployment Considerations

- For Proxy Server deployment with CUSP:
  - Configure TDM originating gateways for resource allocation indication-targets (RAI-targets) to provide status in OPTIONS message to primary and secondary Unified CVP Call Servers, for

reporting purposes. The data is used for reporting, and not routing so the data needs to be sent to Call Servers that have reporting enabled.

- Configure primary and secondary CUSP proxy servers with Server Groups pinging to Unified CVP, VXML Gateways, and Unified Communications Manager elements.
- Configure Unified CVP with Server Group that pings to both primary and secondary CUSP proxies for outbound calls.

- For a non-proxy deployment:
  - Configure TDM originating gateways for RAI-targets to provide status in OPTIONS message to primary and secondary Call Servers. Unified CVP can handle the messages for both reporting and routing purposes. If used for routing, then the gateway must be in a server group by itself on Unified CVP.
  - Configure Unified CVP with Server Groups that pings to Unified CVP, VXML Gateways, and Unified Communications Manager elements for outbound calls.
  - Configure VXML gateways for RAI-targets to provide status in the OPTIONS message to primary and secondary Call Servers.
- Configure the Unified CVP Call Servers to send the same hostname in the contact header of OPTIONS requests to the gateways. This process enables a single RAI-target to be configured to all Call Servers and is important because the limit is five targets. The parameter to set is called Options Header Override.

Note See the Cisco IOS documentation for guidelines on the high and low watermark settings.

Limitations:

- RAI is not supported on Proxy Servers.

  CUSP servers do not handle the RAI header of OPTIONS messages, so they do not mark the status of elements with that information. If VXML Gateways are down, Unified CVP may send the call using the proxy, because the proxy does not handle incoming RAI headers in OPTIONS. It is possible to use a local static route scheme on Unified CVP to send all calls to the proxy except the Voice XML Gateways calls to create a server group for Voice XML Gateways and take advantage of RAI updates for routing.

Apply Contact Center Gateway Debug Settings

Procedure

Step 1 Log in to the gateway.

Step 2 Type `enable` and type your password to enter the enable mode.

Step 3 Enter the configure terminal command to enter configuration mode.

Step 4 Type `ivr contact-center` to apply default debug settings.

Step 5 Configure the logging buffer size using `set logging buffer`.

Example:

```
set logging buffer 1000000
```

Note The logging buffer size should be 1000000 or more.

Step 6 Exit configuration mode and return to the enable prompt by pressing **Ctrl-Z**.

Note To view the current operating configuration, including the changes you made, enter the `show running-config` command.

Step 7 To save the configuration changes, enter the `write` running-config startup-config command at the enable prompt.

Example:

```
User Access Verification
Password:
ccbu-doc-gw4>en
Password:
ccbu-doc-gw4#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ccbu-doc-gw4(config)#ivr
ccbu-doc-gw4(config)#ivr contact-center
ccbu-doc-gw4(config)#^Z
ccbu-doc-gw4#show debug
....
```

Network VRU Types

In Unified ICME, Network VRU is a configuration database entity. It is accessed using the Network VRU Explorer tool of ICM Configuration Manager. A Network VRU entry contains the following information:

- **Type:** A number from 7, 8, and 10, which corresponds to one of the types.
- **Labels:** This is a list of labels, which Unified ICME can use to transfer a call to the particular Network VRU that is being configured. These labels are relevant for Network VRUs of Types 7 and 10. These types use the Correlation ID mechanism to transfer calls. Labels for Type 8 are defined in the Translation Route Explorer tool of ICM Configuration Manager, and are invoked using a Translation Route to VRU node.

  Each label comprises the following components:

  - A digit string, which becomes a DNIS that is understood by a SIP Proxy Server, by a static route table, or by gateway dial-peers.
  - A routing client, also known as a switch leg peripheral. Each peripheral device that can act as a switch leg must have its own label, even if the digit strings are the same in all cases.

Unified ICME introduced Network VRU Type 10, which simplifies the configuration of Network VRU's for Unified CVP. For most call flow models, a single Type 10 Network VRU can take the place of the Type 3, 5, 7, or 8 Network VRUs, which were associated with the Customer Instance and the Switch and VRU leg peripherals. The VRU-Only call flow models still require Type 8. However, in a specific case Type 7 is required.

Network VRU configuration entries themselves have no value until they are associated with active calls. Following are the three places in Unified ICME where you can perform this association:

- Advanced tab for a given peripheral in the PG Explorer tool of the ICM Configuration Manager.
- Customer Instance configuration in the ICM Instance Explorer tool of the ICM Configuration Manager.
- On every VRU Script configuration in the Network VRU Script List tool of the ICM Configuration Manager.

Depending on the call flow model, use Unified ICME to search either the peripheral or the customer instance to determine how to transfer a call to a VRU. Unified ICME examines the following:

- The Network VRU and the Network VRU using the Translation Route mechanism. The network VRU is associated with the switch leg peripheral when the call first arrives on a switch leg and Network VRU is associated with the VRU leg peripheral when the call is being transferred.
- The Network VRU from the System Information tool, when the call is being transferred to the VRU using the Correlation ID mechanism. The Network VRU is associated with the Customer Instance or the default Network VRU.
- The Network VRU, which is associated with the VRU Script every time it encounters a RunExternalScript node in its routing script. If the call is currently not connected to the designated Network VRU, Unified ICME does not rune the VRU Script.

Note The previously supported VRU types still work with Unified ICME 7.1(1) and later for existing deployments. However, new installations should use Type 10 and existing deployments should switch to Type 10 on upgrade.

SIP Dialed Number Pattern Matching Algorithm

Refer to the following points to create dialed number patterns:

- Wildcarded DN patterns can contain “.” and “X” in any position to match a single wildcard character.

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

- Any of the wildcard characters in the set “>*!T” can match multiple characters. However, only one wildcard character can be used for trailing values, else they can always match with remaining characters in the string.
- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. When the number of characters is matched equally by more than one wildcarded pattern, precedence is given from top to bottom of the configured DN list.
- There is no explicit software limit on the number of items in the DN pattern list.

Additional Configuration Instructions

- Comprehensive call flows for prerouted calls. See Comprehensive Call Flows for Pre-Routed Calls, on page 34. This class of call flows is similar to the Unified CVP Comprehensive call flow models, except

that calls are first introduced into Unified ICME or Unified ICMH using a path other than through Unified CVP. A Unified ICME routing script is given the chance to preroute such calls before reaching Unified CVP. After the script transfers the call to Unified CVP for either self-service or queuing, the standard Unified CVP Comprehensive call flow model is used.

- Common Unified ICMH Configuration for Unified CVP Switch Leg. See Configure Common Unified ICMH for Unified CVP Switch Leg, on page 178. It describes Unified ICMH configuration instructions common to Comprehensive Unified ICMH and VRU-Only with NIC routing, with Correlation ID call routing call flow models for Unified CVP switch legs.
- Common Unified ICMH Configuration: Define Unified CVP ECC Variables, on page 181. It provides instructions on how to set up ECC variables that Unified CVP uses to exchange information with Unified ICMH.
- Using the Metadata ECC Variable. See Metadata ECC Variable, on page 188. It defines the values for the *user.microapp.metadata* ECC variable.
- Common Configuration for Differentiating VRUs (Unified CVPs) Based on Dialed Number. See Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189. It provides instructions on how to configure Unified ICME to differentiate the VRUs.
- SIP Proxy Redundancy. See Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209 and Set Up Call Server with Redundant Proxy Servers, on page 209.

Related Topics

Comprehensive Call Flows for Pre-Routed Calls, on page 34
Configure Common Unified ICMH for Unified CVP Switch Leg, on page 178
Define Unified CVP ECC Variables, on page 181
Metadata ECC Variable, on page 188
Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189
Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209

Order of Device Operations

Based on your call flow model, set up the device operations in the following order.

Table 4: Order of Devices

Device Operations	Settings
Device Deployment	• SIP Proxy Server device (optional) • Unified CVP Call Server device • Unified CVP VXML Server device • Unified CVP Reporting Server device • Other Devices (for example, Gateways and Unified CM)

Device Operations	Settings
System Configuration	• SIP Server Groups • Dialed Number Pattern • Locations • Courtesy Callback
Miscellaneous	• Register with Smart Licensing (required) • Transfer of VXML applications (required) • Bulk transfer of default Gateway files (required)

Manage Devices

Procedure

Step 1 Add new Unified CVP device.

Step 2 Configure Unified CVP device.

Step 3 Save and deploy Unified CVP device.

Step 4 Verify that Unified CVP devices are active in Operations Console.

Step 5 Deploy system-level configuration, Dialed Number Pattern, SIP Server Groups, Locations, and Courtesy Callback, and verify their statuses.

Step 6 Save and deploy the SNMP Configuration.

Smart Licensing Configurations

Unified CVP Release12.5 uses the following configuration files for Smart Licensing operations.

- C:\Cisco\CVP\conf\smartlicense.properties
- C:\Cisco\CVP\conf\licensetype.properties
- C:\Cisco\CVP\conf\Entitlementmapper.csv

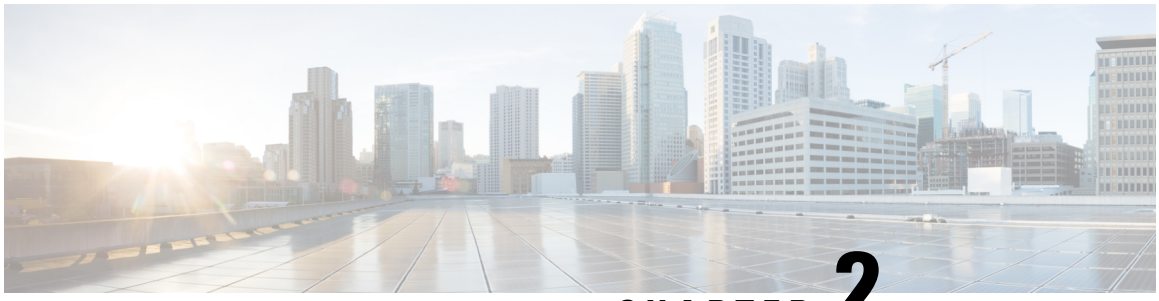
Note Do not edit, delete, or access these files without contacting Cisco TAC. Any change to these files can cause operational impact.

Handling SocketTimeoutException:

If there is a delay in communication between the OMAP and CVP servers, and the **SocketTimeoutException** error is seen in the Catalina log, perform the following steps:

1. In the OAMP server, navigate to the following location:
   `%CVP_HOME%\OPSConsoleServer\Tomcat\webapps\ROOT\WEB-INF\classes`
2. Open the file shindig.properties and edit as follows:
   a. Change `shindig.http.client.connection-timeout-ms=5000` to `shindig.http.client.connection-timeout-ms=10000`.
   b. Add the read-timeout configuration after the connection-timeout configuration:

      ```
      shindig.http.client.read-timeout-ms=100000
      ```
3. Save the shindig.properties file.
4. Restart the CVP OPS Console service and login to OAMP again.



CHAPTER 2

Unified CVP Call Flow Models

Common Tasks for Unified CVP Call Flow Models

Call Services for Call Flow Models

Based on your call flow model, select the required call services in the Call Server Configuration window:

Table 5: Call Services for Call Flow Models

Call Flow Model	Required Call Services
Comprehensive Call Flow Model, on page 21	ICM, IVR, SIP
VRU-Only Call Flow Model with NIC Routing, on page 53	ICM, IVR
Call Director Call Flow Model, on page 41	ICM, IVR
Standalone Call Flow Model, on page 14	No Service

Related Topics

Comprehensive Call Flow Model, on page 21
VRU-Only Call Flow Model with NIC Routing, on page 53
Call Director Call Flow Model, on page 41
Standalone Call Flow Model, on page 14

Standalone Call Flow Model

In this call flow model, the VXML Server is a J2EE-compliant server that provides a complete solution for rapidly creating and deploying dynamic VoiceXML applications. You can install the VXML Server as a standalone component without the Unified CVP Call Server component and with or without the Reporting.

The following table lists the required and optional Unified CVP components needed for the Standalone call flow model:

Table 6: Required and Optional Unified CVP Components for Standalone Call Flow Model

CVP components	Related topics
Required CVP components	
VXML Server	• VXML Server Configuration, on page 105
Ingress Gateway	• Gateway Configuration, on page 249 • Example: Gateway Settings for Standalone Call Flow Model, on page 252 • Call Survivability, on page 442 **Note** Not recommended for Cisco VVB implementation.
VoiceXML Gateway	• Gateway Configuration, on page 249 • Example: Gateway Settings for Standalone Call Flow Model, on page 252 • Call Survivability, on page 442
Cisco VVB	• Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285 • Example: Dial-Peer for Standalone Call Flow Model with Cisco VVB, on page 254
Operations Console	Operations Console, on page 67
Call Server	• Call Server Configuration, on page 77 • REFER Transfers, on page 33
Media Servers	Media Server Configuration, on page 217
Optional CVP components	
Reporting Server	Reporting Server Configuration, on page 163
Speech Servers	Speech Server Configuration, on page 245

CVP components	Related topics
Unified ICM Enterprise	Unified ICM Configuration, on page 171

The Unified CVP VXML Server (Standalone) call flow model is available in the following variations:

- Standalone without reporting: Use the **VXML Server (Standalone)** option in the Operations Console. This call flow model *does not* require a Call Server and a Reporting Server.
- Standalone with reporting: Use the **VXML Server** option in the Operations Console. This call flow model *requires* a Call Server and a Reporting Server.
- Standalone, but adding reporting *after* the VXML Server (Standalone) version has already been configured: Configure the Unified CVP Call Server, delete the VXML Server (Standalone), and use the **VXML Server** option in the Operations Console to add the VXML Server.

See VXML Server Configuration, on page 105 for configuration instructions.

In this call flow model with reporting, the Unified CVP Call Server is used to route messages between the components. Calls arrive through a VoiceXML gateway and interact directly with a VXML Server to run VoiceXML applications. The gateway performs both ingress and VoiceXML functions. This call flow model provides a sophisticated VoiceXML-based VRU, for applications which, in many cases, do not need to interact with a Unified ICME Server.

In the Unified CVP VXML Server (standalone) call flow model, *only* the VXML Server, Call Studio, and a Gateway are required, except when using reporting which requires a Call Server and a Reporting Server.

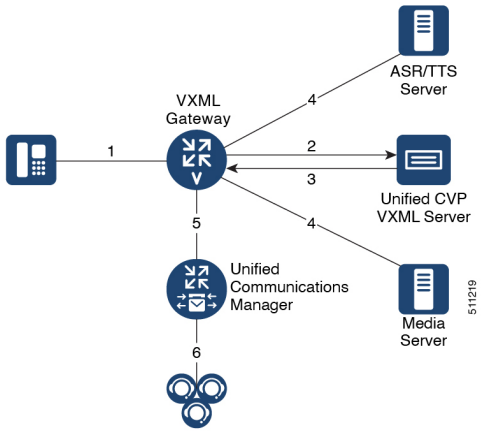
This standalone model has functions similar to the VRU-Only Call Flow Model with NIC Routing, on page 53.

Note The CVP VXML standalone call flow model allows only one synchronous blind or bridged transfer. A synchronous blind transfer indicates that once the call has been transferred, a Unified CVP Standalone script has no ability to asynchronously take it back and deliver it somewhere else, whereas Unified ICME scripts, in the Unified ICME-integrated models, do have that ability.

Call Flow for the Unified CVP VXML Server (Standalone) Call Flow Model using VXML Gateway

The following figure displays the call flow for the Unified CVP VXML Server (standalone) call flow model using VXML Gateway.

Figure 1: Call Flow for the Unified CVP VXML Server (Standalone) Call Flow Model using VXML Gateway



The following, numbered, call flow description for the previous figure assumes:

- You installed and licensed the VXML Server.
- You created a Call Studio application and deployed it on the VXML Server.

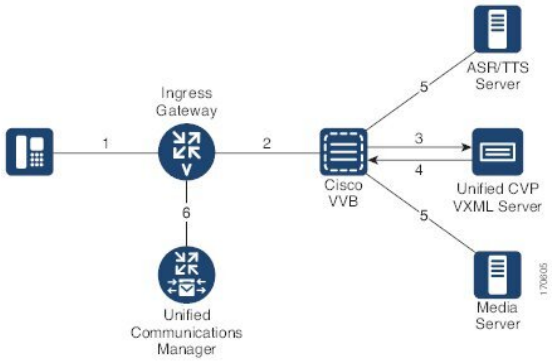
The call flow shown in the previous figure is as follows:

1. The call arrives from the PSTN network to the Gateway.
2. The Gateway sends an HTTP URL request to the VXML Server.
3. The VXML Server returns the VoiceXML instructions to be run on the VXML Gateway.
4. The VoiceXML instructions returned to the Gateway can include references to ASR/TTS to recognize voice input and play TTS files, and references to Media Servers to play .wav files.
5. The gateway can, optionally, transfer the call to any destination that it can deliver a call to, such as Unified CM.
6. Unified CM can then send the call to an agent.

Call Flow for the Unified CVP VXML Server (Standalone) Call Flow Model using Cisco VVB

The following figure displays the call flow for the Unified CVP VXML Server (standalone) call flow model using Cisco VVB.

Figure 2: Call Flow for the Unified CVP VXML Server (Standalone) Call Flow Model using Cisco VVB



1. The call arrives from the PSTN network or the service provider to the Ingress Gateway or Cisco Unified Border Element (CUBE).
2. The Gateway sends an SIP invite to Cisco VVB with the trigger number configured in Cisco VVB for the Self Service application.
3. Cisco VVB sends an HTTP URL request to the VXML Server.
4. The VXML Server returns the VoiceXML instructions to be run on Cisco VVB.
5. The VoiceXML instructions returned to Cisco VVB can include references to ASR/TTS to recognize voice inputs and play TTS files, and references to the media servers to play .wav files.
6. The Gateway can, optionally, transfer the call to any destination that it can deliver a call to, such as the Unified CM.
7. The Unified CM can then send the call to an agent.

Related Topics

VXML Server Configuration, on page 105
Gateway Configuration, on page 249
Configure Gateway Settings for Standalone Call Flow Model, on page 251
Call Survivability, on page 442
Cisco VVB Configuration
Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285
Operations Console, on page 67
Call Server Configuration, on page 77
REFER Transfers, on page 33
Media Server Configuration, on page 217
Reporting Server Configuration, on page 163
Speech Server Configuration, on page 245
Unified ICM Configuration, on page 171
Configure VXML Server (Standalone), on page 105
VRU-Only Call Flow Model with NIC Routing, on page 53

Configure VXML Server Standalone Call Flow Model

The following steps apply to all variations of standalone call flow model:

Procedure

Step 1 Configure the gateway for VXML Server (Standalone) applications:

a) Define the VXML Server applications on the gateway for a VXML Gateway deployment.

Note Backup server is optional. For the Tomcat Application Server, set the port to **7000**. The backup server cannot be the same server as the Primary Server.

b) Configure the base gateway and Cisco VVB settings.

For gateway settings, see the Example: Gateway Settings for Standalone Call Flow Model, on page 252.

For Cisco VVB settings, see the Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285.

c) Configure the service settings on the gateway for a VXML Gateway deployment.

See the Example: Gateway Settings for Standalone Call Flow Model, on page 252.

d) Configure a dial-peer, which will call the service to reach the Unified CVP VXML Server for a VXML Gateway deployment.

See the Example: Dial-Peer for Standalone Call Flow Model with VXML Gateway, on page 254.

e) Configure a dial-peer, which will trigger the self-service application on Cisco VVB and reach the Unified CVP VXML Server.

See the Example: Dial-Peer for Standalone Call Flow Model with Cisco VVB, on page 254.

f) (Optional) Create additional dial-peers for any outgoing transfer destinations your application uses.

Review the updated gateway configuration by issuing the **show run** command to examine the running configuration.

Step 2 Create an application using Call Studio and deploy it as a zip file.

For information about Unified Call Studio, see the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

Related Topics

Example: Gateway Settings for Standalone Call Flow Model, on page 252
Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285
Example: Dial-Peer for Standalone Call Flow Model with VXML Gateway, on page 254

Enable Reporting for Standalone Call Flow Model

Procedure

Step 1 Follow steps 1 and 2 from Configure VXML Server Standalone Call Flow Model, on page 18.

Step 2 Enable loggers on the Call Studio.

See the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio for details on configuring loggers using Call Studio.

Step 3 Configure the Call Server.

For more information on configuring a Call Server, see Configure Call Server, on page 77

Step 4 Configure the VXML Server.

a) In the Operations Console, select **Device Management** > **VXML Server** and add a VXML Server with an associated Primary Call Server.
b) To enable reporting for this VXML Server, in the Operations Console, select the **Configuration** tab and select **Enable Reporting for this VXML Server**.
c) Add appropriate filtering.

For more information on configuring a VXML Server, see the Configure VXML Server section.

Step 5 Click **Save and Deploy**.

Step 6 Deploy the Call Studio application on the VXML Server.

Note By default, CVPSNMPLogger is enabled when a new Call Studio application is created and deployed to the VXML Server.

Step 7 Configure the Reporting Server.

a) In the Operations Console, select **Device Management** > **CVP Reporting Server** > **General tab** and configure the Reporting Server.
b) Select a Call Server to associate with this Reporting Server.
c) Check the default values of the Reporting properties and change, if desired.

For more information, see the Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Step 8 Click **Save and Deploy**.

Related Topics

Configure VXML Server Standalone Call Flow Model, on page 18
Configure Call Server, on page 77

Enable ICM Lookup for Standalone Call Flow Model

Procedure

Step 1 Follow steps 1 and 2 from Configure VXML Server Standalone Call Flow Model, on page 18.

Step 2 Use the ReqICMLabel element in the Call Studio script as a decision element.

The ReqICMLabel element has two exit states: error and done. The *done* path must connect to a transfer element to transfer the caller to ReqICMLabel as referenced by the ReqICMLabel Element.

For information about Unified Call Studio, see the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

Step 3 Enable loggers on the Call Studio.

See the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio for details on configuring loggers using Call Studio.

Step 4 Configure the Call Server and enable the ICM Service.

For more information on configuring a Call Server, see the Configure Call Server, on page 77.

Step 5 Configure the VXML Server.

For more information on configuring a VXML Server, see the Configure VXML Server section.

Step 6 Deploy the Call Studio application on the VXML Server.

Note By default, CVPSNMPLogger is enabled when a new Call Studio application is created and deployed to the VXML Server.

Step 7 Using the ICM Script Editor, create a Unified ICME script that returns a label.

In order to transfer information from Unified ICME to the VXML Server besides the label, use the ToExtVXML0 - 4 ECC Variables and Peripheral Variables 1 - 10. The format for using the ToExtVXML 0 - 4 is with name value pairs that are delimited by semi-colons.

Example:

```
ToExtVXML0 = "company=Cisco Systems;state=MA".
```

Use the Peripheral Variables 1 - 10 to pass information to the VXML Server. The values in the variables are taken as is.

For more information about creating a Unified ICME script that returns a label in, see the Unified ICME documentation.

For more information about using the ReqICMLabel element, see the Pass Data to Unified ICME, on page 201.

Related Topics

Configure VXML Server Standalone Call Flow Model, on page 18
Configure Call Server, on page 77
Pass Data to Unified ICME, on page 201

Call Director Call Flow Model for Unified ICME, on page 42
Call Director Call Flow Model for Unified ICMH, on page 44

Comprehensive Call Flow Model

The Comprehensive call flow model is deployed where the Unified CVP acts as a switch or is deployed at the Network Application Manager (NAM) to act as a switch. The call flow models to deploy these scenarios are listed in the Comprehensive Call Flow Model for ICME, on page 21 and Comprehensive Call Flow Model for ICMH, on page 23 sections. In these call flow models, a call can have two legs one with the Ingress Gateway and other with the Cisco VVB:

- **Switch leg:** For the Switch leg, the Gateway provides Gateway capabilities from TDM to VoIP and call-switching capabilities
- **VRU leg:** For the VRU leg, the VXML Gateway provides VRU voice treatment.

Note Unified ICMH sees these as a single call routed through different peripherals for different purposes.

The SIP calls using the Unified CVP micro-applications use the IVR Service of Call Server that has the switch leg of the call. VoiceXML fetches are sent to the Call Server. The VoiceXML traffic for micro-applications must return only to the same Call Server as the switch leg.

Sending VoiceXML traffic to multiple application servers is implemented in Unified CVP 4.0(1) onwards by extracting the IP address of Call Server from the SIP signaling messages in the bootstrap service rather than using static configuration in the service parameter for the bootstrap servicesound of VoiceXML Gateway.

The Comprehensive call flow model extracts the Call Server host from the SIP signaling. The Unified CVP SIP Service is handling the switch legs of the call. If you make a SIP call that does not involve the switch leg with Unified CVP, the service parameters below applies for the VRU leg only. Comprehensive calls always use the same Call Server for both switch leg and VRU legs. Using the same Call Server simplifies the solution and makes it easier to troubleshoot and debug.

Note The **app-info header** parameter is for SIP calls only. If this parameter is blank, the primary Call Server IP address configured on the service, is used. In case the Call Server is non-functional, this parameter tries to access the backup Call Server.

Related Topics

Comprehensive Call Flow Model for ICME, on page 21
Comprehensive Call Flow Model for ICMH, on page 23

Comprehensive Call Flow Model for ICME

The Comprehensive call flow model for ICME combines the Call Director using SIP and the VRU-Only call flow model 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 the following port licensing levels:

- **Basic:** Supports the .wav files and input using dual tone multi-frequency (DTMF) signaling.
- **Advanced:** Supports ASR/ TTS Servers, and VXML Server applications.
- Unified CVP acts as the switch, transferring the call to the Network VRU and to agents. The Unified CVP IVR service in the Operations Console is configured to work with the VoiceXML Gateway to provide VRU treatment, which may include ASR/TTS Servers.
- Both the Voice Gateway and the Call Server have two legs for the same call: the Switch leg and the VRU leg. For the Switch leg, the Gateway provides Gateway capabilities from TDM to VoIP, and call-switching capabilities whereas for the VRU leg, the Gateway provides VRU voice treatment.
- A Network VRU: Type 10, serves both the Switch and VRU legs.
- Use the SendToVRU node of the ICM Script Editor to connect the call to the Network VRU.

The following figures show the call flow for Comprehensive call flow model for ICME using SIP without and with a Proxy Server. The solid lines in these figures indicate voice paths and dashed lines indicate signaling paths.

Figure 3: Comprehensive Call Flow Model for ICME Using SIP Without a Proxy Server

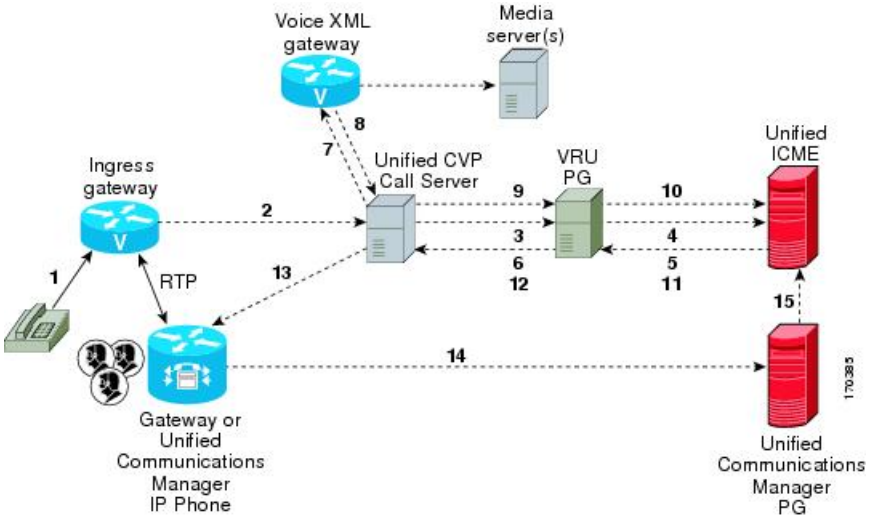
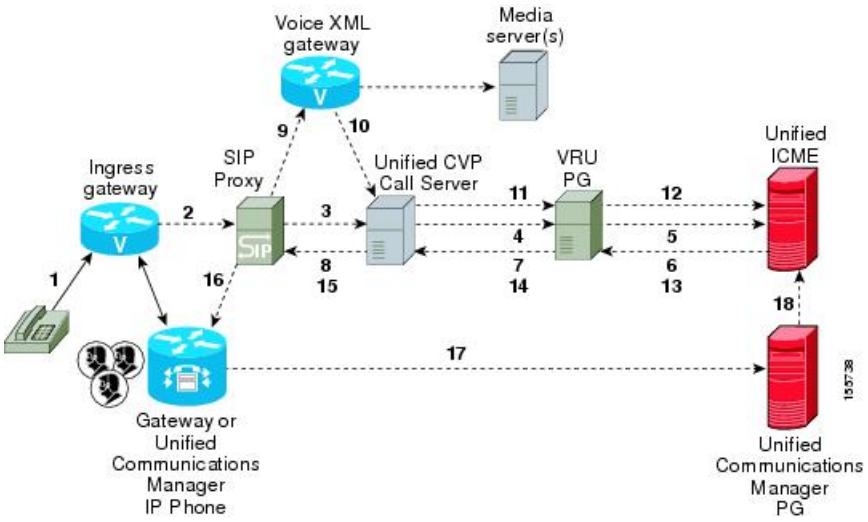


Figure 4: Comprehensive Call Flow Model for ICME Using SIP With a Proxy Server



Note

- The figures show two Gateways: the one where a call arrives and the other for the VRU leg. However, one physical Gateway can be used for both the purposes.
- For simplicity, the figures do not illustrate redundancy and failover.
- For more information, see REFER Transfers, on page 33 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65.

Related Topics

REFER Transfers, on page 33
Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65

Comprehensive Call Flow Model for ICMH

In the Comprehensive call flow model for ICMH, Unified CVP is deployed at the NAM where it acts as the switch, transferring the call to the Network VRU and to agents. The Network VRU uses the Correlation ID transfer mechanism. On the Operations Console, the IVR Service is configured to work with the VoiceXML Gateway to provide VRU treatment, and can include the ASR/TTS Servers.

In this call flow model:

- There are two the Network VRUs: one on the NAM for the Switch leg and the VRU leg (Type 10) and the other for the CICM for the INCRP connection.
- The Network VRU names (where applicable) and the ECC variable configurations must be identical on the NAM and CICM. All labels must also be duplicated but their routing clients will be different.
- Use the SendToVRU node of the ICM Script Editor to connect the call to the Network VRU.

Note

- This call flow model does not support calls that originate in IP address.
- For instructions on how to implement IP-originated calls in a way which is supplemental to the Unified CVP Comprehensive Call Flow Model for ICME and ICMH, see the Calls Originated by Unified CM, on page 37 section. This implementation requires an additional Unified CVP Call Server to be connected to the CICM.

The following figures show the call flow for Comprehensive call flow model for ICMH using SIP without and with a Proxy Server. The solid lines in these figures indicate voice paths and dashed lines indicate signaling paths. The numbers in the figure indicate call flow progression.

Figure 5: Comprehensive Call Flow Model for ICMH Using SIP Without a Proxy Server

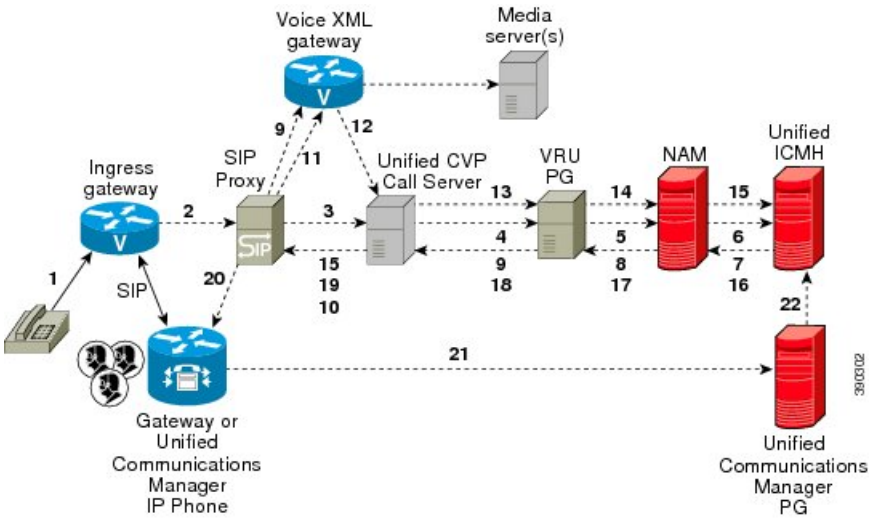
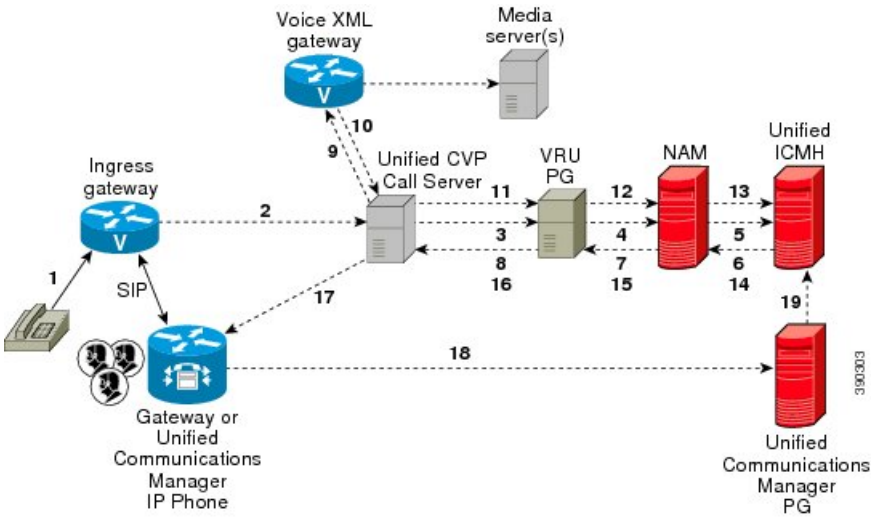


Figure 6: Comprehensive Call Flow Model for ICMH Using SIP With a Proxy Server



Note

- The figures show two Gateways: the one where a call arrives and the other for the VRU leg. However, one physical Gateway can be used for both the purposes. Similarly, the IVR Service configured through the Operations Console and the peripheral gateway can be on the same server.
- For simplicity, the figures do not illustrate redundancy and failover.
- For more information, see REFER Transfers, on page 33 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65.

Table 7: Required and Optional CVP Components for Comprehensive Call Flow Model

CVP components	Related topics
Required CVP components	
Operations Console	Operations Console
Ingress Gateway	• Gateway Configuration • Configure Gateway Settings for Comprehensive Call Flow Model • Call Survivability
VoiceXML Gateway	• Gateway Configuration • Configure Gateway Settings for Comprehensive Call Flow Model • Call Survivability
Unified ICME	• Unified ICM Configuration • Comprehensive Call Flow Model for ICME • Comprehensive Call Flows for Pre-Routed Calls • Calls Arriving at ICME through a Pre-Route-Only NIC • Calls Originated by Unified CM • Calls Originated by an ACD or Call Routing Interface • Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH • Define Unified CVP ECC Variables

CVP components	Related topics
Unified ICMH	• Unified ICM Configuration • Comprehensive Call Flow Model for ICMH • Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH • Configure Common Unified ICMH for Unified CVP Switch Leg • Define Unified CVP ECC Variables
Call Server	• Call Server Configuration • REFER Transfers
Optional CVP components	
Speech Servers	Speech Server Configuration
SIP Proxy Server	SIP Proxy Server Configuration
Media Servers	Media Server Configuration
DNS Servers	DNS Zone File Configuration for Comprehensive Call Flow Model
Reporting Server	Reporting Server Configuration

Related Topics

Calls Originated by Unified CM, on page 37
REFER Transfers, on page 33
Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65

Set Up Comprehensive Call Flow Model Using SIP for ICME and ICMH

Procedure

Step 1 Perform Steps 1 to 5 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 2 (Optional) Configure a dial-peer for ringtone and error.

Step 3 If you are using a Proxy Server, configure your session target in the outbound Dial-peer to point to the Proxy Server.

Step 4 If you are using the sip-server global configuration, configure the sip-server in the sip-ua section to be your Proxy Server and point the session target of the dial-peer to the sip-server global variable.

Note

a. Make sure your Dial plan includes this information. See the Dial plan when you configure the SIP Proxy Server for Unified CVP.

b. The SIP Service voip dial-peer and the destination pattern on the Ingress Gateway must match the DNIS in static routes on the SIP Proxy Server or Unified CVP Call Server.

See the SIP Devices Configuration, on page 209 and SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

Step 5 Perform Steps 6 to 10 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 6 Configure the ICM VRU Label. See *Example of Dial-peer for ICM VRU Label for Type 8 Call Flow Model* of the Configure ICM Settings for VRU-Only Call Flow Model: Type 8, on page 192 section.

Step 7 (Optional) Enable security for media fetches.

Note
- The VXML that the IVR Service returns as a response to an HTTP/HTTPS request from the VXML gateway contains URLs to media servers, so that the gateway knows where to fetch the media files from.
- To enable HTTPS communication between CVP and VVB or IOS, use the ICM Script Set Variables to specify the protocol/port in the call.user.microapp_server. An example of a URL that explicitly specifies an HTTP scheme is `http://<servername>:80`. One that specifies an HTTPS scheme is `https://<servername>:443`. An example of a URL that does **not** specify the scheme is <*servername*>.

  In the Operations Console, the user-visible text for this property is "Use Security for Media Fetches." Do not restart the Call Server for this property to take effect.

Click the **Use Security for Media Fetches** check box on the IVR Service tab.

See the *Operations Console online help* for detailed information about the IVR Service.

Step 8 Perform Steps 11 to 13 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 9 Configure the speech servers to work with Unified CVP.

Caution The Operations Console can only manage speech servers installed on *Windows*, not on Linux. If the speech server is installed on Linux, the server cannot be managed.

To ensure that the speech servers work with Unified CVP, make the following changes on each speech server as part of configuring the Unified CVP solution.

Step 10 Configure the characteristics for the VRU leg.

Characteristics for VRU legs require ASR and TTS treatment. On IOS VXML Gateway, if you have other requirements for DTMF relay, codecs or VAD settings, you must modify the commands accordingly.

Step 11 Perform Steps 14 and 15 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 12 Define Network VRUs.

a) On Unified ICME or the NAM, ICM Configuration Manager, select **Network VRU Explorer** tool, define a Network VRU for the VRU leg and labels for each Unified CVP Call Server.

b) On the *CICM only*, ICM Configuration Manager, select **Network VRU Explorer tool**, define a Network VRU for the VRU leg and labels for reaching the NAM.

For each of the two previous substeps, specify the following:

- Type: **10**
- Name: <*Network VRU Name*>

For example: **cvp**

- Define a label for each Unified CVP Call Server that is handling the Switch leg:
  - Label: *<Network Routing Number>*
  - Type: **Normal**
  - Routing client for Unified ICME or the NAM: Select the routing client configured for that Unified CVP Call Server peripheral from the drop-down list.
  - Routing client for *CICM only* : Select the INCRP routing client from the drop-down list.

Note The Network VRU label in the NAM and CICM must be identical. The Network VRU Names on the NAM and CICM should also be identical to avoid confusion.

Step 13 Define network VRUs and PGs for the switch leg in the ICM Configuration Manager.

On Unified ICMH, on the NAM and CICMs, Network VRU Explorer tool, define one label per Unified CVP Call Server or NIC routing client.

Note Use the same Type 10 Network VRU that you defined in the previous steps for the VRU leg.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 14 Set the client type for the INCRP NIC.

On the **CICM**, ICM Configuration Manager, NIC Explorer tool, set the client type for the INCRP NIC.

- Client Type: **VRU**

Step 15 Define a VRU that uses INCRP.

On the **CICM**, ICM Configuration Manager, Network VRU Explorer tool:

a) Define a Network VRU with a label that uses INCRP as its routing client.

Specify the following:

- Type: **10**
- Name: *<name of Unified CVP VRU>*

  For example: **cvpVRU**

b) Define one label for the NAM routing client.

Specify the following:

- Type: **Normal**
- Label: *<Network Routing Number>*
- Routing client: **INCRP NIC**

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition .

Step 16 Perform Step 16 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 17 Define a default network VRU on Unified ICME or the NAM, in the ICM Configuration Manager, the **System Information** tool:

a) For Unified ICME or on the **CICM only**, define a default Network VRU.

- Define the Default Network VRU: <*Network VRU Name*>

  For example: **cvpVRU**

b) If there are Routing Scripts on the **NAM**, define a default Network VRU.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 18 Configure dialed numbers, call types, and customers on the Unified ICME or Unified ICMH Server in the ICM Configuration Manager:

a) **Dialed Number List Tool** tab: Configure the dialed numbers.
b) **Call Type List tool** tab: Configure the call types.
c) **ICM Instance Explorer tool** tab: Configure the applicable customers.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 19 Configure ECC variables.

On Unified ICME, ICM Configuration Manager, configure ECC variables.

For more information, see Define Unified CVP ECC Variables, on page 181.

Step 20 Create a routing script that handles the incoming calls.

On the Unified ICME or Unified ICMH Server in the ICM Script Editor tool, use the SendToVRU node to connect the call to the Network VRU.

See Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for more information.

Step 21 (Optional) Configure the **SIP Proxy**.

If using a SIP Proxy Server, configure it in the Unified CVP Operations Console.

Select: **Device Management** > **SIP Proxy Server**

Step 22 Install and configure the **Call Server(s)**.

In the Operations Console:

a) Enable the ICM, IVR, and SIP Services on the Call Server.

- In the Operations Console select **Device Management** > **Unified CVP Call Server**.
- Select the**ICM** and **SIP** check boxes.

b) Configure the IVR service.

- In the Operations Console select **Device Management** > **Unified CVP Call Server** > **IVR tab** and configure the and configure the **IVR service**.

  Check the default values and change, if desired. Refer to the Operations Console online help for information about other settings you might want to adjust from their default values.

c) In the Operations Console select **Device Management** > **Unified CVP Call Server** > **SIP**. Configure the SIP Service:

- If you are using a SIP Proxy Server, enable the Outbound Proxy and select the SIP Proxy Server.

  Select the **SIP tab** and configure the following:

  - Enable Outbound Proxy: **Yes**
  - Outbound Proxy Host: Select from drop-down list.
  - Configure Local Static Routes on the SIP Proxy Server itself.

- If you are not using a SIP Proxy Server, configure Local Static Routes using the Dialed Number Pattern system configuration on the Operations Console. A Local Static Route must be configured for each SIP gateway/ACD, SIP endpoint in order to receive calls.

  Local Static Routes, Dialed Number (DN): Specify the dialed number pattern for the destination.

  Valid number patterns include the following characters:

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

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

  - Use the greater than (**>**), asterisk (*****), or exclamation (**!**) characters as a wildcard for 0 or more digits at the end of the DN.
  - Do not use the **T** character for wildcard matching.
  - Dialed numbers must not be longer than 24 characters.
  - See Valid Format for Dialed Numbers, on page 93 for format and precedence information.

  Example: **9>** (Errors are 9292 and ringtone is 9191)

  See SIP Dialed Number Pattern Matching Algorithm, on page 9 for more information.

  The following examples show the incorrect and correct static route configurations. The incorrect static route configuration does not show the least explicit routes at the end. Also, load balancing and failover of calls require DNS SRV domain names, not multiple routes with the same DN Pattern, but a single route to an SRV domain name.

  Example: Incorrect static route configuration

```
1>,10.2.6.1
2>,10.2.6.2
3>,10.2.6.20
2229191>,10.2.6.241
2229292>,10.2.6.241
2229191>,10.2.6.242
2229292>,10.2.6.242
2>,ccm-subscribers.cisco.com
3>,ccm-subscribers.cisco.com
```

  Example: Correct static route configuration

```
22291>,cvp-ringtone.cisco.com
22292>,cvp-error.cisco.com
1>,ccm-subscribers.cisco.com
2>,ccm-subscribers.cisco.com
3>,ccm-subscribers.cisco.com
```

Note "91919191>" pattern does not match an exact DN of "91919191."

- Check the default values for the SIP Service and change, if desired.

d) Configure the ICM Service by setting the maximum length DNIS to the length of the Network Routing Number.

Select **Device Management** > **CVP Call Server** > **ICM tab**: Maximum Length of DNIS: length of the Network Routing Number.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is **10**.

Step 23 Configure Local Static Routes:

If an outbound proxy is enabled on the Operations Console, configure local static routes on the SIP Proxy Server.

If no outbound proxy is enabled, configure local static routes using the Operations Console Dialed Number Pattern system configuration. Refer to SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

The following example shows a local static route configuration. A local static route contains a dialed number pattern and a routing address (IP Address, Hostname, or SIP Server Group name):

- 22291>,cvp-ringtone.cisco.com
- 22292>,cvp-error.cisco.com
- 1>,ccm-subscribers.cisco.com
- 2>,ccm-subscribers.cisco.com
- 3>,ccm-subscribers.cisco.com

Step 24 Configure custom ringtone patterns. See Add and Deploy Dialed Number Pattern, on page 340.

Step 25 (Optional) Configure the Reporting Server and associate it with a Call Server.

On the Operations Console, select **Device Management** > **CVP Reporting Server** > **General** and complete the following steps:

a) Configure the Reporting Server.
b) Select a Call Server to associate with this Reporting Server.
c) Check the default values of the Reporting properties and change, if desired.

For more information, see the Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

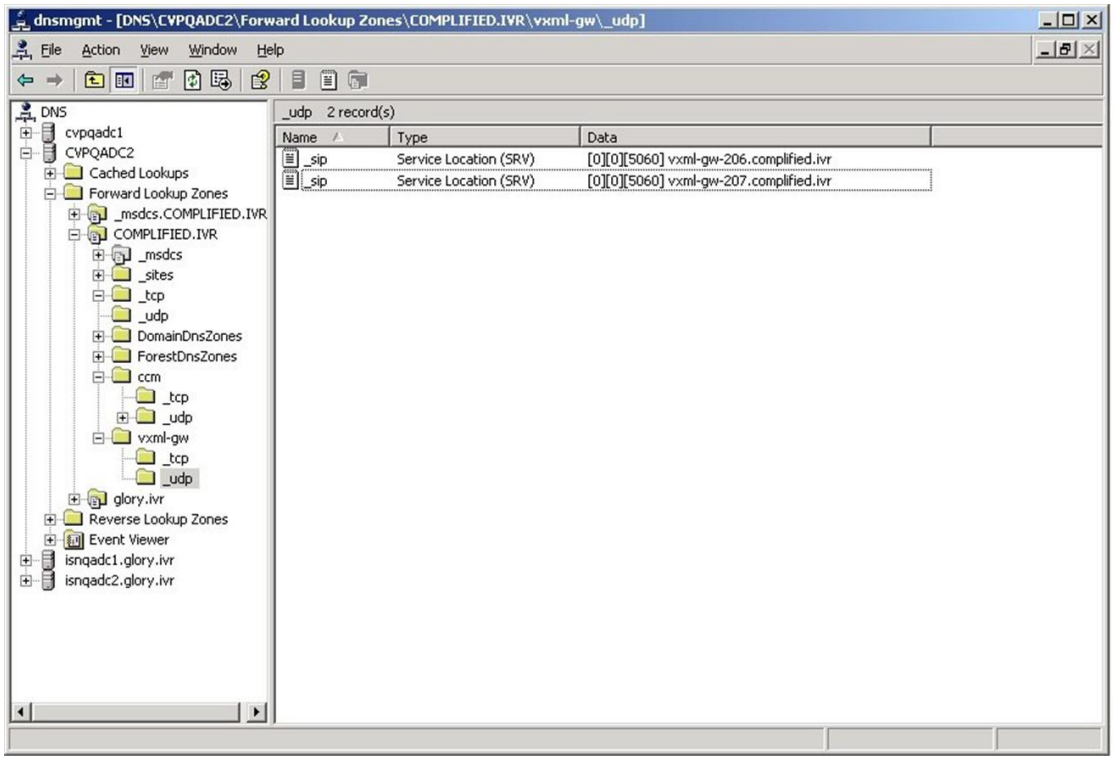
DNS Zone File Configuration for Comprehensive Call Flow Model

DNS Zone File Linux NAMED Configuration Example

```
ringtone-1 IN A 10.86.129.20
```

```
ringtone-2 IN A 10.86.129.229
vxml-1 IN A 10.86.129.20
vxml-2 IN A 10.86.129.229
vxml-3 IN A 161.44.81.254
cvp-1 IN A 10.86.129.211
cvp-2 IN A 10.86.129.220
cvp-3 IN A 161.44.81.254
; Priority Weight Port Target
sip._tcp.ringtone.sox.cisco.com. SRV 1 1 5060 ringtone-1.sox.cisco.com.
_
SRV 1 1 5060 ringtone-2.sox.cisco.com.
sip._udp.ringtone.sox.cisco.com. SRV 1 1 5060 ringtone-1.sox.cisco.com.
_
SRV 1 1 5060 ringtone-2.sox.cisco.com.
_sip._tcp.vxml.sox.cisco.com. SRV 1 1 5060 vxml-1.sox.cisco.com.
SRV 1 1 5060 vxml-2.sox.cisco.com.
SRV 1 1 5060 vxml-3.sox.cisco.com.
_sip._udp.vxml.sox.cisco.com. SRV 2 1 5060 vxml-1.sox.cisco.com.
SRV 2 1 5060 vxml-2.sox.cisco.com.
SRV 1 1 5060 vxml-3.sox.cisco.com.
_sip._tcp.cvp.sox.cisco.com. SRV 1 1 5060 cvp-1.sox.cisco.com.
SRV 2 1 5060 cvp-2.sox.cisco.com.
SRV 3 1 5060 cvp-3.sox.cisco.com.
_sip._udp.cvp.sox.cisco.com. SRV 1 1 5060 cvp-1.sox.cisco.com.
SRV 2 1 5060 cvp-2.sox.cisco.com.
SRV 3 1 5060 cvp-3.sox.cisco.com.
```

DNS Zone File MS DNS Configuration Example



Characteristics for the VRU Leg for Comprehensive Call Flow Model in IOS Gateway

Use the following commands to provide voice treatment:

Note This applies only to IOS VXML Gateway.

new-call is a required name.

Continue with the VRU Leg Example.

```
service vru-leg flash:bootstrap.tcl
 !
service new-call flash:bootstrap.vxml
 !
service handoff flash:handoff.tcl
 !
service ringtone flash:ringtone.tcl
 !
service cvperror flash:cvperror.tcl
 !
service cvp-survivability flash:survivability.tcl
 !
```

REFER Transfers

Unified CVP SIP Service can perform a SIP REFER transfer instead of using SIP re-invites, which allows Unified CVP to remove itself from the call, thus freeing up licensed Unified CVP ports.

Unified CVP cannot run further call control operations after this kind of label has been run. For example, it cannot perform subsequent transfers back to Unified CVP for self service or queuing to another agent.

However, if the transfer fails, configure survivability to transfer the call elsewhere. This process is not the same as an ICM router requery; for example, it will appear as a new call to Unified ICME, but it is a way to take an alternate action, if the transfer fails.

Note

- This feature can be used in Comprehensive (SIP only), Call Director, and Standalone call flow models.
- Router requery can be performed with a REFER transfer only if the NOTIFY messages are sent back to Unified CVP with the result of the REFER operation. Unified CVP does not end the call after sending REFER and hence, it is possible to requery Unified ICM, get another label, and send another REFER.
- The use of the survivability tcl service on the ingress gateway cannot currently support sending the NOTIFY messages with a failed transfer result, so router requery cannot be used with REFER when it is handled by the survivability service. Survivability service can handle REFER, except that it will always report a successful transfer to Unified CVP, even when the transfer failed. This is a known limitation of the TCL IVR API for REFER handling in IOS, including ingress and CUBE gateways.

Using this feature, the call can be queued at the VoiceXML gateway and then sent to an agent with a Unified ICME label that begins with the letters "rf." Otherwise, standard Unified ICME agent labels enable Unified CVP to remain in the signaling path for the duration of the call, and the licensed Unified CVP resource will not be freed until the end of the call. REFER transfers can be made to Unified CM or other SIP endpoints in the SIP cloud, such as an ACD. The ECC variable "user.sip.refertransfer" can also be set in Unified ICME scripts. (When using this ECC variable in a Unified ICME script, it must be set to the value of the single character "y" and Unified CVP will use REFERs when transferring to the agents.

When using REFER transfers, including the REFER used to play back critical_error.wav for abnormal disconnects, the Ingress gateway must include an outbound voip dial peer. This outbound dial peer is necessary because when the REFER message enters the gateway from the Call Server, it needs to match an outbound dial peer in order for the call to succeed; otherwise, a 503 rejection occurs if no dial peers match the REFER-TO header URI. Dial peer destination targets must match the labels in the REFER-TO SIP URI; meaning that <errorDN>@<sip-server> and other labels that may be used in the Unified ICME routing label. For example:

```
dial-peer voice 1050
voip destination-pattern 1...
voice-class codec 1
session protocol sipv2
session target <your sip-server destination>
dtmf-relay rtp-nte
no vad
```

When configuring Route Patterns on Unified CM for REFERs to destinations outside of the cluster, such as to the CUSP Server or the gateways directly, you must add **SIP Route Pattern** for the SIP Trunk associated with that endpoint. For example, if you use REFER to Error DN to the IP Originated caller on Unified CM, and the host of the REFER To header SIP URL is the CUSP Server, you must create a SIP Route Pattern with that IP address or domain name and associate it with your SIP Trunk for the CUSP Server.

Note

- When a TDM gateway handles REFER, and not Cisco Unified Border Element (CUBE), a REFER triggered INVITE is sent out. The REFER triggered INVITE requires a dial peer with a session target and typical codec information. The REFER-TO header URI host that is formulated by the CVP routing algorithm configuration, is ignored.
- When CUBE receives a CVP initiated REFER, it does not send it transparently through to the originator. A dial peer is required to match the DN (user portion of the REFER-TO header URI) and the host portion of the URI is rewritten to match the session target of the dial peer. The REFER is passed to the originator using cli "supplementary-service sip refer"; otherwise, CUBE will handle the REFER and send the triggered invite to the refer DN on its own as a back to back user agent.

Comprehensive Call Flows for Pre-Routed Calls

This class of call flows is similar to the Unified CVP Comprehensive call flow models, except that the calls are first introduced into Unified ICME or Unified ICMH using a path other than through Unified CVP. A Unified ICME routing script is run to pre-route such calls before Unified CVP even sees them. After the script transfers the call to Unified CVP, for either self-service or queuing, a standard Unified CVP Comprehensive call flow model is used.

All the above call flows are similar because the original routing client is capable of a single route request only. A routing client is an NIC, a Unified CM, an ACD, or a VRU. A routing client makes a single request to Unified ICME, then the Unified ICME returns a destination label, and the routing client affects the transfer. At that point the route request dialog is ended, and Unified ICME neither sends a subsequent label nor conducts any form of third-party call control.

If the returned label was a translation route to VRU label, or if it was a correlation ID label resulting from a SendToVRU node, the routing script may run. In such a case, the call is transferred to Unified CVP, and the routing script continues to run after Unified CVP receives the call. The script then invokes micro-application

requests as part of its queuing or self service treatment. If the call is then transferred to an agent or skill group, that label goes to Unified CVP rather than to the original routing client. If the call is to be blind-transferred later to another agent or skill group, or back into Unified CVP for additional queuing or self service, that label too goes to Unified CVP rather than to the original routing client.

When the call arrives at Unified CVP, for micro-applications to be supported, it must establish both the Switch and the VRU leg. In other words, it must enter a general Unified CVP Comprehensive call flow model. The only difference between the pre-routed call and Comprehensive call flow model is the way a call first arrives at Unified CVP. If a call is pre-routed, it arrives using either a translation route or correlation-id transfer, whereas in the Comprehensive call flow model, the call arrives as a new call from the public switched telephone network (PSTN). In both the cases, a subsequent transfer to VRU leg of Unified CVP is required.

This section focuses on the following call flows:

- Calls Arriving at ICME Through a Pre-Route-Only NIC, on page 35.
- Calls Originated by Unified CM, on page 37.
- Calls Originated by an ACD or Call Routing Interface, on page 39.

Note If the ICM Lookup is meant to transfer the call to the Comprehensive call flow model deployment, then a VXML Server running as a Standalone with ICME Lookup call flow also falls in this category.

Calls Arriving at ICME Through a Pre-Route-Only NIC

The following Unified ICME NICs fall into this category: ATT, GKTMP, MCI, Sprint, Stentor. This call flow applies to both the Comprehensive call flow models for ICME and ICMH. In the latter, both Unified CVP and the NIC are deployed at NAM.

Based on the Release number of ICME, perform the following tasks:

Table 8: Procedure for Different Releases of ICME

ICME Release	Procedure
ICME Release 7.1 onwards	**1.** Configure a single Type 10 Network VRU and associate it with all Unified CVP peripherals in the PG Explorer configuration tool, and in the System Information tool, define it as the default system Network VRU. **2.** To support the initial call transfer to Unified CVP from the preroute routing client, configure Translation Route labels to target the Unified CVP peripherals. **3.** To support the transfer to VRU leg, configure the Type 10 Network VRU that you defined in Step 1 with Network Routing Number labels for each Unified CVP peripheral routing client. **4.** Associate all micro-application VRU scripts with that same Type 10 Network VRU. When the routing script transfers the call to Unified CVP, it must use a **TranslationRouteToVRU** node. The transfer to VRU leg of Unified CVP happens automatically. **Note** Non-prerouted calls can also share the same Network VRU and Call Servers.
ICME Release 7.0 onwards	**1.** Configure Type 7 and Type 10 Network VRUs. **2.** In the PG Explorer tool, assign all Unified CVP Call Servers to the Type 7 Network VRU. **3.** Configure one set of Translation Route labels to target the Type 7 Call Servers. These sets are used to transfer the call from the original routing client to the Unified CVP Switch leg. **4.** Assign a label to the Type 10 Network VRU for each Unified CVP Call Server routing client, whose label string is set to the Network Routing Number. **5.** In the System Information configuration tool, configure the Type 10 Network VRU as the system default Network VRU. **6.** Associate all micro-application VRU scripts with the Type 10 Network VRU. **Note** • When the routing script transfers the call into Unified CVP, it must use two nodes in succession: first, a TranslationRouteToVRU, and then an explicit SendToVRU node. The first node transfers the call from the initial routing client to one of the Type 7 Call Servers (Unified CVP Switch leg); the second one transfers the call from the Type 7 Call Server to the Unified CVP VRU leg. (The VRU leg will usually end up running through the same Unified CVP Call Server as the Switch leg.) • Non-prerouted calls can also share the same Type 7 Call Servers and Type 7 and Type 10 Network VRUs; however, scripts which handle non-prerouted calls must also use an explicit SendToVRU node before they can run any micro-applications.

Calls Originated by Unified CM

This category includes the following types of calls:

- Internal Help Desk calls: For these calls, the Unified Communication Manager (CM) phone user calls a CTI Route Point, which starts a routing script that can optionally deliver the call to Unified CVP for queuing or self-service.
- Unified ICME Outbound Option calls: For these calls, a dialer makes outbound calls and then transfers them to a CTI Route Point, which starts a routing script that can optionally deliver the call to Unified CVP for queuing or self-service.
- Consultative Warm Transfer: For these calls, a Unified CM agent places the caller on hold and dials in to Unified ICME to reach a second agent; this starts a routing script that can optionally deliver the call to Unified CVP for queuing or self-service.

Note For information about Consultative Warm Transfer, see Configure Unified ICME Warm Consult Transfer/Conference to Unified CVP, on page 423.

Note If these call flows are used in a Cisco Unified Contact Center Management Portal environment, the target Unified CVP Call Servers are required to be connected to the same CICM as the Unified CM from which the call originates. For example, multiple CICMs will require multiple Unified CMs, so will they require multiple Unified CVP Call Servers.

Further configuration points differ depending on whether Unified CVP is being deployed with Unified ICME Release 7.0 or 7.1 and later.

ICME Release	Task
Unified ICME Release 7.0 onwards	**1.** Configure a single Type 10 Network VRU and defined as the default system Network VRU in the System Information tool. **2.** Configure the Type 10 Network VRU with two sets of labels. Associate the first set with the Unified CM routing client, which contains a label that Unified CM uses to transfer the call to Unified CVP. Configure Unified CM with a series of route patterns, which include that label followed by one to five arbitrary digits. For example, if the selected label is 1111, then the following route pattern is needed: 1111!. The second set of Network VRU labels must contain the usual Comprehensive Model "Network Routing Number," which must be associated with each Unified CVP Call Server routing client. **3.** • When the routing script transfers the call into Unified CVP, it should use a single SendToVRU node. No subsequent node is necessary in order to perform the transfer to Unified CVP's VRU leg; this will take place automatically. (The SendToVRU node can be omitted since any micro-application script node will invoke the same functionality automatically; however, you can include this node explicitly in the script for troubleshooting purposes). • Non-prerouted calls can also share the same Network VRU and the same Unified CVP Call Servers as those calls which are transferred from Unified CM. However, the scripts which handle non-prerouted calls must also use an explicit SendToVRU node before they can run any micro-applications. Associate all micro-application VRU scripts with that same Type 10 Network VRU. **Note** • When the routing script transfers the call into Unified CVP, it should use a single SendToVRU node. No subsequent node is necessary in order to perform the transfer to Unified CVP's VRU leg; this will take place automatically. (The SendToVRU node can be omitted since any micro-application script node will invoke the same functionality automatically; however, you can include this node explicitly in the script for troubleshooting purposes.) • Non-prerouted calls can also share the same Network VRU and the same Unified CVP Call Servers as those calls which are transferred from Unified CM. However, the scripts which handle non-prerouted calls must also use an explicit SendToVRU node before they can run any micro-applications.

ICME Release	Task
Unified ICME Release 7.1 onwards	**1.** Configure two Network VRUs: one Type 7 and one Type 10. **2.** In the PG Explorer tool, assign the Unified CVP Call Servers to the Type 7 Network VRU. **3.** Configure one set of Translation Route labels to target the Type 7 Call Servers; these will be used to transfer the call from the original routing client to the Unified CVP Switch leg. **4.** Assign a label to the Type 10 Network VRU for each Unified CVP Call Server routing client, whose label string is set to the Network Routing Number. **5.** Configure the Type 10 Network VRU as the system default Network VRU in the System Information configuration tool. **6.** Associate all micro-application VRU scripts with the Type 10 Network VRU. **Note** • When the routing script to transfers the call into Unified CVP, it should use *two* nodes in succession: first, a TranslationRouteToVRU, and then an explicit SendToVRU node (which contrary to the Unified ICME 7.1 case, is *not* optional). The first node transfers the call from the initial routing client to one of the Type 7 Call Servers (Unified CVP Switch leg); the second one transfers the call from the Type 7 Call Server to the Unified CVP VRU leg. (The VRU leg will usually end up running through the same Unified CVP Call Server as the Switch leg.) • Non-prerouted calls can also share the same Type 7 Call Servers and Type 7 and Type 10 Network VRUs.

Calls Originated by an ACD or Call Routing Interface

These calls are very similar to those which arrive from a preroute-only NIC, except that the routing client is connected to Unified ICME using a PG rather than using a NIC. Therefore, if this call flow is used in a Unified ICMH environment, the target Unified CVP Call Servers are required to be connected to the same CICM as the ACD or CRI-based VRU from which the call originates. Just as multiple CICMs will require multiple ACD or VRU peripherals, so will they require multiple Unified CVP Call Servers.

Further configuration points differ depending on whether Unified CVP is being deployed with Unified ICME Release 7.0 or 7.1 and later

Table 9: Procedure for Different Releases of ICME

ICME Release	Tasks
ICME Release 7.1 onwards	1. Configure a single Type 10 Network VRU and associate it with all Unified CVP peripherals in the PG Explorer configuration tool, and also define it as the default system Network VRU in the System Information tool. 2. In order to support the initial call transfer to Unified CVP from the pre-route routing client, configure Translation Route labels to target the Unified CVP peripherals. 3. In order to support the transfer to VRU leg, configure the Type 10 Network VRU with Network Routing Number labels for each Unified CVP peripheral routing client. 4. Associate all micro-application VRU scripts with that same Type 10 Network VRU. **Note** • When the routing script transfers the call into Unified CVP, it must use a TranslationRouteToVRU node. No subsequent node is necessary in order to perform the transfer to Unified CVP's VRU leg; this will take place automatically. • Non-prerouted calls can also share the same Network VRU and the same Unified CVP Call Servers.

ICME Release	Tasks
ICME Release 7.0 onwards	**1.** Configure two Network VRUs: one Type 7 and one Type 10. **2.** In the PG Explorer tool, assign all Unified CVP Call Servers to the Type 7 Network VRU. **3.** Configure one set of Translation Route labels to target the Type 7 Call Servers; these will be used to transfer the call from the original routing client to the Unified CVP Switch leg. **4.** Assign a label to the Type 10 Network VRU for each Unified CVP Call Server routing client, whose label string is set to the Network Routing Number. **5.** Configure the Type 10 Network VRU as the system default Network VRU in the System Information configuration tool. **6.** Associate all micro-application VRU scripts with the Type 7 Network VRU. **Note** • When the routing script transfers the call into Unified CVP, it should use *two* nodes in succession: first, a TranslationRouteToVRU, and then an explicit SendToVRU node. The first node transfers the call from the initial routing client to one of the Type 7 Call Servers (Unified CVP Switch leg); the second one transfers the call from the Type 7 Call Server to the Unified CVP VRU leg. (The VRU leg will usually end up running through the same Unified CVP Call Server as the Switch leg.) • Non-prerouted calls can also share the same Type 7 Call Servers and Type 7 and Type 10 Network VRUs.

Call Director Call Flow Model

In Call Director call flow model, Unified CVP provides ICME with VoIP call routing capabilities only. If you are using an ICM Server to queue calls or queue calls directly on an ACD, use your own Service Control VRU. 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 works with customer-provided SIP endpoints that have been tested and certified to interoperate with Unified CVP. No VXML Server or VXML Gateway is used in this model.

The following table lists the required and optional CVP components needed for the Call Director call flow model:

Table 10: Required and Optional CVP Components for Call Director Call Flow Model

CVP components	Related topics
Required CVP components	
Call Server	• Call Server Configuration, on page 77 • REFER Transfers, on page 33
Unified ICME	• Unified ICM Configuration, on page 171 • Call Director Call Flow Model for Unified ICME, on page 42 • Call Director Call Flow Model for Unified ICMH, on page 44 • Configure ICM Settings for Call Director Call Flow Model, on page 190 • Define Unified CVP ECC Variables, on page 181
Ingress Gateway	• Gateway Configuration, on page 481 • Set Up Call Director Call Flow Model, on page 45 • Call Survivability, on page 442
Operations Console	Operations Console, on page 67
Optional CVP components	
Reporting Server	Reporting Server Configuration, on page 163
SIP Proxy Server, if Call Server is configured to use SIP signaling	SIP Proxy Server Configuration, on page 319

This section describes the following Call Director call flow models:

- Call Director Call Flow Model for Unified ICME, on page 42
- Call Director Call Flow Model for Unified ICMH, on page 44

Call Director Call Flow Model for Unified ICME

In this call flow model, Unified CVP provides Unified ICME with VoIP call switching capabilities. Provide your own Service Control VRU, if you are using Unified ICME to queue calls or you might queue calls directly on your ACD. Calls might be transferred multiple times, from Ingress, to customer-provided VRU, to either Unified CCE or customer-provided ACD or agent, and back again. When calls are connected to customer-provided equipment (either VoIP or TDM), their voice paths must go to an egress gateway, which

is connected by TDM to that equipment. If the signaling is SIP, then this call flow model works with customer-provided SIP endpoints which have been tested and certified to interoperate with Unified CVP.

The following figures show the call flow for Call Director call flow model for ICME using SIP without and with a Proxy Server. The solid lines in these figures indicate voice paths and dashed lines indicate signaling paths.

Figure 7: Call Director Call Flow Model for ICME Using SIP Without a Proxy Server

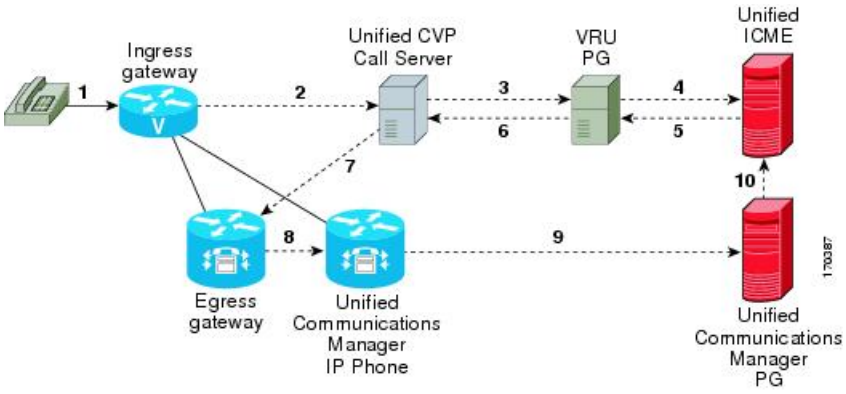
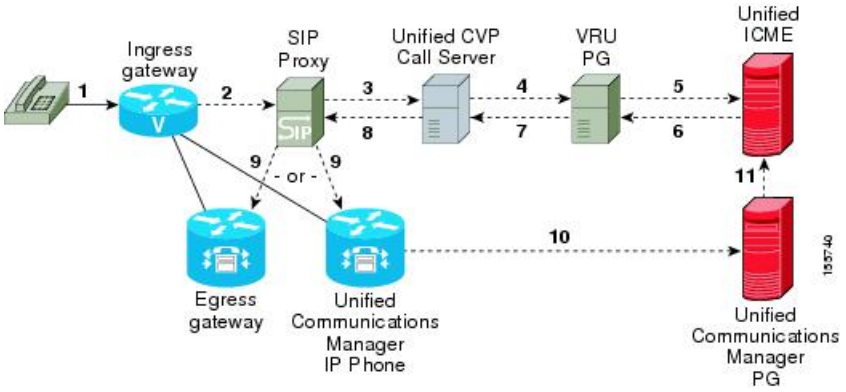


Figure 8: Call Director Call Flow Model for ICME Using SIP With a Proxy Server



Note

- In this call flow model, Unified CVP stays in the signaling path after the transfer.
- In this call flow model, VRU scripts and transfer to a VRU leg are not available .
- For more information, see REFER Transfers, on page 33 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65.

Related Topics

REFER Transfers, on page 33
Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65

Call Director Call Flow Model for Unified ICMH

In this call flow model, Unified CVP only provides the Network Applications Manager (NAM) with VoIP call switching capabilities. If you are using the NAM to queue calls, or you might queue calls directly on your ACD, provide your own Service Control VRU. Calls may be transferred multiple times, from Ingress, to customer-provided VRU, to either the NAM 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 this call flow model works with customer-provided SIP endpoints which have been tested and certified to interoperate with Unified CVP.

The following figures show the call flow for Call Director call flow model for ICMH using SIP without and with a Proxy Server. The solid lines in these figures indicate voice paths and dashed lines indicate signaling paths.

Figure 9: Call Director Call Flow Model for ICMH Using SIP Without a Proxy Server

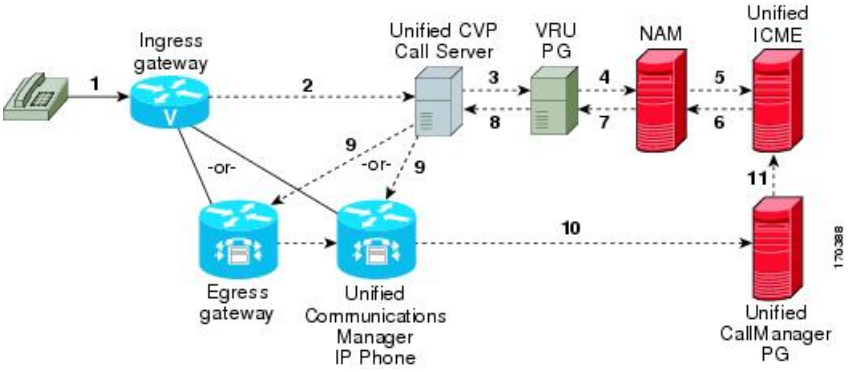
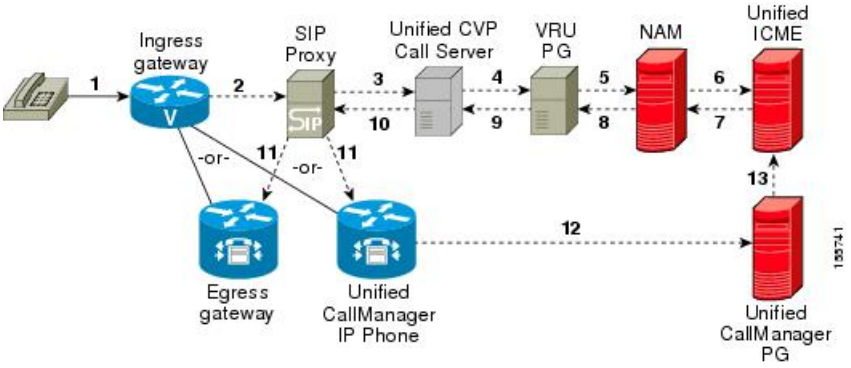


Figure 10: Call Director Call Flow Model for ICMH Using SIP With a Proxy Server



Note

- VRU scripts and transfer to a VRU leg are not available in this call flow model.
- For more information, see REFER Transfers, on page 33 and Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65.

Related Topics

REFER Transfers, on page 33

Set Up sendtooriginator Setting in the SIP Service of a Call Server, on page 65

Set Up Call Director Call Flow Model

Procedure

Step 1 Perform Steps 1 to 5 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 2 Configure the Ingress Gateway:

a) Configure the Ingress Gateway dial-peer for the Unified CVP Call Server.
b) Configure a dial-peer for ringtone and error.
c) If you are using a Proxy Server, configure your session target in the outbound dial peer to point to the Proxy Server.
d) If you are using the sip-server global configuration, then configure the sip-server in the sip-ua section to be your Proxy Server and point the session target of the dial-peer to the sip-server global variable.

Note Make sure your dial plan includes this information. You will need to see the Dial plan when you configure the SIP Proxy Server for Unified CVP.

The SIP Service voip dial peer and the destination pattern on the Ingress Gateway must match the DNIS in static routes on the SIP Proxy Server or Unified CVP Call Server.

See the SIP Devices Configuration, on page 209 and SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

Step 3 For SIP without a Proxy Server, complete the following steps:

a) If you are using DNS query with SRV or A types from the gateway, configure the gateway to use DNS.

See the Operations Console online help for details. If you are using DNS query with SRV or A types from the gateway, use the gateway configuration CLI as shown below:

Non-DNS Setup:

```
sip-ua
sip-server ipv4:xx.xx.xxx.xxx:5060
!
```

DNS Setup:

```
ip domain name patz.cisco.com
ip name-server 10.10.111.16
!
sip-ua
sip-server dns:cvp.pats.cisco.com
!
```

b) Configure the DNS zone file for the separate DNS server that displays how the Service (SRV) records are configured.

Note SRV with DNS can be used in *any* of the SIP call flow models, with or without a Proxy server. Standard A type DNS queries can be used as well for the calls, without SRV, but they lose the load balancing and failover capabilities.

See the DNS Zone File Configuration for Call Director Call Flow Model, on page 52 for more information.

Step 4 For SIP with a Proxy Server, use one of the following methods:

Note You can configure the Gateway statically instead of using DNS.

The following example shows how both the A and SRV type records could be configured:

```
ip host cvp4cc2.cisco.com 10.4.33.132
ip host cvp4cc3.cisco.com 10.4.33.133
ip host cvp4cc1.cisco.com 10.4.33.131
```

For **SIP/TCP**:

```
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

For **SIP/UDP**:

```
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

Note The DNS Server must be configured with all necessary A type or SRV type records.

See the SIP Devices Configuration, on page 209.

If you are using the DNS Server, you can set your SIP Service as the Host Name (either A or SRV type).

Step 5 On the Unified CM server, CCMAdmin Publisher, complete the following SIP-specific actions:

a) Create SIP trunks.

- If you are using a SIP Proxy Server, set up a SIP trunk to the SIP Proxy Server.
- Add a SIP Trunk for the Unified CVP Call Server.
- Add a SIP Trunk for each Ingress gateway that will send SIP calls to Unified CVP that might be routed to Unified CM.

To add an SIP trunk, select **Device** > **Trunk** > **Add New** and use the following parameters:

- Trunk Type: **SIP trunk**
- Device Protocol: **SIP**
- Destination Address: IP address or host name of the SIP Proxy Server (if using a SIP Proxy Server). If not using a SIP Proxy Server, enter the IP address or host name of the Unified CVP Call Server.
- DTMF Signaling Method: **RFC 2833**
- Do **not** check the *Media Termination Point Required* check box.
- If you are using UDP as the outgoing transport on Unified CVP, also set the outgoing transport to **UDP** on the SIP Trunk Security Profile.
- Connection to CUSP Server: use 5060 as the default port.

b) Add route patterns for outbound calls from the Unified CM devices using a SIP Trunk to the Unified CVP Call Server. Also, add a route pattern for error DN.

Select **Call Routing** > **Route/Hunt** > **Route Pattern** > **Add New**

Add the following:

- Route Pattern: Specify the route pattern; for example: **3XXX** for a TDM phone that dials 9+3xxx and all Unified ICME scripts are set up for 3xxx dialed numbers.
- Gateway/Route List: Select the SIP Trunk defined in the previous substep.

Note For warm transfers, the call from Agent 1 to Agent 2 does not typically use a SIP Trunk, but you must configure the CTI Route Point for that dialed number on the Unified CM server and associate that number with your peripheral gateway user (PGUSER) for the JTAPI gateway on the Unified CM peripheral gateway. An alternative is to use the Dialed Number Plan on Unified ICME to bypass the CTI Route Point.

c) If you are sending calls to Unified CM using an SRV cluster domain name, select **Enterprise Parameters** > **Clusterwide Domain Configuration** and add the Cluster fully qualified domain name **FQDN**.

Step 6 (Optionally) Configure the **SIP Proxy Server**.

a) Configure the SIP static routes to the Unified CVP Call Servers, Unified CM SIP trunks, and Gateways.

Configure the SIP static routes for intermediary transfers for ringtone, playback dialed numbers, and error playback dialed numbers.

Note For failover and load balancing of calls to multiple destinations, configure the CUSP server static route with priority and weight.

b) Configure Access Control Lists for Unified CVP calls.

Select **Proxy Settings** > **Incoming ACL**.

Address pattern: **all**

c) Configure the service parameters.

Select **Service Parameters**, then set the following:

- Add record route: **off**
- Maximum invite retransmission count: **2**
- Proxy Domain and Cluster Name: if using DNS SRV, set to the FQDN of your Proxy Server SRV name

d) Write down the IP address and host name of the SIP Proxy Server. (You need this information when configuring the SIP Proxy Server in Unified CVP.)

e) If using redundant SIP Proxy Servers (primary and secondary or load balancing), then decide whether to use DNS server lookups for SRV records or non-DNS based local SRV record configuration.

Note If a single CUSP Server is used, then SRV record usage is not required.

Configure the SRV records on the DNS server or locally on Unified CVP with a .xml file (local xml configuration avoids the overhead of DNS lookups with each call).

Note See the Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210 section for details.

The Call Director call flow model with SIP calls will typically be deployed with dual CUSP servers for redundancy. In some cases, you might want to purchase a second CUSP server. Regardless, the default transport for deployment will be UDP; make sure you *always* disable the record-route in a CUSP server as this advanced feature is not supported in Contact Center deployments.

For the required settings in the Unified CM Publisher configuration, see the Cisco Unified SIP Proxy documentation.

Step 7 Configure the PGs for the switch leg.

On Unified ICME, ICM Configuration Manager, **PG Explorer** tool:

a) Configure each peripheral gateway (PG) to be used for the **Switch** leg. In the tree view pane, select the applicable PG, and set the following:

1. **Logical Controller** tab:
   - Client Type: **VRU**
   - Name: A name descriptive of this PG

     For example: **<location>_A** for side A of a particular location

2. **Peripheral** tab:
   - Peripheral Name: A name descriptive of this Unified CVP peripheral

     For example: **<location>_<cvp1> or <dns_name>**
   - Client Type: **VRU**
   - Select the check box: **Enable Post-routing**

3. **Routing Client** tab:
   - Name: By convention, use the same name as the peripheral.
   - Client Type: **VRU**

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

b) Configure a peripheral for each Unified CVP Call Server to be used for a Switch leg connected to each PG.

Step 8 Configure dialed numbers.

On the Unified ICME or Unified ICMH Server, in the ICM Configuration Manager, configure the following items:

a) **Dialed Number List Tool** tab: Configure the dialed numbers.
b) **Call Type List tool** tab: Configure the call types.
c) **ICM Instance Explorer tool** tab: Configure the applicable customers.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 9 Create a Routing Script.

On the Unified ICME or Unified ICMH Server in the ICM Script Editor tool:

Create a routing script that handles the incoming call. The routing script must run a Label node or Select node (node that returns a label right away).

Note *Do not* use the Queue node in the routing script.

The label must be configured in the SIP Proxy Server to the IP address of the device that the label corresponds to. The Proxy Server is optional. If you do not have one, you must configure the Gateway dial-peer to point to the Call Server (refer to the first step in this process). Also, you must configure the **destination labels** in the SIP Service for the Call Server.

See the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for more information.

Step 10 Configure the SIP Proxy Server using the Operations Console.

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

Step 11 In the Operations Console, install and configure Call Servers.

a) Enable the ICM and SIP Services on the Call Server.

In the Operations Console, select **Device Management** > **Unified CVP Call Server**.

Select the check boxes: **ICM** and **SIP**

b) Configure the SIP Service:

Select **Device Management** > **CVP Call Server** > **SIP tab**.

- If you are using a SIP Proxy Server, enable the Outbound Proxy and select the SIP Proxy Server. If using a SIP Proxy Server, configure Local Static Routes on the SIP Proxy Server itself.
- If you are not using a SIP Proxy Server, configure Local Static Routes using the Dialed Number Pattern system configuration in the Operations Console. A local static route must be configured for each SIP gateway/ACD, SIP endpoint in order to receive calls.
- Check the default values for the SIP Service and change, if desired.

See the SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

c) Configure the ICM Service by setting the maximum length DNIS to the length of the Network Routing Number:

- Select **Device Management** > **CVP Call Server** > **ICM tab**.
- Set the Maximum Length of DNIS to length of the Network Routing Number.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

For detailed information, see the *Operations Console online help*.

Step 12 Configure local static routes:

If an outbound proxy is enabled on the Operations Console, configure local static routes on the SIP Proxy Server.

If no outbound proxy is enabled, configure local static routes using the Operations Console Dialed Number Pattern system configuration. See the SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

The following is an example of a local static route configuration. A local static route contains a dialed number pattern and a routing address (IP Address, Hostname, or SIP Server Group name):

- **22291>,cvp-ringtone.cisco.com**
- **22292>,cvp-error.cisco.com**
- 1>,ccm-subscribers.cisco.com
- 2>,ccm-subscribers.cisco.com
- 3>,ccm-subscribers.cisco.com

Step 13 (Optional) On the Operations Console, configure the **Reporting Server**. Select **Device Management** > **CVP Reporting Server** > **General tab**:

a) Configure the Reporting Server.
b) Select a Call Server to associate with this Reporting Server.
c) Check the default values of the Reporting properties and change, if desired.

For more information, see the Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Related Topics

Configure Gateway Settings for Comprehensive Call Flow Model, on page 255
Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210
Load-Balancing SIP Calls , on page 210
Cisco Unified SIP Proxy (CUSP) Configuration , on page 210
Configure Custom Streaming Ringtones, on page 213
SIP Dialed Number Pattern Matching Algorithm, on page 9
DNS Zone File Configuration for Call Director Call Flow Model, on page 52
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210

Examples: Ingress Gateway Configuration

Example: Gateway Settings for Call Director Call Flow Model

The first part of the following example provides the basic configuration for setting an Ingress gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets

- Configures gateway settings

The last part of this example provides the following:

- Allows SIP to play a .wav file that enables caller to hear message from critical_error.wav
- Performs survivability
- Enables SIP to play ring tone to caller while caller is being transferred to an agent
- Logs errors on the gateway when the call fails
- Defines requirements for SIP Call Server

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
service internal
logging buffered 99999999 debugging
no logging console
!
ip cef
!
voice rtp send-recv
!
voice service voip
signaling forward unconditional
h323
sip
min-se 360
header-passing
!
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
application
service cvperror flash:cvperror.tcl
!
service cvp-survivability flash:survivability.tcl
!
service ringtone flash:ringtone.tcl
!
service handoff flash:handoff.tcl!gateway
!
gateway
timer receive-rtcp 6
!
ip rtcp report interval 3000
!
sip-ua
retry invite 2
timers expires 60000
sip-server ipv4:<IP of CUSP Server or Call Server>:5060
reason-header override
!
```

Example: Incoming Pots Dial-peer for Call Director Call Flow Model

```
dial-peer voice 8 pots
description Example incoming POTS dial-peer
service cvp-survivability
incoming called-number <your DN pattern here>
```

```
direct-inward-dial
!
```

Example: SIP Ringtone Dial-peer for Call Director Call Flow Model

```
dial-peer voice 9191 voip
description SIP ringtone dial-peer
service ringtone
voice-class codec 1
voice-class sip rel1xx disable
incoming called-number <your ringtone DN pattern here>
dtmf-relay rtp-nte
no vad
!
```

Example: SIP Error Dial-peer for Call Director Call Flow Model

```
dial-peer voice 9292 voip
description SIP error dial-peer
service cvperror
voice-class codec 1
voice-class sip rel1xx disable
incoming called-number <your error DN pattern here>
dtmf-relay rtp-nte
no vad
!
```

Example: Dial-peer to Reach the Unified CVP Call Server or CUSP Server for Call Director Call Flow Model

```
dial-peer voice 800 voip
description Example Call Server Dialpeer with CUSP Server
destination-pattern <your DN pattern here>
voice-class codec 1
session protocol sipv2
session target sip-server
dtmf-relay rtp-nte
no vad
!
```

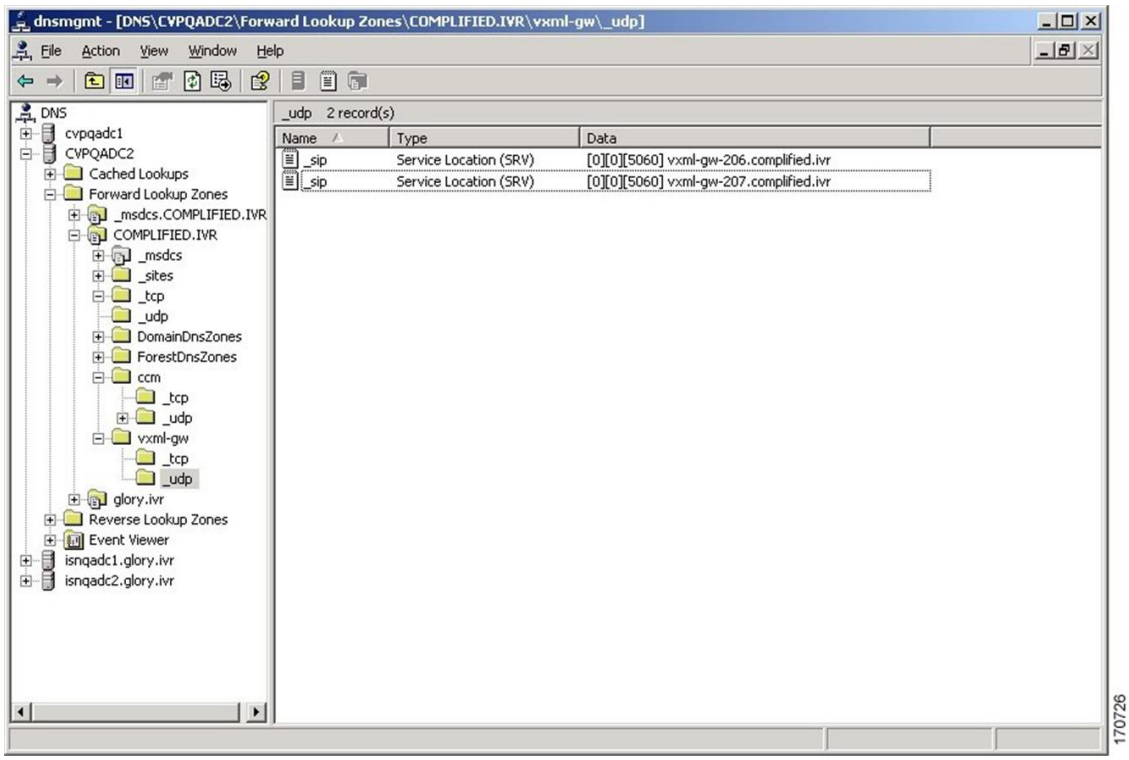
DNS Zone File Configuration for Call Director Call Flow Model

Example: DNS Zone File Linux NAMED Configuration

```
ringtone-1 IN A 10.86.129.20
         ringtone-2 IN A 10.86.129.229
         vxml-1 IN A 10.86.129.20
         vxml-2 IN A 10.86.129.229
         vxml-3 IN A 161.44.81.254
         cvp-1 IN A 10.86.129.211
         cvp-2 IN A 10.86.129.220
         cvp-3 IN A 161.44.81.254
         ; Priority Weight Port Target
         sip._tcp.ringtone.sox.cisco.com. SRV 1 1 5060 ringtone-1.sox.cisco.com.
         _
         SRV 1 1 5060 ringtone-2.sox.cisco.com.
         sip._udp.ringtone.sox.cisco.com. SRV 1 1 5060 ringtone-1.sox.cisco.com.
         _
         SRV 1 1 5060 ringtone-2.sox.cisco.com.
         _sip._tcp.vxml.sox.cisco.com. SRV 1 1 5060 vxml-1.sox.cisco.com.
         SRV 1 1 5060 vxml-2.sox.cisco.com.
         SRV 1 1 5060 vxml-3.sox.cisco.com.
```

```
_sip._udp.vxml.sox.cisco.com. SRV 2 1 5060 vxml-1.sox.cisco.com.
SRV 2 1 5060 vxml-2.sox.cisco.com.
SRV 1 1 5060 vxml-3.sox.cisco.com.
_sip._tcp.cvp.sox.cisco.com.  SRV 1 1 5060 cvp-1.sox.cisco.com.
SRV 2 1 5060 cvp-2.sox.cisco.com.
SRV 3 1 5060 cvp-3.sox.cisco.com.
_sip._udp.cvp.sox.cisco.com. SRV 1 1 5060 cvp-1.sox.cisco.com.
SRV 2 1 5060 cvp-2.sox.cisco.com.
SRV 3 1 5060 cvp-3.sox.cisco.com.
```

Example: DNS Zone File MS DNS Configuration



VRU-Only Call Flow Model with NIC Routing

Unified CVP provides ICM with VRU services for calls which are routed in a manner, such as by a carrier switched network through an ICM network interface card (NIC). VRU services can 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.

Depending on the type of routing client being 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 former, the Call Server determines that the arriving call is a VRU leg call by matching the arriving DNIS with its configured list of arriving DNIS numbers. In latter, it determines 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

This section describes the following VRU-Only call flow models:

- Type 8 VRU-Only Call Flow Model for ICME, on page 54

- Type 8 VRU-Only Call Flow Model for ICMH, on page 55
- Configure Gateway Settings for VRU-Only: Type 7, on page 270

Note In VRU-Only call flow model, Unified CVP by itself does not provide queuing capability. However, it can hold calls being queued when used with Unified ICME/Unified CCE with appropriate Unified ICME network interface controllers.

Related Topics

Call Server Configuration, on page 77
REFER Transfers, on page 33
Gateway Configuration, on page 249
Configure Gateway Settings for VRU-Only: Type 7, on page 270
Call Survivability, on page 442
Operations Console, on page 67
Comprehensive Call Flow Model for ICME, on page 21
Calls Arriving at ICME Through a Pre-Route-Only NIC, on page 35
Calls Originated by Unified CM, on page 37
Calls Originated by an ACD or Call Routing Interface, on page 39
Define Unified CVP ECC Variables, on page 181
Configure Common Unified ICMH for Unified CVP Switch Leg, on page 178
Type 8 VRU-Only Call Flow Model for ICME, on page 54
Type 8 VRU-Only Call Flow Model for ICMH, on page 55
VXML Server Configuration, on page 105
Speech Server Configuration, on page 245
Media Server Configuration, on page 217
Reporting Server Configuration, on page 163

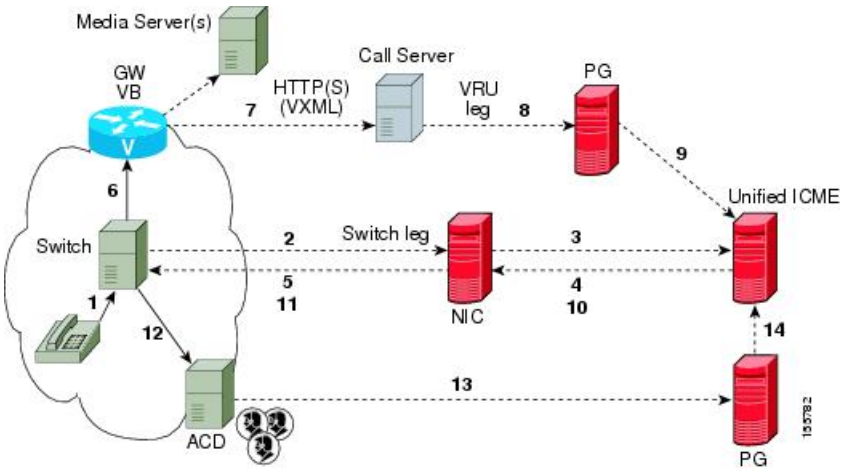
Type 8 VRU-Only Call Flow Model for ICME

In this call flow model, Unified CVP works with the Voice Gateway to act as the VRU. The VRU voice treatment is provided by the Gateway and can include ASR/TTS Servers.

When deployed with an NIC being used to queue and transfer calls (VRU Type 8), the NIC interfaces with the TDM switch or with the PSTN to transfer the call to an agent. The Unified CVP SIP Service is part of this call flow model.

The following figure shows the Type 8 VRU-Only call flow model where the NIC transfers the call. In the figure, solid lines indicate voice paths and dashed lines indicate signaling paths.

Figure 11: Type 8 VRU-Only Call Flow Model Where NIC Transfers a Call



Note

- Numbers in the figure represent call flow progression.
- Confirm that there is one Network VRU: a Type 8 when NIC is queuing and transferring calls.
- Define a Translation Route and labels for the VRU Peripheral (Network VRU labels do not need to be configured).
- Use the TranslationRouteToVRU node of the ICM Script Editor to connect the call to the Network VRU.

Type 8 VRU-Only Call Flow Model for ICMH

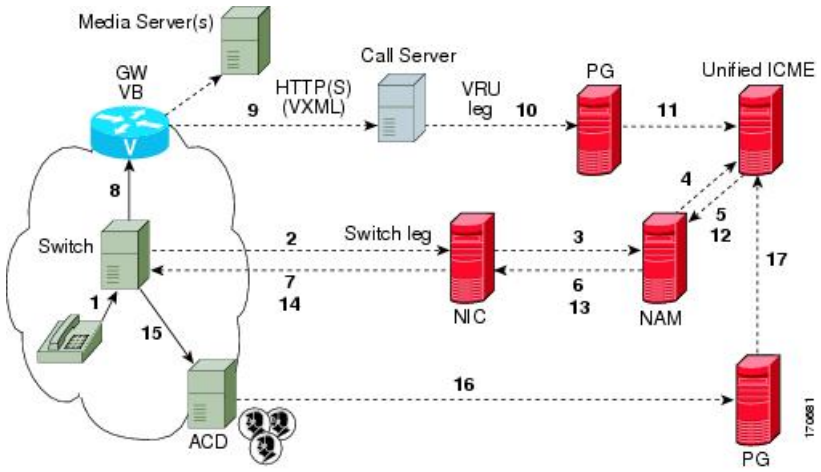
In this call flow model, the Unified CVP Call Server is deployed at the CICM level to act only as the VRU leg for the call. The VRU voice treatment is provided at the Voice Gateway, and may include ASR/TTS Servers.

Note This call flow model is used when Unified CVP is connected to the CICM. The routing client in this call flow model is connected to the NAM.

When deployed with a NIC being used to queue and transfer calls (VRU Type 8), the NIC interfaces to the TDM switch to transfer the call to an agent. The SIP Service is part of this call flow model.

The following figure shows the Type 8 VRU-Only call flow model for ICMH. The solid lines in this figure indicate voice paths and dashed lines indicate signaling paths.

Figure 12: Type 8 VRU-Only Call Flow Model for ICMH



Note

- For simplicity, the figure does not illustrate a call flow model for redundancy and failover.
- Two Network VRUs are configured:
  - One on the NAM (Type 8).
  - One on the CICM for the INCRP connection (Type 8).
- Use the ICM Script Editor's TranslationRouteToVRU node to connect the call to the Network VRU.

Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH

Procedure

Step 1 From the Operations Console (or the Unified CVP product CD), transfer the following script, configuration, and .wav files to the **VoiceXML Gateway** used for the VRU leg.

Transfer the following files:

- bootstrap.tcl
- handoff.tcl
- survivabilty.tcl
- bootstrap.vxml
- recovery.vxml
- ringtone.tcl
- cvperror.tcl

- ringback.wav
- critical_error.wav

Step 2 Configure the VXML gateway base settings.

Step 3 Configure the VXML gateway service settings.

Step 4 Configure the ICM VRU Label.

Step 5 Define a Network VRU on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

On the ICM Configuration Manager, the **Network VRU Explorer** tool, specify the following:

- Type: **8**
- Name: **cvpVRU**

Note Although any name will work, **cvpVRU** is used by convention, and is the example name referenced elsewhere in this document.

Step 6 Configure the Peripheral Gates (PGs) on Unified ICME or (for Unified ICMH) on each CICM.

a) Configure each PG.
b) Configure a peripheral for each Unified CVP ICM Service connected to each PG.

Use the ICM Configuration Manager, the **PG Explorer** tool. For each Unified CVP ICM Service connected to this PG, in the tree view pane, select the applicable PG and configure the following items:

Logical Controller tab:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  Example: `<location>_A` for side A of a particular location

Peripheral tab:

- Peripheral Name: A name descriptive of this Unified CVP peripheral

  Examples: `<location>_<cvp1>` or `<dns_name>`
- Client Type: **VRU**
- Select the checkbox: **Enable Post-routing**

Advanced tab:

- From the Network VRU field drop-down list, select the name: **cvpVRU**

Routing Client tab:

- Name: By convention, use the same name as the peripheral.
- Client Type: **VRU**

Step 7 Configure a Service and Route for each VRU on Unified ICME or (for Unified ICMH) on each CICM.

Note You can also use service arrays. Refer to the Unified ICME documentation set for more information.

Using the ICM Configuration Manager, the **Service Explorer** tool, specify the following:

- Service Name: **cvpVRU**
- Route Name: **PeripheralName_cvpVRU**
- Peripheral Number: **2**

  Must match the "Pre-routed Call Service ID" in the Call Server configuration on the ICM tab in the Operations Console
- Select the checkbox: **Enable Post-routing**

Step 8 Define trunk groups.

Note You must configure one Network Transfer Group and one associated Trunk Group for each VRU leg Unified CVP ICM Service.

Define and configure the network trunk group on Unified ICME or (for Unified ICMH) on each CICM.

Using the ICM Configuration Manager, the Network **Trunk Group Explorer** tool:

a) Identify the network trunk group.
   - Network Trunk Group Name: A name descriptive of this trunk group

b) For each Unified CVP ICM Service for the VRU leg, configure an associated trunk group.
   - Peripheral Name: A name descriptive of this trunk group
   - Peripheral Number: **200**

     Must match the "Pre-routed Call Trunk Group ID" in the Call Server configuration on the ICM tab in the Operations Console
   - Trunk Count: Select **Use Trunk Data** from the drop-down list
   - *Do not* configure any trunks

Step 9 Define translation route(s).

Define and configure a Translation Route for each VRU Peripheral on Unified ICME or (for Unified ICMH) on each CICM.

On Unified ICME, ICM Configuration Manager, **Translation Route Explorer** tool:

a) Define a Translation Route for each VRU Peripheral. Specify the following:

   Translation Route tab:
   - Set the **Name** field to the name of the target VRU peripheral. (This is by convention; this value must be unique in the enterprise)
   - Set the **Type** field to **DNIS** and select the Service defined in the previous step

b) Configure translation route and label information for each VRU peripheral. Complete the following:

   Route tab:

- Set the **Name**: by convention, this is the name of the target VRU peripheral, followed by the DNIS that this route will use, for example, MyVRU_2000

  This value must be unique in the enterprise

- Service Name drop-down list, select: **PeripheralName.cvpVRU**

Peripheral Target tab:

- Enter the first DNIS that will be seen by the VRU that you will be using for this translation route.

  Note The DNIS pool used for each VRU peripheral must be unique

- From the drop-down list, select a **Network Trunk Group** which belongs to the target VRU

Label tab:

- Enter the translation route label (which might or might not be the same DNIS you entered on the Peripheral Target tab)
- Type: **Normal**
- Routing Client: Select the NIC Routing Client

You must create an additional label for each NIC routing client.

Note Repeat the Route and corresponding Peripheral Target and Label information for each DNIS in the pool.

Step 10 Create VRU and routing scripts.

Create VRU scripts and routing scripts for IVR treatment and agent transfer on Unified ICME or (for Unified ICMH) on each CICM .

Using the ICM **Script Editor** tool, create the VRU scripts and routing scripts to be used for IVR treatment and agent transfer, as described in other sections of this manual and in the ICM manuals.

The VRU scripts are associated with the applicable Network VRU.

For example, **cvpVRU**

Use the ICM Script Editor's TranslationRouteToVRU node to connect the call to the Network VRU.

Step 11 Configure the ECC variables on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

Using the ICM Configuration Manager, create the ECC variables.

For more information, see Define Unified CVP ECC Variables, on page 181.

Step 12 Configure dialed numbers and call types on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

On Unified ICME, using the ICM Configuration Manager, configure dialed numbers and call types.

For more information, refer to ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 13 On Unified CM configure Unified CM.

For more information, refer to the Unified CM user documentation.

Step 14 Install and configure the Call Server(s).

Using the Operations Console, select **Device Management** > **CVP Call Server** and install and configure the **Call Server(s)**.

Select the check boxes: **ICM** and **IVR**

For detailed information, refer to the Operations Console online help.

Step 15 Configure the ICM service.

Using the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. On **each** Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a) VRU connection port number.

Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b) Maximum Length of DNIS.

Set the maximum length DNIS to a number which is at least the length of the translation route DNIS numbers.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c) Call service IDs: New Call and Pre-routed.

Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab.

d) Trunk group IDs: New Call and Pre-routed.

- Enter the new and pre-routed call trunk group IDs
- Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route
- Configure the number of ports according to the licenses purchased and capacity
- Configure each of the numbers used for translation routes. (The “New Call” group is not used since the calls are being sent to the VRU (Unified CVP) after some initial processing by the NIC/Unified ICME)

e) Dialed numbers used in the translation route.

Add the dialed numbers in the DNIS field.

f) Check the default values of the other settings and change, if desired.

Step 16 Configure the **IVR Service**.

In the Operations Console, select **Device Management** > **CVP Call Server** > **IVR** tab.

Check the default values and change, if desired.

Refer to the Operations Console online help for information about other settings you might want to adjust from their default values.

Step 17 (Optional) Configure the Reporting Server.

In the Operations Console, select **Device Management** > **CVP Reporting Server** > **General tab**:

a. Configure the Reporting Server.

b. Select a Call Server to associate with this Reporting Server.

c. Check the default values of the Reporting properties and change, if desired.

For more information, refer to Reporting Guide for Cisco Unified Customer Voice Portal

Related Topics

Define Unified CVP ECC Variables, on page 181

Type 7 VRU-Only Call Flow Model Network VRU for ICMH

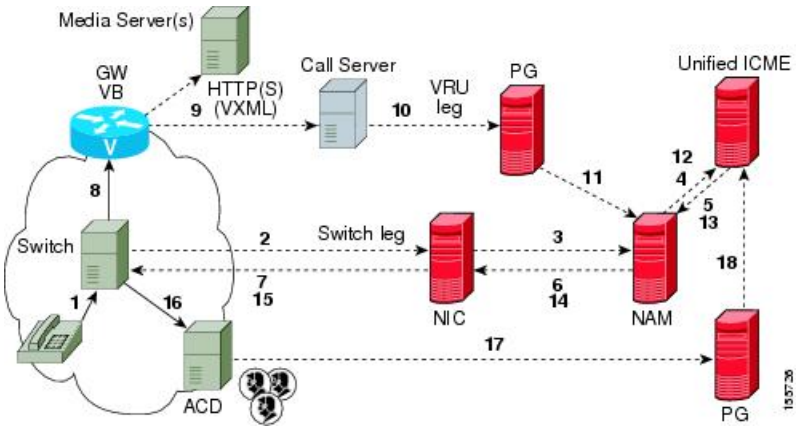
In this call flow model, Unified CVP is deployed as a Network VRU at the NAM. The Unified CVP IVR Service in the Operations Console works with the Voice Gateway to act as the VRU. The VRU voice treatment is provided at the Voice Gateway and can include ASR/TTS. (This call flow model is used when Unified CVP is connected to the NAM.)

The NIC interfaces to the TDM switch to transfer calls to Unified CVP for VRU treatment and to queue and transfer calls using a VRU Type 7 call flow.

Note Use this call flow model only if the PSTN to which the NIC is connected can transport a Correlation ID when it transfers a call. If this is not the set up you are using, then use the Type 8 VRU-Only Call Flow Model for ICMH, on page 55. The Unified CVP SIP Service is part of this call flow model.

The following figure shows the Type 7 VRU-only call flow model network VRU for ICMH. In the figure, solid lines indicate voice paths and dashed lines indicate signaling paths.

Figure 13: Type 7 VRU-Only Call Flow Model Network VRU for ICMH



Note

- For simplicity, the figure does not illustrate a call flow model for redundancy and failover.
- The numbers in the figure indicate call flow progression.
- Set the Network VRU Type to Type 7. There is no difference between these two types except that Type 7 causes ICME to explicitly inform Unified CVP when it is about to transfer the call away from Unified CVP. (Most customers use Type 7.)
- The Network VRU names (where applicable), correlation IDs, and the ECC variable configurations must be identical on the NAM and CICM. All Labels must also be duplicated, although their routing clients will be different.
- Use the SendToVRU node of CICM Script Editor to connect the call to the Network VRU.

Related Topics

Type 8 VRU-Only Call Flow Model for ICMH, on page 55

Set Up Type 3 or 7 VRU-Only Call Flow Model Network VRU for ICMH

Procedure

Step 1 Perform Steps 1 to 4 of the Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56 procedure.

Step 2 Configure each PG.

On the **NAM**, ICM Configuration Manager, **PG Explorer** tool:

a) Configure each PG to be used for the **VRU Client** leg.
b) Configure a peripheral for each Unified CVP ICM Service to be used as a VRU leg connected to each PG.

For each Unified CVP ICM Service connected to this PG, in the tree view pane, select the applicable PG.

Logical Controller tab, configure:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  For example: `<location>_A` for side A of a particular location

Peripheral tab, configure:

- Peripheral Name: A name descriptive of this VRU peripheral.

  For example: `<location>_<cvp1>` or `<dns_name>`
- Client Type: **VRU**
- Select the checkbox: **Enable Post-routing**

Routing Client tab:

- Name: By convention, use the same name as the peripheral.
- Client Type: **VRU**

Step 3 Define a Network VRU and labels.

On the **CICM**, ICM Configuration Manager, **Network VRU Explorer** tool, define a Network VRU for the VRU leg and labels for reaching the NAM.

Specify the following:

- Type: **3** or **7**
- Name: **cvpVRU**

  Note This name is used by convention. Although any name will do, since it is referenced elsewhere in this document, **cvpVRU** is assumed.

- Define a **Label** for the NAM.
  - Label: Network routing number
  - Type: **Normal**
  - Routing client: Select the INCRP Routing Client from the drop-down list.

Step 4 Define a Network VRU and a label for each NIC.

On the **NAM**, ICM Configuration Manager, **Network VRU Explorer** tool, define a Network VRU and a label for each NIC that is using this VRU.

Specify the following:

- Type: **3** or **7**
- Name: **cvpVRU**

  Note This name is used by convention. Although any name will work, since it is referenced elsewhere in this document, **cvpVRU** is assumed.

- Define a **Label** for each NIC that is using this VRU:
  - Label: Network routing number
  - Type: **Normal**
  - Routing client: Select the Routing Client for that NIC from the drop-down list.

Note Make sure the Network VRU label is identical in the NAM and CICM. The Network VRU Name must be identical as well to avoid confusion.

Step 5 If there will be Routing Scripts on the NAM, define a default Network VRU.

On the **NAM**, ICM Configuration Manager, **System Information** tool, in the General section:

- Define the Default Network VRU: **cvpVRU**

Step 6 Define a default VRU.

On the **CICM**, ICM Configuration Manager, **System Information** tool, in the General section:

- Define a default Network VRU: **cvpVRU**

Step 7 Create the VRU and routing scripts.

On the **CICM**, ICM **Script Editor** tool:

Create the VRU scripts and routing scripts to be used for IVR treatment and agent transfer, as described in other sections of this manual and in the Unified ICME manuals. The VRU scripts are associated with the applicable Network VRU, that is, **cvpVRU**.

Use the ICM Script Editor's SendToVRU node to connect the call to the Network VRU.

Note A RunVRU Script or Queue node is an "implicit" SendToVRU node, although error handling will be easier if the explicit "SendToVRU" node is used.

Step 8 Configure the ECC variables.

On the **NAM** and **CICM**, ICM Configuration Manager, configure the ECC variables.

For more information, see Define Unified CVP ECC Variables, on page 181.

Step 9 Configure dialed numbers and call types.

On the **NAM** and **CICM**, ICM Configuration Manager, configure dialed numbers and call types.

For more information, refer to ICM Configuration Guide for Cisco ICM Enterprise Edition

Step 10 Define customers.

On the **NAM** and **CICM**, ICM Configuration Manager:

a. If necessary, differentiate VRUs (Unified CVPs) based on dialed number.

b. Define customers and their Network VRU.

For more information, see Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189.

Step 11 On Cisco Unified CM, configure Unified CM.

For more information, refer to the Unified CM user documentation.

Step 12 Install and configure the Call Server(s).

In the Operations Console, select **Device Management** > **CVP Call Server**.

Step 13 Configure the ICM Service for each Call Server.

In the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. For each Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a. VRU connection port number.

Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b. Set the maximum length DNIS to the length of the Network Routing Number.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c. Call service IDs: New Call and Pre-routed.

Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab

d. Trunk group IDs: New Call and Pre-routed.

Enter the new and pre-routed call trunk group IDs. Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route.

Configure the number of ports according to the licenses purchased and capacity. Configure each of the numbers used for translation routes. (The “New Call” group is not used since the calls are being sent to the VRU (Unified CVP) after some initial processing by the NIC/Unified ICME.)

e. Check the default values of other settings and change, if desired.

Step 14 Configure the IVR service.

In the Operations Console, select **Device Management** > **CVP Call Server** > **IVR tab** and configure the **IVR Service**.

Check the default values and change, if desired.

Refer to the Operations Console online help for information about other settings you might want to adjust from their default values.

Step 15 (Optionally) Configure the Reporting Server.

In the Operations Console, select **Device Management** > **CVP Reporting Server** > **General** tab and configure the Reporting Server.

a. Configure the Reporting Server.

b. Select a Call Server to associate with this Reporting Server.

c. Check the default values of the Reporting properties and change, if desired.

For more information, refer to Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Related Topics

Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56
Define Unified CVP ECC Variables, on page 181
Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189

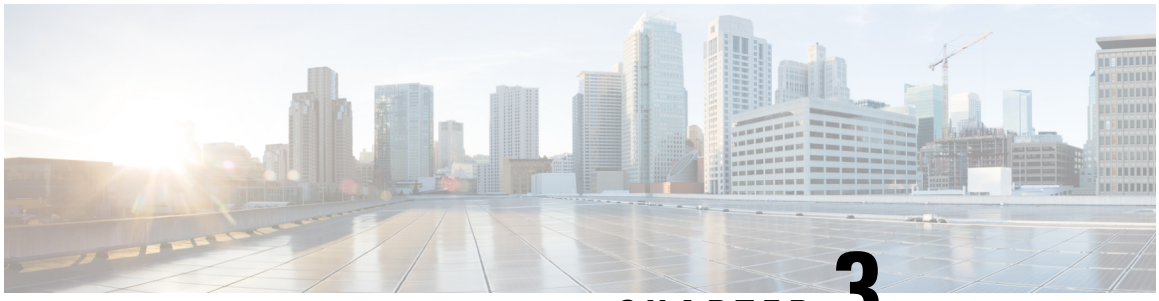
Set Up sendtooriginator Setting in the SIP Service of a Call Server

For the Unified CVP Branch call flow model, incoming calls into the Unified CVP Call Server from a gateway can be automatically routed back to the originating gateway at the branch using the *sendtooriginator* setting in the SIP Service of the Call Server. This setting overrides sending the call to the outbound proxy or to any

locally configured static routes on Unified CVP. If the label returned from Unified ICME for the Unified CVP transfer matches one of the configured patterns in the Unified CVP *sendtoorginator* settings, then the call is routed to the `sip:<label>@<host portion from header of incoming invite>` SIP URL.

Note

- The setting on the IOS gateway for *signaling forward unconditional* is required only if ISDN call variables needs to be available in the Unified ICME scripting environment. If these call variables are not required, then this setting can be omitted. The setting makes the SIP INVITE message larger in terms of bytes due to the extra payload in the message body for GTD variables. If the packet size is significantly greater than 1300 bytes, then TCP transport may be used over UDP transport due to the possibility of a network fragmentation of messages. See the Operations Console online help for more information.
- If the pattern matches the label returned from ICM, then the call is routed to the originating host derived from the incoming calls remote party ID header or contact header.
- The call is sent to the origination gateway if the following statements are true:
  - The remote party ID header is present on the incoming SIP invite.
  - The user agent header of the INVITE indicates an IOS gateway.
  - The pattern matcher on the label is configured for send-to-origin.



CHAPTER 3

Operations Console

Sign In to Operations Console

Before you begin

- Install Operations Console from the Unified CVP software CD.
- Make a note of the password for the default Administrator account that you created during the installation.

Note By default, the Operations Console session expires after 60 minutes. Relogin to Operations Console after the session expires.

Procedure

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

The main Unified CVP window opens.

Step 2 Enter your user ID in the **Username** field.

Enter **`Administrator`**, which is the default user account.

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

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

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

The main Cisco Unified Customer Voice Portal window opens.

Step 4 Check your security policy and, if needed, change the settings to a less restrictive level.

Default security settings can prevent users from using the Operations Console.

Sign Out of Operations Console

From the Operations Console header, click **Sign out**.

The Login page of Unified Customer Voice Portal window appears.

Operations Console Menus and Options

Table 11: Operations Console—Menus and Options

Menu	Options	Use To
System	Control Center	View the status of the Cisco Unified CVP environment in a network control center. View the status and statistics by Device Type or Device Pools, logical groups of devices in the Cisco Unified CVP solution. Initiate Start, Shutdown, or Graceful Shutdown actions on devices in the Control Center.
	Device Pool	Create, modify, and delete device pool names and descriptions for logical groups of devices (for example, all devices located in a geographical region).
	Import System Configuration	Import a previously-saved Operations Console Server configuration file and apply it to the current system.
	Export System Configuration	Save and export all configuration information for the Operations Console Server to a single file on your local computer. You can later use this file to restore an Operations Console Server during disaster recovery.
	Location	Add, edit, synchronize, and delete Unified CM location information.
	SIP Server Groups	Configure server groups for SIP and view Call Server deployment status.
	Web Services	Configure Diagnostic Portal servlet credentials.
	Dialed Number Pattern	Configure the Dialed Number Patterns for a destination. You can define the dialed numbers for the Error Tone, Ring Tone, and other destinations.
	IOS Configuration	

Menu	Options	Use To
		IOS Template Management - Add, Delete, Edit, Copy, and View an IOS template configuration pushed to an IOS gateway. The template contains the IOS commands required for use in a Unified CVP deployment. IOS Template Deployment - Deploy a gateway configuration template to an IOS gateway. The template provisions the gateway and substitutes any variables in the template with the source devices that are chosen when it is deployed.
	Courtesy Callback	Configure allowed and denied dialed numbers, maximum callbacks per number, and Call Server deployment.

Menu	Options	Use To
Device Management	Unified CVP Call Server	Configure Call Server general and infrastructure settings; specify call services settings for each deployment model; associate Call Servers with device pools and the SIP Proxy Server.
	Unified CVP Reporting Server	Configure Reporting Server general and infrastructure settings, associate Reporting Servers with Call Servers, specify reporting properties, and associate Reporting Servers with device pools. Perform Reporting database administration: schedule database backups and purges; manage database and reporting user names and passwords.
	Unified CVP VXML Server	Configure VXML Server general and infrastructure settings; specify primary and backup Call Servers; enable VXML Server reporting and specify VoiceXML data filters; associate VXML Servers with device pools; and transfer scripts to a VXML Server.
	Unified CVP VXML Server (standalone)	Configure VXML Server (standalone) general settings; associate VXML Server (standalone) with device pools; and transfer scripts to a VXML Server (standalone). **Note** A VXML Server (standalone) handles calls that arrive through a VoiceXML gateway. (No statistics are provided when the VXML Server is configured this way.) Also, you cannot configure a database to and capture data from VXML Server (standalone) applications.
	Gatekeeper	Configure a Gatekeeper and add this device to the Device Pool.
	Gateway	Configure Gateway general settings; associate Gateways with device pools; run a subset of IOS commands; view gateway statistics; and transfer files.
	Virtualized Voice Browser	Configure VVB general settings and associate VVB with device pools.
	Device Past Configurations	Review and Restore past device configurations.

Menu	Options	Use To
	Media Server	Configure Media Server general settings and associate a Media Server with device pools. **Note** A Media Server administers the media files that contain messages and prompts callers hear.
	Unified CM	ConfigureUnified CM general settings; specify the URL to theUnified CM Device Administration page; and associate theUnified CM with device pools.
	Unified ICM	Configure ICM Server general settings and associate the ICM Server with device pools.
	SIP Proxy Server	Configure SIP Proxy Server general settings; specify the URL to the SIP Proxy Server Device Administration page; and associate the SIP Proxy Server with device pools.
	Unified IC	Configure CUIS Server general settings and associate the CUIS Server with device pools.
	Device Past Configurations	Review and Restore past device configurations.
	Device Versions	View version information for the Call Server, Reporting Server, VXML Server, and VXML Server (standalone).
User Management	User Roles	Create, modify, and delete user roles. Assign SuperUser, Administrator, or Read Only access privileges to roles.
	User Groups	Create, modify, and delete user groups. Assign roles to user groups.
	Users	Manage Unified CVP users, and assign them to groups and roles.
Bulk Administration	File Transfer	Transfer script files to multiple devices at a time. The **File Transfer** submenu consists of the following options: • Scripts and Media • VXML Applications

Menu	Options	Use To
SNMP	V1/V2c	Configure the SNMP agent that runs on the Unified CVP device to use the V1/V2 SNMP protocol to communicate with an SNMP management station; add and delete SNMP V1/V2c community strings; configure a destination to receive SNMP notifications from an SNMP management station; and associate community strings with the device. The **V1/V2c** submenu consists of the following options: • Community String • Notification Destination
	V3	Configure the SNMP agent that runs on the Unified CVP device to use the V3 SNMP protocol to communicate with an SNMP management station; add and delete SNMP users and set their access privileges; configure a destination to receive SNMP notifications from an SNMP management station; and associate SNMP users with devices. The **V3** submenu consists of the following options: • User • Notification Destination
	System Group	Configure the MIB2 System Group system contact and location settings, and associate the MIB2 System Group with devices. The **System Group** submenu consists of the **MIB2** option.
Tools	SNMP Monitor	Launch the SNMP Monitor application in a new browser window.
	Configure	Display the URLs that launch the SNMP Monitor.
Help	Contents	Display the table of contents for the help system.
	This Page	Display help of the current screen.
	About	Display the version of the help system.

System-Level Operation States

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

Table 12: Description of States Displayed in the Status Window

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

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

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

IP Address Modification

This procedure describes how to change the IP address of the OAMP Server.

Before you begin

You must have completed the IP address change of the following devices in this sequence:

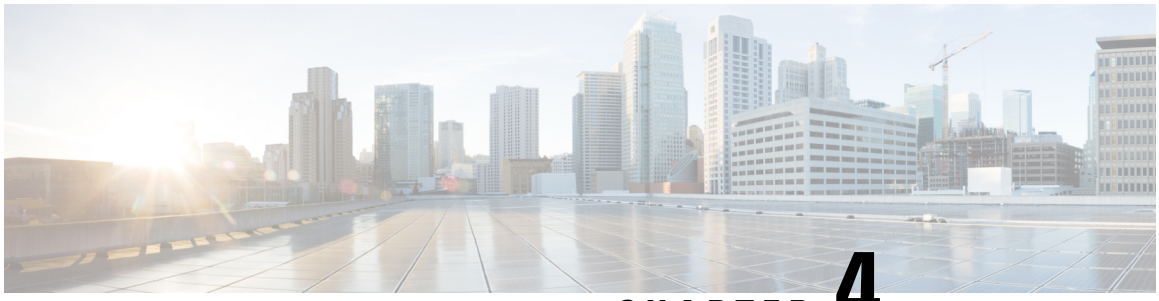
1. Reporting Server
2. VXML Server
3. Call Server

Procedure

Step 1 Configure the new IP address on the OAMP Server network card.

Step 2 Go to **C:\Cisco\CVP\bin\UpdateRMIServerIP\updatermiserverip.bat**. Double-click the batch file to update the IP address in the windows registry and the wrapper.conf file.

Step 3 Restart the server.



CHAPTER 4

Call Server Configuration

Configure Call Server

Procedure

Step 1 Log in to the Operations Console and click **Device Management** > **Unified CVP Call Server**.

Step 2 Click **Add New**.

Note To use an existing Call Server as a template for configuring a new Call Server, select a Call Server from the list of available Call Servers, click **Use As Template**, and perform Steps 3 to 5.

Step 3 Click the **General** tab, enter the field values, and click **Next**. See General Settings, on page 78.

The Services you select in the **General** tab appear as tabs.

Step 4 Click the following tabs and modify the default values of fields, if required:

a) ICM. See ICM Service Settings, on page 79.
b) SIP. See SIP Service Settings, on page 82.
c) IVR. See IVR Service Settings, on page 94.
d) Device Pool. See Add or Remove Device From Device Pool, on page 97.
e) Infrastructure. See Infrastructure Service Settings, on page 98.

Step 5 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and configure the Call Server later.

Related Topics

General Settings, on page 78
ICM Service Settings, on page 79

SIP Service Settings, on page 82
IVR Service Settings, on page 94
Add or Remove Device From Device Pool, on page 97
Infrastructure Service Settings, on page 98

Call Server Settings

General Settings

To add or edit a Call Server, click the **General** tab and enter or modify the field values, as listed in the following table:

Table 13: Call Server General Tab Configuration Settings

Property	Description	Default Value	Range	Restart Required
General				
IP Address	The IP address of the Call Server.	None	Valid IP address	No
Hostname [1]	The hostname/IP address of the Call Server.	None	A valid DNS name, which includes the uppercase and lowercase letters, the numbers 0 through 9, and a dash	No
Description	The description of the Call Server.	None	0 to 1024 characters	No
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. **Note** Enable this option after you configure secure communications.	None	Enabled or Disabled	Yes
Device Version	Lists the Release and Build Number for this device.	Read-only	Read-only	No
Turn On Services				

Property	Description	Default Value	Range	Restart Required
ICM	Enables a Call Server to communicate with an ICM Server. **Note** You must configure an ICM Server before the Call Server can communicate with it.	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. **Note** If you are adding a new Call Server or editing a Call Server and you are using the Call Director or Comprehensive call flow model, configure the SIP service.	None	Not applicable	Yes

[1] If secure communication is being used, ensure that the hostname/IP address specified in the hostname field must match the CN or SAN field value of the TLS certificate being used; or an equivalent mapping of the same exists in DNS or local hosts file. Usage of FQDN (Fully Qualified Domain Name) is also recommended for the same purpose.

ICM Service Settings

Restart the Call Server if you configure the ICM Service on a Call Server for the first time. To configure ICM service settings on a Call Server, on the **ICM** tab, enter or modify the field values, as listed in the following table:

Table 14: ICM Service Configuration Settings

Property	Description	Default Value	Range	Restart Required
General Configuration				

Property	Description	Default Value	Range	Restart Required
VRU Connection Port	The Port Number on which the Intelligent Call Management (ICM) Service listens for a TCP connection from the ICM PIM.	5000	Any valid TCP/IP connection port	Yes
Maximum Length of DNIS	The maximum length of an incoming Dialed Number Identification Service (DNIS). DNIS is a phone service that identifies the number a caller dialed. Your network dial plan has the information for the maximum length of DNIS. The number of DNIS digits from the PSTN must be less than or equal to the maximum length of DNIS field. For example, if the Gateway dial pattern is 1800******, the value of **Maximum Length of DNIS** field should be 10. **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. Valid input for this field is 1 to 99999 characters.	No
Translation Routed DNIS Pool				
Add	Enter a single DNIS number for translation routed calls. Validations for DNIS field are: • The DNIS must be a positive integer and can begin with a zero. • The first and the last values for the DNIS range must be of the same length. • You cannot add a DNIS or DNIS range that already exists or overlaps with DNIS or is in the range of a DNIS.	None	Integer up to 32 characters	No

Property	Description	Default Value	Range	Restart Required
Add a Range	This range is a list of DNIS numbers used for translation of routed calls. Click **Add a Range** and enter the first and the last DNIS numbers 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. The first and the last values for the DNIS range must be of the same length.	None	Integer up to 32 characters	No
Advanced Configuration				
New Call Service ID	Enter a value that 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 prerouted by ICM software.	1	Integer	Yes
Pre-routed Service ID	Enter a value that identifies calls prerouted with either 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 New 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 Pre-routed Trunk Group ID as part of the REQUEST_INSTRUCTION message to ICM.	200	Integer	Yes
Trunk Utilization				
Enable Gateway Trunk Reporting	Check this check box to enable gateway trunk reporting. **Note** While adding or editing a gateway, you can use the optional field, **Trunk Group ID** to customize the trunk group ID for each gateway.	None	Not applicable	No

Property	Description	Default Value	Range	Restart Required
Maximum Gateway Ports	The value used for setting the maximum number of ports that a gateway supports in a CVP deployment. This value is be used to calculate the number of ports to report to the Unified ICM Server for each gateway.	700	1 to 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

SIP Service Settings

Restart the Call Server if you configure SIP service settings for the first time. To configure SIP service settings on a Call Server, on the **SIP** tab, enter or modify the field values, as listed in the following table:

Table 15: SIP Service Configuration Settings

Property	Description	Default	Range	Restart Required
Configuration				
Enable Outbound Proxy	If you want to use a Cisco Unified SIP Proxy Server, in the **Enable outbound proxy** field, select **Yes**. Else, select **No**.	No	Yes or No	Yes
Enable Outbound Proxy	If you want to use a Cisco Unified SIP Proxy Server, in the **Enable outbound proxy** field, select **Yes**. Else, select **No**.	Yes	Yes or No	Yes
Use DNS SRV type query	If you want to use DNS SRV for outbound proxy lookup, select **Yes** in the **Use DNS SRV type query** field. Else, select **No**. **Note** If you enable **Resolve SRV records locally**, select **Yes** to ensure that the feature works properly.	Yes	Yes or No	Yes

Property	Description	Default	Range	Restart Required
Resolve SRV records locally	Check the **Resolve SRV records locally** check box to resolve the SRV domain name with a local configuration file instead of a DNS Server.	Enabled	Yes or No	Yes
Outbound proxy Host	If you selected **Enable Outbound Proxy**, from the **Outbound proxy Host** drop-down list, select an Outbound Proxy Server. **Note** An Outbound Proxy Server is a the SIP Proxy Server that is added to the Operations Console.	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, in the **Outbound SRV domain name/Server group name (FQDN)** text box, enter a fully qualified domain name that is configured on the DNS server. Else, the field contains an SRV configuration file. **Example:** Outbound calls made from CVP SIP service are addressed to the URL of *sip:<label>@<srvfqdn>*. A server, such as Redundant Proxy Server, can route calls using this configuration.	None	Follows the same validation rules as hostname, which includes uppercase and lowercase letters, the numbers 0 through 9, and a dash. 0 to 256 character length.	Yes
DN on the Gateway to play the ringtone	Enter the dialed number configured on the gateway to play the ringtone, which is dedicated VoIP dial peer.	9191	Any valid label	No
DN on the Gateway to play the error tone	Enter a dial number pattern that you want to be played for an error tone. To find out which DN is configured on the gateway to play the error tone, run the **sh** command on the gateway and look for the dial peer that matches the incoming dialed number.	9292	Any valid label	No

Property	Description	Default	Range	Restart Required
DN on the Gateway to play the whisper announcement	Enter a dial number pattern that you want to be played for whisper announcement.	9191919100 If location ID exists, then append the location ID to the dial number.	Any valid label	No
Override System Dialed Number Pattern Configuration	For upgraded devices, check the **Override System Dialed Number Pattern Configuration** check box. For new devices, keep this field unchecked.	Unchecked	The default state of the override check box 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
Local Static Routes				

Property	Description	Default	Range	Restart Required
Static routes for local routing without an outbound proxy - Dialed Number (DN)	In the **Dialed Number (DN)** text box, enter a dialed number. The **Static routes for local routing without an outbound proxy - Dialed Number (DN)** field is used to create a Static Proxy Route Configuration Table. Create static routes if you do not use a SIP Proxy Server. Before adding a local static route, enter a value into both the **Dialed Number (DN)** and **IP Address/Hostname/Server Group Name** fields so that the local static route is complete. Click **Add** to create a proxy route using the DN and the IP address or hostname entered in the **IP Address/Hostname/Server Group Name** fields. The newly created proxy route is added to the list of proxy routes displayed in the box below the **Add** button.	None	Dialed number pattern, destination must be format of NNN.NNN.NNN.NNN or a hostname. See Valid Format for Dialed Numbers, on page 93.	No
IP Address/Hostname/ Server Group Name	Enter an IP address, hostname, or server group name.	None	Valid IP address, hostname, or SRV domain name	No
Advanced Configuration				
General				
Outbound proxy port	Enter a value for port on which the SIP service sends requests to the outbound proxy server.	5060	Any available port number. Valid port numbers are integers between 1 and 65535.	Yes
Outgoing transport type	Select a transport type for outgoing SIP requests. Select **TCP** when reliability is important or packet size is an issue. Select **UDP** in the high availability deployments, because the SIP retry counter and retransmission time settings make the change to a second priority DNS SRV destination occur faster.	TCP	TCP and UDP	Yes

Property	Description	Default	Range	Restart Required
Incoming transport type	The type of transport the SIP Service uses to listen for incoming SIP requests.	UDP+TCP	UDP+TCP	Yes
Time to wait for ICM instructions	The maximum number of milliseconds to wait for ICM to send further instructions.	2000	50 to 5000	No
SIP info tone duration	The maximum number of milliseconds for tone durations sent in when sending Dual Tone Multi-Frequency (DTMF) *8 outpulse digits to the gateway.	100 milliseconds	50 to 2000	No
SIP info comma duration	The maximum number of milliseconds to pause for each comma in the label when sending DTMF to the gateway. **Note** SIP info comma duration is a pause between the *8 and the number. For example, four commas imply four times the value.	100 milliseconds	50 to 2000	No

Property	Description	Default	Range	Restart Required
Generic Type Descriptor (GTD) Parameter Forwarding	Enter a value for passing GTD (UUI) data to ICM in a new call.	UUS	48 characters **Note** • You can extract other parameters in the GTD and send them to ICM. Use commas for multiple values, such as UUS, PRN, GCI. • You can extract any parameter contained in the NSS IAM message.	No

Property	Description	Default	Range	Restart Required
Prepend digits	From the **Prepend digits** drop-down list, select the number of digits that are stripped from the beginning of the incoming Dialed Number (DN) before it is submitted to ICM for the scheduled routing script. **Note** • When Unified ICM returns a label, Unified CVP prepends the stripped digits before initiating the transfer. • If you customized the **Prepend Digits** value manually, in the sip.properties files, set this value in Operations Console after upgrading to ensure that your custom value is not overwritten later. Set the Prepend Digits value and then click **Save & Deploy** to ensure the values of both Operations Console and Call Server devices are in sync.	0	0 to 20 digits	No
UDP Retransmission Count	From the **UDP Retransmission Count** drop-down list, select an option to set the UDP retry count for SIP retries.	3	1 to 6	No
Use Error Refer	Check the **Use Error Refer** check box to enable the SIP Use Error Refer property. Else, keep the check box unchecked.	Checked	Checked or unchecked	No

Property	Description	Default	Range	Restart Required
IOS Gateway Options Dynamic Routing	Check the **IOS Gateway Options Dynamic Routing** check box to identify if resource availability indication on a specific route or service basis is required for real-time routing based on trunk utilization data.	Checked	Checked or unchecked	No
IOS Gateway Options Reporting	Check the **IOS Gateway Options Reporting** check box to identify if trunk utilization reporting and resource availability on a router basis is required after the call is completed.	Checked	Checked or unchecked	No
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.	None	210 characters	No
Parameter	This field is optional for list addition.	None	210 characters	No
Dialed Number (DN) patterns				

Property	Description	Default	Range	Restart Required
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. 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 User Agent header value of the incoming invite 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 postroute 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 originated by TDM and have survivability configured on the pots dial peer.	None	24 characters. See Valid Format for Dialed Numbers, on page 93.	No

Property	Description	Default	Range	Restart Required
Patterns for RNA timeout on outbound SIP calls - Dialed Number (DN)	Creates a 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.	None	24 characters. See Valid Format for Dialed Numbers, on page 93.	No
Timeout	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 ring-no-answer (RNA) timeout setting of the Call Server, it 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.	60 seconds	5 to 60	No
Custom ringtone patterns - Dialed Number (DN)	Specify a custom DN pattern. Click **Add** to add the newly created DN pattern to the list displayed in the box below the Add button. To know which DN is configured on the gateway to play ringtone, run the **sh** command on the gateway and look for the dial peer that matches the incoming dialed number.	None	24 characters. See Valid Format for Dialed Numbers, on page 93.	No

Property	Description	Default	Range	Restart Required
Ringtone media file name	The filename of the ringtone to be played for the respective dialed number. You must save the ringtone media file to the VXML Gateway.	None	0 to 256 characters without spaces. 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				
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.	None	Dialed Number pattern, destination (must be in the form of NNN.NNN.NNN.NNN or a hostname). See Valid Format for Dialed Numbers, on page 93.	No
Survey Dialed Number (DN)	Click **Add** to add the newly created DN to the list. Click **Remove** to delete the selected DN from the list.	None	Alphanumeric characters	No

Note

- The **Call Max Threshold** property specifies the simultaneous active calls that are allowed on a CVP Server instance. Requests above this value are rejected with a *503 Server Unavailable* status.

  The default value is -1, which disables the check performed by this property. The expected range of values is 0 to the maximum number of concurrent sessions supported on CVP Servers for a given Unified CVP release. For more information, see the Section, *Sizing for Unified CVP* in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html.

  To change or update this property, you must manually edit the *sip.properties* file in `\Cisco\CVP\conf` folder.

  Property: #Calls Max Threshold

  Value: SIP.CallsMaxThreshold= -1

  To use the **Call Max Threshold** property, install the appropriate ES specified against CSCvf87136 in https://www-author3.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/ES_MR/ES/ccvp_b_ccvp-eng-es-spl.html.

- To add CauseCode property in the excluded list for Unreachable Table (for example: 47) in `\Cisco\CVP\conf` folder:

  SIP.System.ExcludedCauseCodeFromUnreachableTable =

Related Topics

Valid Format for Dialed Numbers, on page 93

Ring No Answer Settings with SIP

If you use the Unified CVP Ring No Answer (RNA) settings in SIP, ensure that the RNA value is lower than the Unified ICME Agent Desk Setting RNA timeout. The range of RNA value is from 5 to 60 seconds; the default value is 15 seconds.

Unified CVP makes a call to the ringtone service on the VXML gateway. This call is followed by sending the call to the Unified Communications Manager trunk for the agent. During this period, an agent has sufficient time to receive the delivered event after being reserved, and also ensures that Unified ICME reporting is correct in terms of handled time and RNA call disposition calls reporting.

Valid Format for Dialed Numbers

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

- Dialed numbers can be up to 24 characters.
- Use the period (.) or the letter X for single-digit wildcard matching in any combination. Avoid using the letter “T” for wildcard matching.

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

- Use the greater than (>), asterisk (*), or exclamation (!) character as a wildcard for zero or more digits at the trailing end of a dialing number.
- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. When the number of characters is matched equally by more than one wildcard pattern, precedence is given from top to bottom of the configured DN list.

IVR Service Settings

The IVR service creates VXML documents that are used to implement miroapplications 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 microapplications to engage the Unified CVP VXML Server to generate the VXML documents.

The IVR Service plays a significant role in implementing a failover mechanism. This capability is achieved without Automatic Speech Recognition (ASR)/Text To Speech (TTS) Server and VXML Servers. Up to two of each such server are supported, and the IVR Service orchestrates retries and failover between them.

Note Configure the following servers before you configure the IVR service:

- ICM Server
- Media Server
- ASR/TTS Servers
- VXML Server
- Gateway

To configure IVR settings on a Call Server, on the **IVR** tab, enter or modify the field values, as listed in the following table:

Table 16: IVR Service Settings

Property	Description	Default	Range	Restart Required
CVP H.323 Service Configuration				
Heartbeat timeout	Enter the number of seconds after which the heartbeat times out.	120		
IOS Voice Browser Configuration				
Last Access Timeout (seconds)	Enter 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 to 2147483647	No

Property	Description	Default	Range	Restart Required
Media Server Timeout	Enter the number of seconds the Gateway should wait to connect to the HTTP Media Server before timing out.	4	0 to 2147483647	No
Media Server Retry Attempts	Maximum number of times the non-Unified CVP Voice Browser, such as 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 tries the same number of times to retrieve the media from a backup media server before failing and reporting an error. **Note** The backup media server is defined on the gateway as <mediaserver>-backup.	0	0 to 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 tries the same number of times to connect to a backup ASR/TTS server before failing and reporting an error. **Note** The backup ASR and TTS servers are defined on the gateway as asr-<locale>-backup and tts-<locale>-backup.	0	0 to 2147483647	No
IVR Service Timeout	The number of seconds the gateway should wait to connect to the IVR Service before being timed out. This setting controls call results only. The initial NEW_CALL timeout from the Gateway to the IVR Service is controlled through the `fetchtimeout` property within the bootstrap VXML in flash memory on the Gateway.	7	0 to 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 to 2147483647	No
Use Backup ASR/TTS Servers	Click **Yes** if an ASR/TTS Server is unavailable so that the gateway attempts to connect to the backup ASR/TTS server. Else click **No**.	Yes	Yes or No	No
Use Backup Media Servers	Click **Yes** if the Media Server is unavailable so that the gateway attempts to connect to the backup Media Server. Else click **No**.	Yes	Yes or No	No
Use hostnames for default Media/VXML servers	Click **No** to use IP address VXML Server and Media Server. Click **Yes** to use hostnames instead of IP addresses.	No	Yes or No	No
Use Security For Media Fetches	Click **No** to generate HTTP URLs to Media Servers. Click **Yes** to generate HTTPS URLs to Media Servers. **Note** The default option is available for a client using SIP Service and the Media Server is not set to a URL that explicitly specifies an HTTP/ HTTPS scheme.	No	Yes or No	No
Advanced				

Property	Description	Default	Range	Restart Required
Call timeout	The number of seconds the IVR Service waits for a response from the SIP Service before being timed out. Call-timeout should be longer than the longest prompt, transfer, or digit collection at a Voice Browser. On timeout, the call is canceled without affecting other calls. **Note** Having a longer Call-timeout duration is useful even when calls are being stranded, they are not removed from the IVR service until the timeout.	7200	6 seconds or greater	No
ASR/TTS Use the Same MRCP Server	Click this option if your ASR and TTS Servers are on the same computer. **Note** This option helps to minimize the number of MRCP connections on the ASR/TTS Server.	No	Yes or No	No

Device Pool

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

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

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

Add or Remove Device From Device Pool

Procedure

Step 1 From the **Device Management** menu, select a device to add to the Device Pool.

Example:

To add a Call Server to a device pool, select Unified CVP Call Server from the **Device Management** menu.

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

Step 2 Select a device pool from the **Device Pool** list and click **Edit**.

Step 3 On the **Device Pool** tab:

- In the **Available** list box, select one or multiple devices and click the **Add** arrow. The added devices appear in the **Selected** list box.
- To remove the added devices from the **Selected** box, select them and click the **Remove** arrow. The added devices appear in the **Selected** list box.

Step 4 Click **Save & Deploy**.

Note
- Click **Save** to save the changes in Operations Console and add or remove a device from Device Pool later.
- Some edit-device windows have an **Apply** button instead of **Save**. Click **Apply** to copy the configuration to the device.

Infrastructure Service Settings

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, when you change the **syslog** server setting, the changes are applied to all services that write to syslog.

To configure Infrastructure settings, on the **Infrastructure** tab, enter or modify the field values, as listed in the following table:

Table 17: Infrastructure Service Configuration Settings

Property	Description	Default	Range	Restart Required
Configuration: Thread Management				
Maximum Threads	Enter the maximum number of threads allocated in the thread pool that can be shared by all services running as part of a CVP Web Application.	500	100 to 1000	No
Statistics				

Property	Description	Default	Range	Restart Required
Statistics Aggregation Interval	Enter the duration in minutes during which system and service statistics are published to the log file and SNMP events are sent. After the statistics are published, the counters reset and aggregate data for the next interval. Real-time statistics are generated on-demand and have no intervals. Statistics Publishing Interval is used for attributes, such as the number of calls in last interval, the number of transfers in last interval, and the number of HTTP sessions in last interval. **Note** The interval is different than the real time snapshot statistics (for the number of concurrent calls).	30 minutes	10 to 1440 minutes	No
Log File Properties				
Max Log File Size	Enter the maximum size of a log file in megabytes before a new log file is created. **Note** To increase the log file size, go to `C:\Cisco\CVP\conf`, open log4j.xml file and update the MaxFileSize value as shown: `<param name="MaxFileSize" value="10000000"/>` Save the file and restart Call Server to deploy the changes.	10 MB	1 through 100 MB	No
Max Log Directory Size	Enter the 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.	20,000 MB	500 to 500000 The log folder size divided by the log file size must be less than 5000.	No
Configuration: Primary Syslog Settings				
Primary Syslog Server	Enter a hostname or IP address of Primary Syslog Server to send syslog events from a CVP Application.	None	Valid IP address or hostname.	No

Property	Description	Default	Range	Restart Required
Primary Syslog Server Port Number	Enter a 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	Enter a hostname or IP address of the Primary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server is not reachable.	None	Valid IP address or host name.	No
Primary Backup Syslog Server Port Number	Enter a 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	Enter the 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	Enter 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	Enter hostname or IP address of the Secondary Backup Syslog Server to send syslog events from a CVP Application when the Syslog Server is not reachable.	None	Valid IP address or hostname.	No
Secondary Backup Syslog Server Port Number	Enter the port number of Secondary Backup Syslog Server.	None	Any available port number. Valid port numbers are integers between 1 and 65535.	No
License Thresholds				

Property	Description	Default	Range	Restart Required
Critical Threshold	Percentage of licenses in use required to reach Critical licensing state. See License Thresholds, on page 101.	97%	Positive integer less than or equal to 100 and greater than the Warning threshold.	No
Warning Threshold	Percentage of licenses in use required to reach Warning licensing state. See License Thresholds, on page 101.	94%	Positive integer less than the Critical threshold and greater than the Safe threshold.	No
Safe Threshold	Percentage of licenses in use required to reach Safe licensing state. See License Thresholds, on page 101.	90%	Positive integer less than the Warning threshold and greater than 0.	No

Related Topics

License Thresholds, on page 101

License Thresholds

The three thresholds namely safe, warning, and critical describe the percentage of licenses that must be in use to reach their respective licensing state.

Crossing a threshold does not always mean the state changes. For example, if you have 100 licenses and the Safe, Warning, and Critical license thresholds are set to the defaults of 90%, 94%, and 97%, and 89 licenses are in use, licenses are at a Safe level. When the number of licenses in use reaches 94, the license state changes from Safe to Warning level. If one more license is used, the license state remains at the Warning level. If three licenses, which are no longer in use, are released, 92 licenses remain in use and the license state remains at the Warning level. After the licenses in use return to the previous threshold (90), the state changes from Warning to Safe.

IP Address Modification

This section describes how to change the IP address of Call Server, VXML Server, and the Reporting Server. Follow this sequence for changing the IP Address of the devices:

1. Reporting Server
2. VXML Server

3. Call Server
4. OAMP Server

Procedure

Step 1 Select the device from the Operations Console to change the IP address.

Step 2 From the menu bar of the device, select the device and click **Use As Template**.

Step 3 Assign the new IP address to the device and change the Host Name temporarily, which you will revert in Step 8, and click **Save**.

Note Do not click the **Save and Deploy** option until you have changed the physical server to the new IP address.

Step 4 Delete the device from the Operations Console before changing the IP address of the server.

Step 5 Configure the new IP address on the local server.

Step 6 Go to **C:\Cisco\CVP\bin\UpdateRMIServerIP\updatermiserverip.bat** and double-click the batch file to update the IP address in the windows registry and the wrapper.conf file.

Step 7 From the Operations Console, select the device and change the Host Name to the original one. Click **Save and Deploy** for the device. (Restart the server if network-related message is seen).

Step 8 Restart the server.

Note
a. Make sure to change the configuration of VXML Application, Gateway, VVB, ICM PIM, Proxy, and CUCM to reflect the new Call Server IP address.
b. Associate Reporting Server to the Call Server.
c. Delete the existing Media Server and create a new one with the Call Server IP address and deploy the Media Server.

What to do next

Change the IP address of the OAMP Server.

Graceful Shutdown of Call Server or Reporting Server

As a local administrator, you can use the following procedure to gracefully shut down the Call Server or Reporting Server services from the CLI.

Procedure

Step 1 Log in to the CVP Call Server box.

Step 2 Go to the `%CVP_HOME%\bin\ServiceController` folder.

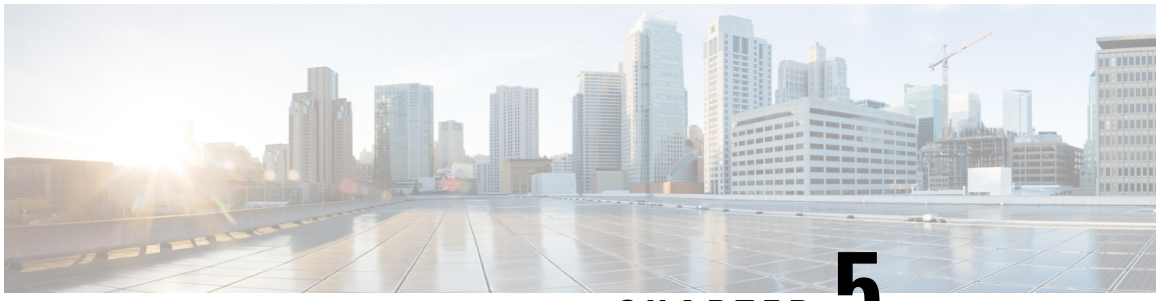
Step 3 Run the `service-controller.bat` file.

Step 4 Enter the administrator credentials, service name, and IP address details at the prompt:

```
CALLSERVER-HOSTNAME: <Hostname of the Call Server>
CALLSERVER-USERNAME: <Username of the Call Server>
CALLSERVER-PASSWORD:  <Password of the Call Server>
SERVICE-NAME: <Name of the service to shutdown gracefully('callserver' for Call Server or
'reportingserver' for Reporting Server)>
REPORTINGSERVER-HOSTNAME: <Hostname of the Reporting Server>
```

Note
- If the CVP Call Server is in domain, ensure that you provide the IP address or the Fully Qualified Domain Name (FQDN).
- Only the users with the appropriate permissions and access rights can perform the above procedure. The user must be part of a specific domain or have administrative privileges on the server.

Note
- To shut down the Reporting Server gracefully, ensure that the CVP Call Server is up and running.
- To shut down the Reporting Server gracefully, provide the hostname or IP address of the Call Server and the IP address of its associated Reporting Server in the respective entries.
- If you have specified an IP Address instead of a hostname, then ensure that the IP address is in the CN or SAN fields of the SSL certificate of that host.



CHAPTER 5

VXML Server Configuration

Configure VXML Server (Standalone)

The Unified CVP VXML Server is a J2EE-compliant application server that provides a complete solution for rapidly creating and deploying dynamic VoiceXML applications. You can install the Unified CVP VXML Server as a standalone component, without the Call Server component. The Unified CVP VXML Server (Standalone) is designed to handle self-service VoiceXML applications.

Procedure

Step 1 On the Unified CVP Operations Console, select **Device Management** > **Unified CVP VXML Server (standalone)**.

Step 2 Click **Add New** to add a new VXML Server (standalone) or click **Use As Template** to use an existing template to configure the new VXML Server (standalone).

Step 3 Click the following tabs and configure the settings based on your call flow:

a) **General** tab. For more information, see General Settings, on page 114.

b) **Device Pool** tab. For more information about adding, deleting and editing device pool, see Add or Remove Device From Device Pool, on page 97.

Step 4 Click **Save** to save the settings in the Operations Server database. Click **Save and Deploy** to deploy the changes to the VXML Server page.

Related Topics

General Settings, on page 114
Add or Remove Device From Device Pool, on page 97

Configure VXML Server

Beginning with Unified CVP 11.5(1) Release, the Call Server IVR service is moved to the VXML Server. As a result, the VXML Server now handles the creation of VXML pages that implement the Unified CVP microapplications. To configure the IVR settings on VXML Server, on the IVR tab, see IVR Service Settings, on page 94.

Before you begin

- Obtain the hostname or IP address of the VXML Server during the installation of the Cisco Unified Customer Voice Portal (CVP) software.
- Install and configure at least one Call Server. To install Call Server, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*. To configure a Call Server, see Configure Call Server, on page 77.

Note Do not install a Call Server if you are adding a Unified CVP VXML Server (standalone).

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

Procedure

Step 1 Log in to the Operations Console and click **Device Management** > **Unified CVP VXML Server**.

Step 2 Click **Add New**.

Note To use an existing VXML Server as a template for configuring a new VXML Server, select a VXML Server from the list of available VXML Servers. Click **Use As Template**, and perform Steps 3 to 5.

Step 3 Click the following tabs and modify the default values of fields, if necessary:

a) General. See General Settings, on page 114.
b) Configuration. See Configuration Settings, on page 116.
c) Device Pool. See Add or Remove Device From Device Pool, on page 97.
d) Infrastructure. See Infrastructure Service Settings, on page 117.

Step 4 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and configure the VXML Server later.

Step 5 Restart the following services:

- Cisco CVP VXML Server
- Cisco CVP WebServicesManager
- Cisco CVP Call Server

Related Topics

IVR Service Settings, on page 94
Configure Call Server, on page 77
General Settings, on page 114
Configuration Settings, on page 116
Add or Remove Device From Device Pool, on page 97
Infrastructure Service Settings, on page 98

Configure VXML Server (Standalone) with ICM Lookup Call Flow Model

The following procedure describes how to configure the Unified CVP VXML Server (standalone) with ICM Lookup call flow model.:

Procedure

Step 1 Copy the following files from the Unified CVP VXML Server CD to the gateway flash memory using tftp:

CVPSelfService.tcl

critical_error.wav

For example:

copy tftp: flash:CVPSelfService.tcl

copy tftp: flash:CVPSelfServiceBootstrap.vxml

copy tftp: flash:critical_error.wav

Step 2 Define the Unified CVP VXML Server applications on the gateway. The following lines show an example configuration:

```
service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
!
service [gateway application name] flash:CVPSelfService.tcl
param CVPBackupVXMLServer 12.34.567.890
param CVPSelfService-port 7000
param CVPSelfService-app [name of application on the VXML Server, exactly how it appears]
param CVPPrimaryVXMLServer 12.34.567.891
```

Note CVPSelfService is required. Backup server is optional. For Tomcat Application Server, set the port to 7000.

After completing the gateway configuration, run the following to load and activate the applications:

```
call application voice load CVPSelfService
call application voice load [gateway application name]
```

Step 3 Define a dial-peer for the gateway application, for example:

```
dial-peer voice [dial-peer unique ID] voip /* for IP originated call */
service [gateway application name]
incoming called-number [dialed number]
dtmf-relay rtp-nte
codec g711ulaw
!
dial-peer voice [dial-peer unique ID] pots /* for TDM originated calls */
service [gateway application name]
incoming called-number [dialed number]
direct-inward-dial
```

Step 4 Optionally, create another dial peer to do transfers using the Unified ICME label that is returned.

Step 5 Create the application in Call Studio. In the Call Studio application, the ReqICMLabel has two exit states: error and done. The done path grabs a transfer element to transfer the caller to that label. The gateway needs another dial peer to transfer the label it gets from this process (see Step 4). If you want to do real transfers, you must have the transfer element set up inside the Call Studio application.

Step 6 Drag the ReqICMLabel element onto the application created in Call Studio and configure it.

Note This step is necessary to obtain a label from Unified ICME. For more information, see Pass Data to Unified ICME, on page 201.

Step 7 Save and deploy the application from Call Studio using the VoiceXML Service on the Operations Console.

Step 8 Install the Call Server, selecting only the Core Software component.

Step 9 Configure the Unified CVP VXML Server to communicate with the Call Server through the Operations Console.

Step 10 Transfer the application using File Transfer to the Unified CVP VXML Server. This automatically deploys the application on the selected Unified CVP VXML Server.

Related Topics

Pass Data to Unified ICME, on page 201

Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup)

The following procedure describes how to configured Unified CVP VXML Server (standalone) call flow model:

Procedure

Step 1 Copy the following files from the Unified CVP VXML Server CD to the gateway flash memory using tftp:

CVPSelfService.tcl

critical_error.wav

For example:

```
copy tftp: flash:CVPSelfService.tcl
copy tftp: flash:CVPSelfServiceBootstrap.vxml
copy tftp: flash:critical_error.wav
```

Step 2 Define the Unified CVP VXML Server applications on the gateway. The following lines show an example configuration:

```
service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
!
service [gateway application name] flash:CVPSelfService.tcl
param CVPBackupVXMLServer 10.78.26.28
param CVPSelfService-port 7000
param CVPSelfService-app [name of application on the VXML Server, exactly how it
appears]
param CVPPrimaryVXMLServer 10.78.26.28
```

Note CVPSelfService is required. Backup server is optional. For the Tomcat Application Server, set the port to 7000.

After completing the gateway configuration, run the following to load and activate the applications:

```
call application voice load CVPSelfService
call application voice load [gateway application name]
```

Step 3 Define a dial-peer for the gateway application, for example:

```
dial-peer voice [dial-peer unique ID] voip /* for IP originated call * /
service [gateway application name]
incoming called-number [dialed number]
dtmf-relay rtp-nte
codec g711ulaw
!
dial-peer voice [dial-peer unique ID] pots /* for TDM originated calls */
service [gateway application name]
incoming called-number [dialed number]
```

```
direct-inward-dial
```

Step 4 Create the application in Call Studio. This application *must* have the same name as the CVPSelfService-app defined in the gateway configuration above.

Step 5 If there is an Operations Console, save and deploy the Call Studio application locally. Create a Unified CVP VXML Server (Standalone) configuration, and upload and transfer the application script file to the required Unified CVP VXML Server or Unified CVP VXML Server (standalone).

Note See User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

Step 6 If Operations Console is not deployed, save and deploy the Call Studio Application to the desired installed Unified CVP VXML Server. Then, on the Unified CVP VXML Server, run the deployallapps.bat file (`c:/Cisco/CVP/VXMLServer/admin directory`).

Note See User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

Sample Gateway Configuration

Unified CVP VXML Server:

```
application
 service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
 service HelloWorld flash:CVPSelfService.tcl
 param CVPBackupVXMLServer 10.78.26.28
 param CVPSelfService-app HelloWorld
 param CVPSelfService-port 7000
 param CVPPrimaryVXMLServer 10.78.26.28
dial-peer voice 4109999 voip /* for IP originated call */
 service HelloWorld
 incoming called-number 88844410..
 dtmf-relay rtp-nte
 codec g711ulaw
 dial-peer voice 4109999 voip /* for TDM originated call */
 service HelloWorld
 incoming called-number 88844420..
 direct-inward-dial
```

Takeback and Transfer in VoiceXML Scripts

Unified CVP provides the following takeback and transfer methods that you invoke from a VoiceXML script:e

- Two B-Channel Transfer (TBCT) - A call transfer standard for ISDN interfaces. This feature enables a Cisco voice gateway to request an NI-2 switch to directly connect two independent calls. The two calls can be served by the same PRI or by two different PRIs on the gateway.
- Hookflash Relay - A brief interruption in the loop current that the originating call entity (PBX or Public Switch Telephone Network switch) does not interpret as a call disconnect. Instead, once the PBX or Public Switch Telephone Network switch senses the hookflash, it puts the current call on hold and provides a secondary dial tone, which allows Unified CVP VXML Server to transfer the caller to another destination.

- SIP Refer - VoiceXML applications can use a SIP REFER transfer instead of a blind or bridged transfer. This allows Unified CVP to remove itself from the call, to free up licensed Unified CVP VXML Server ports. Unified CVP cannot run further call control or IVR operations after the label has been run.

Configure Two B-Channel Transfer

This procedure describes now to configure Two B-Channel Transfer (TBCT) with Unified CVP from a VoiceXML script.

Procedure

Step 1 Configure the originating gateway for TBCT call transfer.

Step 2 Locate the following files on the Unified CVP VXML Server and copy them to flash memory on the gateway, using the tftp command:

en_holdmusic.wav

en_pleasewait.wav

survivability.tcl

CVPSelfService.tcl

CVPSelfServiceBootstrap.vxml

Step 3 Add the following lines to the gateway:

```
service takeback flash:survivability.tcl
param icm-tbct 1
```

Step 4 Configure the CVPSelfService application, as follows:

```
service [gateway application name] flash:CVPSelfService.tcl
param CVPBackupVXMLServer 10.78.26.28
param CVPSelfService-port 7000
param CVPSelfService-app [name of application on the VXML Server, exactly how it appears]
param CVPPrimaryVXMLServer 12.34.567.891
```

Note CVPSelfService is required. Backup server is optional. For Tomcat Application Server set the port to 7000.

Step 5 From command line mode:

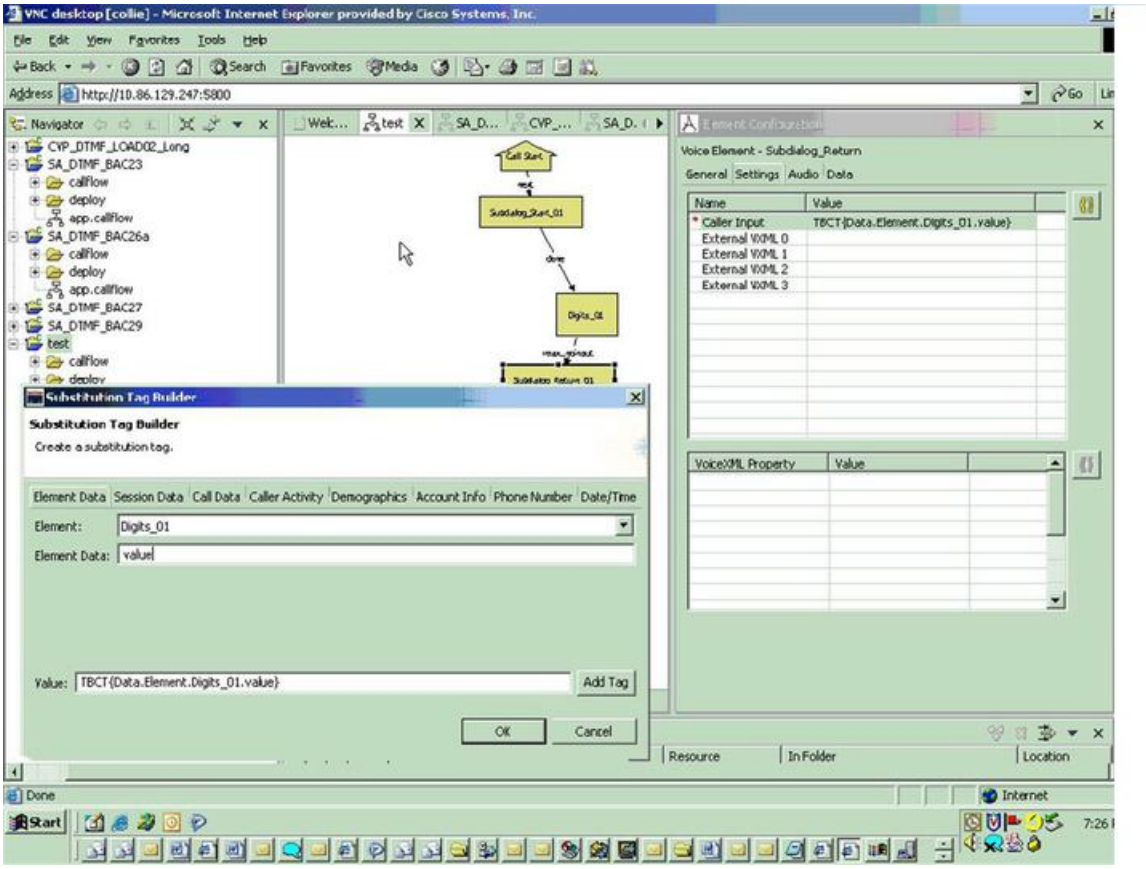
```
call application voice load takeback
call application voice load CVPSelfService
```

Step 6 Specify the target destination for the TBCT transfer either by entering the number manually, or dynamically by using caller input.

a) Manually. In the SubdialogReturn node in the Unified CVP VXML Server application, next to Caller Input in the Settings Tab, enter **TBCT<target_destination_number>**, where *target_destination_number* is the target destination of the TBCT transfer. For example:

TBCT8005551212

b) Dynamically. The target destination is created dynamically using input entered by the caller during the call. Click the **Substitution** icon next to the Caller Input variable and select substitution values. For example:



Configure Hookflash Relay

The following procedure describes how to configure Hookflash Relay for use with Unified CVP from VoiceXML scripts.

Procedure

Step 1 Configure the originating gateway for Hookflash Relay call transfer.

Step 2 Locate the following files on the Unified CVP VXML Server and copy them to flash memory on the gateway.

en_holdmusic.wav

en_pleasewait.wav

survivability.tcl

en_0.wav en_1.wav

en_2.wav en_3.wav

en_4.wav

en_5.wav

en_6.wav

en_7.wav

en_8.wav

en_9.wav

en_pound.wav

en_star.wav

Step 3 Add the following lines to the gateway:

```
service hookflash flash:survivability.tcl
```

Step 4 If you have not already done so, configure the CVPSelfService application:

```
service [gateway application name] flash:CVPSelfService.tcl
param CVPBackupVXMLServer 10.78.26.28
param CVPSelfService-port 7000
param CVPSelfService-app [name of application on the VXML Server, exactly how it appears]
param CVPPrimaryVXMLServer 10.78.26.28
```

Note CVPSelfService is required. Backup server is optional. For the Tomcat Application Server set the port to 7000.

Step 5 From the command line mode:

```
call application voice load hookflash
call application voice load CVPSelfService
```

Step 6 In the SubdialogReturn node in the Unified CVP VXML Server application, next to Caller Input in the Settings Tab, enter HF8005551212, replacing 8005551212 with the target destination of the hookflash transfer.

The label can also be defined dynamically using digits entered by the caller in conjunction with the Unified CVP VXML Server substitution tags. If the switch requires a pause after the hookflash, insert commas between the HF and the transfer number. Each comma represents 100ms.

Configure SIP REFER

To configure SIP REFER for use with Unified CVP VXML Server from a VoiceXML script, follow this procedure:

Procedure

Step 1 Configure the gateway through the Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup), on page 109 or Configure VXML Server (Standalone) with ICM Lookup Call Flow Model, on page 107 procedure, according to your implementation.

Note The incoming dial-peer running the CVPSelfService application must be a VoIP dial-peer, not a POTS dial-peer.

Step 2 Specify the target destination for the REFER transfer in the Call Studio application by entering the number manually, or dynamically using caller input.

a) Manually — In the SubdialogReturn node in the Unified CVP VXML Server application, next to CallerInput in the Settings tab, enter RF<target_destination_number>, where target_destination_number is the target destination of the REFER transfer. For example, RF8005551212.

b) Dynamically — The target destination is created dynamically using input entered by the caller during the call. Click the **Substitution** icon next to the Caller Input variable and select the substitution values.

Step 3 The following configuration must be added to the gateway configuration for the handoff to survivability.tcl to occur and to send the REFER:

```
service takeback flash:survivability.tcl
```

Related Topics

Configure the Unified CVP VXML Server (Standalone) Call Flow Model (Without ICM Lookup), on page 109
Configure VXML Server (Standalone) with ICM Lookup Call Flow Model, on page 107

VXML Server Settings

General Settings

You can configure settings that identify the 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.

To configure General settings, on the **General** tab, enter or modify the field values, as listed in the following table:

Table 18: VXML Server General Settings

Field	Description	Default	Values	Restart Required
General				
IP Address	The IP address of the VXML Server	None	A valid IP address	No
Hostname[2]	The hostname/IP address of the VXML Server.	None	A valid DNS name, which includes uppercase and lowercase letters, the numbers 0 through 9, and a dash.	No
Description	Enter additional information about the VXML Server.	None	Up to 1024 characters	No

Field	Description	Default	Values	Restart Required
Trunk Group ID	This option is used for Gateway trunk reporting if you checked the **Enable Gateway Trunk Reporting** check box for the Call Server that is associated with this Gateway.	None	300 1 to 65535	No
Location ID	View the location ID for the Gateway.	None	Blank, if not assigned to a system-level configuration location.	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.	None	Checked or unchecked	Yes
Device Version	Lists the release and build number for this device.	Read-only	Read-only	No
Unified CVP Call Servers				
Primary Unified CVP Call Server	The 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 VXML Server
Backup Unified CVP Call Server	The 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 that were added to the Operations Console.	None	Not applicable	Yes—Restart Call Server and VXML Server

[2] If secure communication is being used, ensure that the hostname/IP address specified in the hostname field must match the CN or SAN field value of the TLS certificate being used; or an equivalent mapping of the same exists in DNS or local hosts file. Usage of FQDN (Fully Qualified Domain Name) is also recommended for the same purpose.

Configuration Settings

Use Configuration settings to enable the reporting of Unified CVP VXML Server and call activities to the Reporting Server. When the reporting is enabled, the Unified CVP VXML Server reports on call and application session summary data. Call summary data includes call identifier, start and end time stamps of calls, ANI, and Dialed Number Identification Service (DNIS). Application session-data includes application names, session ID, and session time stamps.

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 that you add in the **Add to Log** element configuration section in Unified Call Studio applications are also included in reporting data. You can also create report filters that define which data is included and excluded from the report.

To add configuration settings on VXML Server, on the **Configuration** tab, enter or modify the field values, as listed in the following table:

Table 19: VXML Server Configuration Settings

Field	Description	Default	Values	Restart Required
Configuration				
Enable Reporting for this Unified CVP VXML Server	Indicates whether the VXML Server sends data to the Reporting Server. If this check box is unchecked, no data is sent to Reporting Server, and reports do not contain any VXML application data.	Checked	Checked or unchecked	No
Enable Reporting for VXML Application Details	Indicates whether VXML application details are reported.	Unchecked	Checked and unchecked	No
Max. Number of Messages	Define the maximum number of reporting messages that are saved in a file if both Primary and Backup Call Servers become unreachable. (Limited by amount of free disk space.)	100,000	Not applicable	Not applicable
VXML Applications Details: Filters				

Field	Description	Default	Values	Restart Required
Inclusive Filters	List of applications, element types, element names, element fields, and ECC variables to include in reporting data.	None	A semicolon-separated list of text strings. The wildcard character, asterisk (*), is allowed within each element in the list. For information about filter syntax and rules, see Inclusive and Exclusive VXML Reporting Filters, on page 122.	Yes
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. The wildcard character, asterisk (*), is allowed within each element in the list. For information about filter syntax and rules, see Inclusive and Exclusive VXML Reporting Filters, on page 122.	Yes

Related Topics

Inclusive and Exclusive VXML Reporting Filters, on page 122

Add VXML Server to Device Pool

See Device Pool, on page 97 and Add or Remove Device From Device Pool, on page 97.

Related Topics

Device Pool, on page 97
Add or Remove Device From Device Pool, on page 97

Infrastructure Service Settings

To configure infrastructure settings, on the **Infrastructure** tab, enter or modify the field values, as listed in the following table:

Table 20: VXML Server Infrastructure Settings

Field	Description	Default	Values	Restart Required
Configuration: Thread Management				
Maximum Threads	The maximum thread pool size in the VXML Server Java Virtual Machine.	300	100 to 1000	Yes
Advanced				
Statistics Aggregation Interval	Interval during which the VXML Server publishes statistics.	30 minutes	10 to 1440 minutes	Yes
Log File Properties				
Max Log File Size	Enter the maximum size of a log file in megabytes before a new log file is created. The log file name follows this format: `CVP.DateStamp.SeqNum.log`. For example: `CVP.2006-07-04.00.log` Every midnight, a new log file is automatically created with a new date stamp. Also, when a log file exceeds the maximum 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 created automatically. **Note** To increase the log file size, go to `C:\Cisco\CVP\conf`, open log4j_vxml.xml file and update the MaxFileSize value as shown: `<param name="MaxFileSize" value="10000000"/>` Save the file and restart VXML Server to deploy the changes.	10 MB	1 through 100 MB	Yes

Field	Description	Default	Values	Restart Required
Max Log Directory Size	Enter the 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 to 500000 MB • The value of Max Log File Size must be less than Max Log Directory Size. • The value of the Max Log File size must be greater than 1. • The value of Max Log directory Size or Max Log File Size must not 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
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

Field	Description	Default	Values	Restart Required
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 is not reachable.	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

Enable Active and Standby VXML Server

This feature enables failover mechanism for VXML Servers.

If the active VXML Server fails, then the configured backup VXML Server takes over.

Configuration in CVP

Enable the active/standby VXML Server feature in CVP by modifying the sip.properties.

```
SIP.UseBackupIVRSS=true
```

Configuration in Gateway

Enable the active/standby VXML Server feature in Gateway by configuring a backup VXML server.

Example:

If the active VXML Server's hostname is *Callserver1* with the IP address 10.1.1.1 and the backup VXML Server's hostname is Callserver2 with the IP address 10.2.2.2, then the backup VXML Server is configured as:

```
service bootstrap flash:bootstrap.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
  param Callserver1  10.1.1.1
  param Callserver1-backup 10.2.2.2
```

Configuration in Cisco VVB

Enable the active/backup VXML Server feature in Cisco VVB by configuring a backup VXML server.

This can be done using CLI command *utils vvb add host-to-ip <hostname> <ip_address>*

Example

```
utils vvb add host-to-ip Callserver1 10.1.1.1

utils vvb add host-to-ip Callserver1-backup 10.2.2.2
```

Voice XML Service

The VoiceXML Service provides Unified ICME call control capabilities and data to the Reporting Service.

The VoiceXML Service

- Resides outside of the Call Server that gives call control capabilities to the Standalone Mode.
- Is the connection between the VXML Server and the ICM Service that feeds data to the Reporting Service.
- In a Standalone Mode with ICM Lookup deployment:
  - Interacts with the VXML Server and the ICM Service to do call control piece
  - Interacts with VXML Server and Reporting Service to populate the Reporting database.

Note For more information, see Pass Data to Unified ICME, on page 201.

Related Topics

Pass Data to Unified ICME, on page 201

VXML Server Reporting

VXML Server applications can function in a wide range of paradigms, from the VXML Server virtually controlling the entire user interaction to performing individual interactions on a scale similar to that of the Unified CVP micro-applications. Between these extremes, you can design the VXML Server applications to implement specific transactions. For example, in a banking application a transaction can consist of all the user interactions required to successfully complete a balance transfer or a telephone bill payment. The high-level menus which the user can use to select a particular type of transaction is controlled by the Unified ICME routing script, using standard Unified CVP micro-applications, such as Menu and Play Media. Once a particular transaction type is chosen, the Unified ICME routing script issues an External VoiceXML micro-application to invoke the appropriate VXML Server application which implements that transaction type. Once the VXML Server application completes, control returns to the Unified ICME routing script for further menus. Typically, audit information about the transaction is returned, and can be stored in the Unified ICME database. It is also determines whether the transaction was successful, or it needs to be transferred or queued to an agent, and so on.

While Unified ICME VRU Progress reporting capabilities are always in effect, they compliment VXML Server applications most effectively when this transaction-oriented design is used. The customer defines a Unified ICME CallType for each type of transaction, and uses the audit information returned from the VXML Server to determine how to set the Unified ICME's VRUProgress variable. The setting selected dictates how the transaction is counted in the aggregate VRU reporting fields in the CallTypeHalfHour table.

VRU reporting enhancements are described in the Unified ICME 6.0(0) and online help.

Inclusive and Exclusive VXML Reporting Filters

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 the following purposes:

- Save space in the reporting database.
- Preserve messaging communication bandwidth.

VXML Inclusive and Exclusive Filter 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 Inclusive/Exclusive filters can have one of the following syntaxes:
  - `Appname.ElementType.ElementName.FieldName`
  - `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.
- Form element types, element names, and field names that contain alphanumeric characters, underscores, and a space character.
- Use an application name that contains alphanumeric characters and underscores, without a space. For example, `A_aa.B_bb.*C_cc_DD.E_ee_F*` is valid.

VXML Filter Wildcard Matching Examples

Table 21: Examples - VXML Filter Wildcard Matching

Filter	What It Matches
MyApplication.voice.*.*	Matches all voice elements in MyApplication

Filter	What It Matches
.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

Configure Inclusive and Exclusive VXML Reporting Filters

Procedure

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

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

Step 2 Search for a VXML Server.

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 (Optional) Enter an exclusive filter that excludes some of the data specified by the inclusive filter.

Step 8 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 Restart the VXML Server and the primary and backup Call Servers.

Create Policy Based QoS

To create a Windows-policy-based QoS, refer to the Microsoft site.

VXML Server with Unified ICME

This section describes how to integrate VoiceXML and Unified ICME scripts.

Integrate VoiceXML Scripts with Unified ICME Scripts

This section describes how to integrate the Unified CVP VXML Server into the Unified CVP solution. This process involves:

- Creating a Unified ICME script with ECC variables configured for Unified CVP VXML Server.

- Creating a VRU Script to run in the Unified ICME script.

Procedure

Step 1 Specify the URL (remove and port number) of the Unified CVP VXML Server that you want to reach, for example:

http://10.78.26.28:7000/CVP/Server?application=HelloWorld

In the example, **10.78.26.28** is the IP address of the Unified CVP VXML Server, **7000** is the port number, and the application name is HelloWorld. The values are delimited by a colon (:).

Note 7000 is the default port number for a Unified CVP VXML Server. The new port for Unified CVP 4.0 and later is 7000 for Tomcat with Unified CVP VXML Server.

Step 2 In the Unified ICME script, first set the media_server ECC variable to:

http://10.78.26.28:7000/CVP

Step 3 Set the app_media_lib ECC Variable to "..", (literally two periods in quotes).

Step 4 Set the user.microapp.ToExtVXML[0] ECC variable to: application=HelloWorld

Note This example indicates that the Unified CVP VXML Server will run the *HelloWorld* application. To run a different application, change the value of user.microapp.ToExtVXML[0].

Step 5 Set the UseVXMLParams ECC Variable to **N**.

Step 6 Create a Run External Script node within the Unified ICME script with a VRU Script Name value of GS,Server,V.

Note Remember to link this node to the nodes configured in the previous steps.

- The timeout value set in the Network VRU Script should be substantially greater than the length of the timeout in the Unified CVP VXML Server application. Use this timeout only for recovery from a failed Unified CVP VXML Server.
- Always leave the **Interruptible** check box in the Network VRU Script Attributes tab checked. Otherwise, calls queued to a Unified CVP VXML Server application might stay in the queue when an agent becomes available.

Step 7 After you configure the Unified ICME script, configure a corresponding Unified CVP VXML Server script with Call Studio.

The Unified CVP VXML Server script must:

- Begin with a Unified CVP Subdialog_Start element (immediately after the Call Start element)
- Contain a Unified CVP Subdialog_Return element on all return points (script must end with a Subdialog_Return element)
- The Unified CVP Subdialog_Return element must include a value for the call input
- To enable reporting, you must add Data Feed/SNMP loggers

Correlate Unified CVP and Unified ICME Logs with Unified CVP VXML Server Logs

When using the Unified CVP VXML Server option in the Unified CVP solution, you can correlate Unified CVP/Unified ICME logs with VoiceXML logs by passing the Call ID to the Unified CVP VXML Server by URL. Building upon the URL used in the previous example, the URL is as follows:

http://10.78.26.28:7000/CVP/Server?application=Chapter1_HelloWorld&callid=XXXXX-XXXXX-XXXXXX-XXXXXX

Note Unified CVP VXML Server (by default) receives callid (which contains the call GUID), _dnis, and _ani as session variables in comprehensive mode even if the variables are not configured as parameters in the ToExtVXML array. If the variables are configured in ToExtVXML then those values are used. These variables are available to VXML applications as session variables, and they are displayed in the Unified CVP VXML Server log. This change is backwards compatible with the following script. That is, if you have added the following script, you do not need to change it. However, if you remove this script, you save an estimated 40 bytes of ECC variable space .

To configure logging, in the Unified ICME script, use the formula editor to set *ToExtVXML[1]* variable. Set the value of *ToExtVXML[1]* variable to `concatenate("callid=",Call.user.media.id);`

Note

- Always include "callid" when sending the call to the Unified CVP VXML Server using the Comprehensive call flow model. The Call ID can also be used in Unified CVP VXML Server (standalone) solutions.
- When you concatenate multiple values, use a comma for the delimiter.
- The value of ICMInfoKeys must contain RouterCallKey, RouterCallDay, and RouterCallKeySequenceNumber separated by a “-“.

  For example,
  concatenate("ICMInfoKeys=",Call.RouterCallKey,"-",Call.RouterCallDay,"-",Call.RouterCallKeySequenceNumber).

See *Feature Guide - Writing Scripts for Unified Customer Voice Portal* for more information.

Error Codes for VXML Server

The following are some of the error codes that you may see with the VXML Server application:

- Error Code 40 -- System Unavailable

  This is returned if the VXML Server is unavailable (shutdown, network connection disabled, and so forth).

- Error Code 41 -- App Error

  This is returned if a Unified CVP VXML Server application error occurs (For example, a java exception).

- Error Code 42 -- App Hangup

  This is returned if the Hang Up element is used instead of the Unified CVP Subdialog_Return element.

Note If the application is configured correctly, this does not occur.

- Error Code 43 -- Suspended

  This is returned if the Unified CVP VXML Server application is suspended.

- Error Code 44 -- No Session Error

  This is returned when an emergency error occurs (for example, an application is called that has not been loaded in the Unified CVP VXML Server application).

- Error Code 45 -- Bad Fetch

  This is returned when the Unified CVP VXML Server encounters a bad fetch situation. This code is returned when either a .wav file or an external grammar file is not found.

IP Address Modification

This section describes how to change the IP address of Call Server, VXML Server, and the Reporting Server. Follow this sequence for changing the IP Address of the devices:

1. Reporting Server
2. VXML Server
3. Call Server
4. OAMP Server

Procedure

Step 1 Select the device from the Operations Console to change the IP address.

Step 2 From the menu bar of the device, select the device and click **Use As Template**.

Step 3 Assign the new IP address to the device and change the Host Name temporarily, which you will revert in Step 8, and click **Save**.

Note Do not click the **Save and Deploy** option until you have changed the physical server to the new IP address.

Step 4 Delete the device from the Operations Console before changing the IP address of the server.

Step 5 Configure the new IP address on the local server.

Step 6 Go to **C:\Cisco\CVP\bin\UpdateRMIServerIP\updatermiserverip.bat** and double-click the batch file to update the IP address in the windows registry and the wrapper.conf file.

Step 7 From the Operations Console, select the device and change the Host Name to the original one. Click **Save and Deploy** for the device. (Restart the server if network-related message is seen).

Step 8 Restart the server.

Note

a. Make sure to change the configuration of VXML Application, Gateway, VVB, ICM PIM, Proxy, and CUCM to reflect the new Call Server IP address.

b. Associate Reporting Server to the Call Server.

c. Delete the existing Media Server and create a new one with the Call Server IP address and deploy the Media Server.

What to do next

Change the IP address of the OAMP Server.

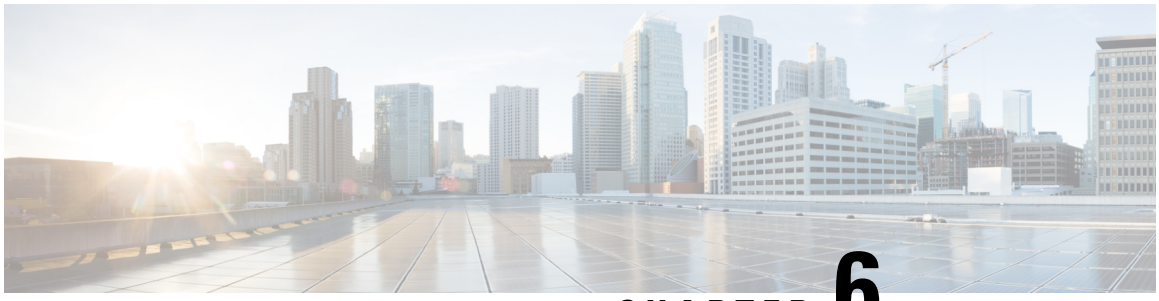
Proxy Settings in VXML Server for Virtual Agent–Voice

For Virtual Agent–Voice to function, the VXML server must be connected to the internet. Enable direct access to the internet or configure HTTP proxy settings in the VXML server. To configure HTTP proxy settings in VXML server, perform the following steps:

1. Open Windows regedit in the VXML server.
2. Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java\Options`.
3. Add the following entries:

```
-Dhttps.proxyHost=<proxy-server hostname or fqdn>
-Dhttps.proxyPort=<port>
```

4. Restart the CVP VXML server from Windows services.



CHAPTER 6

Remote Custom API Server Configuration

Overview

Remote execution of custom code facilitates the execution of custom code and libraries in the remote server outside VXML Server. This feature allows the separation of core IVR application (business logic) and extended business logic (custom code not shipped with the Call Studio application) and operates on a distinct instance that is not shared by Call or VXML Server. This improves system stability and performance because the fundamental services are functioning exclusively for their respective applications. This in turn provides the sufficient resources and reduces the application instability caused by excessive resource utilization. A component is introduced in Call Studio to facilitate the communication and separation between external applications and core applications.

The table below provides the list of elements and whether those elements have the remote execution option or not. For more information on the configuration details, see the Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio.

Element Type	Element Name	Remote Execution Option
Audio	Audio	No
	Custom_Audio	Yes
Call Control	Transfer	No
Cisco	ReqICMLabel	No

Element Type	Element Name	Remote Execution Option
Callback	Callback_Add	No
	Callback_Disconnect_Caller	
	Callback_Enter_Queue	
	Callback_Get_Status	
	Callback_Reconnect	
	Callback_Set_Queue_Defaults	
	Callback_Update_Status	
	Calback_Validate	
	Callback_Wait	
	Callback_Ready	
Commerce	Currency	No
	Currency_with_confirm	
Context	Application_Modifier	No
Date & Time	Date	No
	Date_With_Confirm	
	Time	
	Time_With_Confirm	
Form	Form	No
	Custom Form	Yes
	Form_With_Confirm	No
	Custom Form_With_Confirm	Yes
Integration	Database	Yes
	FTP_Client	No
	REST_Client	No
Math	Counter	No
	Math	
	Set Value	Yes

Element Type	Element Name	Remote Execution Option
Menu	Yes_No_Menu	No
	Custom Yes_No_Menu	Yes
	2_Option_Menu	No
	Custom 2_Option_Menu	Yes
	3_Option_Menu	No
	Custom 3_Option_Menu	Yes
	4_Option_Menu	No
	Custom 4_Option_Menu	Yes
	5_Option_Menu	No
	Custom 5_Option_Menu	Yes
	5_Option_Menu	No
	Custom 4_Option_Menu	Yes
	6_Option_Menu	No
	Custom 6_Option_Menu	Yes
	7_Option_Menu	No
	Custom 7_Option_Menu	Yes
	8_Option_Menu	No
	Custom 8_Option_Menu	Yes
	9_Option_Menu	No
	Custom 9_Option_Menu	Yes
Notification	Alert	No
	Email	

Element Type	Element Name	Remote Execution Option
Number Capture	Digits	No
	Custom Digits	Yes
	Digits_With_Confirm	No
	Custom Digits_With_Confirm	Yes
	Number	No
	Custom Custom Number	Yes
	Number_With_Confirm	No
	Custom Number_With_Confirm	Yes
	Phone	No
	Custom Phone	Yes
	Phone_With_Confirm	No
	Custom Phone_With_Confirm	Yes
Record	Record	No
	Record_With_Confirm	
Video	Video Connect	No
Virtual Agent	Dialogflow	No
	DialogflowCX	
	DialogflowIntent	
	DialogflowParam	
	Transcribe	
	VirtualAgentVoice	
Wxm	WxM_PCS	No
Say it Smart Plugin	Say it Smart Plugin	Yes
Logger	Remote Custom Logger	Yes

Installation and Configurations

Set Up Remote Server

Before you begin

You must set up the Remote Server VM on Windows OS similar to the VXML Server OVA configuration.

Procedure

Step 1 In the Remote Server VM, install OpenJDK 8 (version 1.8.0_271 or higher).

Download OpenJDK at: https://www.openlogic.com/openjdk-downloads?field_java_parent_version_target_id=416&field_operating_system_target_id=436&field_architecture_target_id=All&field_java_package_target_id=All.

Step 2 Configure the `JAVA_HOME` environment variable under **System Variables**, with the respective Java installed path. For example, the path may be `C:\Program Files\OpenLogic\jdk-8.0.372.07-hotspot`.

Step 3 Install Apache Tomcat 9 (version 9.0.60 or higher).

Download Tomcat at: https://tomcat.apache.org/download-90.cgi.

Step 4 Stop the Tomcat server.

Step 5 Copy the `customapis.war` file to the `webapps` folder of Tomcat (for example, `C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps`).

Note The spring boot SDK `customapis.war` file is located at `%CVP_HOME%\util\remoteexecution` folder of the VXML Server. To run the `customapis.war` file, you need Apache Tomcat as the web server.

Step 6 Start the Tomcat server. A folder named `customapis` is created in `%Apache Software Foundation%\Tomcat 9.0\webapps`.

Templates for `web.xml` and `server.xml` are bundled in the `customapis` folder in the following locations:

- `\customapis\WEB-INF\classes\tomcatConfig\conf\web.xml`
- `\customapis\WEB-INF\classes\tomcatConfig\conf\server.xml`

Use these files only as a reference and configure them properly according to your requirements.

The existing `web.xml` and `server.xml` files are available at the following locations:

- `%Apache Software Foundation%\Tomcat 9.0\conf\server.xml`
- `%Apache Software Foundation%\Tomcat 9.0\conf\web.xml`

You can replace or modify the above files.

Running Custom Code Using Remote Server

Procedure

Step 1 Bundle all the custom code that you want to run remotely in a `.jar` file.

Step 2 Copy the `.jar` file and all the dependencies to the `%Apache Software Foundation%\webapps\customapis\WEB-INF\lib` folder.

Step 3 Restart the Tomcat server.

The HTTP port listens at **8080** and the gRPC port listens at **8090**.

You can change the port for gRPC in the `application.properties` file located at `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes`.

Name of the property:

```
#server.grpc.port =8090
```

You can change the port for HTTP in the `server.xml` file located at `%Apache Software Foundation%\Tomcat 9.0\conf`.

Name of the property:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443"
maxParameterCount="1000"
 />
```

For secure connection, configure the port **8080** in the `server.xml` file. For more information, see Enable Security over HTTP (Self-Signed Certificate) in Remote Server.

Note To confirm if the application is running, check the spring boot starter logs in the `cvp.log` file located in the `%Apache Software Foundation%\logs` folder.

Step 4 Check the status of the application at: *http://remote_ip:8080/customapis/actuator/health*. **UP** status denotes that the application is running.

Step 5 To check if the gRPC server is up and running, run the command **netstat -a | findstr 8090**.

Step 6 Configure the **dynamic configuration** and **remote execution** URLs for the Call Studio application in the **Remote URL Settings** tab and redeploy the application.

Step 7 Restart the VXML Server for the changes to be effective.

Step 8 To run the loggers remotely, see the *Loggers* chapter in the Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio.

Step 9 In a failure scenario:

a) Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.

b) To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.

Remote Server Application Properties

The following table lists the properties in the `application.properties` file that is located at `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes`.

Property Name	Usage
loggerPath = C:\\<any folder>\\CustomLogger	Specifies the path for running the application loggers in the remote server.
server.grpc.port = 8090 server.grpc.keyStorePath = C:\\Program Files\\OpenLogic\\jdk-8.0.372.07-hotspot\\jre\\lib\\security\\cacerts	Specifies the port and keystore path configured for gRPC.
server.grpc.keyStoreType = JCEKS	Specifies the KeyStoreType for gRPC connection.
server.grpc.keyAlgorithm = SunX509	Specifies the key algorithm used.
server.grpc.transport = TLS	Specifies the incoming secure protocol.
server.grpc.outgoing.secure.Transport = TLS	Specifies the outgoing secure protocol.
server.grpcciphers = TLS_RSA_WITH_AES_128_CBC_SHA	Colon (;) seperated secure ciphers, for example TLS_RSA_WITH_AES_128_CBC_SHA.
server.grpctlsv1dot2Enabled = true	Secure TLS versions flags, for example TLSv1.
server.grpc.protocol = TLS	Specifies the secure protocol used.
server.grpc.useClientAuth = true	Specifies whether a client certificate is needed or not.
server.grpc.enableRemoteAuthentication = false	Specifies whether gRPC authentication is needed or not.
server.grpc.maxAllowedRequests = 1000	Specifies the maximum allowed calls at a time.
restapi.security.enabled = false	Specifies whether HTTP authentication is needed or not.

Heartbeat Settings in VXML Server

The heartbeat mechanism monitors each remote endpoint URL, be it HTTP or RPC.

For the End point heartbeat control following properties have been added in the `vxml.properties` .

These three properties have been added in the `%CVP_HOME%\conf\vxml.properties`.

- VXML.EndpointHeartbeatEnabled = true
- VXML.EndpointPingInterval = 30000
- VXML.EndpointMaxPingFailure = 1

After you update the `vxml.properties` file, restart the VXML Server.

Configuring HTTP Proxy Settings in VXML Server

To configure HTTP proxy settings in VXML Server, perform the following steps:

Procedure

Step 1 Open Windows Registry Editor (regedit) in the VXML Server.

Step 2 Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java\Options`.

Step 3 Add the following entries:

- `Dhttps.proxyHost=<proxy-server hostname or fqdn or IP>`
- `Dhttps.proxyPort=<port>`

Step 4 Restart the Unified CVP VXML Server from Windows services.

Firewall Port Settings

To allow remote execution of custom code, add the following ports to the firewall exclusion list:

- HTTP port - 8080
- gRPC port - 8090

Run the Launcher Script

A launcher script file helps you execute commands inside the docker container. The launcher script accepts commands, options, and other arguments to modify its behavior.

On the windows host, after downloading the `customapis-docker-windows-<version>.zip` installer, you will find a `launcher.bat` file. To run the launcher script from the `C:/Cisco/customapis` directory, use the following command:

```
launcher.bat <parameter>
```

On the linux host, after downloading the `customapis-docker-linux-<version>.zip` installer, you will find a `launcher.sh` file. To run the launcher script from the `/usr/local/customapis` directory, use the following command:

```
launcher.sh <parameter>
```

Table 22: Parameters to Run the Launcher Script

Parameter	Action
`create`	Creates a directory structure
`load`	Loads the docker image and run the docker container
`run`	Run the docker container

Parameter	Action
`stop`	Stops the existing docker container
`status`	Displays the status of running docker container

Running Custom Code Using Remote Server on Windows

Complete the following procedures to run the custom code using remote server on the windows host.

Load Docker image and Container on Windows Host

Follow the below steps to load the docker image and run the docker container on the windows host machine.

Procedure

Step 1 Download or copy the `customapis-windows-docker-<version>.zip` installer zip file on the windows host.

Step 2 Create the following directory structure on the host: `C:\Cisco\customapis`

Step 3 Extract the archive (.zip) to the following location: `C:\Cisco\customapis`, where you need the Installer to be running from.

Step 4 Open the PowerShell application on the windows host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Note All PowerShell commands in this procedure must be run in Administrator mode from the following location: `C:\Cisco\customapis`.

Step 5 Use the `launcher.bat` file to initiate creation of external mounted folders by providing the `create` parameter by running the following command:

```
PS .\launcher.bat create
```

After you run the command, `external` mount folder gets created at location: `C:\Cisco\customapis`

Step 6 Bundle all the custom code that you want to run remotely in .jar file.

Step 7 Copy the .jar files and all the dependency jars to the `C:\Cisco\customapis\external\lib` folder.

Step 8 Use the `launcher.bat` file to load the container by providing the `load` parameter by running the following command:

```
PS .\launcher.bat load
```

Step 9 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.bat` file to view the status of the container by providing the status parameter by running the following command:

```
PS .\launcher.bat status
```

Step 10 Configure the **dynamic configuration** and **remote execution** URLs for the Call Studio application in the **Remote URL Settings** tab and redeploy the application.

Step 11 Restart the VXML Server for the changes to be effective.

Step 12 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.
- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Windows Host docker container logs: `C:\Cisco\customapis\cvpLogs\cvp.log`.
- Check Tomcat logs: `C:\Cisco\customapis\tomcatLogs`

Configure Secure and Authenticate Calls for Docker Container on Windows Host

Follow the below steps to configure secure call and authenticate calls for docker containers on the windows host machine.

Note The configuration of secure and authenticated setup is a one-time activity and not required for subsequent Docker releases.

Note If the Windows system reboots or Docker restarts, you need to start the Docker container again by running the `launcher.bat` file with the run parameter.

Procedure

Step 1 Bundle all the custom code that you want to run remotely in .jar file.

Step 2 Copy the .jar files and all the dependency jars to the `C:\Cisco\customapis\external\lib` folder.

Step 3 Open the Powershell application on the windows host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Note All PowerShell commands in this procedure must be run in Administrator mode from the following location: `C:\Cisco\customapis`.

Step 4 Use the `launcher.bat` file to start the container by providing the run parameter by running the following command:

```
PS .\launcher.bat run
```

Step 5 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.bat` file to view the status of the container by providing the status parameter by running the following command:

```
PS .\launcher.bat status
```

Step 6 Perform steps **a** to **c** of the Create Credentials for Authentication in Remote Server and Create Keystore Password for Remote Server procedures respectively.

Step 7 Use the following command in PoweShell application to get the `<container_id>`:

```
PS &$Env:DOCKER_HOME\docker ps
```

Step 8 Use the following command in PowerShell application to open the command prompt of running docker container:

```
PS &$Env:DOCKER_HOME\docker exec -it <container_id>  cmd.exe
```

Step 9 Use the following command in the command prompt of the docker container and perform steps **1** to **3** of the Generate Self-Signed Certificate for Remote Custom Server HTTP or gRPC procedure:

```
%JAVA_HOME%\bin\keytool -genkey -keyalg RSA -alias customcode_certificate -keystore
C:\Users\ContainerAdministrator\external\security\cacerts -storetype JCEKS -keysize 2048
```

After adding the certificate, close the command prompt terminal of the docker container.

Note If you already have a CA-signed certificate for the host, refer to the steps in the section Import CA-signed Certificate for Remote Server (Docker), on page 148.

Step 10 Use the `launcher.bat` file to stop the container by providing the stop parameter by running the following command:

```
PS .\launcher.bat stop
```

Step 11 Modify the **application.properties** file and **server.xml** file to configure these files with proper values for a secure and authenticated gRPC and HTTP call as provided in the section External Mounted Folders or Files Usage and Location, on page 142.

Step 12 Perform steps **3** to **5** of this procedure again to start the container and view the status of the container.

Step 13 Perform steps **1** to **6** of the Import Self-Signed Certificate of Remote Server in VXML Server for HTTP or gRPC procedure to add the remote server certificate in VXML Server.

Step 14 Perform steps **1** to **7** of the Enable Secure Connection in Call Studio and VXML Server procedure to configure the applications on Call studio and VXML Server for a secure and authenticated call.

Note Refer to the Remote Execution section of the Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studios.

Step 15 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.
- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Windows Host docker container logs: `C:\Cisco\customapis\cvpLogs\cvp.log`.
- Check Tomcat logs: `C:\Cisco\customapis\tomcatLogs`.

Running Custom Code Using Remote Server on Linux

Complete the following procedures to run the custom code using remote server on the Linux host.

Load Docker Image and Container on Linux Host

Follow the below steps to load the docker image and run the docker container on the linux host machine.

Procedure

Step 1 Download or copy the `customapis-docker-linux-<version>.zip` installer zip on the linux host.

Step 2 Create the following directory structure on the host: `/usr/local/customapis`

Step 3 Run the following command to extract the archive (.zip) to the location: `/usr/local/customapis`, where you need the Installer to be running from:

```
$ unzip customapis-docker-linux-<version>.zip
```

Step 4 Run the following command to provide permission to the `launcher.sh` file:

```
$ chmod +x launcher.sh
```

Note Ensure that you have permissions to directory location: `/usr/local/customapis`

Step 5 Open the Terminal application on the linux host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Step 6 Use the `launcher.sh` file to initiate creation of external mounted folders by providing the `create` parameter by running the following command:

```
$ ./launcher.sh create
```

After you run the command, `external` mount folder gets created at location: `/usr/local/customapis`

Step 7 Bundle all the custom code that you want to run remotely in .jar file.

Step 8 Copy the .jar files and all the dependency jars to the `/usr/local/customapis/external/lib` folder.

Step 9 Use the `launcher.sh` file to load the container by providing the `load` parameter by running the following command:

```
$ ./launcher.sh load
```

Step 10 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.sh` file to view the status of the container by providing the status parameter by running the following command:

```
$ ./launcher.sh status
```

Step 11 Configure the **dynamic configuration** and **remote execution** URLs for the Call Studio application in the **Remote URL Settings** tab and redeploy the application.

Step 12 Restart the VXML Server for the changes to be effective.

Step 13 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.

- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Linux Host docker container logs: `/usr/local/customapis/logs/cvp.log`.

Configure Secure and Authenticate Calls for Docker Container on Linux Host

Follow the below steps to configure secure call and authenticate calls for docker containers on the linux host machine.

Note The configuration of secure and authenticated setup is a one-time activity and does not need to be repeated for subsequent Docker releases.

Note If the Linux system reboots or Docker restarts, you need to start the Docker container again by running the `launcher.sh` file with the run parameter.

Procedure

Step 1 Bundle all the custom code that you want to run remotely in .jar file.

Step 2 Copy the .jar files and all the dependency jars to the `/usr/local/customapis/external/lib` folder.

Step 3 Open the Terminal application on the linux host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Step 4 Use the `launcher.sh` file to start the container by providing the run parameter by running the following command:

```
$ ./launcher.sh run
```

Step 5 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.sh` file to view the status of the container by providing the status parameter by running the following command:

```
$ ./launcher.sh status
```

Step 6 Perform steps **a** to **c** of the Create Credentials for Authentication in Remote Server and Create Keystore Password for Remote Server procedures respectively.

Step 7 Use the following command to get the `<container_id>`:

```
$ docker ps
```

Step 8 Use the following command to open the command prompt for running docker container:

```
$ docker exec -it <container_id> /bin/sh
```

Step 9 Use the following command in the command prompt of the docker container and perform steps **1** to **3** of the Generate Self-Signed Certificate for Remote Custom Server HTTP or gRPC procedure:

```
$JAVA_HOME/bin/keytool -genkey -keyalg RSA -alias customcode_certificate -keystore
/usr/local/customapis/external/security/cacerts -storetype JCEKS -keysize 2048
```

Note If you already have a CA-signed certificate for the host, refer to the steps in the section Import CA-signed Certificate for Remote Server (Docker), on page 148.

Step 10 Use the `launcher.sh` file to stop the container by providing the stop parameter by running the following command:

```
$ ./launcher.sh stop
```

Step 11 Modify the **application.properties** file and **server.xml** file to configure these files with proper values for a secure and authenticated gRPC and HTTP call as provided in the section External Mounted Folders or Files Usage and Location, on page 142.

Step 12 Perform steps **3** to **5** of this procedure again to start the container and view the status of the container.

Step 13 Perform steps **1** to **6** of the Import Self-Signed Certificate of Remote Server in VXML Server for HTTP or gRPC procedure to add the remote server certificate in VXML Server.

Step 14 Perform steps **1** to **7** of the Enable Secure Connection in Call Studio and VXML Server procedure for a secure and authenticated call.

Note Refer to the Remote Execution section of the Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studios.

Step 15 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.
- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Linux Host docker container logs: `/usr/local/customapis/logs/cvp.log`.
- Check Tomcat logs: `/usr/local/customapis/logs`.

External Mounted Folders or Files Usage and Location

The following table lists various configuration files and log files being used and their usages for running the docker container with proper config values.

Note Ensure to restart the container after modifying the files for the changes to take effect.

Table 23: External Mounted Folders or Files Usage and Location

File and Location	Usage
.jar file and dependencies • **Linux**: `/usr/local/customapis/external/lib` • **Windows**: `C:\Cisco\customapis\external\lib`	Bundles all the custom code that you want to run remotely in a .jar file. Copy the .jar file and all the dependencies to the `C:\Cisco\customapis\external\lib`folder (Windows) and `/usr/local/customapis/external/lib` folder (Linux)
.class files • **Linux**: `/usr/local/customapis/external/classes` • **Windows**: `C:\Cisco\customapis\external\classes`	Keeps all external classes in the folder location
application.properties • **Linux**: `/usr/local/customapis/external/conf/application.properties` • **Windows**: `C:\Cisco\customapis\external\conf\application.properties`	For grpc Authentication, set the `server.grpc.enableRemoteAuthentication` flag to **true**. For grpc Secure: • set the `server.grpc.secure` flag to **true**. • (For Windows) set the `server.grpc.keyStorePath` to `C:/Users/ContainerAdministrator/external/security/cacerts`. For http authentication, set the `restapi.security.enabled` flag to **true**.

File and Location	Usage
server.xml • **Linux**: /usr/local/customapis/external/conf/tomcatConfig/conf/server.xml • **Windows**: C:\Cisco\customapis\external\conf\tomcatConfig\conf\server.xml	For http Secure Connection, replace the existing connector `<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" />` with the following: `<Connector SSLEnabled="true" acceptCount="1500" ciphers="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256" clientAuth="false" disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool" keyAlias="customcode_certificate" keystoreFile="C:\Users\ContainerAdministrator\external\security\cacerts" keystorePass="changeit" keystoreType="JCEKS" maxHttpHeaderSize="8192" port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true" sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation" sslProtocol="TLS" sslEnabledProtocols="TLSv1.2"/>` **Note** Ensure that you add the following parameters to the connector according to the configurations done for your remote server: • keyAlias • keystoreFile • keystorePass • port

log4j2.xml
• **Linux**:
/usr/local/customapis/external/conf/conf/log4j2.xml
• **Windows**:
C:\Cisco\customapis\external\conf\log4j2.xml
	For enhanced logging, ensure that you change the level of logging from **info** to **debug** as shown below:
	`<Logger name="com.cisco.cvp.customapi" level="debug" additivity="false">`
	`<AppenderRef ref="LogToFile" />`
	`</Logger>`

setenv.bat • **Linux**: /usr/local/customapis/external/conf/setenv.bat • **Windows**: C:\Cisco\customapis\external\conf\setenv.bat	For setting user defined variables for the tomcat service, you can modify the setenv.bat file according to requirement. A pre-configured setenv.bat has already been added to the specific location.

File and Location	Usage
context.xml • **Linux**: `/usr/local/customapis/external/conf/context.xml` • **Windows**: `C:\Cisco\customapis\external\conf\tomcatConfig\conf\context.xml`	For adding resource, you can modify the context.xml according to your requirement.
Tomcat logs: • **Linux**: `/usr/local/customapis/logs/` • **Windows**: `C:\Cisco\customapis\tomcatLogs` Remote server logs: • **Linux**: `/usr/local/customapis/logs/cvp.log` • **Windows**: `C:\Cisco\customapis\cvpLogs\cvp.log`	For debugging, tomcat catalina logs and remote server logs are available here.
docker-compose.yaml • **Linux**: `/usr/local/customapis/docker-compose.yaml` • **Windows**: `C:\Cisco\customapis\docker-compose.yaml`	For modifying the memory limit and CPU usage specified for the container, use the docker-compose.yaml file.

Upgrade Subsequent Docker Released Images (Windows)

Procedure

Step 1 Open the PowerShell application on the windows host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Note All PowerShell commands in this procedure must be run in Administrator mode from the following location: `C:\Cisco\customapis`.

Step 2 Use the `launcher.bat` file to stop the container by providing the `stop` parameter by running the following command:

```
PS .\launcher.bat stop
```

Step 3 Download or copy the `customapis-windows-docker-<version>.zip` installer zip file on the windows host.

Step 4 Extract the archive (.zip) to the following location and replace the existing files if necessary: `C:\Cisco\customapis`, where you need the Installer to be running from.

Step 5 Use the `launcher.bat` file to load the container by providing the `load` parameter by running the following command:

```
PS .\launcher.bat load
```

Step 6 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.bat` file to view the status of the container by providing the status parameter by running the following command:

```
PS .\launcher.bat status
```

Step 7 Configure the **dynamic configuration** and **remote execution** URLs for the Call Studio application in the **Remote URL Settings** tab and redeploy the application.

Step 8 Restart the VXML Server for the changes to be effective.

Step 9 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.
- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Server or Windows Host docker container logs:

  ```
  C:\Cisco\customapis\cvpLogs\cvp.log
  ```

- Check Tomcat logs:

  ```
  C:\Cisco\customapis\tomcatLogs
  ```

Upgrade Subsequent Docker Released Images (Linux)

Procedure

Step 1 Open the Terminal application on the linux host to run the launcher script. Refer to the Run the Launcher Script, on page 136 section for more information on using the launcher script.

Step 2 Use the `launcher.sh` file to stop the container by providing the `stop` parameter by running the following command:

```
$ ./launcher.sh stop
```

Step 3 Download or copy the `customapis-docker-linux-<version>.zip` installer zip on the linux host.

Step 4 Create the following directory structure on the host: `/usr/local/customapis`

Step 5 Run the following command to extract the archive (.zip) to the location and replace the existing files if necessary: `/usr/local/customapis`, where you need the Installer to be running from:

```
$ unzip customapis-docker-linux-<version>.zip
```

Step 6 Run the following command to provide permission to the `launcher.sh` file:

```
$ chmod +x launcher.sh
```

Note Ensure that you have permissions to directory location: `/usr/local/customapis`

Step 7 Use the `launcher.sh` file to load the container by providing the `load` parameter by running the following command:

```
$ ./launcher.sh load
```

Step 8 Check the status of the application at: `http://remote_ip:8080/customapis/actuator/health`. **UP** status denotes that the application is running.

Use the `launcher.sh` file to view the status of the container by providing the status parameter by running the following command:

```
$ ./launcher.sh status
```

Step 9 Configure the **dynamic configuration** and **remote execution** URLs for the Call Studio application in the **Remote URL Settings** tab and redeploy the application.

Step 10 Restart the VXML Server for the changes to be effective.

Step 11 In a failure scenario:

- Check the error logs in VXML Server: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ErrorLog`.
- To check the lifecycle of an element, check the activity log: `%CVP_HOME%\VXMLServer\applications\{App name}\logs\ActivityLog`.
- Check Remote Server or Linux Host docker container logs:

  ```
  /usr/local/customapis/logs/cvp.log
  ```

- Check Tomcat logs:

  ```
  /usr/local/customapis/logs
  ```

Remote Execution of Custom Logger

Follow the steps to enable remote execution of custom logger on Windows or Linux host:

Before you begin

- For changes specific to the VXML Server, see the **Remote Execution of Custom Logger** section of the Loggers chapter in the Programming Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio.
- Ensure that you run the launcher script. Refer to the section Run the Launcher Script, on page 136 for more information.

Procedure

Step 1 Use the `launcher.bat` file (Windows) or `launcher.sh` file (Linux) stop the container by providing the `stop` parameter by running the following command:

- **Windows**:

  ```
  PS .\launcher.bat stop
  ```

- **Linux**:

```
$ ./launcher.sh stop
```

Step 2 Provide the existing path in the `application.properties` file of the remote server for the `loggerPath`.

For example:

Linux: `loggerPath= /usr/local/customapis/external/CustomLogger`

Windows: `loggerPath= C:/Users/ContainerAdministrator/external/Customlogger`

Step 3 Copy the `VXMLServer\applications\<applicationName>\data` folder to the `loggerPath` in the remote server machine.

For example:

Linux: `loggerPath= /usr/local/customapis/external/CustomLogger`

Windows: `loggerPath= C:/Users/ContainerAdministrator/external/Customlogger`

Step 4 Copy the `VXMLServer\dtds` folder to the `loggerPath` in the remote server machine. The logger folder must contain both `/applications` and `/dtds` folders.

Step 5 Use the `launcher.bat` file (Windows) or `launcher.sh` file (Linux) to run the container by providing the `run` parameter by running the following command:

- **Windows**: `PS .\launcher.bat run`
- **Linux**: `$ ./launcher.sh run`

Step 6 Load the custom logger instances of the remote windows host machine using the `cvp.log` file located at `/usr/local/customapis/logs/cvp.log` (Linux) or `C:\Cisco\customapis\cvpLogs\cvp.log` (Windows).

Generate CA-signed Certificate for Remote Server (Docker)

Note If you already have a CA-signed certificate for the host, follow the steps below. If not, generate a self-signed certificate using the procedure in Generate Self-Signed Certificate for Remote Custom Server HTTP or gRPC, on page 152 and sign it with the relevant Certificate Authority (CA).

Import CA-signed Certificate for Remote Server (Docker)

Procedure

Step 1 To import the root certificate issued by the Certificate Authority, follow the below steps:

a. Copy the `root.pem` file in the following external directory location:

Windows Docker: `C:\Cisco\customapis\external\security\root.pem`

Linux Docker: `/usr/local/customapis/external/security/root.pem`

b. Access the Docker container by running the following command:

Windows Docker: `PS &$Env:DOCKER_HOME\docker exec -it <container_id> cmd.exe`

Linux Docker: `$ docker exec -it <container_id> /bin/sh`

c. Run the following command to import the root certificate into a Java KeyStore (JKS):

Windows Docker:

```
%JAVA_HOME%\bin\keytool -storetype JCEKS -keystore
C:\Cisco\customapis\external\security\cacerts -import -v -trustcacerts -alias root -file
 C:\Cisco\customapis\external\security\root.pem
```

Linux Docker:

```
$JAVA_HOME/bin/keytool -storetype JCEKS -keystore
/usr/local/customapis/external/security/cacerts -import -v -trustcacerts -alias root
-file /usr/local/customapis/external/security/root.pem
```

Step 2 To import the CA-signed certificate to the remote server, follow the below steps:

a. Copy the `host.pem` file in the following external directory location:

Windows Docker: `C:\Cisco\customapis\external\security\root.pem`

Linux Docker: `/usr/local/customapis/external/security/root.pem`

b. Access the Docker container by running the following command:

Windows Docker: `PS &$Env:DOCKER_HOME\docker exec -it <container_id> cmd.exe`

Linux Docker: `$ docker exec -it <container_id> /bin/sh`

c. Run the following command to import the root certificate into a Java KeyStore (JKS):

Windows Docker:

```
%JAVA_HOME%\bin\keytool -storetype JCEKS -keystore
C:\Cisco\customapis\external\security\cacerts -import -v -trustcacerts -alias
customcode_certificate -file C:\Cisco\customapis\external\security\host.pem
```

Linux Docker:

```
$JAVA_HOME/bin/keytool -storetype JCEKS -keystore
/usr/local/customapis/external/security/cacerts -import -v -trustcacerts -alias
customcode_certificate -file /usr/local/customapis/external/security/host.pem
```

Security Configuration

This section covers the steps which need to be configured for enabling a secure connection between the remote server and VXML Server.

Authentication for Remote Server

Create Credentials for Authentication in Remote Server

Before you begin

It is necessary to create credentials for the remote server before activating authentication on the remote server. Use the **add-user-credentials** API both for creating and updating the credentials.

Procedure

In a REST client, for example Postman, enter the following details to create credentials:

a. In the *POST* request, add the URL *http://<remote_machine_IP>:8080/customapis/actionapi/add-user-credentials*.

In the above URL, replace remote server, IP address, and port as needed.

b. In **Request Body**, add *userid* and *secret* as key-value. Make sure the provided *userid* and *secret* to be non-null values.

c. In the **Headers** tab, you must enable **Content-Type** as *application/x-www-form-urlencoded*.

Note After authentication is enabled, you must change the credentials. Use basic authentication if the credentials were updated in the same POST request and the username and password were changed previously.

Enable gRPC Authentication in Remote Server

Procedure

Step 1 Log in to the remote server machine.

Step 2 Navigate to `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes`.

Step 3 Open the `application.properties` file and set the *server.grpc.enableRemoteAuthentication* flag to true.

Step 4 Restart Apache Tomcat Server.

Enable HTTP Authentication in Remote Server

Procedure

Step 1 Log in to the remote server machine.

Step 2 Navigate to `%Apache Software Foundation%\Tomcat9.0\webapps\customapis\WEB-INF\classes`.

Step 3 Open the `application.properties` file and set the *restapi.security.enabled* flag to true.

Step 4 Restart Apache Tomcat Server.

Enabling Authentication in Call Studio and VXML Server

Procedure

Step 1 Go to the Call Studio application.

Step 2 Right-click on the application, which needs to be in secure connection, and select **Properties**.

Step 3 In the **Call Studio Properties** tab, click **Remote URL Settings** .

Step 4 Choose **HTTP** or **RPC** as required.

Step 5 Provide the user ID and password.

Step 6 Save and deploy the Call Studio application and restart the VXML Server.

Secure Connection Setup Between Remote Server and VXML Server

Create Keystore Password for Remote Server

Before you begin

Before activating the security, you must create the remote server keystore password.

Procedure

In a REST client, for example Postman, enter the following details to create credentials:

a. In the *POST* request, add the URL *http://<remote_machine_IP>:8080/customapis/actionapi/add-keystore-password*.

In the above URL, replace remote server, IP address, and port as required.

b. In **Request Body**, add *keyStorePassword* as the *key-value*. Ensure that the provided *keyStorePassword* is a non-null value.

c. In the **Headers** tab, you must enable **Content-Type** as *application/x-www-form-urlencoded*.

Note After authentication is enabled, you must change the credentials. Use basic authentication if the credentials were updated in the same POST request and the username and password were changed previously.

Generate Self-Signed Certificate for Remote Custom Server HTTP or gRPC

Before you begin

It is recommended to change the default keystore password (which is usually 'changeit'). To change the password, run the command: **%JAVA_HOME%\jdk-8.0.372.07-hotspot\jre\bin>keytool -storepasswd -new <newpassword> -keystore ..\lib\security\cacerts -storetype JCEKS -storepass <defaultpassword>**

Procedure

Step 1 Open the command prompt and execute the following command in `cmd.exe` with proper alias: **%JAVA_HOME%\jdk-8.0.372.07-hotspot\jre\bin>keytool -genkey -keyalg RSA -alias customcode_certificate -keystore ..\lib\security\cacerts -storetype JCEKS -keysize 2048**

Step 2 Once you execute the command, answer the questions.

For example:

```
Enter keystore password: *************
What is your first and last name?
  [Unknown]:  CustomRemoteServer----------------→ The CN should same as the FQDN of the
machine
What is the name of your organizational unit?
  [Unknown]:  CCBU
What is the name of your organization?
  [Unknown]:  CISCO
What is the name of your City or Locality?
  [Unknown]:  KA
What is the name of your State or Province?
  [Unknown]:  BLR
What is the two-letter country code for this unit?
  [Unknown]:  IN
Is CN=CustomRemoteServer, OU=CCBU, O=CISCO, L=KA, ST=BLR, C=IN correct?
  [no]:  yes
Enter key password for <customcode_certificate>
        (RETURN if same as keystore password):
done
```

Step 3 Now, you can import the self-signed certificate.

Generate CA-signed Certificate for Remote Server HTTP or gRPC

Note If you already have a CA-signed certificate for the host, follow the steps below. If not, generate a self-signed certificate using the procedure in Generate Self-Signed Certificate for Remote Custom Server HTTP or gRPC, on page 152 and sign it with the relevant Certificate Authority (CA).

Import CA-signed Certificate for Remote Server

Procedure

Step 1 To import the root certificate issued by the Certificate Authority, follow the below steps:

a. Copy the `root.pem` file in the following location: `%JAVA_HOME%\lib\security`

b. Go to directory location `%JAVA_HOME%\jre\bin`.

c. Open the command prompt and execute the following command in `cmd.exe` with proper alias:

```
keytool.exe -storetype JCEKS -keystore ..\lib\security\cacerts -import -v -trustcacerts
 -alias root -file ..\lib\security\root.pem
```

Step 2 To import the CA-signed certificate to the remote server, follow the below steps:

a. Copy the `host.pem` file in the following location: `%JAVA_HOME%\lib\security`

b. Go to directory location: `%JAVA_HOME%\jre\bin`.

c. Open the command prompt and execute the following command in `cmd.exe` with proper alias:

```
keytool.exe -storetype JCEKS -keystore ..\lib\security\cacerts -import -v -trustcacerts
 -alias customcode_certificate -file ..\lib\security\host.pem
```

Generate Remote Server ECDSA Certificate with Open SSL

Before you begin

The Remote Server enables a variant of the Digital Signature Algorithm that are known as an Elliptic Curve Digital Signature Algorithm (ECDSA). Remote Server supports either ECDSA or RSA. RSA remains the default cryptography algorithm. However, looking at the requirements, we can enable or disable ECDSA.

For disabling ECDSA, you must delete the existing ECDSA aliases and generate RSA certificates again.

Procedure

Step 1 Download OpenSSL (64-bit) and install on your remote computer.

Step 2 Add OpenSSL bin path to the Windows environment path variable.

For example, `path=C:\Program Files\OpenSSL-Win64\bin`

Step 3 Go to `C:\Cisco\CVP\conf\security`

Step 4 From the command prompt, run the following command to generate the private keys for the remote server: **openssl ecparam -name prime256v1 -genkey -noout -out remoteserver-private-key.pem**

Step 5 Run the following command to generate the self-signed certificates for the remote server: **openssl req -new -key remoteserver-private-key.pem -x509 -nodes -days 365-out remoteserver-cert.pem**

Step 6 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []: < >
State or Province Name (full name) []: < >
Locality Name (for example, city) []: < >
Organization Name (for example, company) []: < >
Organizational Unit Name (for example, section) []: < >
Common Name (for example, server FQDN or your name) []: < >
Email Address []: < >
Please enter the following extra attributes to be sent with your certificate request:
A challenge password []: < >
An optional company name []: < >
```

Note Enter a period (.) to leave the following fields blank:

- **Common Name**
- **Email Address**
- **Challenge password**
- **An optional company name**

You can generate a certificate after entering all the details.

Step 7 Run the following command to append the keys and certificates in one file: **cat remoteserver-private-key.pem remoteserver-cert.pem > remoteserver-certificate-private.pem**

Step 8 Run the following command to export the certificates to the Remote server: **openssl pkcs12 -export -inkey remoteserver-private-key.pem -in remoteserver-certificate-private.pem -out cert_remoteserver.p12 -name remoteserver_certificate**

```
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 9 Go to `C:\Cisco\CVP\conf\security` and run the following command to delete the existing RSA certificates for the remote server: `C:\Cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias remoteserver-certificate -storepass <CVP keystore password>`

Step 10 Run the following command to import the ECDSA certificates to the keystore: `C:\Cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_remoteserver.p12 -srcstoretype PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias remoteserver_certificate`**Importing keystore cert_remoteserver.p12 to .keystore...**

```
Enter destination keystore password:
Enter source keystore password:
[Storing.keystore]
```

Step 11 Restart the remote server.

Step 12 In the new browser tab, type the following and download the certificates: `https://<remote ip>:8080`

Enable Security over gRPC (Self-Signed Certificate) in Remote Server

Procedure

Step 1 Log in to the remote server machine.

Step 2 Make sure the the self-signed certificate for the remote server machine is generated.

Step 3 Navigate to the `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes` directory.

Step 4 Launch the `application.properties` file and set the **server.grpc.secure** flag to true.

Step 5 Provide the `.keystore` path for the `server.grpc.keyStorePath` flag.

For example: `C:\\Program Files\\OpenLogic\\jdk-8.0.372.07-hotspot\\jre\\lib\\security\\cacerts` (make sure that keystore exists in that machine).

Step 6 Restart the Remote Apache Tomcat server.

Enable Security over HTTP (Self-Signed Certificate) in Remote Server

Procedure

Step 1 Log in to the remote server machine.

Step 2 Ensure that the self-signed certificate for the remote server machine is generated.

Step 3 Navigate to the `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes` directory.

Step 4 Open the `application.properties` file, set the **restapi.security.enabled** flag to true, and save the file.

Step 5 Navigate to the `%Apache Software Foundation%\Tomcat 9.0\conf` directory.

Step 6 Open the `server.xml` file and provide the connector with the port number, and mention the respective keystore password.

For Example:

```
<Connector SSLEnabled="true" acceptCount="1500"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"

clientAuth="false" disableUploadTimeout="true" enableLookups="false"
executor="tomcatThreadPool" keyAlias="customcode_certificate"
keystoreFile="C:\Program Files\Java\jre1.8.0_271\lib\security\cacerts" keystorePass="changeit"
 keystoreType="JCEKS" maxHttpHeaderSize="8192"
port="8080" protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"

sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation" sslProtocol="TLS"
 sslEnabledProtocols="TLSv1.2"/>
```

Step 7 Save the `server.xml` file and restart the remote Apache Tomcat server.

Import Self-Signed Certificate of Remote Server in VXML Server for HTTP or gRPC

To import the certificate:

Procedure

Step 1 Launch the URL `https://<remote_server_IP>:8090/` to download the certificate.

Step 2 Upload the certificate in the `%CVP_HOME%\conf\security` folder where the VXML Server is hosted.

Step 3 Import the certificate using the following command:
%CVP_HOME%\jdk-8.0.372.07-hotspot\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias <any_alias> -file %CVP_HOME%\conf\security\<FQDN_remote_server.cer>

Where, `<FQDN_remote_server.cer>` is the certificate downloaded in step 1, which is named after the FQDN of remote server.

Note Use FQDN instead of IP address for a secure gRPC connection. The common name (CN) of the certificate should be same as the address mentioned in the studio settings.

Step 4 Enter the keystore password when prompted.

Run the **DecryptKeystoreUtil.bat** file located at `%CVP_HOME%\bin` to view the keystore password.

Step 5 Make sure that the connection type in the Call Studio application is changed to HTTP or gRPC accordingly. Also, ensure the **Secure Connection** checkbox is enabled.

Step 6 Save and deploy the Call Studio application and restart the VXML Server.

Enable Secure Connection in Call Studio and VXML Server

Before you begin

Make sure that the Call Studio console is used to establish the necessary secure connection.

Procedure

Step 1 Go to the Call Studio application.

Step 2 Right-click on the application, which needs to be in secure connection, and select **Properties**.

Step 3 In the **Call Studio Properties** tab, click **Remote URL Settings** .

Step 4 Choose **HTTP** or **RPC** as required

Step 5 Click the **Secure Connection** checkbox to provide a secure connection.

Note You must provide FQDN for HTTP and gRPC connection type in the address field for secure connection.

Step 6 For FQDN, add **<IP><space><FQDN(hostname)>** in the `%drivers%\etc\hosts` file in the VXML Server.

Step 7 Save and deploy the application. Restart the VXML Server.

Note The same port cannot be used simultaneously in several applications as secure and non-secure ports.

For example: All the applications utilizing a port on the VXML Server for gRPC must be re-deployed with the same secure or non-secure configurations if the port is used for both secure and non-secure calls.

Note When several remote servers or load end points are added for load balancing, all of those servers must have the same secure or non-secure configurations when used simultaneously. This is because all the added servers have the same remote URL settings.

(Optional) Enabling Mutual TLS for gRPC and HTTP in Remote Server

Follow the steps for each VXML Server.

Procedure

Step 1 Import the certificate for VXML Server in the `RemoteServer java keystore`.

Step 2 For gRPC, in the `application.properties` file, available at `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes`, change the following property to true:

```
server.grpc.useClientAuth = true
```

Step 3 For HTTP, in the `server.xml` file, available at `%Apache Software Foundation%\Tomcat 9.0\conf\server.xml`, change the following property to true:

```
"clientAuth" flag = true
```

Step 4 Restart the Apache Tomcat server.

Monitoring and Serviceability

Spring boot provides enhanced serviceability and has a set of APIs for monitoring and serviceability.

HTTP port listens at **8080** and gRPC port listens at **8090**.

Spring Boot Starter Actuator: *http://<remote_IP>:<Port>/customapis/actuator*. This API provides monitoring facilities around the services:

- **beans**: *http://<IP>:<Port>/customapis/actuator/beans*
- **health-path**: *http://<IP>:<Port>/customapis/actuator/health/{*path}*
- **health**: *http://<IP>:<Port>/customapis/actuator/health*
- **info**: *http://<IP>:<Port>/customapis/actuator/info*
- **shutdown**: *http://<IP>:<Port>/customapis/actuator/shutdown*
- **loggers**: *http://<IP>:<Port>/customapis/actuator/loggers*
- **loggers-name**: *http://<IP>:<Port>/customapis/actuator/loggers/{name}*
- **heapdump**: *http://<IP>:<Port>/customapis/actuator/heapdump*
- **thread dump**: *http://<IP>:<Port>/customapis/actuator/threaddump*
- **Prometheus**: *http://<IP>:<Port>/customapis/actuator/prometheus*

- **metrics-requiredMetricName**: *http://<IP>:<Port>/customapis/actuator/metrics/{requiredMetricName}*
- **metrics**: *http://<IP>:<Port>/customapis/actuator/metrics*
- **scheduled tasks**: *http://<IP>:<Port>/customapis/actuator/scheduledtasks*

To check the health of the application, access the URL: *http://remote_ip:8080/customapis/actuator/health*. The **UP** status denotes that the application is running.

To check the memory used by the application, access the URL: *http://remote_ip:8080/customapis/actuator/metrics/jvm.memory.used*.

To check the CPU usage, access the URL: *http://remote_ip:8080/customapis/actuator/metrics/process.cpu.usage*.

To check the current number of live threads, access the URL: *http://remote_ip:8080/customapis/actuator/metrics/jvm.threads.live*.

To analyze the state of all the threads of an application at a given time, access the URL: *http://remote_ip:8080/customapis/actuator/threaddump*.

A heap dump is a snapshot of all the objects that are in memory in the JVM at a certain moment. It is useful for troubleshooting memory-leak problems and optimising memory usage in Java applications.

To download the heap dump, access the URL: *http://remote_ip:8080/customapis/actuator/heapdump*.

HTTP and gRPC Statistics

To know the statistics of HTTP and gRPC, use the following actuator URL:

/prometheus: *http://remote_ip:8080/customapis/actuator/prometheus*.

HTTP Statistics

HTTP statistics shows the summary of the requests handled along with type, status, and other attributes.

Example

```
# TYPE http_server_requests_seconds summary
http_server_requests_seconds_count{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/actuator",}
 1.0
http_server_requests_seconds_sum{exception="None",method="GET",outcome="SUCCESS",status="200",uri="/actuator",}
 1.095763557
```

gRPC Statistics

gRPC statistics mentioned below represents the total count of gRPC requests handled with attributes. It shows that there is one bidirectional streaming request (BIDI_STREAMING) for the **RemoteVoiceService** method of **com.audium.core.protobuf.RemoteExecutionService** and the response code is "OK".

Example

```
# HELP grpc_server_handled_total Total number of RPCs completed on the server, regardless
of success or failure.
# TYPE grpc_server_handled_total counter
grpc_server_handled_total{grpc_type="BIDI_STREAMING",grpc_service="com.audium.core.protobuf.RemoteExecutionService",
grpc_method="RemoteVoiceService",code="OK",grpc_code="OK",} 1.0
```

VXML Server Statistics

Use the following URL for gRPC registry collection statistics: *http://<IP/hostname of VXML Server>:7000/CVP/Server?stats=true*.

SNMP and Syslog Alerts

The Remote Server application displays SNMP and Syslog alerts when it encounters an exception or error. The alerts contain messages along with the stack trace for monitoring and serviceability of the application.

Following is the sample syslog and SMNP alerts displayed when the class name is not valid.

Syslog Alert

```
98: IP: Oct 05 2023 10:45:40.726 -0700:
%com.cisco.ccbu.infra.serviceability.ServiceabilityManager_VXML-3-VXML_SERVER_SYSTEM_ERROR:
  In application TestSNMP encountered SYSTEM_ERROR_EVENT with message:
'com.cisco.cvp.customaction' is not a valid action element class.
<011 = Level: ERR - error conditions (3)>
```

SNMP Alert

```
Trap OID - 1.3.6.1.4.1.9.9.590 In application TestSNMP encountered SYSTEM_ERROR_EVENT with
 message: 'com.cisco.cvp.customaction' is not a valid action element class.
SNMP    880    trap iso.3.6.1.4.1.9.9.590
```

Similar messages are logged for other scenarios encountered after SNMP and Syslog are properly configured for the VXML Server used.

Create User Credentials for Monitoring in Remote Server

Before you begin:

Ensure that before you activate authentication on the remote server, you must create credentials for it. Use the `add-user-credentials` API to both create and update these credentials. You can now create multiple users for monitoring purposes.

In a REST client, for example Postman, enter the following details to create credentials:

1. In the *POST* request, add the URL *http://<remote_machine_IP>:8080/customapis/actionapi/add-user-credentials*.

   In the above URL, replace remote server, IP address, and port as needed.

2. In Request Body, add *userid* and *secret* as key-value. Make sure the provided *userid* and *secret* to be non-null values.

3. In Request Body, add *admin* as key and value as true. (true is for monitoring credentials and false for normal user credentials)

4. In the Headers tab, you must enable Content-Type as *application/x-www-form-urlencoded*.

Note The above credentials can be used for monitoring .

Note After creating the user credentials for multiple users, modify the `Auth` flag in the `application.properties` file and restart the Tomcat server.

Note For Docker, follow the below steps:

- Stop the container by running the `launcher.bat` file with the stop parameter. Refer to the Run the Launcher Script, on page 136 section for more information.

  ```
  PS .\launcher.bat stop
  ```

- Start the container by running the `launcher.bat` file with the run parameter. Refer to the Run the Launcher Script, on page 136 section for more information.

  ```
  PS .\launcher.bat run
  ```

Remote Server Load Balance Status

A REST endpoint has been implemented to check the load balance status of all the gRPC and HTTP endpoint.

To check for the status of the remote server load balance, use the following URL: *https://<VXML_Server_IP>:7443/CVP/Server?lbstatus=true*. This API provides monitoring facilities around the services.

Logging

VXML Server Configuration for Remote Server

For enhanced VXML logging for custom code, make the required configuration in the VXML Server.

In the `log4j_vxml.xml` file located at `%CVP_HOME%\conf\`, navigate to the **logger** section and add the following **AsyncLogger** tag.

```
<AsyncLogger name="com.cisco.cvp.callserver" level="info" additivity="false">

    <AppenderRef ref="rootUniversalAppender" />

</AsyncLogger>

<AsyncLogger name="io.grpc" level="info" additivity="false">

    <AppenderRef ref="rootUniversalAppender" />

</AsyncLogger>

<AsyncLogger name="com.cisco.cvp.ivr" level="info" additivity="false">

    <AppenderRef ref="rootUniversalAppender" />

</AsyncLogger>
```

You can set the level to **debug** or **info** according to the requirement of logging level.

The log files monitored are:

- `%CVP_HOME%\logs\VXML\CVP <timestamp>.log`
- `%CVP_HOME%\logs\VXML\ERROR <timestamp>.log`

To monitor the health of **RPC end point status**, check the logs in the `VXML\CVP <timestamp>.log` file.

Sample Log

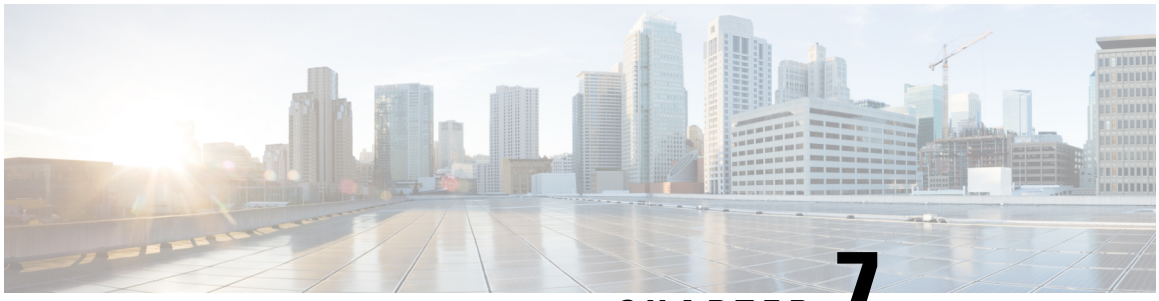
```
RpcEndPoint-6-com.cisco.cvp.callserver.grpc.endpoint.RpcEndPoint:  status of
healthcheckgrpc.health.v1.HealthCheckResponse.ServingStatus.SERVINGEndPoint=
url=<FQDN>/<IP>:8090, statusUrl=cvv, key=<FQDN>:8090:null, status=true
```

Remote Server Configuration for Logging

In the `log4j2.xml` file located at `%Apache Software Foundation%\Tomcat 9.0\webapps\customapis\WEB-INF\classes`, change the level of logging from **info** to **debug** for enhanced logging.

```
<Logger name="com.cisco.cvp.customapi" level="debug"
additivity="false">
<AppenderRef ref="LogToFile" />
</Logger>
```

Log file monitored: `%Apache Software Foundation%\Tomcat 9.0\logs\cvp.log`.



CHAPTER 7

Reporting Server Configuration

Configure Reporting Server

Before you begin

- Configure a Call Server to associate with a Reporting Server. To configure a Call Server, see Configure Call Server, on page 77.

Note You can associate a Call Server with only one Reporting Server.

- Collect the following information about the Reporting Server and Reporting Database during the installation of Unified CVP software:
  - Hostname of the Call Servers that are associated with the Reporting Server.
  - Hostname and IP address of the server on which the Reporting Database resides.
  - Password for the Reporting Database user.

Procedure

Step 1 On the Unified CVP Operations Console, select **Device Management** > **Unified CVP Reporting Server**.

Step 2 Click **Add New** to add a new Reporting Server or click **Use As Template** to use an existing template to configure the new Reporting Server.

Step 3 Click the following tabs and configure the settings based on your call flow model:

a) **General** tab. For more information, see General Settings, on page 164.

b) **Reporting Properties** tab. For more information, see Reporting Properties Settings, on page 165.

c) **Device Pool** tab. For more information about adding, deleting, and editing device pool, see Add or Remove Device From Device Pool, on page 97.

d) **Infrastructure** tab. For more information, see Infrastructure Settings, on page 166.

Step 4 Click **Save and Deploy** to deploy the changes to the Reporting Server page. Click **Save** to save the settings in the Operations Server database and configure the Reporting Server later.

Related Topics

Configure Call Server, on page 77
General Settings, on page 164
Reporting Properties Settings, on page 165
Add or Remove Device From Device Pool, on page 97
Infrastructure Settings, on page 166

Reporting Server Settings

General Settings

Configure settings that identify the Reporting Server, associate it with one or more Call Servers, and enable or disable security on the **General** tab.

Table 24: Reporting Server—General Tab Settings

Field	Description	Default	Value	Restart Required
IP Address	The IP address of the Reporting Server.	None	Valid IP address	Yes
Hostname [3]	The hostname/IP address of the Reporting Server machine.	None	Valid DNS name, which can include letters of the alphabet and numbers 0 through 9.	Yes
Description	An optional text description for the Reporting Server.	None	Up to 1024 characters.	No

Field	Description	Default	Value	Restart Required
Enable Secure Communication with the Operations Console	Select to enable secure communications between the Operations Console and the Reporting Server component. The Reporting Server is accessed using SSH and files are transferred using HTTPS. You must configure secure communications *before* you enable this option. See *Administration Guide for Cisco Unified Customer Voice Portal*.	Off	On or Off	No
Device Version	Lists the release and build number for this device.	None	None	No
Associate Call Servers	Select one or more Call Servers to associate with the Reporting Server. You must select at least one Call Server. Call data for all SIP and VXML calls that are handled by this 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 Call Server from the Selected pane.	None	A Call Server can be associated with only one Reporting Server.	No

[3] If secure communication is being used, ensure that the hostname/IP address specified in the hostname field must match the CN or SAN field value of the TLS certificate being used; or an equivalent mapping of the same exists in DNS or local hosts file. Usage of FQDN (Fully Qualified Domain Name) is also recommended for the same purpose.

Reporting Properties Settings

Configure Reporting Server settings on the **Reporting Properties** tab.

Table 25: 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.	Yes	Yes or No	Yes
Max. File Size (MB):	Defines the maximum size of the file that is used to record the data feed messages during a database failover. This size can be limited by the amount of free disk space.	100	1 through 250 MB	No

Infrastructure Settings

The Reporting Server publishes statistics on the number of reporting events that it receives 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 26: Reporting Server—Infrastructure Tab Configuration Settings

Field	Description	Default	Value	Restart Required
Configuration: Thread Management				
Maximum Threads	(Required) The maximum thread pool size in the Reporting Server Java Virtual Machine.	500	100 to1000	Yes
Advanced				
Statistics Aggregation Interval	The Reporting Server publishes statistics at this interval.	30 minutes	10 to1440	Yes
Log File Properties				

Field	Description	Default	Value	Restart Required
Max Log File Size	(Required) Maximum size of the log file in megabytes. **Note** To increase the log file size, go to `C:\Cisco\CVP\conf`, open log4j.xml file and update the MaxFileSize value as shown: `<param name="MaxFileSize" value="10000000"/>` Save the file and restart Reporting Server to deploy the changes.	10 MB	1 through 100 MB.	Yes
Max Log Directory Size	(Required) Maximum size of the directory containing Reporting Server log files. **Note** If you modify the value to a setting that is below the default value, the log entries might be lost, which can affect troubleshooting.	20,000 MB	500 to 500,000 MB. Max Log File Size is less than Max Log Directory Size. Max Log Directory Size cannot be greater than 500,000 MB.	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 65,535.	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 hostname.	No

Field	Description	Default	Value	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 65,535.	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 65,535.	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 65,535.	No

IP Address Modification

This section describes how to change the IP address of Call Server, VXML Server, and the Reporting Server. Follow this sequence for changing the IP Address of the devices:

1. Reporting Server
2. VXML Server
3. Call Server
4. OAMP Server

Procedure

Step 1 Select the device from the Operations Console to change the IP address.

Step 2 From the menu bar of the device, select the device and click **Use As Template**.

Step 3 Assign the new IP address to the device and change the Host Name temporarily, which you will revert in Step 8, and click **Save**.

Note Do not click the **Save and Deploy** option until you have changed the physical server to the new IP address.

Step 4 Delete the device from the Operations Console before changing the IP address of the server.

Step 5 Configure the new IP address on the local server.

Step 6 Go to **C:\Cisco\CVP\bin\UpdateRMIServerIP\updatermiserverip.bat** and double-click the batch file to update the IP address in the windows registry and the wrapper.conf file.

Step 7 From the Operations Console, select the device and change the Host Name to the original one. Click **Save and Deploy** for the device. (Restart the server if network-related message is seen).

Step 8 Restart the server.

Note

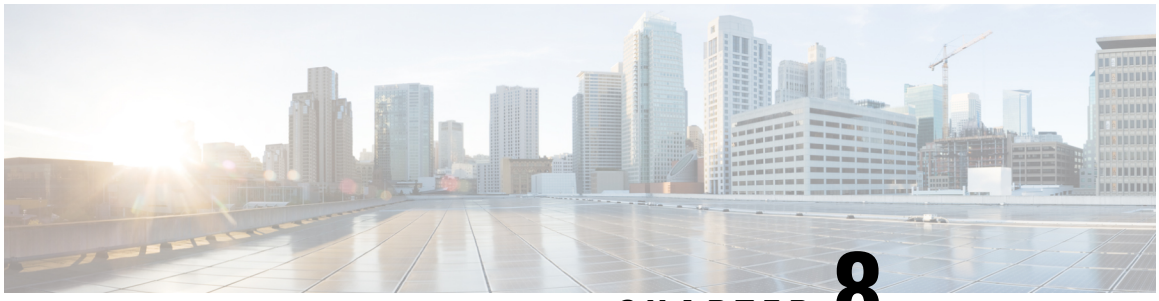
a. Make sure to change the configuration of VXML Application, Gateway, VVB, ICM PIM, Proxy, and CUCM to reflect the new Call Server IP address.

b. Associate Reporting Server to the Call Server.

c. Delete the existing Media Server and create a new one with the Call Server IP address and deploy the Media Server.

What to do next

Change the IP address of the OAMP Server.



CHAPTER 8

Unified ICM Configuration

Configure Unified ICM Server

Procedure

Step 1 Log in to Operations Console and click **Device Management** > **Unified ICM**.

Step 2 Click **Add New**.

Note To use an existing ICM Server as a template for configuring a new ICM Server, select an ICM Server from the list of available Unified ICM Servers and click **Use As Template** and perform Steps 3 to 6.

Step 3 Click the **General** tab and enter the field values. See General Settings, on page 172.

Step 4 (Optional) Click the **Device Pool** tab and add the Unified ICM Server to a device pool. See Add Unified ICM to Device Pool, on page 172.

Step 5 Click **Save**.

Related Topics

General Settings, on page 172

Add Unified ICM to Device Pool, on page 172

ICM Server Settings

General Settings

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. These calls can be routed to ACDs, specific agents, or to VRUs. However, 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.

To configure General settings on an ICM Server, on the **General** tab, enter the field values, as listed in the following table:

Table 27: Unified ICM—General Tab Configuration Settings

Field	Description	Default	Value	Restart Required
IP Address	The IP address of a Unified ICM Server	None	Valid IP address	No
Hostname	The name of the Unified ICM Server	None	Valid DNS name. It includes alphanumeric characters and a dash.	No
Description	Additional information about the Unified ICM Server	None	Up to 1024 characters	No
Device Admin URL	The URL for the Unified ICM Web configuration application.	None	Valid URL	No

Add Unified ICM to Device Pool

See Add or Remove Device From Device Pool, on page 97.

Related Topics

Add or Remove Device From Device Pool, on page 97

Configure ICM Settings for Standalone Call Flow Model

You can convert a configuration from a nonreporting configuration (that is, no Call Server is defined) to a Reporting or ICM Lookup Configuration. If you have configured Unified CVP for a Standalone call flow model without reporting, the version of the VXML Server you defined cannot be associated with a Call Server. This VXML Server definition is required for reporting and for the ICM Lookup. Hence, delete the existing VXML Server definition and begin with Step 4 to incorporate a Call Server, a Reporting Server, and ICM Lookup Configuration steps.

Variations	Applicable steps
Reporting	Steps 2, 5, and 6
Without Reporting	Not applicable
ICM lookup	Steps 1 to 7
All variations	Step 1

Procedure

Step 1 Create an application using Cisco Unified Call Studio and deploy it as a zip file.

Note
- For ICM Lookup, use the **ReqICMLabel Element**. This element has two exit states: **error** and **done**. The **done** state must connect to a transfer element to transfer the caller to **ReqICMLabel** as referenced by the **ReqICMLabel Element**.
- For details on the **ReqICMLabel Element**, see the Element Specifications for Cisco Unified CVP VXML Server and Unified Call Studio.
- For information about Unified Call Studio, see the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio.

Step 2 Enable logging.

See the User Guide for Cisco Unified CVP VXML Server and Unified Call Studio for details on configuring loggers using Unified Call Studio.

Step 3 Enable the **CVPSNMPLogger** for SNMP monitoring.

Note By default, **CVPSNMPLogger** is enabled when a new Unified Call Studio application is created and deployed to the VXML Server.

Step 4 Add and configure a standard Call Server and enable the ICM service. See Configure Call Server, on page 77.

Step 5 Configure the VXML Server.

a) Log in to Operations Console, select **Device Management** > **VXML Server** and add a VXML Server with an associated Primary Call Server.
b) To enable reporting for this VXML Server, in the Operations Console, click the **Configuration** tab and select **Enable Reporting for this VXML Server**.
c) Add appropriate filtering.

Step 6 Deploy the Call Studio Application on the VXML Server.

a) Select **Device Management** > **VXML Server** in the Operations Console.
b) Select the VXML Server and click **Save and Deploy**.

Step 7 Using the ICM Script Editor, create a Unified ICME script that returns a label.

To transfer information from Unified ICME to the VXML Server in addition to the label, use the ToExtVXML 0 - 4 ECC Variables or Peripheral Variables 1 to 10. The format for using the ToExtVXML 0 to 4 is with name-value pairs that are delimited by semicolons.

Example:

```
ToExtVXML0 = "company=Cisco Systems;state=MA"
```

Use the Peripheral Variables 1 to 10 to pass information to the VXML Server. The values in these variables will be taken as is.

For information about creating a Unified ICME script that returns a label in, see the Unified ICME documentation.

For information about using the ReqICMLabel element, see Pass Data to Unified ICME, on page 201.

Related Topics

Configure Call Server, on page 77
Pass Data to Unified ICME, on page 201

Configure ICM Settings for Comprehensive Call Flow Model for ICME and ICMH

Procedure

Step 1 Define Network VRUs, create an instance, and define a customer.

a) On Unified ICME or NAM, in the ICM Configuration Manager, select the **Network VRU Explorer** tool, define a Network VRU for the VRU leg and labels for each Call Server.

b) On the Cisco Intelligent Contact Manager (CICM) only, in the ICM Configuration Manager, select **Network VRU Explorer tool**, define a Network VRU for the VRU leg and labels for reaching the NAM.

For Steps 1(a) and 1(b), enter the following values:

- Type: **10**
- Name: <*Network VRU Name*>. For example: **cvp**
- Define a label for each Unified CVP Call Server that is handling the switch leg:
  - Label: <*Network Routing Number*>
  - Type: **Normal**
  - Routing client for Unified ICME or NAM: From the drop-down list, select the routing client configured for that Call Server peripheral.
  - Routing client for CICM only: From the drop-down list, select the INCRP routing client.

Note The Network VRU label in NAM and CICM must be same. Similarly, the Network VRU Names on the NAM and CICM should also be same.

Step 2 Configure the ICM VRU Label.

Step 3 Define network VRUs and peripheral gateways for the switch leg in the ICM Configuration Manager.

On Unified ICMH, on the NAM and CICMs, in the Network VRU Explorer tool, define one label for each Unified CVP Call Server or NIC routing client.

Note Use the same Type 10 Network VRU that you defined in the Step 1 for the VRU leg.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 4 Set the client type for the INCRP NIC. On the CICM, in the ICM Configuration Manager, NIC Explorer tool, set the client type for the INCRP NIC. Select the **Client Type** as **VRU**.

Step 5 Define a VRU that uses INCRP. On the CICM, in the ICM Configuration Manager, Network VRU Explorer tool:

a) Define a Network VRU with a label that uses INCRP as its routing client.

Specify the following:

- Type: **10**
- Name: *<name of Unified CVP VRU>*

Example:

cvpVRU

b) Define a label for the NAM routing client.

Specify the following:

- Type: **Normal**
- Label: *<Network Routing Number>*
- Routing client: **INCRP NIC**

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 6 Configure Peripheral Gateways .

On the NAM, ICM Configuration Manager, **PG Explorer** tool, configure a peripheral gateway (PG) for the Unified CVP. Configure a PG for each Unified CVP Call Server as follows:

In the tree view pane, select the applicable PG.

Logical Controller tab:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  For example: **<location>_A** for side A of a particular location

Peripheral tab:

- Peripheral Name: Descriptive name of this Unified CVP peripheral. For example: **<location>_<cvp1> or <dns_name>**
- Client Type: **VRU**
- Check the **Enable Post-routing** check box.

Advanced tab: Select the name of the Unified CVP VRU from the Network VRU field drop-down list. For example: **cvpVRU**

Routing Client tab:

- Name: By convention, use the same name as the peripheral
- Client Type: **VRU**
- If you are in a Unified ICMH environment and configuring the CICM, then do the following:
  - Do not check the **Network Transfer Preferred** check box.
  - Routing client: **INCRP NIC**

Step 7 Define a default network VRU on Unified ICME or the NAM, in the ICM Configuration Manager, the **System Information** tool:

a) For Unified ICME or on the **CICM only**, define a default Network VRU.
Define the Default Network VRU: <*Network VRU Name*>. For example: **cvpVRU**

b) If there are Routing Scripts on the **NAM**, define a default Network VRU.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 8 Configure dialed numbers, call types, and customers on the Unified ICME or Unified ICMH Server in the ICM Configuration Manager:

a) **Dialed Number List Tool tab:** Configure the dialed numbers.
b) **Call Type List tool tab:** Configure the call types.
c) **ICM Instance Explorer tool tab:** Configure the applicable customers.

For more information, see ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 9 Install and configure one or multiple Call Servers.

Log in to the Operations Console and perform the following steps:

a) Enable the ICM and SIP Services on the Call Server.
   - On the Operations Console, click **Device Management** > **Unified CVP Call Server**.
   - Check the **ICM** and **SIP** check boxes.

b) Click **Device Management** > **Unified CVP Call Server** > **SIP**. Configure the SIP Service:
   - If you are using a SIP Proxy Server, enable the Outbound Proxy and select the SIP Proxy Server.
     Select the **SIP tab** and configure the following values:
     - Enable Outbound Proxy: **Yes**
     - Outbound Proxy Host: Select from drop-down list.
     - Configure Local Static Routes on the SIP Proxy Server itself.
   - If you are not using a SIP Proxy Server, configure Local Static Routes using the Dialed Number Pattern system configuration on the Operations Console. A Local Static Route must be configured for each SIP gateway or automatic call distributor (ACD) so that SIP endpoint can receive calls.
     Local Static Routes, Dialed Number (DN): Specify the dialed number pattern for the destination.
     Valid number patterns include the following characters:
     - Use the period or the **X** character for single-digit wildcard matching in any position.

Note Small letter **x** cannot be used as a wildcard.

- Use the greater than (>), asterisk (*****), or exclamation mark (**!**) characters as a wildcard for zero or more digits at the end of the DN.
- Avoid the **T** character for wildcard matching.
- Dialed numbers must not exceed 24 characters.
- For valid format and precedence information about dialed numbers, see Valid Format for Dialed Numbers, on page 93.

Example: **9>** (Errors are 9292 and ringtone is 9191)

For more information, see SIP Dialed Number Pattern Matching Algorithm, on page 9.

The following static route configuration is incorrect because the least explicit routes must appear at the end. Load balancing or failover of calls require DNS SRV domain names, not multiple routes with the same DN Pattern, but a single route to an SRV domain name.

Incorrect Example:

```
1>,10.2.6.1
2>,10.2.6.2
3>,10.2.6.20
2229191>,10.2.6.241
2229292>,10.2.6.241
2229191>,10.2.6.242
2229292>,10.2.6.242
2>,ccm-subscribers.cisco.com
3>,ccm-subscribers.cisco.com
```

Correct static route configuration example:

```
22291>,cvp-ringtone.cisco.com
22292>,cvp-error.cisco.com
1>,ccm-subscribers.cisco.com
2>,ccm-subscribers.cisco.com
3>,ccm-subscribers.cisco.com
```

Note “91919191>” pattern does not match the dialed number “91919191”.

- Check the default values for the SIP Service and change, if desired.

c) Configure the ICM Service. Select **Device Management** > **CVP Call Server** > **ICM tab**, In the Maximum Length of DNIS field, enter the length of the Network Routing Number.

Example: For the Gateway dial pattern as 1800******, the maximum DNIS length is **10**.

Related Topics

Valid Format for Dialed Numbers, on page 93
Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210
Load-Balancing SIP Calls , on page 210
Cisco Unified SIP Proxy (CUSP) Configuration , on page 210

Configure Custom Streaming Ringtones, on page 213
SIP Dialed Number Pattern Matching Algorithm, on page 9

Configure Common Unified ICMH for Unified CVP Switch Leg

Procedure

Step 1 On the **NAM**, in the ICM Configuration Manager, **Network VRU Explorer** tool

a) Define a Network VRU for Unified CVP for Type as**10** and Name as**cvpVRU**.

b) Assign labels. Define one **Label** per Unified CVP or NIC routing client. Select the Type as **Normal** and Label as Network Routing Number.

Step 2 Set the client type.

On the **CICM**, using the ICM Configuration Manager, **NIC Explorer** tool:

- Select the **Routing Client** tab for the INCRP NIC.
- Enter the Client Type as**VRU**.

Step 3 Define a Network VRU.

On the **CICM**, using the ICM Configuration Manager, **Network VRU Explorer** tool, define a Network VRU with a label that uses INCRP as its routing client.

Enter the following:

- Type: **10**
- Name: **cvpVRU**
- Define one **Label** for the NAM routing client:
  - Label: Network Routing Number
  - Type: **Normal**
  - Routing client: **INCRP NIC**

Step 4 Define the Peripheral Gateways (PGs).

On the **NAM**, using the ICM Configuration Manager, **PG Explorer** tool, configure a peripheral gate for each ICM Service to be used for a switch leg that is connected to each PG.

For each Unified CVP ICM Service connected to this PG, in the tree view pane, select the applicable PG.

On the **Logical Controller** tab, enter the following:

- Client Type: **VRU**
- Name: A name descriptive of this PG.

  For example: `<location>_A`, for side A of a particular location.

On the **Peripheral** tab, enter the following:

- Peripheral Name: A name descriptive of this Unified CVP peripheral, for example, `<location>_<cvp1>` or `<dns_name>`
- Client Type: **VRU**
- Check the **Enable Post-routing** checkbox

  On the **Advanced** tab, select the name **cvpVRU** from the Network VRU field drop-down list.

On the **Routing Client** tab, enter the following:

- Name: By convention, use the same name as the peripheral
- Client Type: **VRU**
- Do not check the **Network Transfer Preferred** check box.

ECC Payloads

You can define as many ECC variables as necessary. But, you can only pass 2000 bytes of ECC variables on a specific interface at any one time. To aid you in organizing ECC variables for specific purposes, the solution has *ECC payloads*.

An ECC payload is a defined set of ECC variables with a maximum size of 2000 bytes. You can create ECC payloads to suit the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads.The particular ECC variables in a given ECC payload are called its *members*.

Note For ECC payloads to a CTI client, the size limit is 2000 bytes plus an extra 500 bytes for the ECC variable names. Unlike other interfaces, the CTI message includes ECC variable names.

In certain cases, mainly when using APIs, you might create an ECC payload that exceeds the CTI Server message size limit. If you use such an ECC payload in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, “CTI Server was unable to forward ECC variables due to an overflow condition.”

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. TCDs and RCDs record the ID of the ECC payload that had scope during that leg of the call. The *Call.ECCPayloadID* variable contains the ID of the ECC payload which currently has scope.

For VRU and media routing leg of the call, the TCD contains the VRU PayloadID setting associated with the peripheral. If not, TCD contains the default payload ID. The Termination Call Variables are persisted only based on this payload setting.

In solutions that only use the default ECC payload, the system doesn’t create an ECC variable that exceeds the 2000-byte limit for an ECC payload or the 2500-byte CTI Message Size limit. The system does this because it automatically adds all ECC variables to the default ECC payload if that is the only ECC payload.

If you create another ECC payload, the system no longer checks the 2000-byte limit when creating ECC variables. The system creates the ECC variables without assigning them to an ECC payload. Assign the new ECC variable to an appropriate ECC payload yourself through the ECC Payload Tool.

You can create and modify ECC payloads in the **Configuration Manager** > **List Tools** > **Expanded Call Variable Payload List** tool.

Default ECC Payload

The solution includes an ECC payload named "Default" for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

If your solution only has the Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Note You cannot delete the Default payload. But, you can change its members.

Important During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. If the Default payload exceeds the limit, modify it to meet the limit.

In a fresh install, the Default payload includes the predefined system ECC variables. In an upgrade, the Default payload's contents depend on whether the starting release supports ECC payloads:

- **ECC payloads not supported**—During the upgrade, a script adds your existing ECC variables to the Default payload.
- **ECC payloads are supported**—The upgrade brings forward the existing definition of your Default payload.

Note If your solution includes PGs from a previous release that does not support ECC payloads, the Router always sends the Default payload to those PGs. Those PGs can properly handle the Default payload.

ECC Payload Node

The **ECC Payload** node is available from the **General** tab on the **Object Palette**:

Figure 14: Payload icon

Use this node to change the ECC payload that has scope for the following part of your script. Once you select an ECC payload, it has scope for all non-VRU operations until changed. You can select the ECC payload either statically or dynamically by the payload's EnterpriseName or ID.

Define Unified CVP ECC Variables

Set up the ECC variables that Unified CVP uses to exchange information with Unified ICME/ICMH.

Procedure

Step 1 On the ICM Configuration Manager, select **Tools** > **Miscellaneous Tools** > **System Information** and check the **Enable expanded call context** check box.

Step 2 On the ICM Configuration Manager, select **Tools** > **List Tools** > **Expanded Call Variable List**.

Step 3 In the Expanded Call Variable List window, enable the **Add** button by clicking **Retrieve**.

Step 4 Click **Add**.

The Attributes property tab is enabled.

Step 5 Create each of the variables in the following table by clicking **Save** after defining each variable.

Note If you change the configuration of any ECC variable with the Expanded Call Variable List tool, stop and restart the Unified CVP Call Server.

Caution It is important that you enter the ECC's **Name** values listed in following table exactly as specified. If you do not, the Unified ICME/ICMH software does not communicate with the micro-applications on the ICM Service.

Length values are more flexible. Unless the values listed in following table are noted as "required," the value in the Length column is the maximum that Unified ICMH can handle for that ECC. Specify a value between 1 and the maximum length.

Note In a Unified ICME/ICMH configuration, the ECC variable configuration, including the length, defined in the NAM must be defined same in the CICM.

If you create or modify the ECC variables while the Unified CVP ICM Service is running, you must restart the VRU PG during non-production time or during a scheduled maintenance window for the changes to take full effect. To restart the VRU PG, access the service control of the PG in ICM and restart the ICM PIM and Unified CVP Call Server.

Step 6 Click **Save** to apply your changes.

Table 28: Micro-Application ECCs

Name	Length	Definition
`user.CourtesyCallbackEnabled`	Required for using Courtesy Callback. Length:1	Used to determine if Courtesy Callback must be offered to a caller. Valid values are: "1" = Yes "0" = No

Name	Length	Definition
`user.cvp_server_info`	Length: 15	Used by Unified CVP to send the IP address of the Call Server sending the request to Unified ICME. Example: An IPv4 address like 192.168.150.181
`user.microapp.currency`	Value: 6	Currency type.
`user.microapp.error_code`	Value: 2	Return status error code to be returned from the Unified CVP to Unified ICME/ICMH upon a False return code in the Run Script Result.
`user.microapp.fetchaudio`	Recommended length: 20; but length depends on the filename.	Filename for audio to be played by the VXML gateway while the gateway loads and processes the requested resource when there is significant network latency. Default: none Example: "flash:holdmusic.wav" **Note** This feature is not supported in Cisco VVB.
`user.microapp.fetchdelay`	Length: 1	The length of time (in seconds) to wait at the start of the fetch delay before playing the audio specified by *user.microapp.fetchaudio*. This setting only takes effect if the value of fetchaudio is not empty. Default: 2 seconds; used to avoid a "blip" sound heard in a usual network scenario. Setting this value to zero plays hold music immediately, for a minimum of five seconds. Values: 1 to 9 **Note** This feature is not supported in Cisco VVB.

Name	Length	Definition
`user.microapp.fetchminimum`	Length: 1	The minimum length of time to play audio specified by *user.microapp.fetchaudio*, even if the requested resource arrives in the meantime. This setting only takes effect if value of fetchaudio is not empty. Default: 5 seconds Values; 1 to 9 **Note** This feature is not supported in Cisco VVB.
`user.microapp.isPostCallSurvey`	Length: 1	Used to determine if post call survey must be offered to a caller after the agent hangs up. Valid values: "y" or "Y" is "Yes" "n" or "N" is "No" Default value is "Yes"
`user.microapp.locale`	Value: 5	Locale, a combination of language and country which defines the grammar and prompt set to use.
`user.microapp.media_server`	**Required** for any IVR scripting. Maximum length: 210 characters Recommended length: 30	Root of the URL for all media files and external grammar files used in the script. HTTP and HTTPS schemes can be specified as: • HTTP scheme is specified as "http://<servername>" • HTTPS scheme is specified as "https://<servername>"
`user.microapp.play_data`	40	Default storage area for data for Play Data micro-application.
`user.microapp.sys_media_lib`	10	Directory for all system media files, such as individual digits, months, default error messages, and so forth.

Name	Length	Definition
`user.microapp.app_media_lib`	Maximum length: 210 characters Recommended length: 10	Directory for all application-specific media files and grammar files. You can also set this value to ".." (literally two periods in quotes), which bypasses the user.microapp.app_media_lib and user.microapp.locale ECC Variables when writing a URL path. For example, if you set the user.microapp.app_media_lib to "..", the path: http://server/locale/../hello.wav would really be: http://server/hello.wav
Note The system and application media libraries need message and prompt files created or recorded for each locale that is referenced. For more information, see Pass Data to Unified ICME, on page 201.		
`user.microapp.grammar_choices`	Configurable on Unified ICME. Maximum length: 210 characters.	Specifies the ASR choices that a caller can input for the Get Speech micro-application. Each option in the list of choices is delimited by a forward slash (/). **Note** If text is placed in this variable that is longer than the variable is configured to handle, only the first 210 characters are sent.
`user.microapp.inline_tts`	Configurable on the ICM. Maximum length: 210 characters.	Specifies the text for inline Text To Speech (TTS). **Note** If text is placed in this variable that is longer than the variable is configured to handle, only the first 210 characters are sent.

Name	Length	Definition
`user.microapp.input_type`	Value: 1	Specifies the type of input that is allowed. Valid contents are: • **D** - DTMF • **B** - (Both, the default) DTMF and Voice If you are not using an ASR, you can set this variable to D. If you are using an ASR, you can set the variable to either D or B. **Note** With input_mode set to "B" (both), either DTMF or speech is accepted, but mixed mode input is not. Once you begin entering with one mode, input using the other mode is ignored and has no effect.
`user.microapp.caller_input`	Configurable on Unified ICME/ICMH. Maximum length: 210 characters.	Storage area for any ASR input that is collected from Get Speech. **Note** Get Speech text results are written to this ECC variable. Results from Get Digits or Menu micro-applications are written to the CED.
`user.microapp.pd_tts`	Value: 1	Specifies whether Unified CVP's Text To Speech (TTS) or media files must be played to the caller. Valid contents are: • **Y** - Yes, use TTS capabilities • **N** - No, do not use TTS capabilities; play media files instead. **Note** Used only with Play Data micro-application.
`user.microapp.UseVXMLParams`	Value: 1	This parameter specifies the manner in which you pass information to the external VoiceXML. Set this parameter to either "Y" (for yes) or "N" (for no). Y uses the values in the user.microapp.ToExtVXML variable array. N appends the name/value pairs in user.microapp.ToExtVXML to the URL of the external VoiceXML. Default: "N"

Name	Length	Definition
`user.microapp.ToExtVXML`	210	This variable array sends information to the external VoiceXML file. Must be configured as Array variables, not Scalar variables, even if the array length is set to 1. For more information on user.microapp.ToExtVXML variable length, see the *Configure the CCE Script for Courtesy Callback* section.
`user.microapp.FromExtVXML`	210	This variable array returns information from the external VoiceXML file. Must be configured as Array variables, not Scalar variables, even if the array length is set to 1. See Pass Data to Unified ICME, on page 201 for more information. For more information on user.microapp.FromExtVXML variable length, see the *Configure the CCE Script for Courtesy Callback* section.
`user.microapp.override_cli`	Configurable on Unified ICME/ICMH. Maximum length: 200 characters.	Used by system to override the CLI field on outgoing transfers.
`user.microapp.metadata`	The variable length would usually be configured as 62 bytes, but if ECC space is restricted, you can configure it as 21 bytes.	Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP returns information about the micro-application that is run. The user.microapp.metadata ECC variable is structured as follows: m|con|tr|to|iv|duratn|vruscriptname
`user.microapp.uui`	Configurable on Unified ICME/ICMH. Maximum length: 131 characters.	Used to pass user-to-user information back to Unified CVP from Unified ICME/ICMH.
`user.sip.refertransfer`	Optional Maximum length: 1 character.	SIP Service uses REFERs when transferring to the agents: • y - Use REFER when transferring • n - Do not use REFER when transferring

Name	Length	Definition
`user.suppress.sendtovru`	Optional Length: 1	Suppress the Temporary Connect message generated by SendToVRU node (explicitly or implicitly, for example by a Translation Route to VRU node). Used in call flows where the Temporary Connect is generated right before the Connect message (that is, no Run Script messages expected) to avoid the extra overhead of setting up a VRU leg temporarily before the Connect arrives. Valid values are: "y" or "Y" (yes, suppress the message)

`user.CxSurveyInfo`	Optional
	Length: 50 bytes
		This is an optional variable. It is required only when Webex Experience Management (WXM) is integrated with Unified CVP and Unified CCE. It contains data (Vertical bar-separated values) in the following format.
		`AG=<AgentSkillTargetID>|SG=<SkilllGroupID>|`
		`PQ=<PrecisoinQueueID>|AGT=<AgentTeamID>`

What to do next

Before you can use the new ECC variable, you must add it to an ECC payload.

Note If your solution only has a Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Related Topics

Pass Data to Unified ICME, on page 201

Define ECC Payloads

You can create and modify ECC payloads in the **Expanded Call Variable Payload List** tool.

Note The tool checks that the ECC payload does not exceed the 2000-byte limit only when you save your changes. The counters on the **Members** tab only show what the current size is with all the selected members. They are only informational and do not enforce the limit. The limit is enforced when you attempt to save the changes.

To define an ECC payload, you create the ECC payload and then add its members.

Procedure

Step 1 In the Configuration Manager, open **Tools** > **List Tools** > **Expanded Call Variable Payload List**.

The **ECC Payload List** window appears.

Step 2 Click **Retrieve** to enable adding ECC payloads.

Step 3 Click **Add**.

The **Attributes** property tab appears.

Step 4 Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

Step 5 On the **Members** tab, click **Add**.

A dialog box listing all the existing ECC variables appears.

Step 6 Select the members for your ECC payload and click **OK**.

Watch that the **ECC Variable Size** counter does not exceed 2000 bytes. For ECC payloads that go to CTI clients, watch that the **CTI Message Size** counter does not exceed 2500 bytes.

Step 7 Click **Save** to apply your changes.

Metadata ECC Variable

Following the Menu (M), Get Data (GD) and Get Speech (GS) micro-applications, Unified CVP returns information about the micro-application that is run. This information is returned in the **user.microapp.metadata** ECC variable. Its format is defined in terms of a number of subfields, each separated by a vertical bar character ('|'). Also, the subfields are of fixed length in order to facilitate extraction either at reporting time or within the ICM routing script itself.

The **user.microapp.metadata** ECC variable is structured as follows:

m|con|tr|to|iv|duratn|vruscriptname

The following table shows the values for this variable:

Table 29: Metadata ECC Variable Values

Metadata	ECC Variable Value
m	D, V or N - Indicates whether the user responded with Voice (V), DTMF (D), or not at all (N). (Note that for the Menu micro-application, any successful single digit entry will result in m being set to V or D, even if the entry was an invalid menu selection.)
con	000 to 100 - Indicates the ASR percent confidence level at which the voice input was finally recognized. This field is only valid if m is Voice (V).
tr	00 to 99 - Indicates how many tries were required. 01 means user responded successfully after the first prompt.
to	00 to 99 - Indicates how many timeouts occurred. Does not include interdigit timeouts.

Metadata	ECC Variable Value
iv	00 to 99 - Indicates how many invalid entries were received, including interdigit timeouts.
duratn	000000 to 999999 - Indicates the micro-application duration in milliseconds. Duration is defined as the elapsed time between entering and exiting the RunExternalScript node, as measured in the IVR Service.
vru script name	Full name of the VRU script which was run. This is the only variable length field.

This ECC variable is optional. If you have used it, you must define it in the Unified ICME Expanded Call Context Variables configuration tool. Generally, the variable length to be configured is 62 bytes, but if ECC space is restricted, you can configure it as 21 bytes. This configuration drops the vruscriptname subfield. If you do define this variable, its contents get written to the Unified ICME database with every termination record, and can be used to provide a record of meta-information about the each input micro-application that is run.

Common Configuration for Differentiating VRUs Based on Dialed Number

As per the Network VRU configuration instructions, all callers are routed to the same VRUs (Unified CVPs) for VRU treatment purposes. Under this assumption, it is always simplest to rely on the system default Network VRU. However, it is sometimes necessary to differentiate the VRUs (Unified CVPs) based on dialed number.

Note This section is only applicable to call flow models which use the SendToVRU node to transfer the call to Unified CVP's VRU leg (it does not apply to Translation Route transfers).

For example, some calls need to assign different customers or applications to their own Unified CVP machines.

To configure Unified ICME to differentiate the VRUs, perform the following tasks:

- Configure more than one Network VRU.
- On Unified ICME, in the ICM Configuration Manager of the ICM Instance Explorer tool:
  - Configure one or multiple customers.
  - Configure the Network VRU for each customer if that customer wants to use in a Network VRU other than the default in future.
- Associate the dialed number(s) to the customer in the Dialed Number List tool.
- Since each configured VRU script is specific to one specified Network VRU, create a distinct set of VRU scripts for each Network VRU. Also, ensure that the ICM routing script calls the correct set of VRU scripts.

Configure ICM Settings for Call Director Call Flow Model

Procedure

Step 1 On the Unified CM server, CCMAdmin Publisher, perform the following SIP-specific action:

a) Add route patterns for outbound calls from the Unified CM devices using a SIP Trunk to the Unified CVP Call Server. Also, add a route pattern for error DN.

Select **Call Routing** > **Route/Hunt** > **Route Pattern** > **Add New** and add the following:

- Route Pattern: Specify the route pattern; for example: **3XXX** for a TDM phone that dials 9+3xxx and all Unified ICME scripts are set up for 3xxx dialed numbers.
- Gateway/Route List: Select the SIP Trunk defined in the previous substep.

Note For warm transfers, the call from one agent to another does not typically use a SIP Trunk, but you must configure the CTI Route Point for that dialed number on the Unified CM server and associate that number with your peripheral gateway user (PGUSER) for the JTAPI gateway on the Unified CM peripheral gateway. An alternative is to use the Dialed Number Plan on Unified ICME to bypass the CTI Route Point.

Step 2 Configure the peripheral gateways for the switch leg.

On Unified ICME, ICM Configuration Manager, **PG Explorer** tool:

a) Configure each peripheral gateway (PG) to be used for the **Switch** leg. In the tree view pane, select the applicable peripheral gateway, and set the following:

1. On the **Logical Controller** tab:
   - Client Type: **VRU**
   - Name: A name descriptive of this PG

     For example: **<location>_A** for side A of a particular location
2. On the **Peripheral** tab:
   - Peripheral Name: A name descriptive of this Unified CVP peripheral

     For example: **<location>_<cvp1> or <dns_name>**
   - Client Type: **VRU**
   - Select the check box: **Enable Post-routing**
3. On the **Routing Client** tab:
   - Name: By convention, use the same name as the peripheral.
   - Client Type: **VRU**

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

b) Configure a peripheral for each Unified CVP Call Server to be used for a Switch leg connected to each PG.

Step 3 Configure dialed numbers.

On the Unified ICME or Unified ICMH Server, in the ICM Configuration Manager, configure the following items:

a) **Dialed Number List Tool** tab: Configure the dialed numbers.
b) **Call Type List tool** tab: Configure the call types.
c) **ICM Instance Explorer tool** tab: Configure the applicable customers.

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 4 Create a Routing Script.

On the Unified ICME or Unified ICMH Server in the ICM Script Editor tool:

Create a routing script that handles the incoming call. The routing script must run a Label node or Select node (node that returns a label right away).

Note Do not use the Queue node in the routing script.

The label must be configured in the SIP Proxy Server to the IP address of the device that the label corresponds to. The Proxy Server is optional. If you do not have one, you must configure the Gateway dial-peer to point to the Call Server (refer to the first step in this process). Also, you must configure the **destination labels** in the SIP Service for the Call Server.

See the Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted for more information.

Step 5 In the Operations Console, install and configure Call Servers.

a) Enable the ICM and SIP Services on the Call Server.

In the Operations Console, select **Device Management** > **Unified CVP Call Server**.

Select the check boxes: **ICM** and **SIP**

b) Configure the SIP Service:

Select **Device Management** > **CVP Call Server** > **SIP tab**.

- If you are using a SIP Proxy Server, enable the Outbound Proxy and select the SIP Proxy Server. If using a SIP Proxy Server, configure Local Static Routes on the SIP Proxy Server itself.
- If you are not using a SIP Proxy Server, configure Local Static Routes using the Dialed Number Pattern system configuration in the Operations Console. A local static route must be configured for each SIP gateway/ACD, SIP endpoint in order to receive calls.
- Check the default values for the SIP Service and change, if desired.

See the SIP Devices Configuration, on page 209 and SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

c) Configure the ICM Service by setting the maximum length DNIS to the length of the Network Routing Number:

- Select **Device Management** > **CVP Call Server** > **ICM tab**.
- Set the Maximum Length of DNIS to length of the Network Routing Number.

Example: For the Gateway dial pattern as 1800******, the maximum DNIS length is 10.

For detailed information, see the *Operations Console Online Help*.

Related Topics

Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210
Load-Balancing SIP Calls , on page 210
Cisco Unified SIP Proxy (CUSP) Configuration , on page 210
Configure Custom Streaming Ringtones, on page 213
SIP Dialed Number Pattern Matching Algorithm, on page 9

Configure ICM Settings for VRU-Only Call Flow Model: Type 8

Procedure

Step 1 Perform Steps 1 to 4 of the Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56 procedure.

Step 2 Define a Network VRU on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

Using the ICM Configuration Manager, the Network VRU Explorer tool, specify the following:

- Type: **8**
- Name: **cvpVRU**

Note Although any name works, **cvpVRU** is used by convention, and is an example name referenced in this guide.

Step 3 Configure the Peripheral Gates (PGs) on Unified ICME or (for Unified ICMH) on each CICM.

a) Configure each PG.
b) Configure a peripheral for each Unified CVP ICM Service connected to each PG.

Use the ICM Configuration Manager, the **PG Explorer** tool. For each Unified CVP ICM Service connected to this PG, in the tree view pane, select the applicable PG and configure the following items:

Logical Controller tab:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  Example: `<location>_A` for side A of a particular location

Peripheral tab:

- Peripheral Name: A name descriptive of this Unified CVP peripheral

  Examples: `<location>_<cvp1>` or `<dns_name>`

- Client Type: **VRU**
- Select the checkbox: **Enable Post-routing**

Advanced tab:

- From the Network VRU field drop-down list, select the name: **cvpVRU**

Routing Client tab:

- Name: By convention, use the same name as the peripheral.
- Client Type: **VRU**

Step 4 Configure a Service and Route for each VRU on Unified ICME or (for Unified ICMH) on each CICM.

Note You can also use service arrays. See the Unified ICME documentation set for more information.

Using the ICM Configuration Manager, the **Service Explorer** tool, specify the following:

- Service Name: **cvpVRU**
- Route Name: **PeripheralName_cvpVRU**
- Peripheral Number: **2**

  Must match the "Pre-routed Call Service ID" in the Call Server configuration on the ICM tab in the Operations Console
- Select the **Enable Post-routing** checkbox.

Step 5 Define trunk groups.

Note Configure one Network Transfer Group and one associated Trunk Group for each VRU leg Unified CVP ICM Service.

Define and configure the network trunk group on Unified ICME or (for Unified ICMH) on each CICM.

Using the ICM Configuration Manager, the Network **Trunk Group Explorer** tool:

a) Identify the network trunk group.
   - Network Trunk Group Name: A name descriptive of this trunk group

b) For each Unified CVP ICM Service for the VRU leg, configure an associated trunk group.
   - Peripheral Name: A name descriptive of this trunk group
   - Peripheral Number: **200**

     Must match the **Pre-routed Call Trunk Group ID** in the Call Server configuration on the ICM tab in the Operations Console
   - Trunk Count: Select **Use Trunk Data** from the drop-down list
   - Do not configure any trunks

Step 6 Define translation route(s).

Define and configure a Translation Route for each VRU Peripheral on Unified ICME or (for Unified ICMH) on each CICM.

On Unified ICME, ICM Configuration Manager, **Translation Route Explorer** tool:

a) Define a Translation Route for each VRU Peripheral. Specify the following:

Translation Route tab:

- Set the **Name** field to the name of the target VRU peripheral. (This is by convention; this value must be unique in the enterprise)
- Set the **Type** field to **DNIS** and select the Service defined in the previous step

b) Configure translation route and label information for each VRU peripheral. Complete the following:

Route tab:

- Set the **Name**: by convention, this is the name of the target VRU peripheral, followed by the DNIS that this route will use, for example, MyVRU_2000

  This value must be unique in the enterprise
- Service Name drop-down list, select: **PeripheralName.cvpVRU**

Peripheral Target tab:

- Enter the first DNIS that will be seen by the VRU that you will be using for this translation route.

  Note The DNIS pool used for each VRU peripheral must be unique
- From the drop-down list, select a **Network Trunk Group** which belongs to the target VRU

Label tab:

- Enter the translation route label (which might or might not be the same DNIS you entered on the Peripheral Target tab)
- Type: **Normal**
- Routing Client: Select the NIC Routing Client

Note
- You must create an additional label for each NIC routing client.
- Repeat the Route and corresponding Peripheral Target and Label information for each DNIS in the pool.

Step 7 Create VRU and routing scripts.

Create VRU scripts and routing scripts for IVR treatment and agent transfer on Unified ICME or (for Unified ICMH) on each CICM .

Using the ICM **Script Editor** tool, create the VRU scripts and routing scripts to be used for IVR treatment and agent transfer, as described in other sections of this manual and in the ICM manuals.

The VRU scripts are associated with the applicable Network VRU.

For example, **cvpVRU**

Use the ICM Script Editor's TranslationRouteToVRU node to connect the call to the Network VRU.

Step 8 Configure the ECC variables on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

Using the ICM Configuration Manager, create the ECC variables.

For more information, see Define Unified CVP ECC Variables, on page 181.

Step 9 Configure dialed numbers and call types on Unified ICME or (for Unified ICMH) on the NAM and each CICM.

On Unified ICME, using the ICM Configuration Manager, configure dialed numbers and call types.

For more information, see ICM Configuration Guide for Cisco ICM Enterprise Edition.

Step 10 On Unified CM, configure Unified CM.

For more information, see the Unified CM user documentation.

Step 11 Install and configure the Call Servers.

Log in to the Operations Console, select **Device Management** > **CVP Call Server** and install and configure the Call Servers.

Check the **ICM** and **IVR** check boxes.

For detailed information, see the Operations Console online help.

Step 12 Configure the ICM service.

On the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. On **each** Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a) VRU connection port number.

Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b) Maximum Length of DNIS.

Set the maximum length DNIS to a number which is at least the length of the translation route DNIS numbers.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c) Call service IDs: New Call and Pre-routed.

Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab.

d) Trunk group IDs: New Call and Pre-routed.

- Enter the new and pre-routed call trunk group IDs
- Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route
- Configure the number of ports according to the licenses purchased and capacity
- Configure each of the numbers used for translation routes. (The "New Call" group is not used since the calls are being sent to the VRU (Unified CVP) after some initial processing by the NIC/Unified ICME)

e) Dialed numbers used in the translation route.

Add the dialed numbers in the DNIS field.

f) Check the default values of the other settings and change, if desired.

Step 13 Configure the IVR Service.

On the Operations Console, select **Device Management** > **CVP Call Server** > **IVR** tab.

Check the default values and change, if desired.

Refer to the Operations Console online help for information about other settings you might want to adjust from their default values.

Step 14 (Optional) Configure the Reporting Server.

In the Operations Console, select **Device Management** > **CVP Reporting Server** > **General tab**:

a. Configure the Reporting Server.

b. Select a Call Server to associate with this Reporting Server.

c. Check the default values of the Reporting properties and change, if desired.

For more information, see Reporting Guide for Cisco Unified Customer Voice Portal

VoiceXML Gateway Configuration Examples

Example Gateway Settings for Type 8 Call Flow Model

The first part of the following example provides the basic configuration for setting a VoiceXML gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets
- Configures ASR/TTS Server
- Configures gateway settings

The last part of this example provides the following:

- Initiates the VoiceXML leg
- Plays a .wav file that enables caller to hear message from critical_error.wav
- Logs errors on the gateway when the call fails

```
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
logging buffered 99999999 debugging
no logging console
ip cef
```

```
no ip domain lookup
ip host tts-en-us <IP of TTS or MRCP Server>
ip host asr-en-us <IP of ASR or MRCP Server>
voice rtp send-recv
!
voice service voip
allow-connections h323 to h323
signaling forward unconditional
h323
sip
min-se 360
header-passing
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
ivr prompt memory 15000
ivr prompt streamed none
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client cache memory file 500
http client connection timeout 60
http client response timeout 30
http client connection idle timeout 10
gateway
timer receive-rtcp 6
!
ip rtcp report interval 3000
application
service new-call flash:bootstrap.vxml
service cvperror flash:cvperror.tcl
service handoff flash:handoff.tcl
```

Example of Dial-peer for ICM VRU Label for Type 8 Call Flow Model

The following example provides the configuration for an ICM VRU label dial-peer for the Type8 Unified CVP VRU-Only call flow model:

```
dial-peer voice 777 voip
 description ICM VRU label
 service bootstrap
 voice-class codec 1
 incoming called-number <your sendtovru label pattern here>
 dtmf-relay rtp-nte
 no vad
 !
```

Related Topics

Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56
Define Unified CVP ECC Variables, on page 181

Configure ICM Settings for VRU-Only Call Flow Model: Type 7

Procedure

Step 1 Perform Steps 1 to 4 of the Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56 procedure.

Step 2 Configure each PG.

On the **NAM**, ICM Configuration Manager, **PG Explorer** tool:

a) Configure each PG to be used for the **VRU Client** leg.
b) Configure a peripheral for each Unified CVP ICM Service to be used as a VRU leg connected to each PG.

For each Unified CVP ICM Service connected to this PG, in the tree view pane, select the applicable PG.

Logical Controller tab, configure:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  For example: `<location>_A` for side A of a particular location

Peripheral tab, configure:

- Peripheral Name: A name descriptive of this VRU peripheral.

  For example: `<location>_<cvp1>` or `<dns_name>`
- Client Type: **VRU**
- Select the checkbox: **Enable Post-routing**

Routing Client tab:

- Name: By convention, use the same name as the peripheral.
- Client Type: **VRU**

Step 3 Define a Network VRU and labels.

On the **CICM**, ICM Configuration Manager, **Network VRU Explorer** tool, define a Network VRU for the VRU leg and labels for reaching the NAM.

Specify the following:

- Type: **7**
- Name: **cvpVRU**

  Note This name is used by convention. Although any name will do, since it is referenced elsewhere in this document, **cvpVRU** is assumed.
- Define a **Label** for the NAM.

- Label: Network routing number
- Type: **Normal**
- Routing client: Select the INCRP Routing Client from the drop-down list.

Step 4 Define a Network VRU and a label for each NIC.

On the **NAM**, ICM Configuration Manager, **Network VRU Explorer** tool, define a Network VRU and a label for each NIC that is using this VRU.

Specify the following:

- Type: **7**
- Name: **cvpVRU**

  Note This name is used by convention. Although any name will work, since it is referenced elsewhere in this document, **cvpVRU** is assumed.

- Define a **Label** for each NIC that is using this VRU:
  - Label: Network routing number
  - Type: **Normal**
  - Routing client: Select the Routing Client for that NIC from the drop-down list.

Note Ensure the Network VRU label is identical in the NAM and CICM. The Network VRU Name must be same to avoid confusion.

Step 5 If there are Routing Scripts on the NAM, define a default Network VRU.

On the **NAM**, ICM Configuration Manager, **System Information** tool, in the General section:

- Define the Default Network VRU: **cvpVRU**

Step 6 Define a default VRU.

On the **CICM**, ICM Configuration Manager, **System Information** tool, in the General section:

- Define a default Network VRU: **cvpVRU**

Step 7 Create the VRU and routing scripts.

On the **CICM**, ICM **Script Editor** tool:

Create the VRU scripts and routing scripts to be used for IVR treatment and agent transfer, as described in other sections of this manual and in the Unified ICME manuals. The VRU scripts are associated with the applicable Network VRU, that is, **cvpVRU**.

Use the ICM Script Editor's SendToVRU node to connect the call to the Network VRU.

Note A RunVRU Script or Queue node is an **`implicit`** SendToVRU node, although error handling will be easier if the explicit **`SendToVRU`** node is used.

Step 8 Configure the ECC variables.

On the **NAM** and **CICM**, ICM Configuration Manager, configure the ECC variables.

For more information, see Define Unified CVP ECC Variables, on page 181.

Step 9 Configure dialed numbers and call types.

On the **NAM** and **CICM**, ICM Configuration Manager, configure dialed numbers and call types.

For more information, see ICM Configuration Guide for Cisco ICM Enterprise Edition

Step 10 Define customers.

On the **NAM** and **CICM**, ICM Configuration Manager:

a) If necessary, differentiate VRUs (Unified CVPs) based on dialed number.
b) Define customers and their Network VRU.

For more information, see Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189.

Step 11 On Cisco Unified CM, configure Unified CM.

For more information, see the Unified CM user documentation.

Step 12 Install and configure the Call Server.

In the Operations Console, select **Device Management** > **CVP Call Server**.

a) Install and configure the Call Server.
b) To enable the ICM and IVR Services on the Call Server, select the **ICM** and **IVR** check boxes.

Step 13 Configure the ICM Service for each Call Server.

In the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. For each Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a) VRU connection port number.

   Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b) Set the maximum length DNIS to the length of the Network Routing Number.

   Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c) Call service IDs: New Call and Pre-routed.

   Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab

d) Trunk group IDs: New Call and Pre-routed.

   Enter the new and pre-routed call trunk group IDs. Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route.

   Configure the number of ports according to the licenses purchased and capacity. Configure each of the numbers used for translation routes. (The **`New Call`** group is not used because the calls are sent to the VRU (Unified CVP) after an initial processing by the NIC/Unified ICME).

e) Check the default values of other settings and change, if desired.

Step 14 Configure the IVR service.

In the Operations Console, select **Device Management** > **CVP Call Server** > **IVR** and configure the **IVR Service**.

Check the default values and change, if desired.

See the Operations Console online help for information about settings.

Step 15 (Optional) Configure the Reporting Server.

On the Operations Console, select **Device Management** > **CVP Reporting Server** > **General** and configure the Reporting Server.

a) Configure the Reporting Server.
b) Select a Call Server to associate with this Reporting Server.
c) Check the default values of the Reporting properties and change, if desired.

For more information, see Reporting Guide for Cisco Unified Customer Voice Portal available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Related Topics

Set Up Type 8 VRU-Only Call Flow Model for ICME and ICMH, on page 56
Define Unified CVP ECC Variables, on page 181
Common Configuration for Differentiating VRUs Based on Dialed Number, on page 189

Pass Data to Unified ICME

In the Unified CVP VXML Server (standalone) with ICM Lookup call flow model, Unified ICME sends a label to Unified CVP. This process requires the following configuration:

The Standalone with Request ICM Label variation of the Standalone call flow model performs a route request to Unified ICME, and then Unified ICME starts a script (new call). Unified ICME sees whatever the device puts in the new call message, then Unified ICME chooses a target, such as an agent, and sends a label back to the device. That route request to Unified ICME sends other information, such as ECC variables. Unified ICME can pass other ECC variables to Unified CVP. Also, you need to configure a Unified CVP VXML Server in the Unified CVP Call Server for the call flow model.

Configure the Connections

The following procedure describes how to set up a VXML Server that connects to a Call Server through the ICM Service, and the connection from the ICM Service to the peripheral gateway.

Note The VRU PIM initiates the connection from the PG to the Call Server. The ICM Service listens for a connection from the VRU PIM.

Procedure

Step 1 Start the VXML Server. The VXML Server starts the VoiceXML Service using the DataFeed mechanism or the ReqICMLabel element.

The ReqICMLabel element allows a Call Studio script to pass caller input, call variables, and External Call Context (ECC) variables to a Unified ICME script. The ReqICMLabel must be inserted into a Call Studio script as a decision element. In Call Studio, the returned Unified ICME label contains a result which can be used by other elements in the same application, such as the Transfer or Audio element. The Transfer element sends instructions to the IOS Voice Browser to transfer the caller to the desired location.

After the VoiceXML Service starts, it starts communicating with the ICM Service.

Step 2 Log in to the Operations Console and configure a Call Server and ICM service. See Configure Call Server, on page 77. See the Unified ICME documentation for instructions on configuring the VRU PIM to connect to a VRU. For example, Unified CVP.

Related Topics

Configure Call Server, on page 77

Configure a Gateway for IP to TDM Calls

The following components are required for the gateway to process IP to TDM calls:

- Phones and numbers must be configured on the TDM switch.
- Gateway must be defined on Unified CM.
- Route pattern on the Unified CM that sends the call to the gateway.
- Dial peer on the gateway that sends calls that must be configured.
- Dial 888800605x on the IP phone (this is a specific physical phone extension).

Procedure

Step 1 Configure the gateway to send the call to a particular Unified CVP VXML Server application, as follows:

```
dial-peer voice 8888 voip
service [gateway application name]
incoming called-number 888800....
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

Step 2 To match the number in the Unified CVP VXML Server transfer node and send it out the T1 port to the G3 to its destination, use the following configuration:

```
dial-peer voice 8880 pots
destination-pattern 888800....
incoming called-number
```

```
direct-inward-dial
port 1/0:D
```

Configure a Cisco Multiservice IP-to-IP Gateway for Unified CM Connections

For information on configuring the Cisco IOS gateway for Unified CM connections, see the Cisco Multiservice IP-to-IP Gateway Software documentation.

Configure SNMP Monitoring for the Unified CVP VXML Server

When a Call Studio application is created, the simple network management protocol (SNMP) monitoring for the VXML Server is provided. **CVPSNMPLogger** is enabled when a new Call Studio application is created and deployed to the Unified CVP VXML Server. **CVPSNMPLogger** logs error events received from theVXML Server. For example, using this process you can configure to send a page to a technical support representative when a particular error alert is triggered on the customer site.

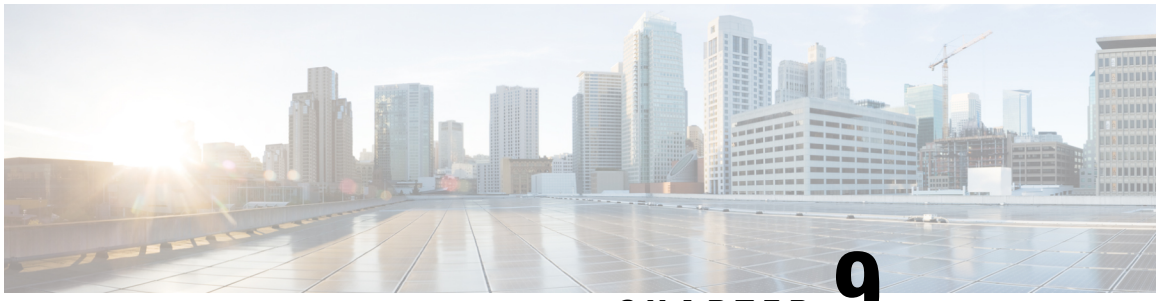
Procedure

Step 1 To view **CVPSNMPLogger** for the Unified CVP VXML Server, access the Call Studio interface.

Step 2 From Call Studio for each Call Studio application, right-click the application and select **Properties** > **Cisco Unified CVP** > **General Settings**.

CVPSNMPLogger appears in the **Loggers** drop-down box.

Caution Do not remove **CVPSNMPLogger** because doing so disables viewing of SNMP events and alerts.



CHAPTER 9

Unified Communications Manager Configuration

Configure Unified Communications Manager Server

Procedure

Step 1 From the Operations Console, select **Device Management** > **Unified CM**.

Step 2 Click **Add New** to add a new Unified CM or click **Use As Template** to use an existing template to configure the new Unified CM.

Step 3 Click the following tabs and configure the settings based on your call flow model:

a) **General** tab. For more information, see General Settings, on page 206 .

b) **Device Pool** tab. For more information about adding, deleting, and editing a device pool, see Add or Remove Device From Device Pool, on page 97.

Note Enable Cisco AXL Web Service on the Unified CM for the synchronization to work.

Step 4 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.

Step 5 Click **Save**.

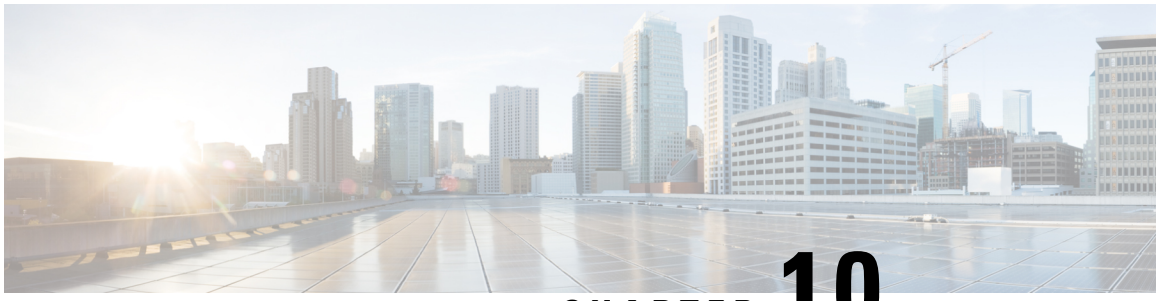
Unified CM Settings

General Settings

Table 30: Unified CM Server—General Tab Settings

Field	Description	Default	Value	Restart Required
IP Address	The IP address of the Unified CM Server.	None	Valid IP address	No
Hostname	The name of the Unified CM Server	None	Valid DNS names, includes letters in the alphabet, the numbers 0 through 9, and a dash.	No
Description	The description of the Unified CM Server	None	Any text	No
Device Admin URL	The Administration URL for the Unified CM Server	None	A valid URL. The Operations Console validates the URL for syntax errors but does no validation for the existence of the URL.	No
Enable Synchronization				
Enable synchronization	Select to enable synchronization for location. If enabled, the Operations Console extracts or synchronizes the Unified CM location information from the Unified CM server.	Disabled When you enable this service, the default value of the Port is 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

Field	Description	Default	Value	Restart Required
Port	The port to which the Unified CM server connects while establishing initial contact.	8443	1 through 65,535	No



CHAPTER 10

SIP Devices Configuration

Set Up Ingress Gateway to Use Redundant Proxy Servers

Configure the gateway with the following code to send calls to redundant proxy servers as resolved using DNS SRV lookup:

```
ip domain name <your domain name>
ip name-server <your DNS server>
sip-ua
sip-server dns:<your SRV cluster domain name>
dial-peer voice 1000 voip
session target sip-server
```

Set Up Call Server with Redundant Proxy Servers

Use redundant proxy servers for Unified CVP outbound calls by using a DNS-based SRV cluster name or a non-DNS SRV cluster name (also known as Server Group Name).

See the *Operations Console User's Guide for Cisco Unified Customer Voice Portal* on how to configure local based SRV records.

Local SRV File Configuration Example for SIP Messaging Redundancy

Load-Balancing SIP Calls

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

- Using the CUSP server, define several static routes with the same route pattern, priorities, and weights.
- Using DNS, configure SRV records with priorities and weights. 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 Unified CM.

Note Refer to DNS Zone File Configuration for Comprehensive Call Flow Model, on page 31 for information about load balancing and failover without a Proxy Server. Only the DNS SRV method is supported for load balancing and failover without a Proxy Server.

Related Topics

DNS Zone File Configuration for Comprehensive Call Flow Model, on page 31

Cisco Unified SIP Proxy (CUSP) Configuration

The following configuration shows a CUSP proxy in Unified CVP. The highlighted lines are specific to a Unified CVP solution. For additional configuration details, refer to the Configuring Cisco Unified SIP Proxy Server guide.

Configuration Example:

```
server-group sip global-load-balance call-id
                            server-group sip retry-after 0
                            server-group sip element-retries udp 1
                            server-group sip element-retries tls 1
                            server-group sip element-retries tcp 1
                            sip dns-srv
                            no enable
                            no naptr
                            end dns
                          !
                          no sip header-compaction
                          no sip logging
                          !
                          sip max-forwards 70
                          sip network netA noicmp
                          non-invite-provisional 200
                          allow-connections
                          retransmit-count invite-server-transaction 9
                          retransmit-count non-invite-client-transaction 9
```

```
retransmit-count invite-client-transaction 2
retransmit-timer T4 5000
retransmit-timer T2 4000
retransmit-timer T1 500
retransmit-timer TU2 32000
retransmit-timer TU1 5000
retransmit-timer clientTn 64000
retransmit-timer serverTn 64000
end network
!
no sip peg-counting
!
sip privacy service
sip queue message
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue radius
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue request
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue response
drop-policy head
low-threshold 80
size 2000
thread-count 20
end queue
!
sip queue st-callback
drop-policy head
low-threshold 80
size 2000
thread-count 10
end queue
!
sip queue timer
drop-policy none
low-threshold 80
size 2500
thread-count 8
end queue
!
sip queue xcl
drop-policy head
low-threshold 80
size 2000
thread-count 2
end queue
!
route recursion
!
```

```
sip tcp connection-timeout 240
sip tcp max-connections 256
!
no sip tls
!
trigger condition in-netA
    sequence 1
    in-network netA
    end sequence
    end trigger condition
    !
    trigger condition mid-dialog
    sequence 1
    mid-dialog
    end sequence
    end trigger condition
    !
    trigger condition out-netA
    sequence 1
    out-network netA
    end sequence
    end trigger condition
!
accounting
no enable
no client-side
no server-side
end accounting
!
server-group sip group cucm-cluster.cisco.com netA
 element ip-address 10.86.129.219 5060 udp q-value 1.0 weight 10
 element ip-address 10.86.129.62 5060 udp q-value 1.0 weight 10
 element ip-address 10.86.129.63 5060 udp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
 !
 server-group sip group cvp-call-servers.cisco.com netA
 element ip-address 10.86.129.220 5060 udp q-value 1.0 weight 10
 element ip-address 10.86.129.224 5060 udp q-value 0.9 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
 !
 server-group sip group vxml-gws.cisco.com netA
 element ip-address 10.86.129.229 5060 udp q-value 1.0 weight 10
 element ip-address 10.86.129.228 5060 udp q-value 1.0 weight 10
 failover-resp-codes 503
 lbtype global
 ping
 end server-group
 !
 route table cvp-route-table
 key 9 target-destination vxml-gws.cisco.com netA
 key 8 target-destination cvp-call-servers.cisco.com netA
 key 7 target-destination vxml-gws.cisco.com netA
 key 700699 target-destination cvp-call-servers.cisco.com netA
 key 2 target-destination cucm-cluster.cisco.com netA
 key 1 target-destination cucm-cluster.cisco.com netA
 key 7000 target-destination 172.19.151.41 netA
 key 777333 target-destination cvp-call-servers.cisco.com netA
 key 1004 target-destination 10.86.139.84 netA
```

```
 key 7105 target-destination dialer-gws netA
 end route table
 !
 policy lookup cvp-policy
 sequence 1 cvp-route-table request-uri uri-component user
 rule prefix
 end sequence
 end policy
 !
 trigger routing sequence 1 by-pass condition mid-dialog
 trigger routing sequence 10 policy cvp-policy condition in-netA
 !
 server-group sip ping-options netA 10.86.129.200 5038
 method OPTIONS
 ping-type adaptive 5000 10000
 timeout 500
 end ping
 !
 server-group sip global-ping
 sip listen netA udp 10.86.129.200 5060
!
end
```

Configure Custom Streaming Ringtones

You can configure custom ringtone patterns that enable you to play an audio stream to a caller in place of the usual ringtone. Customized streaming ringtones are based on the dialed number destination and, when configured, play an in-progress broadcast stream to the caller while the call is transferred an agent.

Procedure

Step 1 Configure Helix for streaming audio.

The default installation and configuration of the Helix server is all that is required for use with Unified CVP. See the *Helix Server Administration Guide* for information about installing and configuring the Helix Server.

Step 2 In the Operations Console, perform the following steps to configure custom streaming ringtones:

a) Select **System** > **Dialed Number Pattern** .
b) Click **Add New**.
c) Complete the following fields to assoicate a dialed number pattern with a custom ringtone.

Table 31: Dialed Number Pattern Configuration Settings

Property	Description	Default	Value
General Configuration			

Property	Description	Default	Value
Dialed Number Pattern	The actual Dialed Number Pattern.	None	Must be unique Maximum length of 24 characters Can contain alphanumeric characters, wildcard characters such as exclamation point (!) or asterisk (*), single digit matches such as the letter X (not x) or period (.) Can end with an optional greater than (>) wildcard character
Description	Information about the Dialed Number Pattern.	None	Maximum length of 1024 characters
Enable Custom Ringtone	Enables customized ring tone. • **Ringtone media filename -** Enter the name of the file that is to be played for the respective dialed number pattern. Provide the URL for the stream name in the following format: `rtsp://<streaming server IP address>:<port>/<directory>/<filename>.rm`	Disabled none	Maximum length of 256 characters Cannot contain whitespace characters

d) Click **Save** to save the Dialed Number Pattern.

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

e) Access the IOS device in global configuration mode and add the following commands on your VXML Gateway:

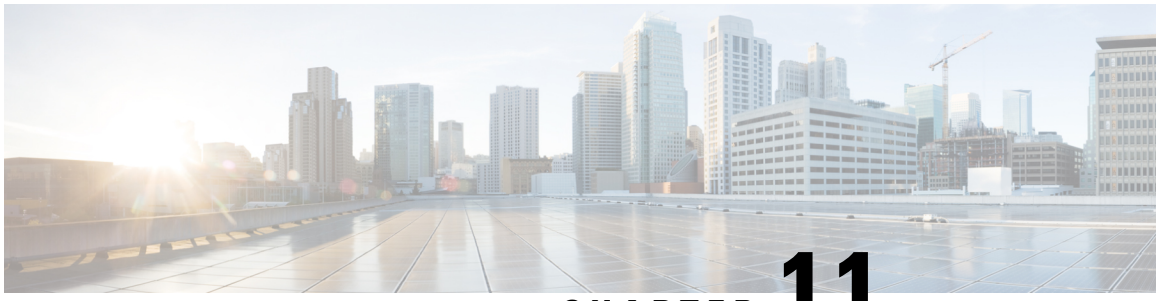
```
rtsp client timeout 10

rtsp message timeout 10
```

The range is 1 to 20; the recommended value is 10 seconds.

Step 3 Add a Send to VRU node in your ICM script before any Queue node.

The explicit Send to VRU node is used to establish the VRU leg before the transfer to the agent; this is required to play streaming audio ringtones to a caller.



CHAPTER 11

Media Server Configuration

Configure Media Server

Procedure

Step 1 From the Unified CVP Operations Console, select **Device Management** > **Media Server**.

Step 2 Click **Add New** to add a new Media Server or click **Use As Template** to use an existing template to configure the new Media Server.

Step 3 Click the following tabs and configure the settings based on your call flow:

a) **General** tab. For more information, see General Settings, on page 218.

b) **Device Pool** tab. For more information about adding, deleting and editing device pool, see Add or Remove Device From Device Pool, on page 97.

Step 4 Click **Save**.

What to do next

All the configured Media Servers appear in the **Default Media Server** drop-down box. To set the default Media Server, select one of the listed Media Servers from the **Default Media Server** drop-down box, and click **Set**.

Related Topics

General Settings, on page 218
Add or Remove Device From Device Pool, on page 97

Media Server Settings

General Settings

Table 32: Media Server—General Tab Settings

Field	Description	Default	Value	Restart Required
IP Address	The IP address of Media Server	None	Valid IP address.	No
Hostname	The name of the Media Server	None	Follow naming conventions for hostnames.	No
Description	The description of the Media Server	None	Up to 1,024 characters.	No
FTP Enabled	Indicates whether a Media Server has FTP enabled. A Media Server, which has FTP enabled, is automatically populated as a session variable to the VXML Server. The default agent greeting recording application automatically uses the Media Servers defined in the Operations Console that have FTP enabled for the agent greeting recording. If Microsoft FTP Service is not enabled in Windows Services Control Panel, then set it to Automatic and start the service. SFTP is also supported with Media Servers.	Disabled	Select the check box to enable this feature.	No Use **Test Sign-in** button to verify the FTP credentials.

Field	Description	Default	Value	Restart Required
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. 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	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). For SFTP, use port 22 or any other custom port that you may have configured.	21	Valid ports are 1 to 65,535.	No Use Test Sign-in button to verify the FTP credentials.

Media Server Association with Call Server and VXML Server

Note Unified CVP Call Server, Media Server, and Unified CVP VXML Server are co-resident on the same server.

If your Unified CVP Call Server, Media Server, and UnifiedCVP VXMLServer reside on the same hardware server and you have multiple co-resident servers, UnifiedCVP does not automatically use the same physical server for call control, VXML, and media file services. If the components are co-resident, no component is forced to use the other co-resident components, and Unified CVP might possibly use the components located on another server.

By default, the components are load balanced across all of the physical servers and do not attempt to use the same server for all of the services. During thousands of calls, all of the components on all of the servers are load balanced and equally utilized, but one specific call could be using several different physical servers. For example, for one particular call you can be using SIP call control on one server, VoiceXML on another server, and the media files on another server.

You can simplify management and troubleshooting by configuring Unified CVP to use the same physical server for all of these functions on a per-call basis. If there is only one server in the system, then simplification is not a concern. The instructions in the following procedures show you how to configure UnifiedCVP so that

it uses components on the same physical server instead of load balancing and using a random server for each component.

Note For routing client name, follow RFC 952 guidelines.

Choose Coresident Unified CVP VXML Server in ICM Script Editor

Procedure

Step 1 Set up the **media_server** ECC variable that specifies your UnifiedCVP VXMLServer in the ICM script by using use the Formula Editor to set the **media_server** ECC variable to **concatenate("http://",Call.RoutingClient,":7000/CVP")**.

Call.RoutingClient is the built-in call variable that ICM sets automatically for you. The routing client name in ICM is usually not the same as the UnifiedCVP Server's hostname.

Step 2 Apply the routing client name as a hostname in the VXML gateway. Do not use noncompliant characters such as an underscore as part of the hostname because the router cannot translate the hostname to an IP address if it contains noncomplaint characters. Use the **ip hostname strict** command in the router to prevent the use of invalid characters in the hostname. This action ensures that the hostname is acceptable to UnifiedCVP.

Step 3 Configure the routing client hostname for every UnifiedCVP Server Routing Client.

Choose Coresident Media Server in Call Studio

Procedure

Step 1 In the ICM script, set one of the **ToExtVXML[]** array variables with the call.routingclient data, such as ServerName=call.routingclient. This variable is passed to the UnifiedCVP VXMLServer, and the variable is stored in the session data with the variable name ServerName.

Step 2 In Cisco Unified Call Studio, use a substitution to populate the Default Audio Path. Add the Application_Modifier element found in the Context folder, and specify the Default Audio Path in the Settings tab in the following format: **http://***{Data.Session.ServerName}*

Choose Coresident VXML Server Using Micro-Apps

If you are using Micro-Apps in conjunction with the Unified CVP VXMLServer, pay careful attention to the **media_server** ECC variable in the ICM script because the same variable is used to specify both the Unified CVP VXML Server and the media server, but the contents of the variable use a different format depending on which server you want to specify. Use the **media_server** ECC variable as indicated in this procedure whenever you want to use a Micro-App for prompting. If you subsequently want to use the Unified CVP VXML Server, rewrite this variable by following the previous procedure.

Procedure

Step 1 Set up the **media_server** ECC variable that specifies your Media server in the ICM script by using the Formula Editor to set the **media_server** ECC variable to **concatenate("http://",Call.RoutingClient)**

Call.RoutingClient is the built-in call variable that ICM sets automatically for you. The routing client name in ICM usually is not the same as the Unified CVP Server hostname.

Step 2 Use the name of the routing client as a hostname in the VoiceXML Gateway.

Do not use noncompliant characters such as an underscore as part of the hostname because the router cannot translate the hostname to an IP address if it contains any noncomplaint characters. Use the **ip hostname strict** command in the router to prevent the use of invalid characters in the hostname and to ensure that the hostname is acceptable to Unified CVP.

Step 3 Configure the routing client hostname for every Unified CVP Server Routing Client.

Microsoft Windows IIS Cache Expiration

Procedure

To allow new media files to replace their predecessor in a reasonable amount of time while minimizing requests for data to the media server from the VXML Gateway or Virtualized Voice Browser, configure a cache expiration value in IIS Manager. The ideal value will require testing as it depends on how frequently media files are changed.

To configure a cache expiration value in IIS Manager:

a) Find the site you are using, go to the folder where the media files are being stored, and then click **HTTP Response Headers**.
b) Click **Set Common Headers** on the Actions panel.
c) Select **Expire Web Content** and set the desired value.

Media File Names and Types

A *media file name* is specified through Unified ICME Network VRU Script Configuration and used in the Run VRU Script request for the Play Media, Play Data, Get Digits, Menu, and Get Speech (in non-TTS applications) micro-applications. The media file naming convention allows alpha-numeric characters with the underbar character as a separator. (Spaces or hyphens are not allowed.) This naming convention provides a mechanism for an “understandable” naming convention as opposed to numeric media file names typically used by stand-alone VRUs.

Caution The Unified Customer Voice Portal includes a library of media files/prompts for individual digits, months (referenced internally by Unified Customer Voice Portal software for a Play Data script type request), default error messages, and so on. **Creation of a full set of media/prompts for each locale referenced by the Unified CVP customer is the responsibility of the customer's Media Administrator.**

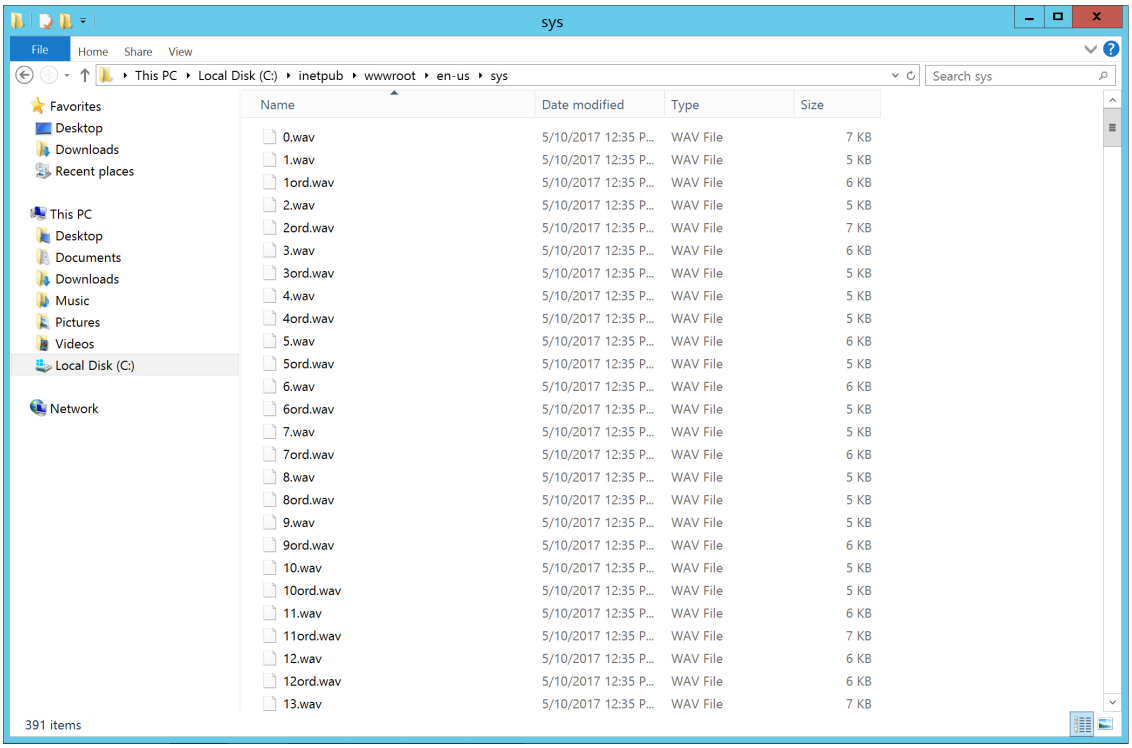
The *media file types* Unified CVP supports are µ-Law 8-bit .wav files and A-law 8-bit .wav files. Media files specified with an extension are used "as is," for example, hello.xxx. (The default file extension is .wav.)

Caution Any unexpected (and unsupported) type of media file encountered generates the logging of an error and a result code of False is returned to Unified ICME along with the ECC **user.microapp.error_code** set appropriately. From the caller's perspective, nothing was played, however it is the Script Editor developer's responsibility to write the script to handle this error condition.

Location of Media Files

The following figure displays the location of the media files if you choose to install System Media Files during Unified CVP installation.

Figure 15: Location of Media Files



Media File Address

The address for media files that reside on the Media Server(s) is generated by the Unified CVP. Unified ICME provides information about the file location or base URL address in the Unified ICME/IVR messages it passes when the Run VRU Script node is run. The Unified ICME/IVR messages include ECC variables for: locale, media server set address, as well as optional system and application library name overrides. (For details about the Unified ICME/IVR messages passed to Unified CVP, see *Feature Guide - Writing Scripts for Unified Customer Voice Portal*.

The table below summarizes the data that combines to form the address of the media file:

Table 33: Media File Address Components

Parameter	Location of Data	Description	Examples
Media Server Set	ECC variable: user.microapp.media _server	File location or base URL for the Media Server. When the Media Server URL is the DNS name and the DNS Server is configured to return multiple IP addresses for a host name, the Unified CVP attempts to get the media files from each Media Server IP address in sequence with the priority given to those on the subnet. **Note** Unified CVP supports playing prompts from flash on the GW. To play these prompts, set the media_server to "flash:" instead of the hostname or IP address of the media server. When using the Media Server set for external grammars or external VXML, if the Media Server URL is the DNS name with multiple IP addresses for the hostname, it is the ASR Engine's responsibility to decide which machine to retrieve the grammar file from. **Note** Tomcat version (9.0.8) packaged with CVP does not support underscore "_" in the hostname. Therefore, it is recommended to set `user.microapp.media_server` to a hostname that does not use "_".	Base URL example: **http://www.machine1.com /dir1/ dirs/cust1** **Note** By convention, the service provider may include their customer names at the end of the Media Server set.
Locale	ECC variable: user.microapp.locale **Default:** en-us	This field is a combination of language and country with a default of en-us for English spoken in the United States.	en-us

Note The Unified CVP supports the following locales: **en-us** (English, United States) and **en-gb** (English, United Kingdom), **es-es** (Spanish, Spain), and **es-mx** (Spanish, Mexico). The locale defines the grammar of a Play Data script type. If a date is to be played with a locale of **en-gb** (English, United Kingdom), the date would be played in the order of day, month, then year; for **en-us**, it is month, day, year.

Parameter	Location of Data	Description	Examples
Media Library Type	The Media Library Type value passed from the VRU Script Name field. Valid options are: **A** - Application prompt library. **S** - System prompt library. **V** - External VXML. **Default:** A	The media library (directory) for the prompt is either the application prompt library defined by ECC variable user.microapp.app_media_lib (default "app") or the system prompt library defined by ECC variable user.microapp.sys_media_lib (default "sys"). **Note** When the Media Library Type is V (external VXML), the VXML file will reside in the Application Prompt Library. **Note** When the Media Library Type is A (Application prompt library), you must create the directory specified by this variable. For example, if you use the default "app" directory, you must create an app directory in ./wwwroot/en-us	**A** (user.microapp.app_media_lib= app_banking)
Media File Name	The Media File Name value passed from the VRU Script Name field. Valid options are the name of the .wav file to be played, or external VXML file name, or <blank>, which translates to playing no media. This file name is ignored if TTS is being used (that is, if the **user.microapp.inline_tts** ECC variable contains a value.) **Default:** none	Name of media file or external VXML file to be played.	Main_menu
Note There are four possible reasons for using <blank> as the Media File Name: (1) For Get Digits, a prompt may not be necessary, (2) the customer may want to have a "placeholder" in the script for playing a prompt which may or may not be there (for example, an emergency conditions message), (3) change the value of barge-in to indicate a buffer flush, and (4) TTS is being used and this field is ignored.			
Media File Name Type	If not given as part of the Media File Name, the type is .wav	Type of media file to be played.	.wav

Based on the examples shown in the table above, a valid address for the Media File might be:

http://www.machine1.com/dir1/dirs/cust1/en-us/app_banking/main_menu.wav

Locale Backward Compatibility

The locale string values are compatible with current industry naming schemes:

- **en_US** has changed to **en-us**, which means that "**en** underscore **US**" (upper case) has changed to "**en** hyphen **u**s" (lower case).
- **en_GB** has changed to **en-gb**, which means that "**en** underscore **GB**" (upper case) has changed to "**en** hyphen **gb**" (lower case).

Existing scripts from previous versions of Unified CVP will continue to work with the current version of Unified CVP:

- **en_US** and **en-us** both map to U.S. English in the Application Server for use by the Application Server's internal grammar
- **en_GB** and **en-gb** both map to U.K. English in the Application Server for use by the Application Server's internal grammar.
- The base URL for media prompts uses the locale that is specified, without making modifications. For example, if the locale is set to **EN_US**, the base URL contains **EN_US**. If the locale is set to **XX**, the base URL contains **XX**.

To use the Unified CVP Version 1.1 default locale directory (for example, **en_US**), you must explicitly set it. When you upgrade to the current version of Unified CVP, only the new files are installed under the Unified CVP default locale directory, **en-us**. You want to have all your system prompts under one directory and all your application prompts and, optionally, external VXML in another directory. Use the **user.microapp.locale** ECC variable to set the locale directory to use, such as **en_US**.

Note Do not set the **user.microapp.locale** ECC variable if you used the default **en-us**. Also, remember that all locale values are case-sensitive.

System Media Files

The following tables describe the English System Media Files installed by Unified CVP. These system media files are intended as samples only. It is the Customer/Media Administrator's responsibility to record all the system prompts for all the locales.

The table that follows lists the System Media File information for cardinal numbers.

Table 34: System Media Files, Cardinal Numbers

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		point	point	Number
		minus	minus	Number
0	48	0	zero	All except DOW
1	49	1	one (masculine version), uno (es-mx and es-es)	All except DOW
2	50	2	two	All except DOW
3	51	3	three	All except DOW
4	52	4	four	All except DOW
5	53	5	five	All except DOW
6	54	6	six	All except DOW
7	55	7	seven	All except DOW
8	56	8	eight	All except DOW
9	57	9	nine	All except DOW
		10	ten	Same for the rest of all the numbers
		11	eleven	
		12	twelve	
		13	thirteen	
		14	fourteen	
		15	fifteen	
		16	sixteen	
		17	seventeen	
		18	eighteen	
		19	nineteen	
		20	twenty	
		21	twenty-one	
		22	twenty-two	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		23	twenty-three	
		24	twenty-four	
		25	twenty-five	
		26	twenty-six	
		27	twenty-seven	
		28	twenty-eight	
		29	twenty-nine	
		30	thirty	
		31	thirty-one	
		32	thirty-two	
		33	thirty-three	
		34	thirty-four	
		35	thirty-five	
		36	thirty-six	
		37	thirty-seven	
		38	thirty-eight	
		39	thirty-nine	
		40	forty	
		41	forty-one	
		42	forty-two	
		43	forty-three	
		44	forty-four	
		45	forty-five	
		46	forty-six	
		47	forty-seven	
		48	forty-eight	
		49	forty-nine	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		50	fifty	
		51	fifty-one	
		52	fifty-two	
		53	fifty-three	
		54	fifty-four	
		55	fifty-five	
		56	fifty-six	
		57	fifty-seven	
		58	fifty-eight	
		59	fifty-nine	
		60	sixty	
		61	sixty-one	
		62	sixty-two	
		63	sixty-three	
		64	sixty-four	
		65	sixty-five	
		66	sixty-six	
		67	sixty-seven	
		68	sixty-eight	
		69	sixty-nine	
		70	seventy	
		71	seventy-one	
		72	seventy-two	
		73	seventy-three	
		74	seventy-four	
		75	seventy-five	
		76	seventy-six	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		77	seventy-seven	
		78	seventy-eight	
		79	seventy-nine	
		80	eighty	
		81	eighty-one	
		82	eighty-two	
		83	eighty-three	
		84	eighty-four	
		85	eighty-five	
		86	eighty-six	
		87	eighty-seven	
		88	eighty-eight	
		89	eighty-nine	
		90	ninety	
		91	ninety-one	
		92	ninety-two	
		93	ninety-three	
		94	ninety-four	
		95	ninety-five	
		96	ninety-six	
		97	ninety-seven	
		98	ninety-eight	
		99	ninety-nine	
		oh	oh	24TOD, Date
		hundred	hundred	Number, 24TOD, Date, Currency

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		thousand	thousand	Number, Date, Currency
		million	million	Number, Currency
		billion	billion	Number, Date, Currency
		trillion	trillion	Number, Currency

The table that follows lists the System Media File information for ordinal numbers.

Note If ordinal system prompts are to be used in a script for a purpose other than dates, they should be recorded as application prompts with the true ordinal values.

Table 35: System Media Files, Ordinal Numbers

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		1ord	first	Date
		2ord	second	Date for all ordinal numbers
		3ord	third	
		4ord	fourth	
		5ord	fifth	
		6ord	sixth	
		7ord	seventh	
		8ord	eighth	
		9ord	nineth	
		10ord	tenth	
		11ord	eleventh	
		12ord	twelveth	
		13ord	thirteenth	
		14ord	fourteenth	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		15ord	fifteenth	
		16ord	sixteenth	
		17ord	seventeenth	
		18ord	eighteenth	
		19ord	nineteenth	
		20ord	twentieth	
		21ord	twenty-first	
		22ord	twenty-second	
		23ord	twenty-third	
		24ord	twenty-fourth	
		25ord	twenty-fifth	
		26ord	twenty-sixth	
		27ord	twenty-seventh	
		28ord	twenty-eight	
		29ord	twenty-nineth	
		30ord	thirtieth	
		31ord	thirty-first	

The table that follows lists the System Media File information for measurements.

Table 36: System Media Files, Measurements

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
½	189	one_half	one half	Char
¼	188	one_quarter	one quarter	Char
¾	190	three_quarters	three quarters	Char
A, a	65,97	a	A	Char
B,b	66,98	b	B	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
C, c	67,99	c	C	Char
D, d	68,100	d	D	Char
E, e	69,101	e	E	Char
F, f	70,102	f	F	Char
G, g	71,103	g	G	Char
H, h	72,104	h	H	Char
I, I	73,105	I	I	Char
J, j	74,106	j	J	Char
K, k	75,107	k	K	Char
L, l	76,108	l	L	Char
M, m	77,109	m	M	Char
N, n	78,110	n	N	Char
O, o	79,111	o	O	Char
P, p	80,112	p	P	Char
Q, q	81,113	q	Q	Char
R, r	82,114	r	R	Char
S, s	83,115	s	S	Char
T, t	84,116	t	T	Char
U, u	85,117	u	U	Char
V, v	86,118	v	V	Char
W, w	87,119	w	W	Char
X, x	88,120	x	X	Char
Y, y	89,121	y	Y	Char
Z, z	90,122	z	Z	Char
Œ, œ	140,156	oe_140_156	Ligature OE	Char
À,à	192,224	a_192_224	A grave	Char
Á,á	193,225	a_193_225	A acute	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Â,â	194,226	a_194_226	A circumflex	Char
Ã,ã	195,227	a_195_227	A tilde	Char
Ä,ä	196,228	a_196_228	A umlaut	Char
Å,å	197,229	a_197_229	A with ring above	Char
Æ,æ	198,230	ae_198_230	Ligature AE	Char
È,è	200,232	e_200_232	E grave	Char
É,é	201,233	e_201_233	E acute	Char
Ê,ê	202,234	e_202_234	E circumflex	Char
Ë,ë	203,235	e_203_235	E umlaut	
Ì,ì	204,236	i_204_236	I grave	Char
Í, í	205,237	i_205	I acute	Char
Î,î	206,238	i_206	I circumflex	Char
Ï,ï	207,239	i_207	I umlaut	Char
Ð	208	char_208	character 208	Char
ð	240	char_240	character 240	
Ò,ò	210,242	o_210_242	O grave	Char
Ó,ó	211,243	o_211_243	O acute	Char
Ô,ô	212,244	o_212_244	O circumflex	Char
Õ,õ	213,245	o_213_245	O tilde	Char
Ö,ö	214,246	o_214_246	O umlaut	Char
x	215	multiply	multiplication sign	Char
Ø,ø	216,248	o_216_248	oh stroke	Char
Ù,ù	217,249	u_217_249	U grave	Char
Ú,ú	218,250	u_218_250	U acute	Char
Û,û	219,251	u_219_251	U circumflex	Char
Ü,ü	220,252	u_220_252	U umlaut	Char
Ý,ý	221,253	y_221_253	Y acute	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Þ	222	char_222	character 222	Char
ß	223	ss	double s	Char
÷	247	divide	division sign	Char
þ	254	char_254	character 254	Char
Ÿ,ÿ	159,255	y_159_255	character 159 or 255	Char

The table that follows lists the System Media File information for month values.

Table 37: System Media Files, Months

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		January	January	Date
		February	February	Date
		March	March	Date
		April	April	Date
		May	May	Date
		June	June	Date
		July	July	Date
		August	August	Date
		September	September	Date
		October	October	Date
		November	November	Date
		December	December	Date

The table that follows lists the System Media File information for month values.

Table 38: System Media Files, Days

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		Sunday	Sunday	DOW

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		Monday	Monday	DOW
		Tuesday	Tuesday	DOW
		Wednesday	Wednesday	DOW
		Thursday	Thursday	DOW
		Friday	Friday	DOW
		Saturday	Saturday	DOW

The table that follows lists the System Media File information for month values.

Table 39: System Media Files, Time

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		hour	hour	Etime, 24TOD per locale, TOD per locale
		hours	hours	Etime,24TOD per locale,TOD per locale
		minute	minute	Etime
		minutes	minutes	Etime
		second	second	Etime,24TOD
		seconds	seconds	Etime,24TOD
		on	on	per locale(unused for en-us)
		at	at	per locale(unused for en-us)
		am	am	TOD
		pm	pm	TOD
		oclock	oclock	TOD

The table that follows lists the System Media File information for currency values.

Note The customer's Media Administrator may want to replace the contents of "currency_minus" (for the negative amount) and "currency_and" (the latter can even be changed to contain silence).

Table 40: System Media Files, Currency

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		currency_ minus	minus	Currency
		currency_and	and	Currency
$	36	USD_dollar	dollar	Currency
		USD_dollars	dollars	Currency
		Note Unified CVP uses the USD_dollar.wav and USD_dollars.wav media files; the dollar.wav and dollars.wav used by ISN Version 1.0 are no longer installed.		
$	36	CAD_dollar	dollar	Currency
		CAD_dollars	dollars	Currency
		HKD_dollar	dollar	Currency
		HKD_dollars	dollars	Currency
¢	162	cent	cent	Currency
		cents	cents	Currency
		euro	euro	Currency
£	163	GBP_pound	pound	Currency
		GBP_pounds	pounds	Currency
		penny	penny	Currency
		pence	pence	Currency
		MXN_peso	peso	Currency
		MXN_pesos	pesos	Currency
		centavo	centavo	Currency
		centavos	centavos	Currency

The table that follows lists the System Media File information for gaps of silence and miscellaneous phrases.

Table 41: System Media Files, Silence and Miscellaneous Phrases

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
		silence_.1_ sec	(.1 second of silence)	Used for pauses where needed
		silence_.25_ sec	(.25 second of silence)	Used for pauses where needed
		silence_.5_ sec	(.5 second of silence)	Used for pauses where needed
		silence_1_sec	(1 second of silence)	Used for pauses where needed
		and	and	Etime,TOD,25TOD

The table that follows lists the System Media File information for ANSI characters.

Table 42: System Media Files, ANSI Characters

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
	32	space	space	Char
!	33	exclamation_ mark	exclamation mark	Char
"	34	double_ quote	double quote	Char
#	35	pound	pound	Char
%	37	percent	percent	Char
&	38	ampersand	ampersand	Char
'	39	apostrophe	apostrophe	Char
(	40	open_ parenthesis	open parenthesis	Char
)	41	close_ parenthesis	close parenthesis	Char
*	42	asterisk	asterisk	Char
+	43	plus	plus	Char
,	44	comma	comma	Char
-	45	hyphen	hyphen	Char
.	46	period	period	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
/	47	slash	slash	Char
:	58	colon	colon	Char
;	59	semicolon	semicolon	Char
<	60	less_than	less than	Char
=	61	equal	equal	Char
	62	greater_than	greater than	Char
?	63	question_ mark	question mark	Char
@	64	at_symbol	at	Char
[	91	left_square_bracket	left square bracket	Char
\	92	backslash	backslash	Char
]	93	right_square_bracket	right square bracket	Char
^	94	caret	caret	Char
_	95	underscore	underscore	Char
`	96	single_quote	single quote	Char
{	123	open_brace	open brace	Char
|	124	pipe	pipe	Char
}	125	close_brace	close brace	Char
~	126	tilde	tilde	Char
’	130	char_130	low single quote	Char
f	131	char_131	F with hook	Char
”	132	low double quote	low double quote	Char
…	133	ellipsis	ellipsis	Char
†	134	char_134	character 134	Char
‡	135	char_135	character 135	Char
ˆ	136	char_136	character 136	Char
‰	137	per_mille	per mile	Char
Š	138	char_138	character 138	

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
<	139	left_pointing _angle	left pointing angle	Char
‘	145	left_single_ quote	left single quote	Char
’	146	right_single_ quote	right single quote	Char
“	147	left_double_ quote	left double quote	Char
”	148	right_double _quote	right double quote	Char
·	149	bullet	bullet	Char
–	150	en_dash	en dash	Char
—	151	em_dash	em dash	
˜	152	small_tilde	small tilde	Char
™	153	trade_mark	trade mark	Char
š	154	char_154	character 154	Char
›	155	char_155	character 155	Char
¡	161	exclamation_ mark_ inverted	inverted exclamation mark	Char
¤	164	char_164	character 164	Char
¦	166	broken_pipe	broken pipe	Char
§	167	section	section	Char
¨	168	char_168	character 168	Char
©	169	copyright	copyright	Char
ª	170	char_170	character 170	Char
«	171	left_double_ angle_ quote	left double angle quote	Char
¬	172	not	not	Char
-	173	char_173	character 173	Char
®	174	registered	registered	Char
¯	175	char_175	character 175	Char
°	176	degree	degree	Char
±	177	plus_minus	plus or minus	Char

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
²	178	superscript_ 2	superscript two	Char
³	179	superscript_ 3	superscript three	Char
´	180	acute_accent	acute accent	Char
µ	181	micro	micro	Char
¶	182	paragraph	paragraph	Char
·	183	middle_dot	middle dot	Char
¸	184	cedilla	cedilla	Char
¹	185	superscript_ 1	superscript one	Char
º	186	char_186	character 186	Char
»	187	right_double _angle_ quote	right double angle quote	Char
¿	191	question_ mark_ inverted	inverted question mark	Char

Miscellaneous Files

The table that follows lists files that are not used by Unified CVP micro-applications; these files are included for use in customer scripts.

Table 43: Miscellaneous Media Files

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
Error	v	invalid_entry_error	Your entry is invalid.	Error message
	v	no_entry_error	Please make a selection.	Error message
	v	system_error	We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.	Error message

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
	v	critical_error	We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.	Error message
	v	critical_error_ULaw .	We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better	Error message
	v	critical_error_ALaw	We are currently experiencing technical difficulties with this site. Please try again later when we can service you much better.	Error message
	v	440beep	<single beep tone>	Unused
	v	busy_tone	<single busy tone>	Unused
	v	busy_tone30	<busy tone 1 per second for 30 seconds>	Unused
	v	central	Central	Unused
	v	credit_of	Credit Of	Unused
	v	dash	dash	Unused
	v	daylight	daylight	Unused
	v	dialtone	<4 seconds of dial tone>	Unused
	v	dialtone2fastbusy60	<9 seconds of dialtone> followed by <30 seconds of fast busy tone>	Unused
	v	dot	dot	Unused
	v	eastern	Eastern	Unused
	v	ENTER_PHONE_NUMBER	Please enter the phone number.	Unused

Symbol (where applicable)	Decimal Value	Media File Name	Media File Content	Data Play Back Types / When Media File Is Used
	v	fastbusy	<a single fastbusy tone + silence (total of 1 second)>	Unused
	v	fastbusy60	30 seconds of <fastbusy tone>	Unused
	v	FINISHED	When you have finished, press	Unused
	v	goodbye	Goodbye	Unused
	v	Mountain	Mountain	Unused
	v	negative	negative	Unused
	v	of	of	Unused
	v	pmgr_sys	pmgr_sys	Unused
	v	pacific	Pacific	Unused
	v	positive	positive	Unused
	v	ringback	<ring back tone for 1 second followed by 2 seconds of silence>	Unused
	v	savings	savings	Unused
	v	standard	Standard	Unused
	v	Star	star	Unused
	v	thankyou	Thank you	Unused
	v	the	the	Unused
	v	time	time	Unused
	v	try_again	Please try again	Unused

System Media File Error Messages

Three error messages are included with the System Media files:

- **Critical error.** Message played when system problem exists and the SIP Service cannot process the call. (Example content for en-us: “We are currently experiencing technical difficulties with the site, please try again later and we can serve you much better.”)

Note If you do not want an English spoken critical media, you need to copy the language specific files to the location specified in this section.

Critical error messages are *not* located on the Media Server:

- For **SIP Service**, the critical_error.wav media file is located in <*install path*> \OpsConsoleServer\GWDownloads (for example, C:\Cisco\CVP\OpsConsoleServer\GWDownloads).
- For **non-Unified CVP SIP Service**, an error.wav media file is located in <*install path*>\CVP\audio (for example, C:\Cisco\VXMLServer\Tomcat\webapps\CVP\audio).

Note You can record "override" prompts to replace the critical media files. However, you must save them with their original hard-coded names and place them in their original locations.

- **no_entry_error**. Message played when the caller does not respond to a menu prompt. (Example content for en-us: "Please make a selection.") The original prompt is then repeated.
- **invalid_entry_error**. Message played when the caller enters an incorrect response to a menu prompt. (Example content for en-us: "Your entry is invalid.") The original prompt is then repeated.

Note These files are shared by all applications.

If a dialogue needs to be altered for a specific Get Digits, Get Speech or Menu request in the Unified ICME script, override flags can be set in the Network VRU Script Configuration Parameters.

Note Override flags are available for the Get Digits, Get Speech, and Menu micro-applications, only. See *Feature Guide - Writing Scripts for Cisco Unified Customer Voice Portal* for details.

You must record the "override" prompts, save them with the hard coded names <prompt name>_no_entry_error.wav and <prompt_name>_invalid_entry_error.wav, and place them with other application-specific media files in the Application Media library.

Note This override will not work when there is not a specific file name used (for instance, when Unified CVP is using the TTS feature).

Unified CVP Microapplication Configuration

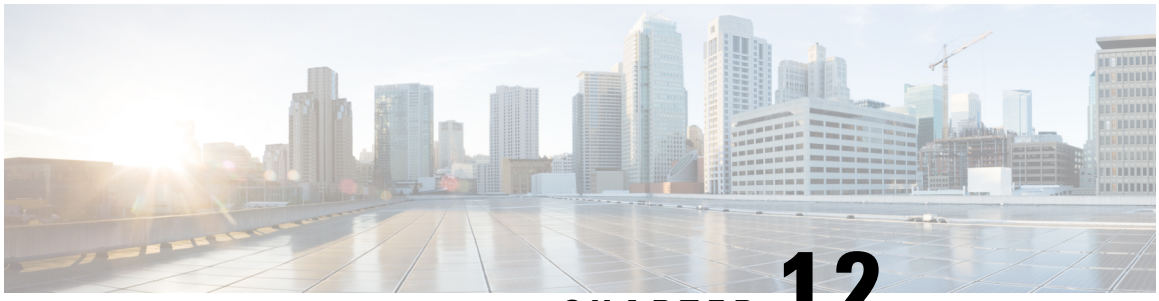
The VoiceXML Gateway sends HTTP requests to an HTTP media server to obtain audio files. It uses the following VoiceXML Gateway configuration parameters to locate a server when not using a load balancer:

```
ip host mediaserver <ip-address-of-primary-media-server>
ip host mediaserver-backup <ip-address-of-secondary-media-server>
```

The backup server is invoked only if the primary server is not accessible, and this is not a load-balancing method. Each new call attempts to connect to the primary server. If failover occurs, the backup server is used for the duration of the call; the next new call will attempt to connect to the primary server.

Note that the Media Server is not a fixed name, and it needs to match whatever name was assigned to the media_server ECC variable in the ICM script.

Note This feature is not required for Cisco VVB as DNS is used to resolve the hostname.



CHAPTER 12

Speech Server Configuration

Configure Speech Server

Before you begin

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

Procedure

Step 1 From the Operations Console, select **Device Management** > **Speech Server**.

Step 2 Click **Add New** to add a new Speech Server or click **Use As Template** to use an existing template to configure the new Speech Server.

Step 3 Click the following tabs and configure the settings based on your call flow model:

a) **General** tab. For more information, see General Settings, on page 246.

b) **Device Pool** tab. Add the Speech Server to a device pool by moving the device pool from **Available** pane to the **Selected** pane. For more information about adding, deleting, and editing device pool, see Add or Remove Device From Device Pool, on page 97.

Step 4 Click **Save** to save the settings in the Operations Server database. Click **Save and Deploy** to deploy the changes to the Speech Server page later.

Related Topics

Add or Remove Device From Device Pool, on page 97

General Settings, on page 246

Speech Server Settings

General Settings

Table 44: Speech Server—General Settings

Field	Description	Default	Value	Reboot/Restart Required
IP Address	The IP address of the Speech Server.	None	Valid IP address	Yes - Reboot Speech Server
Hostname	The host name of the Speech Server.	None	Valid DNS name, includes letters, the numbers 0 through 9, and a dash	Yes - Reboot Speech Server
Description	The description of the Speech Server.	None	Up to 1024 characters	No
Enable secure communication with the Ops console	Select **On** to enable secure communications between the Operations Server and this component. Access the device using SSH and files are transferred using HTTPS.	None	On or Off	No

Generate G729 Prompts for Unified CVP

To generate the G.729 prompts for Unified CVP, perform the following procedure:

- Convert the audio files from G.711 to G.729 format using the Music on Hold (MOH) audio translator.
- Change the G.729 compression identifier in the file header.

Convert the Audio Files from G.711 to G.729 Format

Procedure

Step 1 Log in to the Cisco Unified CM Administration portal and select **Media Resources** > **MOH Audio File Management**.

Step 2 Click **Upload File** and select the G.711 audio files individually.

Step 3 Click **Media Resources** > **MOH Audio File Management** and check whether the audio files have been converted to G.729 format. If the conversion was successful, the recording length of audio files has a nonzero value.

Step 4 Copy the converted audio files to your Windows server using the Secure File Transfer Protocol (SFTP) Server.

Note Do not add spaces when you rename the audio files.

Step 5 Use putty to sign in to the Unified Communications Manager Server as an administrator.

Step 6 From the command prompt, run **file get activelog mohprep/*g729.wav** and provide the SFTP prompts.

Change the G.729 Compression Identifier in the File Header

The G.729 files that the Unified Communications Manager generates have a non-standard compression codec tag in the file header. The VXML Gateway cannot play these audio files, as it does not recognize the codec type. Change the compression codec type value to convert the audio files into the standard G729r8 format.

Use the following procedure to change the compression codec type number in the file header from 0x0133 to the standard 0x14db, G729r8 format.

Procedure

Step 1 Create a folder in the Unified CVP directory. Copy the G.729 audio files that have a nonstandard compression codec tag in the file header into the new folder location.

Step 2 From the command prompt, navigate to the `C:\Cisco\CVP\bin` folder.

Step 3 Perform one of these steps:

- To convert audio files individually, from the command prompt, run **<UCMHeaderFixer.exe Audio file Name>*.***.
- To perform bulk conversion of audio files, from the command prompt, run **UCMHeaderFixer.exe Folder Path**.

The script runs and the audio file is converted from name.g729.wav file into name.wav format.

Step 4 Use the Operations Console to upload the converted audio files to the IOS Gateway.

Configuration

No additional configuration is required for SIP service to use IVR service. By default, the SIP service uses the IVR service that resides on the VXML server. It is also no longer necessary to configure the VoiceXML Gateway with the IP address of the VXML Server's IVR service. When SIP is used, the SIP service inserts the URL of the VXML Server's IVR service into a header in the SIP INVITE message when the call is sent to the VoiceXML Gateway. The VoiceXML Gateway extracts this information from the SIP INVITE and use this information to determine which Call Server to use. The VoiceXML Gateway examines the source IP address of the incoming call from the Call Server. This IP address is used as the address for the VXML Server's IVR service.

The following example illustrates the IOS VoiceXML Gateway bootstrap service that is invoked when a call is received:

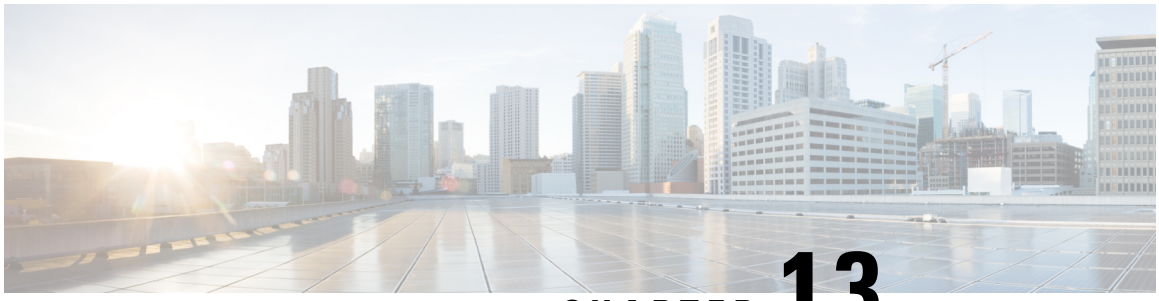
```
service bootstrap flash:bootstrap.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
```

Note For configuring the same feature in Cisco VVB, see section “Cisco VVB configuration for Comprehensive Call Flows”.

With Unified CVP4.0 and later releases, you have to configure the IP address of the Call Server. The bootstrap.tcl learns the IP address of the source Call Server and uses it as its Call Server. There is no need for backup Call Server configuration, because receiving a call from the Call Server means that the server is operational.

The following files in flash memory on the IOS Voice Gateway are also involved with high availability: handoff.tcl, survivability.tcl, recovery.vxml, and several .wav files. Use Trivial File Transfer Protocol (TFTP) to load the proper files into flash. Configuration information for each file can be found within the file itself. For information, see the latest version of the *Configuration Guide for Cisco Unified Customer Voice Portal*, available at:

https://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html



CHAPTER 13

Gateway Configuration

Configure Gateway

Procedure

Step 1 Log in to Operations Console and click **Device Management** > **Gateway**.

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

Step 2 Click **Add New**.

Note To use an existing Gateway as a template for configuring a new Gateway, select a Gateway from the list of available Gateways and click **Use As Template** and perform Steps 3 to 5.

Step 3 Click the **General** tab, enter the field values, and click **Save**. See General Settings, on page 250.

Step 4 (Optional) Click the **Device Pool** tab, enter the field values, and click **Save**. See Add or Remove Device From Device Pool, on page 97.

Step 5 Click **Save**.

Step 6 (Optional) If the call control client placed the Correlation ID in a GTD parameter other than uus.dat, specify the following parameters to configure a gateway to enable incoming UUI to be used as the Correlation ID.

```
conf t
application
service <your-cvp-service-name>
```

```
param use-uui-as-corrid Y (Refer to Note 1)
param correlation-gtd-attribute XXX (Refer to Note 2)
param correlation-gtd-instance N (Refer to Note 2)
param correlation-gtd-field YYY (Refer to Note 2)
dial-peer voice 123 pots
service <your-cvp-service-name>
```

Related Topics

General Settings, on page 250
Add or Remove Device From Device Pool, on page 97

Gateway Settings

General Settings

After adding an IOS Gateway, 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 Time Division Multiplexing (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 and also supports Media Gateway Control Protocol (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 Dual Tone Multi Frequency (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 interactive voice response (IVR) service.

You can deploy the Ingress Gateway 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.

The service configuration parameters for the Call Server host and port are meant for the VRU-Only call flow model for IOS VoiceXML Gateway. These parameters are optional and you can use them to override the IP address or port number of the Call Server that comes through the SIP app-info header.

```
application
service vru-leg flash:bootstrap.tcl
param cvpserverhost xxx.xxx.xxx.xxx  <IP of primary Call Server>
param cvpserverbackup xxx.xxx.xxx.xxx  <IP of backup Call Server>
param cvpserverport 7000 <TCP Port # of Call Server>
```

An Egress Gateway is typically used in Call Director model to provide access to a call center automatic call distributor (ACD) or third-party IVR.

To configure General settings on a Gateway, on the **General** tab, enter the field values, as listed in the following table:

Table 45: Unified ICM—General Tab Configuration Settings

Field	Description	Default	Value	Restart Required
IP Address	The IP address of a Unified ICM Server	None	Valid IP address	No
Hostname	The name of the Unified ICM Server	None	Valid DNS name. It includes alphanumeric characters and a dash.	No
Description	Additional information of the Unified ICM Server	None	Up to 1024 characters	No
Device Admin URL	The URL for the Unified ICM Web configuration application.	None	Valid URL	No

Activate Gateway Configuration

Activate the gateway configuration by entering these commands:

Procedure

Step 1 call application voice load CVPSelfService

Step 2 call application voice load HelloWorld

Add Gateway to Device Pool

See Device Pool, on page 97 and Add or Remove Device From Device Pool, on page 97.

Related Topics

Device Pool, on page 97
Add or Remove Device From Device Pool, on page 97

Configure Gateway Settings for Standalone Call Flow Model

After you configure a gateway through Operations Console, configure settings on the gateway.

Procedure

Step 1 **All Versions:** Transfer the following script, configuration, and .wav files using the Operations Console or through the Unified CVP CD:

- CVPSelfService.tcl

Note This file contains a gateway configuration example.

- CVPSelfServiceBootstrap.vxml
- critical_error.wav

a) Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.
b) From the **Select device type** drop-down list, select **Gateway**.
c) Select the required file from the **Available** list, and click the right arrow to move the device to the **Selected** list.
d) Click **Transfer**.

Note Ensure to check the transfer status after you click **Transfer**, because sometimes transfer may fail.

Step 2 **All Versions:** Perform Steps from the Configure VXML Server Standalone Call Flow Model, on page 18 procedure.

Related Topics

Configure VXML Server Standalone Call Flow Model, on page 18

Example: Gateway Settings for Standalone Call Flow Model

The first part of the following example provides the basic configuration for setting a VoiceXML Standalone gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets
- Configures ASR/TTS Server
- Configures gateway settings

The last part (`application`) of this example provides the following information:

- Standalone Service settings for hello_world application on the VXML Server
- Service requirements for configuring self-service call flow models

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
service internal
logging buffered 99999999 debugging
no logging console
!
ip cef
!
voice rtp send-recv

ip host tts-en-us <IP of TTS or MRCP Server>
ip host asr-en-us <IP of ASR or MRCP Server>
```

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8

voice service voip
signaling forward unconditional
h323
!
gateway
timer receive-rtcp 6
!
ip rtcp report interval 3000
!
ivr prompt memory 15000
ivr prompt streamed none
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer

mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client cache memory pool 15000
http client cache memory file 500
http client connection timeout 60
http client response timeout 30
http client connection idle timeout 10

application
service hello_world flash:CVPSelfService.tcl
param CVPPrimaryVXMLServer <ip address>
param CVPBackupVXMLServer <ip address>
param CVPSelfService-port 7000
param CVPSelfService-SSL 0
-OR-
param CVPSelfService-port 7443
param CVPSelfService-SSL 1
param CVPSelfService-app HelloWorld

service CVPSelfService
flash:CVPSelfServiceBootstrap.vxml
!
```

Note The optional `param CVPSelfService-SSL 1` line enables HTTPS.

Important Calls may be rejected with a *403 Forbidden* response if Toll Fraud security is not configured correctly. The solution is to add the IP address as a trusted endpoint, or else disable the IP address trusted list authentication altogether using the `voice service voip -> "no ip address trusted authenticate"` configuration entry.

Example: Dial-Peer for Standalone Call Flow Model with VXML Gateway

The following example provides the configuration for an incoming Pots and VoIP call for the VXML Server (standalone) call flow model:

Note VXML Server (Standalone) supports an incoming call with a TDM through a T1 port only. Using an FXS port is not supported.

```
dial-peer voice 8 pots
 description Example incoming POTS dial-peer calling HelloWorld VXML

Server app
 service hello_world
 incoming called-number <your DN pattern here>
 direct-inward-dial


dial-peer voice 800 voip
 description Example incoming VOIP dial-peer calling HelloWorld VXML

Server app
 service hello_world
 incoming called-number 800.......
 voice-class codec 1
 dtmf-relay rtp-nte
 no vad
!
```

Example: Dial-Peer for Standalone Call Flow Model with Cisco VVB

The following example provides the configuration for an outbound dial-peer VoIP for the VXML Server (standalone) call flow model with Cisco VVB:

```
dial-peer voice 8181 voip
description dial-peer to CVVB Selfservice application trigger
session protocol sipv2
session target ipv4:<destination IP_address for Cisco VVB>
session transport tcp
codec g711ulaw
destination-pattern 1800T
dtmf-relay rtp-nte
no vad
```

Note 1800XXX is the number dialed which is added as a trigger in Cisco VVB for the self-service application.

Configure Gateway Settings for Comprehensive Call Flow Model

Procedure

Step 1 Install the IOS image on the Ingress Gateway.

For detailed information, see the Cisco IOS documentation.

Step 2 Transfer the following script, configuration, and .wav files to the Ingress gateway through the Operations Console or the Unified CVP product CD:

- bootstrap.tcl
- handoff.tcl
- survivabilty.tcl
- bootstrap.vxml
- recovery.vxml
- ringtone.tcl
- cvperror.tcl
- ringback.wav
- critical_error.wav

Step 3 Configure the Ingress Gateway base settings.

Step 4 Configure the Ingress Gateway service settings.

Step 5 Configure an Ingress Gateway incoming Pots Dial-peer.

Step 6 For **SIP without a Proxy Server** , complete the following steps:

a) If you are using DNS query with SRV or A types from the gateway, configure the gateway to use DNS.

Also, if you are using DNS query with SRV or A types from the gateway, use CLI as shown below:

Note Generally, a non-DNS setup is: **`sip-server ipv4:xx.xx.xxx.xxx:5060`** .

```
ip domain name pats.cisco.com
ip name-server 10.86.129.16
sip-ua
sip-server dns:cvp.pats.cisco.com
OR:
ipv4:xx.xx.xxx.xxx:5060
```

b) Configure the DNS zone file for the separate DNS server that displays how the Service (SRV) records are configured.

Note SRV with DNS can be used in any of the SIP call flow models, with or without a Proxy server. Standard A type DNS queries can be used as well for the calls, without SRV, but they lose the load balancing and failover capabilities.

See DNS Zone File Configuration for Call Director Call Flow Model, on page 52.

Step 7 For **SIP with a Proxy Server**, if you are using the DNS Server, you can set your SIP Service as the Host Name (either A or SRV type).

You can also configure the Gateway statically instead of using DNS. The following example shows how both the A and SRV type records could be configured:

```
ip host cvp4cc2.cisco.com 10.4.33.132
ip host cvp4cc3.cisco.com 10.4.33.133
ip host cvp4cc1.cisco.com 10.4.33.131
```

For SIP/TCP:

```
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

For SIP/UDP:

```
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

Note The DNS Server must be configured with all necessary A type or SRV type records.

See the SIP Devices Configuration, on page 209 and the *Operations Console Online Help*, **Managing devices** > **Configuring a SIP Proxy Server** for details.

Step 8 Transfer files to the **VXML** Gateway using Step 2.

Step 9 Configure the VXML Gateway base settings.

Step 10 Configure the VXML Gateway service settings.

Step 11 If using ASR and TTS Servers, specify IP addresses for those servers for each locale using the applicable name resolution system for the Gateway (DNS or “ip host” commands).

Note If ASR and TTS use the same server, the MRCP server might allocate one license for the ASR session and a second license for the TTS section. If you are hosting both ASR and TTS on the same speech server, you must select the **ASR/TTS use the same MRCP server** option in the IVR Service configuration tab in the Operations Console and follow the instructions in the step below.

Do one of the following:

- The primary and backup servers must be configured. If using name resolution local to the Gateway (rather than DNS) specify:

  ip host asr- <*locale*> <*ASR server for locale*>

  ip host asr- <*locale*>-backup <*backup ASR server for locale*>

  ip host tts- <*locale*> <*TTS server for locale*>

  ip host tts- <*locale*>-backup <*backup TTS server for locale*>

  Example for English US, use:

  ip host asr-en-us 10.86.129.215

Step 12 If you want the ASR and TTS to use the same MRCP server option, you must configure the gateway as follows.

a) In the IVR Service in the Operations Console, select the **ASR/TTS use the same MRCP server** option.

b) Add the following two host names to the gateway configuration:

- ip host asrtts- <*locale*> <*IP Address Of MRCP Server*>

- ip host asrtts- <*locale*> -backup <*IP Address Of MRCP Server*>

  Where the *locale* might be something like en-us or es-es, resulting in `asrtts-en-us` or `asrtts-es-es`.

c) Change the 'ivr asr-server' and 'ivr tts-server' lines as follows for MRCPV1:

- ivr asr-server rtsp://asr-en-server/recognizer
- ivr tts-server rtsp://tts-en-server/synthesizer

d) Change the 'ivr asr-server' and 'ivr tts-server' lines as follows for MRCPV2:

- ivr asr-server sip:asr@10.78.26.103
- ivr tts-server sip:tts@10.78.26.103

Step 13 Configure the speech servers to work with Unified CVP.

Caution The Operations Console can only manage speech servers installed on *Windows*, not on Linux. If the speech server is installed on Linux, the server cannot be managed.

To ensure that the speech servers work with Unified CVP, you must make the following changes on each speech server as part of configuring the Unified CVP solution.

If you are using Nuance SpeechWorks MediaServer (SWMS), the configuration file is osserver.cfg. If you are using Nuance Speech Server (NSS), the configuration file is NSSserver.cfg.

Make the following changes to the Nuance configuration file:

- **Change:** server.resource.2.url VXIString media/speechrecognizer

  To: server.resource.2.url VXIString recognizer
- **Change:** server.resource.4.url VXIString media/speechsynthesizer

  To: server.resource.4.url VXIString synthesizer
- **Change:** server.mrcp1.resource.3.url VXIString media/speechrecognizer

  To: server.mrcp1.resource.3.url VXIString /recognizer
- **Change:** server.mrcp1.resource.2.url VXIString media/speechsynthesizer

  To: server.mrcp1.resource.2.url VXIString media/synthesizer
- **Change:** server.mrcp1.transport.port VXIInteger 4900

  To: server.mrcp1.transport.port VXIInteger 554

If you are using Nuance Speech Server 5 and Nuance Vocalizer for Network 5, then make changes to the configuration files for each application. Make the following changes to the Nuance Speech Server 5 configuration file (NSSserver.cfg):

- **Change:** server.mrcp1.resource.3.url VXIString media/speechrecognizer

  To: server.mrcp1.resource.3.url VXIString /recognizer
- **Change:** server.mrcp1.resource.2.url VXIString media/speechsynthesizer

  To: server.mrcp1.resource.2.url VXIString /synthesizer

- **Change:** server.mrcp1.transport.port VXIInteger 4900

  To: server.mrcp1.transport.port VXIInteger 554

- **Change:** server.mrcp1.transport.dtmfPayloadType VXIInteger 96

  To: server.mrcp1.transport.dtmfPayloadType VXIInteger 101

- **Uncomment the following:** server.rtp.dtmfTriggerLeading VXIInteger 0

  If you are using the Nuance Vocalizer for Network 5 TTS System, the following configuration files will need to be updated:

  <install path>\Nuance Vocalizer for Network 5.0\config\ttsrshclient.xml

- **Change:** <ssml_validation>strict</ssml_validation>

  To:<ssml_validation>warn</ssml_validation>

  <install path>\Nuance Vocalizer for Network 5.0\config\ttssapi.xml

- **Change:** <ssml_validation>strict</ssml_validation>

  To: <ssml_validation>warn</ssml_validation>

If you are using Nuance Recognizer 10.0 and Nuance Speech Server 6.2, make the following changes to the Nuance configuration file (NSSserver.cfg - C:\Program Files (x86)\Nuance\Speech Server\Server\config):

- **Change:** server.mrcp1.resource.3.url VXIString media/speechrecognizer

  To: server.mrcp1.resource.3.url VXIString /recognizer

- **Change:** server.mrcp1.resource.2.url VXIString media/speechsynthesizer

  To: server.mrcp1.resource.2.url VXIString /synthesizer

- **Change**: server.mrcp1.transport.port VXIInteger 4900

  To: server.mrcp1.transport.port VXIInteger 554

- **Change:** server.mrcp1.transport.dtmfPayloadType VXIInteger 96

  To: server.mrcp1.transport.dtmfPayloadType VXIInteger

Make the following change to the Baseline.xml file `C:\Program Files\Nuance\Recognizer\config`

Change: <ssml_validation>strict</ssml_validation>

To:<ssml_validation>warn</ssml_validation>.

If you are using Nuance Recognizer 10.5 and Nuance Speech Server 6.5, then refer to the relevant Nuance Speech Suite Install Guide available at https://network.nuance.com/portal/server.pt/directory/nuance_speech_suite_10_5/16535.

If you are using Nuance Recognizer 11.0 and Nuance Speech Server 7.0, then refer to the relevant Nuance Speech Suite Install Guide available at https://network.nuance.com/portal/server.pt/directory/nuance_speech_suite_11_0.

Step 14 Configure SIP-Specific Actions.

On the Unified CM server, CCMAdmin Publisher, configure **SIP-specific actions**:

a) Create SIP trunks:

- If you are using a SIP Proxy Server, set up a SIP trunk to the SIP Proxy Server.
- Add a SIP Trunk for the Unified CVP Call Server.
- Add a SIP Trunk for each Ingress gateway that will send SIP calls to Unified CVP that might be routed to Unified CM.

Select **Device** > **Trunk** > **Add New** and add the following:

- Trunk Type: **SIP trunk**
- Device Protocol: **SIP**
- Destination Address: IP address or host name of the SIP Proxy Server (if using a SIP Proxy Server). If not using a SIP Proxy Server, enter the IP address or host name of the Unified CVP Call Server.
- DTMF Signaling Method: **RFC 2833**
- Do **not** check the **Media Termination Point Required** checkbox.
- If you are using UDP as the outgoing transport on Unified CVP, also set the outgoing transport to **UDP** on the SIP Trunk Security Profile.

b) Add route patterns for outbound calls from Unified CM devices using a SIP Trunk to the Unified CVP Call Server. Also, add a route pattern for error DN.

Note CVP solution does not support 100rel. On the SIP profile for the Trunk, confirm that SIP Rel1xx Options are disabled.

For warm transfers, the call from Agent 1 to Agent 2 does not typically use a SIP Trunk, but you must configure the CTI Route Point for that dialed number on the Unified CM Server and associate that number with your peripheral gateway user (PGUSER) for the JTAPI gateway on the Unified CM peripheral gateway. An alternative is to use the Dialed Number Plan on Unified ICME to bypass the CTI Route Point.

c) Select **Call Routing** > **Route/Hunt** > **Route Pattern** > **Add New**.

- Route Pattern: Specify the route pattern; for example: 3xxx for a TDM phone that dials 9+3xxx and all Unified ICME scripts are set up for 3xxx dialed numbers.
- Gateway/Route List: Select the SIP Trunk defined in Step 2.

d) If you are sending calls to Unified CM using an SRV cluster domain name, configure the cluster domain name.

- Select: **Enterprise Parameters** > **Clusterwide Domain Configuration**.
- Add the Cluster fully qualified domain name: **FQDN**.

For detailed instructions about using Unified CM and the CUSP Server, see the Cisco Unified SIP Proxy Server documentation.

Step 15 (Optional) Configure the **SIP Proxy Server**.

From the CUSP Server Administration web page (**http://<CUSP server>/admin**):

a) Configure the SIP static routes to the Unified CVP Call Server(s), Unified CM SIP trunks, and Gateways.

Configure the SIP static routes for intermediary transfers for ring tone, playback dialed numbers, and error playback dialed numbers.

Note For failover and load balancing of calls to multiple destinations, configure the CUSP Server static route with priority and weight.

See the SIP Devices Configuration, on page 209 and SIP Dialed Number Pattern Matching Algorithm, on page 9 for detailed information.

b) Configure Access Control Lists for Unified CVP calls.

- Select **Proxy Settings** > **Incoming ACL**.
- Set address pattern: **all**

c) Configure the service parameters.

Select **Service Parameters**, and set the following:

- Add record route: **off**
- Maximum invite retransmission count: **2**
- Proxy Domain and Cluster Name: if using DNS SRV, set to the FQDN of your Proxy Server SRV name.

d) Write down the IP address and host name of the SIP Proxy Server. You need this information when configuring the SIP Proxy Server in Unified CVP.

e) If using redundant SIP Proxy Servers (primary and secondary or load balancing), decide whether to use DNS server lookups for SRV records or non-DNS based local SRV record configuration.

The Comprehensive call flow model with SIP calls will typically be deployed with dual CUSP Servers for redundancy. In some cases, you might want to purchase a second CUSP Server. Regardless, the default transport for deployment will be UDP. Make sure you *always* set the AddRecordRoute setting to **Off** with CUSP Servers.

Configure the SRV records on the DNS server or locally on Unified CVP with an .xml file (local xml configuration avoids the overhead of DNS lookups with each call).

Step 16 Configure Peripheral Gateways (PGs).

On the NAM, ICM Configuration Manager, **PG Explorer** tool, configure a peripheral gateway (PG) for the Unified CVP. Configure a PG for each Unified CVP Call Server as follows:

In the tree view pane, select the applicable PG.

Logical Controller tab:

- Client Type: **VRU**
- Name: A name descriptive of this PG

  For example: **<location>_A** for side A of a particular location

Peripheral tab:

- Peripheral Name: Descriptive name of this Unified CVP peripheral

For example: **<location>_<cvp1> or <dns_name>**

- Client Type: **VRU**
- Select: **Enable Post-routing**

Advanced tab:

- Select the name of the Unified CVP VRU from the Network VRU field drop-down list.

  For example: **cvpVRU**

Routing Client tab:

- Name: By convention, use the same name as the peripheral
- Client Type: **VRU**
- If you are in a Unified ICMH environment and configuring the CICM, then do the following:
  - *Do not* select the **Network Transfer Preferred** checkbox
  - Routing client: **INCRP NIC**

Note If you are using a VXML gateway that is not co-located, then configure the following dial-peer to handle the error case:

Example:

```
dial-peer voice 9292 voip
description SIP error dial-peer
session protocol sipv2
session target ipv4:<destination IP_address for the VXML gateway>
session transport tcp
codec g711ulaw
destination-pattern 929292T
dtmf-relay rtp-nte
no vad
```

This may vary depending on the type of deployment.

Ingress and VoiceXML Gateway Configuration Examples

Example Gateway Settings for Comprehensive Call Flow Model

The first part of the following example provides the basic configuration for setting an Ingress gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets
- Configures gateway settings

The last part of this example provides the following:

- Allows SIP to play a .wav file that enables caller to hear message from critical_error.wav
- Performs survivability
- Enables SIP to play ringtone to caller while caller is being transferred to an agent
- Logs errors on the gateway when the call fails
- Defines requirements for SIP Call Server

Note CVP solution does not support 100rel. It can be disabled on the dial-peer level or on a global level under the voice service VoIP section.

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
service internallogging buffered 99999999 debuggingn
no logging console
!
ip cef
!voice rtp send-recv
!
voice service voip
signaling forward unconditional
sip
min-se 360
header-passing
!voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
application
service cvperror flash:cvperror.tcl
!
service cvp-survivability flash:survivability.tcl
!
service ringtone flash:ringtone.tcl
!
service handoff flash:handoff.tcl
!gateway
timer receive-rtcp 4
!
ip rtcp report interval 2000
!sip-ua
retry invite 2
timers expires 60000
sip-server ipv4:<IP of CUSP server or Call Server>:5060
reason-header override
!
```

VoiceXML: Example Gateway Settings for Comprehensive Call Flow Model

The first part of the following example provides the basic configuration for setting a VoiceXML gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging

- Turns off printing to the command line interface console
- Sends RTP packets
- Configures ASR/TTS Server
- Configures gateway settings

The last part of this example provides the following:

- Initiates the VoiceXML leg
- Initiates the switch leg of the call
- Plays a .wav file that enables caller to hear message from critical_error.wav
- Logs errors on the gateway when the call fails

```
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
logging buffered 99999999 debugging
no logging console
ip cef
no ip domain lookup
ip host tts-en-us <IP of TTS or MRCP Server>
ip host asr-en-us <IP of ASR or MRCP Server>
voice rtp send-recv
!
voice service voip
signaling forward unconditional
sip
min-se 360
header-passing
voice class
codec 1 codec preference 1 g711ulaw
codec preference 2 g729r8
!
ivr prompt memory 15000
ivr prompt streamed none
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client cache memory pool 15000
http client cache memory file 500
http client connection timeout 60
http client response timeout 30
http client connection idle timeout 10
gateway
timer receive-rtcp 6
!
ip rtcp report interval 3000
application
service new-call flash:bootstrap.vxml
service cvperror flash:cvperror.tcl
service handoff flash:handoff.tcl
service bootstrap flash:bootstrap.tcl
```

```
param cvpserverss1 1
!
```

Note The optional param cvpserverss1 1 line enables HTTPS.

Related Topics

DNS Zone File Configuration for Comprehensive Call Flow Model, on page 31
Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210
Load-Balancing SIP Calls , on page 210
Cisco Unified SIP Proxy (CUSP) Configuration , on page 210
Configure Custom Streaming Ringtones, on page 213
Configure High Availability for Unified CVP, on page 465
SIP Dialed Number Pattern Matching Algorithm, on page 9

Configure Gateway Settings for Call Director Call Flow Model

Procedure

Step 1 Perform Steps 1 to 4 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 2 Configure the Ingress Gateway:

a) Configure the Ingress Gateway dial-peer for the Unified CVP Call Server.
b) Configure a dial-peer for ringtone and error.
c) If you are using a Proxy Server, configure your session target in the outbound dial peer to point to the Proxy Server.
d) If you are using the sip-server global configuration, then configure the sip-server in the sip-ua section to be your Proxy Server and point the session target of the dial-peer to the sip-server global variable.

Note Make sure your dial plan includes this information. You will need to see the Dial plan when you configure the SIP Proxy Server for Unified CVP.

The SIP Service voip dial peer and the destination pattern on the Ingress Gateway must match the DNIS in static routes on the SIP Proxy Server or Unified CVP Call Server.

Step 3 For SIP without a Proxy Server, complete the following steps:

a) If you are using DNS query with SRV or A types from the gateway, configure the gateway to use DNS.

See the SIP Devices Configuration, on page 209 and *Operations Console online help* for detailed instructions. If you are using DNS query with SRV or A types from the gateway, use the gateway configuration CLI as shown below:

Non-DNS Setup:

```
sip-ua
sip-server ipv4:xx.xx.xxx.xxx:5060
!
```

DNS Setup:

```
ip domain name patz.cisco.com
ip name-server 10.10.111.16
!
sip-ua
sip-server dns:cvp.pats.cisco.com
!
```

b) Configure the DNS zone file for the separate DNS server that displays how the Service (SRV) records are configured.

Note SRV with DNS can be used in *any* of the SIP call flow models, with or without a Proxy server. Standard A type DNS queries can be used as well for the calls, without SRV, but they lose the load balancing and failover capabilities.

See the DNS Zone File Configuration for Call Director Call Flow Model, on page 52 for more information.

Step 4 For SIP with a Proxy Server, use one of the following methods:

Note You can configure the Gateway statically instead of using DNS.

The following example shows how both the A and SRV type records could be configured:

```
ip host cvp4cc2.cisco.com 10.4.33.132
ip host cvp4cc3.cisco.com 10.4.33.133
ip host cvp4cc1.cisco.com 10.4.33.131
```

For **SIP/TCP**:

```
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

For **SIP/UDP**:

```
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc3.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc2.cisco.com
ip host _sip._udp.cvp.cisco.com srv 50 50 5060 cvp4cc1.cisco.com
```

Note The DNS Server must be configured with all necessary A type or SRV type records.

If you are using the DNS Server, you can set your SIP Service as the Host Name (either A or SRV type).

Step 5 On the Unified CM server, CCMAdmin Publisher, complete the following SIP-specific actions:

a) Create SIP trunks.

- If you are using a SIP Proxy Server, set up a SIP trunk to the SIP Proxy Server.
- Add a SIP Trunk for the Unified CVP Call Server.
- Add a SIP Trunk for each Ingress gateway that will send SIP calls to Unified CVP that might be routed to Unified CM.

To add an SIP trunk, select **Device** > **Trunk** > **Add New** and use the following parameters:

- Trunk Type: **SIP trunk**
- Device Protocol: **SIP**
- Destination Address: IP address or host name of the SIP Proxy Server (if using a SIP Proxy Server). If not using a SIP Proxy Server, enter the IP address or host name of the Unified CVP Call Server.
- DTMF Signaling Method: **RFC 2833**
- Do **not** check the *Media Termination Point Required* check box.
- If you are using UDP as the outgoing transport on Unified CVP, also set the outgoing transport to **UDP** on the SIP Trunk Security Profile.
- Connection to CUSP Server: use 5060 as the default port.

b) Add route patterns for outbound calls from the Unified CM devices using a SIP Trunk to the Unified CVP Call Server. Also, add a route pattern for error DN.

Select **Call Routing** > **Route/Hunt** > **Route Pattern** > **Add New**

Add the following:

- Route Pattern: Specify the route pattern; for example: **3XXX** for a TDM phone that dials 9+3xxx and all Unified ICME scripts are set up for 3xxx dialed numbers.
- Gateway/Route List: Select the SIP Trunk defined in the previous substep.

Note For warm transfers, the call from Agent 1 to Agent 2 does not typically use a SIP Trunk, but you must configure the CTI Route Point for that dialed number on the Unified CM server and associate that number with your peripheral gateway user (PGUSER) for the JTAPI gateway on the Unified CM peripheral gateway. An alternative is to use the Dialed Number Plan on Unified ICME to bypass the CTI Route Point.

c) If you are sending calls to Unified CM using an SRV cluster domain name, select **Enterprise Parameters** > **Clusterwide Domain Configuration** and add the Cluster fully qualified domain name **FQDN**.

Step 6 (Optionally) Configure the **SIP Proxy Server**.

a) Configure the SIP static routes to the Unified CVP Call Servers, Unified CM SIP trunks, and Gateways.

Configure the SIP static routes for intermediary transfers for ringtone, playback dialed numbers, and error playback dialed numbers.

Note For failover and load balancing of calls to multiple destinations, configure the CUSP server static route with priority and weight.

b) Configure Access Control Lists for Unified CVP calls.

Select **Proxy Settings** > **Incoming ACL**.

Address pattern: **all**

c) Configure the service parameters.

Select **Service Parameters**, then set the following:

- Add record route: **off**

- Maximum invite retransmission count: **2**
- Proxy Domain and Cluster Name: if using DNS SRV, set to the FQDN of your Proxy Server SRV name

d) Write down the IP address and host name of the SIP Proxy Server. (You need this information when configuring the SIP Proxy Server in Unified CVP.)

e) If using redundant SIP Proxy Servers (primary and secondary or load balancing), then decide whether to use DNS server lookups for SRV records or non-DNS based local SRV record configuration.

Note If a single CUSP Server is used, then SRV record usage is not required.

Configure the SRV records on the DNS server or locally on Unified CVP with a .xml file (local xml configuration avoids the overhead of DNS lookups with each call).

Note See the Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210 section for details.

The Call Director call flow model with SIP calls will typically be deployed with dual CUSP servers for redundancy. In some cases, you might want to purchase a second CUSP server. Regardless, the default transport for deployment will be UDP; make sure you *always* disable the record-route in a CUSP server as this advanced feature is not supported in Contact Center deployments.

For the required settings in the Unified CM Publisher configuration, see the Cisco Unified SIP Proxy documentation.

Step 7 Configure the PGs for the switch leg.

On Unified ICME, ICM Configuration Manager, **PG Explorer** tool:

a) Configure each peripheral gateway (PG) to be used for the **Switch** leg. In the tree view pane, select the applicable PG, and set the following:

1. **Logical Controller** tab:
   - Client Type: **VRU**
   - Name: A name descriptive of this PG

     For example: **<location>_A** for side A of a particular location

2. **Peripheral** tab:
   - Peripheral Name: A name descriptive of this Unified CVP peripheral

     For example: **<location>_<cvp1> or <dns_name>**
   - Client Type: **VRU**
   - Select the check box: **Enable Post-routing**

3. **Routing Client** tab:
   - Name: By convention, use the same name as the peripheral.
   - Client Type: **VRU**

For more information, see the ICM Configuration Guide for Cisco ICM Enterprise Edition.

b) Configure a peripheral for each Unified CVP Call Server to be used for a Switch leg connected to each peripheral gateway.

Related Topics

Configure Gateway Settings for Comprehensive Call Flow Model, on page 255
Set Up Ingress Gateway to Use Redundant Proxy Servers, on page 209
Set Up Call Server with Redundant Proxy Servers, on page 209
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210
Load-Balancing SIP Calls , on page 210
Cisco Unified SIP Proxy (CUSP) Configuration , on page 210
Configure Custom Streaming Ringtones, on page 213
SIP Dialed Number Pattern Matching Algorithm, on page 9
DNS Zone File Configuration for Comprehensive Call Flow Model, on page 31
Local SRV File Configuration Example for SIP Messaging Redundancy, on page 210

Configure Gateway Settings for VRU-Only Call Flow Model: Type 8

Procedure

Step 1 Using the Unified CVP Operations Console or the Unified CVP product CD, transfer the following script, configuration, and .wav files to the **VoiceXML Gateway** used for the VRU leg. Perform Step 2 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 2 Configure the VXML gateway base settings.

Step 3 Configure the VXML gateway service settings.

Step 4 Configure the ICM service.

Using the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. On **each** Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a) VRU connection port number.

Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b) Maximum Length of DNIS.

Set the maximum length DNIS to a number which is at least the length of the translation route DNIS numbers.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c) Call service IDs: New Call and Pre-routed.

Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab.

d) Trunk group IDs: New Call and Pre-routed.

- Enter the new and pre-routed call trunk group IDs
- Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route
- Configure the number of ports according to the licenses purchased and capacity
- Configure each of the numbers used for translation routes. (The "New Call" group is not used since the calls are being sent to the VRU (Unified CVP) after some initial processing by the NIC/Unified ICME)

e) Dialed numbers used in the translation route.

Add the dialed numbers in the DNIS field.

f) Check the default values of the other settings and change, if desired.

VoiceXML Gateway Configuration Examples

Example Gateway Settings for Type 8 Call Flow Model

The first part of the following example provides the basic configuration for setting a VoiceXML gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets
- Configures ASR/TTS Server
- Configures gateway settings

The last part of this example provides the following:

- Initiates the VoiceXML leg
- Plays a .wav file that enables caller to hear message from critical_error.wav
- Logs errors on the gateway when the call fails

```
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
logging buffered 99999999 debugging
no logging console
ip cef
no ip domain lookup
ip host tts-en-us <IP of TTS or MRCP Server>
ip host asr-en-us <IP of ASR or MRCP Server>
voice rtp send-recv
!
voice service voip
allow-connections h323 to h323
signaling forward unconditional
h323
```

```
sip
min-se 360
header-passing
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
ivr prompt memory 15000
ivr prompt streamed none
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client cache memory file 500
http client connection timeout 60
http client response timeout 30
http client connection idle timeout 10
gateway
timer receive-rtcp 6
!
ip rtcp report interval 3000
application
service new-call flash:bootstrap.vxml
service cvperror flash:cvperror.tcl
service handoff flash:handoff.tcl
```

Example of Dial-peer for ICM VRU Label for Type 8 Call Flow Model

The following example provides the configuration for an ICM VRU label dial-peer for the Type8 Unified CVP VRU-Only call flow model:

```
dial-peer voice 777 voip
 description ICM VRU label
 service bootstrap
 voice-class codec 1
 incoming called-number <your sendtovru label pattern here>
 dtmf-relay rtp-nte
 no vad
 !
```

Related Topics

Configure Gateway Settings for Comprehensive Call Flow Model, on page 255

Configure Gateway Settings for VRU-Only: Type 7

Procedure

Step 1 Transfer the following script, configuration, and .wav files to the **VoiceXML Gateway** used for the VRU leg, using the Unified CVP Operations Console. Perform Step 2 of the Configure Gateway Settings for Comprehensive Call Flow Model, on page 255 procedure.

Step 2 Configure the VoiceXML gateway base settings.

Step 3 Configure the VoiceXML gateway service settings.

Step 4 Configure the ICM Service for each Call Server.

In the Operations Console, select **Device Management** > **CVP Call Server** > **ICM tab**. For each Unified CVP Call Server, configure the **ICM Service** by specifying the following required information:

a) VRU connection port number.

Set the VRU Connection Port to match the VRU connection Port defined in ICM Setup for the corresponding VRU peripheral gateway (PIM).

b) Set the maximum length DNIS to the length of the Network Routing Number.

Example: if the Gateway dial pattern is 1800******, the maximum DNIS length is 10.

c) Call service IDs: New Call and Pre-routed.

Enter the new and pre-routed call service IDs. Configure the ports for both groups according to the licenses purchased, call profiles, and capacity by completing the required fields on this tab

d) Trunk group IDs: New Call and Pre-routed.

Enter the new and pre-routed call trunk group IDs. Configure the group number for the Pre-routed Call Trunk group. The group number must match the trunk group number in the Network Trunk group used for the translation route.

Configure the number of ports according to the licenses purchased and capacity. Configure each of the numbers used for translation routes. (The “New Call” group is not used since the calls are being sent to the VRU (Unified CVP) after some initial processing by the NIC/Unified ICME.)

e) Check the default values of other settings and change, if desired.

VoiceXML Gateway Configuration: Example Gateway Settings for Type 7

VoiceXML Gateway Configuration: Example of Dial-Peer for ICM VRU Label for Type 7

Note While using ASR/TTS, use a single version of MRCP (v1/v2) instead of using it in mixed mode.

The first part of the following example provides the basic configuration for setting a VoiceXML gateway:

- Applies a timestamp to debugging and log messages
- Turns on logging
- Turns off printing to the command line interface console
- Sends RTP packets
- Configures ASR/TTS Server
- Configures gateway settings

The last part of this example provides the following:

- Initiates the VoiceXML leg
- Plays a .wav file that enables caller to hear message from critical_error.wav
- Logs errors on the gateway when the call fails

```
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
logging buffered 99999999 debugging
no logging console
ip cef
no ip domain lookup
ip host tts-en-us <IP of TTS or MRCP Server>
ip host asr-en-us <IP of ASR or MRCP Server>
voice rtp send-recv
!
voice service voip
 allow-connections h323 to h323
 signaling forward unconditional
 h323
 sip
 min-se 360
 header-passing
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
ivr prompt memory 15000
ivr prompt streamed none
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client cache memory pool 15000
http client cache memory file 500
http client connection timeout 60
http client response timeout 30
http client connection idle timeout 10
gateway
 timer receive-rtcp 6
!
ip rtcp report interval 3000
application
 service new-call flash:bootstrap.vxml
 service cvperror flash:cvperror.tcl
 service handoff flash:handoff.tcl
 service bootstrap flash:bootstrap.tcl
 !
```

The following example provides the configuration for an ICM VRU label dial-peer for the Type 7 Unified CVP VRU-Only call flow model:

```
dial-peer voice 777 voip
 description ICM VRU label
 service bootstrap
 voice-class codec 1
 incoming called-number <your sendtovru label pattern here>
 dtmf-relay rtp-nte
```

```
no vad
!
```

Related Topics

Configure Gateway Settings for Comprehensive Call Flow Model, on page 255

Transfer Script and Media File to Gateway

Transfer a single script or media file at a time from the Operations Console.

Procedure

Step 1 Log in to the Operations Console and from the Device Management menu, select the type of server to which to transfer the script file.

Example:

To transfer a script or a media file to a Gateway, select **Device Management** > **Gateway**..

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

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

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

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

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

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

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

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

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

VoiceXML Gateway

The VoiceXML Gateway parses and renders VoiceXML documents obtained from the Unified CVP Call Server (from its IVR Service), the UnifiedCVP VXMLServers, or some other external VoiceXML source. Rendering a VoiceXML document consists of retrieving and playing prerecorded audio files, collecting and processing user input, or connecting to an ASR/TTS Server for voice recognition and dynamic text-to-speech conversion.

For a discussion of using mixed codecs in CVP deployments, see Mixed G.729 and G.711 Codec Support, on page 460. For a discussion of the benefits and drawbacks of each codec, refer to Voice Traffic section of *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

Note VoiceXML Gateway must not have a load balanced path because this route on the VoiceXML Gateway will cause a call HTTP Client Error. If the VoiceXML Gateway has a load balancing route to the CVP Call Server, it may use a different source address to send HTTP message to the CVP Call Server. CVP would return a 500 Server Error address to send HTTP message to CVP Call Server, which would cause CVP to return a 500 Server Error message.

In VoiceXML Gateway, it is not possible to bind any specific interface for the HTTP Client side. If VoiceXML Gateway sends NEW_CALL using one interface and CALL_RESULT using another interface, CVP will return a 500 Server Error. Starting from IOS version 15.5.3M1, you have the capability to bind the VXML/HTTP traffic to a specific interface.

Related Topics

Mixed G.729 and G.711 Codec Support, on page 460

Configuration

The high-availability configuration for VoiceXML Gateways is controlled by the SIP proxy for SIP, or the Unified CVP Call Server (Call Server). Whether the VoiceXML Gateways are distributed or centralized also influences how high availability is achieved.

If a Call Server is unable to connect to a VoiceXML Gateway, an error is returned to the ICM script. In the ICM script, the Send to VRU node is separate from the first Run External script node in order to catch the VoiceXML Gateway connection error. If an END script node is used off the X-path of the Send to VRU node, the call is default-routed by survivability on the originating gateway. (Survivability does not apply in VRU-only models.) A Queue to Skill group node is effective only if there is an agent available. Otherwise, ICM tries to queue the caller, and that attempt fails because the Call Server is once again unable to connect to a VoiceXML Gateway. An END node could then also be used off the X-path of the Queue to Skill Group node to default-route the call.

Note VXML Server uses two features that assist with load balancing:

- Limiting load balancer involvement
- Enhanced HTTP probes for load balancers

See the configuration options ip_redirect and license_depletion_probe_error in the *User Guide for Cisco Unified CVP VXML Server and Cisco Unified Call Studio*, available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Centralized VoiceXML Gateways

In this configuration, the VoiceXML Gateways reside in the same data center as the Unified CVP Call Server.

SIP VoiceXML Gateways

If you are using SIP static routes on the Unified CVP Call Server, under the SIP Service configuration for the Call Server, configure a static route for each Network VRU label and gateway. If the VRU label is 5551000, the static route pattern would be 5551000>. The > is a wildcard representing one or more digits, and it is needed so that the correlation-id appended to the DNIS number can be passed to the VoiceXML Gateway correctly.

Note Other wildcard characters can be used. See the topic **Valid Formats for Dialed Numbers** in the Ops Console online help for complete wildcard format and precedence information.

In the case of both SIP proxy or Unified CVP static routes, the next-hop address of the route can be either the IP address of the gateway or a DNS SRV record. If you are using an IP address, you must create multiple static routes, one for each VoiceXML Gateway. In the case of DNS SRV, only one route for each Network VRU label is needed, and the SRV record provides for load balancing and redundancy.

High-Availability Hardware Configuration on Voice Gateways

The individual hardware components have the following high-availability options:

- Redundant power supplies
- Separate components for higher availability
- Dedicated components, which have fewer interaction issues

Example 1: Separate PSTN Gateway and VoiceXML Gateway

A PSTN Gateway and a separate VoiceXML Gateway provide greater availability for a combined PSTN and VoiceXML Gateway.

Example 2: Duplicate components for higher availability

- Two 8-T1 PSTN Gateways provide greater availability than one 16-T1 PSTN Gateway.
- Two 96-port UnifiedCVP VXMLServers provide greater availability than one 192-port UnifiedCVP VXMLServer.
- Larger designs can use N+1 spares for higher availability.

Example 3: Geographic redundancy for higher availability

Geographical redundancy and high availability can be achieved by purchasing duplicate hardware for Side A and Side B.

Distributed VoiceXML Gateways

In this configuration, the gateway that processes the incoming call from the PSTN is separated from the Unified CVP servers by a low-bandwidth connection such as a WAN. The VoiceXML Gateway is different from the Ingress Gateway and can be located at the same site. The configuration keeps the media stream at the same site and without consuming bandwidth on the WAN and optimizes VoiceXML Gateway sizing when it is appropriate to separate Ingress and VoiceXML Gateways. In this case, setTransferLabel and Send to Originator cannot be used because you do not want the IVR leg of the call to go back to the Ingress Voice

Gateway. It is also impractical to use a SIP Proxy to control the call routing because you would have to configure separate Network VRUs, Network VRU labels, and customers in ICM for each remote site. Instead, use SetSigDigits functionality.

With this method, the Call Server strips the leading significant digits from the incoming DNIS number. The value that is stripped is saved and prepended when subsequent transfers for the call occur.

SIP VoiceXML Gateways

When SIP is used, the significant digits are prepended to the DNIS number, and a SIP Proxy can be configured to route calls based on those prepended digits. The static routes in the SIP Proxy for the VoiceXML Gateway should have the digits prepended. Because these prepended digits were originally populated by the Ingress Gateway, the SIP Proxy can use them to determine which VoiceXML Gateway to use based on the incoming gateway. In this way, calls arriving at a particular site can always be sent back to VoiceXML treatment, with the result that no WAN bandwidth is used to carry the voice RTP stream. The Unified CVP indiscriminately prepends the **sigdigits** value to all transfers, including those to UnifiedCM. Therefore, when using UnifiedCM in this scenario, it is necessary to strip the prepended digits when the call arrives, so that the real DNIS number of the phone can be used by UnifiedCM to route the call, as illustrated in the following example.

Note The configurations mentioned below are only applicable to IOS Voice Gateway.

Configuration of Ingress Voice Gateway:

Apply a translation rule to the incoming DNIS to prepend the value 3333:

```
translation-rule 99
 rule 1 8002324444 33338002324444

dial-peer voice 1000 voip
 translate-outgoing called 99
```

Assuming the DNIS number is 8002324444, the final DNIS string routed to Unified CVP is 33338002324444.

Configuration of Unified CVP SIP service:

To configure the SIP service, in the Operations Console, select **Call Server > SIP**. Many of the settings are in the Advanced Configuration window.

Configuration of IOS VoiceXML Gateway:

Configure the Voice XML Gateway to match the DNIS string, including the prepended digits:

```
dial-peer voice 3000 voip
 incoming-called number 33335551000T
 service bootstrap
 ...
```

Configure the Unified CVP bootstrap.tcl application with the **sigdigits** parameter, indicating how many digits to strip off of the incoming DNIS string:

```
application
 service bootstrap flash:bootstrap.tcl
 param sigdigits 4
 ...
```

Cisco UnifiedCM configuration (if used):

Configure UnifiedCM to strip the prepended digits, either by using the Significant Digits configuration on the SIP Trunk configuration page or by using translation patterns.

SIP Proxy configuration:

Define static routes on the SIP Proxy, with the prepended digit present, to be sent to the appropriate VoiceXML Gateway. Because transfers to agents on a UnifiedCM cluster have prepended digits, the static routes for agent phones must also contain the prepended digits.

Summary of call routing:

1. A call arrives at Unified CVP with a DNIS number of 33338002324444.
2. Unified CVP removes four digits (3333) from the beginning of the DNIS string, leaving 8002324444.
3. The number 8002324444 is passed to ICM for call routing.
4. When it is time to transfer, ICM returns the label 5551000102. Unified CVP prepends 3333, resulting 33335551000102.
5. The SIP Service then resolves the address using the SIP Proxy or local static routes, and it sends the call to the VoiceXML Gateway.
6. The VoiceXML Gateway bootstrap.tcl removes 3333, leaving 5551000102 for the destination address.

Cache Types

There are two types of cache involved in storing media files: the IVR Media Player cache and the HTTP Client cache.

The HTTP Client cache is used for storing files that are downloaded from the HTTP server. In nonstreaming mode, the entire media file is stored inside the HTTP Client cache. In streaming mode, the first chunk of the media file is stored in the HTTP Client cache and in the IVR cache, and all subsequent chunks of the file are saved in the IVR cache only. The HTTP Client cache can store 100 MB of prompts, while the IVR cache is limited to 32 MB.

Use only nonstreaming mode, so that the IVR prompt cache is never used and the HTTP Client cache is the primary cache. In nonstreaming mode, the HTTP Client cache can also store 100MB of prompts, while the IVR cache is limited to 16MB.

To configure the HTTP Client cache, use the following Cisco IOS commands:

http client cache memory file *1-10000*

The 1–10000 value is the file size in kilobytes. The default maximum file size is 50KB, but you can also have a file size up to 600 KB file size. Any file that is larger than the configured HTTP Client memory file size will not be cached.

http client cache memory pool *0-100000*

The 0–100000 value is the total memory size available for all prompts, expressed in kilobytes. A value of zero disables HTTP caching. The default memory pool size for the HTTP Client cache is 10MB. The memory pool size is the total size of all prompts stored on the media server, which is up to 100MB.

Configure Gateway Settings to modify Outgoing SIP Header

In some scenarios a gateway may need to interact with third-party ACDs, which requires modifications to certain SIP headers.

In this example, the SIP Refer-To header in the outgoing SIP REFER message is modified to pass the Application-to-Application information (AAI) as User-to-User information (UUI):

1. Create SIP-Copylist.

```
voice class sip-copylist 1
 sip-header Refer-To
```

2. Create SIP-Profile.

```
voice class sip-profiles 1
 request REFER peer-header sip Refer-To copy ";(.*)" u01
 request REFER sip-header Refer-To modify "Refer-To: (.*)" "Refer-To: <\1;\u01”
```

3. Profile at the dial peer level:
   a. Copy-list to be applied under the inbound dial-peer: voice-class sip copy-list 1.
   b. SIP-profiles to be applied under the outbound dial-peer: voice-class sip profiles 1.

```
Example:
=============================================================================================
1. Example of SIP copy-list:
voice class sip-copylist 2
sip-header Refer-To

2. Example of SIP Profile:
voice class sip-profiles 2
request REFER peer-header sip Refer-To copy ";aai=(.*)" u02
request REFER sip-header Refer-To modify "Refer-To: (.*)" "Refer-To:
<\1;User-to-User=\u02"

3. Example of dial peer:

Dial peer to fwd the call to VVB
----------------------------------------
dial-peer voice 345679 voip
destination-pattern 369852147
session protocol sipv2
session target ipv4:10.78.0.94
session transport tcp
voice-class sip copy-list 2
codec g711ulaw

Dial peer to modify the outgoing SIP REFER message
-------------------------------------------------------------------
dial-peer voice 345678 voip
session protocol sipv2
session target sip-server
session transport tcp
incoming called-number 369852147
voice-class sip profiles 2
codec g711ulaw
```

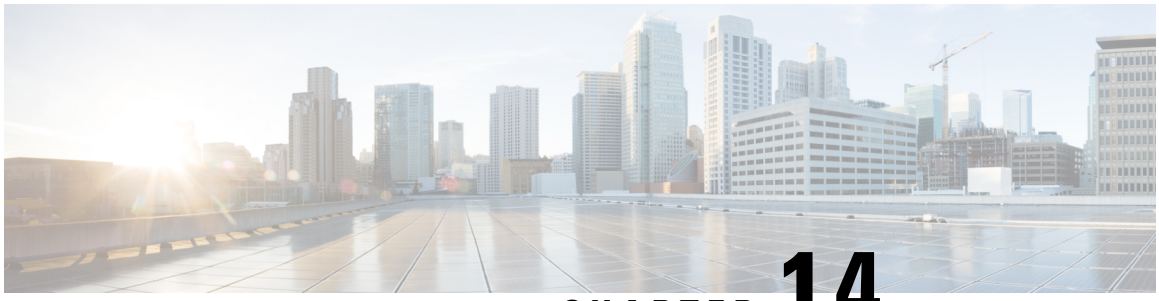
Once the aforesaid configuration is done, the SIP REFER message with the following SIP header:

Refer-To:
<sip:1247@72.163.166.103;**aai=PD%2C04%3BC8%2C48656c6c652074686572652 1%3BFA%2C0000101642131107095 6**>

is modified to:

Refer-To:
<sip:1247@72.163.166.103;**User-to-User=PD%2C04%3BC8%2C48656c6c652074686572652 1%3BFA%2C0000101642131107095 6**>

With similar configuration on gateway, other SIP headers can also be modified according to the call flow needs.



CHAPTER 14

Cisco VVB Configuration

Note Cisco VVB does not support clustering. Therefore, you may ignore any message on the Cisco VVB Admin UI/CLI that refers to **cluster**, **publisher**, **subscriber**, etc.

Configure Cisco VVB on Unified CVP

Procedure

Step 1 Log in to CVP Operations Console and click **Device Management** > **Virtualized Voice Browser**.

Step 2 Click **Add New**.

Note To use an existing Virtualized Voice Browser (VVB) as a template for configuring a new VVB, select a VVB from the list of available VVB and click **Use As Template** and perform Steps 3 to 5.

Step 3 In the **General** tab, enter the field values, and click **Save**.

To configure General settings on a VVB, on the **General** tab, enter the field values, as listed in the following table:

Table 46: General Settings

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

Table 47: Administration Credentials Settings

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

Table 48: Cisco VVB Serviceability Fields

Field	Description	Data Range	Default
Enable Serviceability	Check to enable this feature.	N/A	Not Checked
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.	N/A

Field	Description	Data Range	Default
Password/Confirm Password	The password required to sign in (VVB CLI Platform credentials).	Any text that follows the requirements for choosing secure passwords.	N/A
Port	The port on which Serviceability is configured on Cisco VVB.	N/A	8443

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 (Optional) On the **Device Pool** tab, select the field values and move to **Selected**.

Step 5 Click **Save**.

Related Topics

Add or Remove Device From Device Pool, on page 97

Add or Remove Device From Device Pool

Procedure

Step 1 From the **Device Management** menu, select a device to add to the Device Pool.

Example:

To add a Call Server to a device pool, select Unified CVP Call Server from the **Device Management** menu.

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

Step 2 Select a device pool from the **Device Pool** list and click **Edit**.

Step 3 On the **Device Pool** tab:
- In the **Available** list box, select one or multiple devices and click the **Add** arrow. The added devices appear in the **Selected** list box.
- To remove the added devices from the **Selected** box, select them and click the **Remove** arrow. The added devices appear in the **Selected** list box.

Step 4 Click **Save & Deploy**.

Note
- Click **Save** to save the changes in Operations Console and add or remove a device from Device Pool later.
- Some edit-device windows have an **Apply** button instead of **Save**. Click **Apply** to copy the configuration to the device.

Configure Cisco VVB Call Flow

Cisco VVB provides the standard list of scripts that require you to configure for the Unified CVP call flow to work. The primary steps are to create application and assign corresponding SIP trigger.

Log in to Cisco VVB Administration Console and follow these tasks:

Procedure

Step 1 Create an application to define the call flow through the scripts.

To configure standalone application, see Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285.

To configure comprehensive and ringtone application, see Configure Cisco VVB Settings for Comprehensive Call Flow Model, on page 286.

To configure error application, see Configure Error Application, on page 290.

Step 2 Create triggers to invoke an application using the incoming directory number.

To configure the trigger, see Configure SIP Triggers, on page 291.

Step 3 Cisco VVB can play recorded audio prompts and detect DTMF tones. To recognize speech and play text, configure Automatic Speech Recognition (ASR) and Text-To-Speech (TTS).

To configure ASR and TTS, see Configure Speech Servers, on page 293.

Step 4 Manage prompt files to add custom ringtone for comprehensive call flow or to use custom prompts.

To configure and manage prompts, see Configure Prompt Management , on page 296.

Related Topics

Configure Cisco VVB Settings for Standalone Call Flow Model, on page 285
Configure Cisco VVB Settings for Comprehensive Call Flow Model, on page 286
Configure Error Application, on page 290
Configure SIP Triggers, on page 291
Configure Speech Servers, on page 293
Configure Prompt Management , on page 296

Configure Cisco VVB Settings for Standalone Call Flow Model

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

Step 2 Click the **Add New** icon that is displayed in the toolbar in the upper left corner of the window or the **Add New** button that is displayed at the bottom of the window.

Step 3 Type the application name in the **Name** field.
The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

Note This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

Step 4 Select the `SelfService.aef` script from the drop-down list for a standalone application.
The following table describes the parameters:

Parameter	Description	Default	Base Type
Application Name	Application name that is present on the VXML server. Mandatory field to enter.	"HelloWorld"	Alphanumeric
Port	Port on which the VXML server or load balancer is running. **Note** Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later. For earlier versions of CVP, configure ports 8000/8443.	"7000"	Numeric
PrimaryVXMLServer	VXML server or load balancer IP address.	""	Alphanumeric
BackupVXMLServer	VXML server backup server IP address.	""	Alphanumeric

Parameter	Description	Default	Base Type
Secured	If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default it is not enabled. **Note** If you have enabled secure communication, then ensure to: **a.** Change the port number in the above field to 7443. **b.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide.* **c.** Restart Tomcat server and Engine from command line.	false	Boolean

Step 5 Use the Tab key to automatically populate the **Description** field.

Step 6 Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

Step 7 Click **Add**.

The Cisco Script Application page refreshes and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

Step 8 Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 291.

Related Topics

Configure SIP Triggers, on page 291

Configure Cisco VVB Settings for Comprehensive Call Flow Model

This topic provides information about comprehensive and ringtone applications.

Note Cisco VVB is prepopulated with comprehensive application (also called bootstrap) and the ringtone application.

To create a custom comprehensive (CVP/VRU comprehensive) or ringtone application, follow the steps:

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

Step 2 Click **Add New**.

Step 3 (Mandatory) Type the application name in the **Name** field.

Step 4 The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

Note This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

Step 5 Select the script from the drop-down list.

The following scripts are provided for comprehensive call flow:

- CVPComprehensive.aef (bootstrap)
- Ringtone.aef

The following table describes the parameters:

Parameter	Description	Default	Base Type
Secured	If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default, it is not enabled. **Note** If you have enabled secure communication, then ensure to: **a.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Cisco Unified Communications Operating System Administration Guide.* **b.** Restart Tomcat server and Engine from command line. If you are using a coresident VXML and Call Server, use CA-signed certificate.	false	Boolean

Parameter	Description	Default	Base Type
Sigdigit	Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives the call, the CVP comprehensive service is configured to strip the digits. When the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.	0	Numeric

Step 6 Use the Tab key to automatically populate the **Description** field.

Step 7 Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

Step 8 Click **Add**.

The Cisco Script Application page refreshes and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

Step 9 Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 291.

Related Topics

Configure SIP Triggers, on page 291

Configure Cisco VVB Settings for VRU-Only Call Flow Model

This topic provides information to create VRU-Only applications.

Use the *VRUComprehensive.aef* script if your CVP implementation needs to support non-reference VRU call flows or VRU-Only call flows. For more details on non-reference call flows, see *Solution Design Guide for Cisco Unified Contact Center Enterprise.*

To support the comprehensive call flow in addition to the non-reference VRU call flows, add relevant options to this script. The *CVPComprehensive* script must not be separately configured to handle a mixed implementation.

To create a VRU-Only application, follow the steps:

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

Step 2 Click **Add New**.

Step 3 (Mandatory) Type the application name in the **Name** field.

Step 4 The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

Note This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

Step 5 From the **Script** drop-down list, select the *VRUComprehensive.aef* script.

Parameter	Description	Default	Base Type
PrimaryVXMLServer	VXML server or load balancer IP address	""	Alphanumeric
BackupVXMLServer	VXML backup server or load balancer IP address	""	Alphanumeric
Port	Port on which VXML server or load balancer is running. **Note** Ports 7000/7443 must be configured for interworking with CVP Release 11.5 and later.	"7000"	Numeric
Secured	If enabled, HTTPS is used while fetching VXML application from Unified CVP. By default, Secured is not enabled. **Note** If you have enabled secure communication, then ensure to: **a.** Change the port number to 7443. **b.** Upload the relevant certificate. To upload certificate, see *Upload certificate or certificate trust list* topic in *Configuration Guide for Cisco Unified Customer Voice Portal.* **c.** Restart Tomcat server and engine from command line. If you are using a co-resident VXML and Call Server, use a CA-signed certificate.	false	Boolean
Sigdigit	Enable this parameter to use Significant Digits feature. Enter the number of digits that are used as sigdigit. When Cisco VVB receives a call, the VRU comprehensive service is configured to strip the digits. When the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.	0	Numeric

Step 6 Use the Tab key to automatically populate the **Description** field.

Step 7 Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

Step 8 Click **Add**.

Cisco Script Application page refreshes. The **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

Step 9 Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 291.

Configure Error Application

To create a comprehensive application, follow the steps:

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **Applications** > **Application Management**.

Step 2 Click **Add New**.

Step 3 Type the application name in the **Name** field.
The **Maximum Number of Sessions** field is prepopulated based on the OVA profile. You can edit this field.

Note This number must not exceed the maximum number of ports supported for Cisco VVB profile. For more information, see *Virtualization for Cisco Virtualized Voice Browser* available at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-virtualized-voice-browser.html.

Step 4 Select the `Error.aef` script from the drop-down list. This script is used to play error tone.

The following table describes the parameter details:

Parameter	Default	Base Type
CVPErrorPrompt—Select and associate custom wav file from VVB application. To override system default wav file, upload custom wav file from **Prompt Management** menu. **Note** You can upload custom wav files only for `Error.aef` script.	92929292	Numeric

Step 5 Use the Tab key to automatically populate the Description field.

Step 6 Enable the application by selecting the radio button. You can choose to disable the application to retain the configurations for later use.

Step 7 Click **Add**.

Cisco Script Application page is refreshed and the **Add New Trigger** hyperlink appears in the left navigation bar. The following message is displayed in the status bar on top:

```
The operation has been executed successfully.
```

Step 8 Create a trigger using the **Add New Trigger** hyperlink or follow the procedure Configure SIP Triggers, on page 291.

Related Topics

Configure SIP Triggers, on page 291

Configure SIP Triggers

An SIP trigger responds to calls that arrive on a specific route point and uses telephony and media resources to complete the call and to invoke the application script.

You must add SIP triggers to invoke Cisco applications in response to incoming contacts.

Add SIP Trigger

To add an SIP trigger:

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP Triggers**.

Step 2 Click **Add New** and enter the following fields:

Field	Description
Directory Information	
Dial Number Pattern	A unique phone number. The value includes digits and optionally includes " * " to mask multiple digits. Examples of **valid** Directory Numbers: 9191* Examples for valid triggers: • 10.919191 where 10. is the same as 101, 102 • *12* or 12*23 where *12* is the same as "*" and 12*23 is the same as 12* **Note** The trigger cannot contain only a wildcard character (*). If it contains *, it must also contain numbers. Capital letter "X" can be used as a wildcard, but small letter "x" cannot be used.
Trigger Information	
Application Name	From the drop-down list, choose the application to associate with the trigger.

Field	Description
Advanced Trigger Information (available only if you click **Show More**)	
Enabled	Click a radio button to choose the required option: • **Yes—**Enable the trigger (default) • **No—**Disable the trigger
Idle Timeout (in ms)	The number of milliseconds (ms) the system waits before rejecting the SIP request for this trigger.
Override Media Termination	Click a radio button to choose the required options: **Yes—**Override media termination. **No—**Enable media termination (default). If you select Yes, two panes open: • Selected Dialog Groups — displays the default or selected group. **Note** You must not change the default Selected Dialog Group associated with the application. • Available Dialog Groups — displays the configured dialog.
Description	Click the **Tab** key to populate it.

The new trigger is created and listed on the SIP Trigger page.

Configure SIP Properties

Cisco VVB does not send 180 Ringing Provisional Response for an incoming SIP INVITE. To enable SIP 180 Ringing Provisional Response:

Procedure

Step 1 From the Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP Properties**.

Step 2 Select the **Enable** radio button and click **Update**.

Configure SIP RAI

The Resource Available Indication (RAI) feature supports:

- Monitoring of CPU and memory resources

- Reporting of VVB resource status to an externally configured device

To configure RAI to a server:

Procedure

Step 1 From the Cisco VVB Administration menu bar, choose **Subsystems** > **SIP Telephony** > **SIP RAI**.

Step 2 On the SIP RAI Configuration page, click **Add New**.

Step 3 Enter the following fields:

Field	Default Value / Range	Description
Server Name		Hostname or IP address of SIP server.
Port	5060 Range: 1 to 65535	SIP server port number for communication.
Interval	60 Range: 30 to 86400 (in seconds)	Interval time to send RAI reports.

Step 4 Click **Add** to add a SIP server.

Step 5 (Optional) To update a server port or interval time, click the server name and update the **Port** and **Interval** fields.

Step 6 (Optional) To delete a server, click the **Delete** icon present on the SIP RAI List or from the update server page.

Configure Speech Servers

Cisco VVB supports ASR and TTS through two subsystems:

ASR
This subsystem allows users to navigate through a menu of options by speaking instead of pressing keys on a touch-tone telephone.

TTS
This subsystem converts plain text into spoken words to provide a user with information, or prompt a user to respond to an action.

Note Only G711 codec is supported for ASR and TTS integrations.

Prepare to Provision ASR/TTS

The customer must perform the following tasks:

- Order ASR and TTS speech servers from Cisco-supported vendors.

Note For more information about supported speech servers for Cisco VVB, see the Solutions Compatibility Matrix available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

- Work with the ASR and TTS vendor to size the solutions.
- Provision, install, and configure the ASR and TTS vendor software on a different server (in the same LAN) and not where the Cisco VVB runs.

Provision ASR Servers

Use the Automatic Speech Recognition Server Configuration web page to specify information about the speech server name and port location.

Procedure

Step 1 From the Cisco VVB Administration menu bar, choose **Subsystems** > **Speech Servers** > **ASR Servers**.

Column	Description
Server Name	Hostname or IP address of the ASR server. **Note** ASR server deployment over WAN is not supported in Cisco VVB. Place the ASR server in the same LAN as Cisco VVB. You need to specify the ASR server hostname or IP address that is local with Cisco VVB node while installing the ASR server software in this field.
Port	Port number used to connect to a Speech server.
Status	Status or state of the server.

Step 2 Click the **Add New** button to provision a new ASR Server.

Step 3 Enter the following fields:

Field	Description
Server Name	Hostname or IP address of the ASR server.
Port Number	Port numbers that are used to connect to a Speech server. The default value for MRCPv1 is 4900 and for MRCPv2 is 5060. **Note** If the administrator has configured any other the port value for MRCP/ASR servers, then use the same port value here. Do not use these default values. Whenever the administrator changes from MRCP protocol, ensure ASR server is deleted and re-created with the appropriate port values.

Step 4 Click **Add** to apply the changes.

Step 5 (Optional) Click the **Refresh** button to refresh the status of the server.

Provision TTS Servers

Use the Text-to-Speech Server Configuration web page to configure the TTS server name and port location.

Procedure

Step 1 From the Cisco VVB Administration menu bar, choose **Subsystems** > **Speech Servers** > **TTS Servers**.

The TTS Server Configuration web page opens displaying a list of previously configured servers, if applicable, with the following information:

Column	Description
Server Name	Hostname or IP address of the TTS server. **Note** TTS server deployment over WAN is not supported in Cisco VVB. In other words, the TTS servers must be in the same LAN as Cisco VVB. Therefore, you need to specify the TTS server hostname or IP address that is local with Cisco VVB node while installing the TTS server software in this field.
Port Number	Port number used to connect to a Speech server.
Status	Status or state of the server.

Step 2 Click the **Add New** button to provision a new TTS Server.

Step 3 Enter the following fields:

Field	Description
Server Name	Hostname or IP address of the TTS server.
Port Number	Port number used to connect to a TTS server. The default value for MRCPv1 is 4900 and for MRCPv2 is 5060. **Note** If the administrator has configured any other the port value for MRCP/TTS servers then use the same port value here, do not use these default values. Whenever the administrator changes from MRCP protocol, ensure TTS server are deleted and recreated with appropriate port values.

Step 4 Click **Add** to apply the changes.

Step 5 (Optional) Click the **Refresh** button to refresh the status of the server.

Configure Prompt Management

Several system-level prompt files are loaded during Cisco VVB installation. However, any file you create must be available to the Cisco VVB Engine before the Cisco VVB application can use it. Files are made available through the Cisco VVB Repository datastore, where the prompt files are created, stored, and updated.

Note Use Prompt Management to store prompt WAV files locally. It helps you avoid any fetch latency while playing the large prompt. You can also use it to override the system default prompts.

Manage Prompt Files

Many applications make use of prerecorded prompts. These are stored as *.wav* or *.au* files, and are played back to the callers to provide information and elicit caller response.

To access the Prompt Management page:

Procedure

Step 1 From Cisco VVBAdministration menu bar, choose **Applications** > **Prompt Management**.

Step 2 The **Prompt Management** page opens to display the following fields.

Field	Description
Name	Name of the folder.
Size	The size of the prompt file in kilobytes (KB). **Note** This column is usually blank on the root page because the items on this page are usually folders. The maximum limit for the uploaded prompt file is 20MB.
Date Modified	The date and time when the document was last uploaded or changed along with the time zone.
Modified By	The user ID of the person who made these modifications.
Delete	To remove the folder and its contents from the repository.
Rename	To rename the folder in the repository.
Refresh	To refresh the folder in the repository.
Create New Folder	To create a new subfolder.

Field	Description
Upload Prompt	To upload a prompt (.wav/.au) file or prompts packaged in a zip. **Note** The maximum limit for the uploaded prompt file is 20MB.

Local Audio Files Stored on VVB

Local Audio Files Stored on VVB

Local audio files that are uploaded to default prompt folder of VVB can be accessed by setting the audio source path starting with "flash:" in microapps or VXML application. The audio files must be pre-uploaded to default folder.

Example: "flash:holdmusic.wav"

If you are creating a custom folder in prompt management and uploading an audio file, then mention the folder name in the URL.

Example: flash:/<folder_name>/<file_name>

Overriding Default Ringtone using CVP

Follow these steps to override default ringtone:

1. Go to **System** > **Dialed Number Pattern**.
2. From the listed patterns, click **Pattern** for which custom ringtone needs to be added.
3. From **Dialed Number Pattern Types**, check the **Enable Custom Ringtone** check box.
4. Specify the custom ringtone filename in the text box.

Note

- Custom ringtone cannot be named to ringback.wav.
- The audio file in Cisco VVB and the filename you entered in CVP under DNP is case-sensitive (should be same with .wav extension)

Configure System Parameters

Use the System Parameters web page to configure system parameters such as port settings and locale settings and to default session timeout.

The parameters in the System Parameters Configuration page are grouped logically into sections with headings. Each parameter has a corresponding suggested or default value on the right side of the page. Where applicable, radio buttons are used to toggle between the parameter options.

Choose **System** > **SystemParameters** from the Cisco VVB Administration menu bar to access the System Parameters Configuration web page.

Manage System Parameters

On System Parameters page, you can configure basic system settings such as Audio Codec, MRCP version,TLS (SIP), and other parameters.

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

Procedure

Step 1 From Cisco VVB Administration menu bar, choose **System** > **SystemParameters**.

Step 2 To update, click the **Update** icon in the toolbar or the **Update** button at the bottom of the window.

The System Parameters Configuration web page displays the following fields.

Table 49: System Parameters Configuration

Field	Description
Generic System Parameter	
System Time Zone	The system time zone of Cisco VVB server configured during installation.
Media Parameters	
Codec	G711 and G729 audio codecs with sampling rate 8K are supported. Default: G711U
MRCP Version	Select the MRCP version to communicate between Nuance and Cisco VVB. Default: MRCPv2 **Note** • The default value for ASR/TTS server port for MRCPv1 is 4900 and for MRCPv2 is 5060. Whenever the administrator changes from MRCP protocol, ensure ASR/TTS server is deleted and re-created with appropriate port values. • ASR-TTS service is not supported using G729 codec; therefore, MRCP is not applicable.

Field	Description
User Prompts override System Prompts	When enabled, custom recorded prompt files can be uploaded to the appropriate language directory under **Prompt Management**. The custom prompts override the system default prompt files for that language. By default, this feature is disabled. **Note** For overriding the system default prompt files for ringtone application: • Create a new folder named **vb**. Select **Applications** > **Prompt Management** and click **Create New Folder**. • Upload the custom ringtone. Choose **Applications** > **Prompt Management** and click **Upload Prompt**. Upload custom ringtone wav file(named same as **ringback.wav**) under folder **vb**.
Security Parameters	
TLS(SIP)	TLS (SIP) is disabled by default. When enabled, this setting secures SIP signaling on the IVR leg. TLS (SIP) version supported is TLSv1.2, and the default cipher suites are `TLS_RSA_WITH_AES_128_CBC_SHA` and `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`. SSL certificates need to be exchanged between VVB and any SIP endpoint (CVP, Ingress Gateway, and so on.) to talk over TLS. For more details on this configuration, see the *Upgrade Unified CVP > Postupgrade Tasks > Manual Configuration of Unified CVP Properties* section in the *Configuration Guide for Cisco Unified Customer Voice Portal, Release 12.5(1)* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html. **Note** Cisco VVB Engine restart is required after a change to this configuration.
Supported TLS (SIP) Versions	This allows you to select the version of TLS (SIP). TLS (SIP) version supported is TLSv1.2. When you select a given TLS (SIP) version, Cisco VVB will support SIP TLS requests for this version and the higher supported versions. **Note** • Supported TLS (SIP) Versions is available only if TLS (SIP) is enabled. • Cisco VVB Engine restart is required after a change to this configuration. • The supported TLS (SIP) versions as client or server for securing SIP signaling in the IVR leg can alternatively be specified via the CLI command **set tls server min-version** as documented in the *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html

Field	Description

Cipher Configuration	This field defines the ciphers that are supported by Cisco VVB with key size lesser than or equal to 2048 bits.
	The following ciphers are pre-populated.
	• `TLS_RSA_WITH_AES_128_CBC_SHA`
	• `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
	Note • Cipher configuration is available only if TLS (SIP) is enabled.
	• You must restart the Cisco VVB engine after modifying the cipher configuration.
	• If you are using CUBE version 16.6 and higher, you must manually change the crypto suite to 128/256 by enabling CLI on the dial-peer towards VVB as shown:
	`voice class srtp-crypto 1`
	` crypto 1 AES_CM_128_HMAC_SHA1_32`
	`dial-peer voice xxxx voip (Dial-peer to VVB srtp)`
	`  ...`
	`  voice-class sip srtp-crypto 1`

SRTP	• SRTP is disabled by default. When SRTP is disabled, the media is not encrypted. • When SRTP is enabled, it secures the IVR leg. SRTP uses Crypto-Suite AES_CM_128_HMAC_SHA1_32 for encrypting the media stream. • When **Allow RTP (Mixed mode)** check box is checked, the system accepts both SRTP and RTP call flows. This check box can be checked only when SRTP is enabled. **Note** • SRTP is available only if TLS (SIP) is enabled. • Check the **Allow RTP (Mixed mode)** check box if device is configured to work in the RTP mode and interacts with MRCP ARS-TTS servers. • For more details on mixed mode call flow scenarios, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html. • Cisco VVB engine restart is required after a change to this configuration. • SRTP is not supported with VVB XU (Export Unrestricted) software image releases.
System Port Parameter	

Field	Description
RMI Port	The port number used by Cisco VVB to serve Remote Method Invocation (RMI) requests. This field is mandatory. Default: 6999

HTTPS Client TLS Configuration

The supported TLS versions as client for securing HTTPS signaling to fetch the VXML applications from VXML server use the CLI command **set tls client min-version** in *Cisco Unified Contact Center Express Administration and Operations Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html

IP Address and Hostname Management

This section provides the steps you need to follow whenever there is a change in IP address or hostname for Cisco VVB deployment.

IP Address Modification

This section describes how to change the IP address.

Caution Changing the IP address can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts such as ServerDown. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

Note As a prerequisite ensure that the DNS is reachable and the DNS record exists for the server if DNS is enabled.

Change IP Address using CLI Commands

Before you begin

Use this procedure to change the IP address of Cisco VVB.

Procedure

Step 1 If DNS is enabled, change the DNS record of the server to point to the new IP address.

Step 2 If you want to change the IP address of the server on the same subnet or a different subnet that requires a new default gateway address, then use either CLI Commands or Cisco Unified Operating System Administration interface.

Step 3 To change the default gateway, enter the following CLI command: **set network gateway <IP Address>**

The following is a sample output:

```
admin: set network gateway 10.10.10.1
     ***   W A R N I N G   ***
This will cause the system to temporarily lose network connectivity
Continue (y/n)?
```

Caution Ensure that the server is moved to the new subnet and has access to the default gateway before proceeding to the following sub-step

Note Skip this step if you want to change only the IP address of the server.

Step 4 To change the IP address of the server, enter the following CLI command: **set network ip eth0 <ip_address> <netmask> <default gateway>**

The following sample output displays:

```
admin:set network ip eth0 10.10.10.170 255.255.255.0 10.10.10.1
          ***   W A R N I N G   ***
This command will restart system services
======================================================
 Note: Please verify that the new ip address is unique
       across the cluster and, if DNS services are
       utilized, any DNS configuration is completed
       before proceeding.
======================================================
Continue (y/n)?
```

Enter **y** and press **Enter** to continue.

Step 5 Reboot the system using the CLI command **utils system restart**.

Change IP Address using OS Administration interface

Procedure

Step 1 Log in to the Cisco Unified OS Administration using administrator login.

Step 2 Go to **Settings** > **IP** > **Ethernet**.

Step 3 Change the Port (IP Address and Subnet Mask) and Gateway information and click **Save**.

Step 4 Reboot the system using the CLI command **utils system restart**.

Hostname Modification

This section describes how to change the hostname.

Caution Changing the hostname can interrupt call processing and other system functions. Changing the hostname can also cause the system to generate certain alarms and alerts such as ServerDown. Because of this potential impact to the system, you must perform hostname changes during a planned maintenance window.

Note If DNS is enabled, as a prerequisite ensure that the DNS is reachable and the DNS record exists for the server.

Change Hostname using CLI Commands

Procedure

Step 1 Change the DNS record of the server to point to the new hostname. Ensure that you correctly update both the forward (A) and reverse (PTR) records, and there are no duplicate PTR records.

Step 2 You can change the hostname of the server either using the CLI (command line interface) command or using Cisco Unified OS Administration interface. To change the hostname using CLI command, go to Step 3 or to change the hostname using Cisco Unified OS Administration interface, go to Step 4.

Step 3 At the CLI prompt, enter **set network hostname** and press **Enter** key.

The following is a sample output:

```
***   W A R N I N G   ***
Do not close this window without first canceling the command.
This command will automatically restart system services.
The command should not be issued during normal operating hours.
=====================================================
Note:
Please verify that the new hostname is a unique name across the cluster and,
if DNS services are utilized, any DNS configuration is completed before proceeding.
=====================================================
Security Warning :
This operation will regenerate all UCCX Certificates including any third party
signed Certificates that have been uploaded.
Enter the hostname::
```

Step 4 Enter the hostname and press Enter.

Step 5 Reboot the system using the CLI command **utils system restart**.

Change Hostname using OS Administration Interface

Procedure

Step 1 Login to the Cisco Unified OS Administration using administrator login.

Step 2 Go to **Settings** > **IP** > **Ethernet**.

Step 3 Change the hostname and click **Save**.

Step 4 Reboot the system using the CLI command **utils system restart**.

Configure Reporting and Monitoring Services

Real-Time Monitoring Tool

Cisco VVB system includes software components called *plug-in* to enhance Cisco VVBEngine. You can download Real-Time Monitoring Tool (RTMT) plug-in from the web page.

To access the Plug-in web page, choose **Tools** > **Plug-in** from Cisco VVBAdministration menu bar.

The Plug-in web page contains the following hyperlink:

- **Cisco Unified Real-Time Monitoring Tool for Windows**—Click this hyperlink to install client-side Cisco Unified Serviceability RTMT for Windows. RTMT uses HTTP/HTTPS and TCP to monitor device status, system performance, device discovery, and CTI applications. It also connects directly to devices by using HTTP/HTTPS for troubleshooting system problems. This plug-in is available only for users with administrator capability.

Note To download, click the **Download** hyperlink and select **Save File**.

Real-Time Reporting

Caution The Real-Time Reporting (RTR) tool is a Java applet that can generate various reports that provide detailed information about the status of your Cisco VVB system. You use the Application Reporting web page to access the RTR tool.

To access the Application Reporting web page, choose **Tools** > **Real-Time Reporting** from the Cisco VVB Administration menu bar.

Note To access RTR tool, ensure to add Cisco VVB IP address under **Exception Site List** in **Java Control Panel** > **Security**. Example IP address entry is as follows: `https://10.10.10.10`.

For more information, see Cisco VVB Real-Time Reports, on page 305.

Related Topics

Cisco VVB Real-Time Reports, on page 305

Logging

A trace file is a log file that records activity from the Cisco VVB component subsystems and steps. Trace files let you obtain specific, detailed information about the system that can help you troubleshoot problems.

This information is stored in a trace file. To help you control the size of the trace file, you specify the components for which you want to collect information and the level of information that you want to collect.

The Cisco VVB server stores the trace files in the Log directory. You can collect and view trace information using the Real-Time Monitoring Tool (RTMT).

To activate and turn off logging, follow this procedure:

Service Management

Installed automatically, network services include services that the system requires to function; for example, system services. Because these services are required for basic functionality, you cannot activate them in the Service Activation window. After the installation of your application, network services start automatically.

To start, stop, or restart Cisco VVB services, follow these steps:

Procedure

Step 1 From the Navigation drop-down list, select **Cisco VVB Serviceability.**

Note For freshly installed VVB, **Cisco VVB Serviceability** is accessible only after completing the setup procedure from the VVB Administration page.

Step 2 Select **Tools** > **Control Center - Network Services**.

Step 3 Select the **Engine** radio button and click your desired operation button.

The page displays the following information for the network services:

- Name of the network services, their dependent subsystems, managers, or components
- Status of the service (IN SERVICE, PARTIAL SERVICE, or SHUT DOWN; for individual subsystems, the status can be OUT OF SERVICE or NOT CONFIGURED)
- Start Time of the service
- Up Time of the service

Cisco VVB Real-Time Reports

Related Topics

Report Menu, on page 310

Available Cisco VVB Real-Time Reports

Cisco VVB real-time reporting provides real-time reports you can use to monitor Cisco VVB system activity. The following table briefly describes each of these reports.

Report	Description
Application Tasks	Provides information about currently active applications.
Application Tasks Summary	Provides a summary of specific application activity.
Applications	Provides a list of all applications loaded on the Cisco VVB server.
Contacts Summary	Provides information for call contacts and total number of contacts.
Contacts	Provides information about currently active contacts.
Engine Tasks	Provides information about currently active Engine tasks.
Sessions	Provides information on all active sessions.

Related Topic

Report Menu, on page 310

Open Real-Time Reports

Real-Time reporting is available from the Cisco VVBAdministration web interface.

Real-Time Reporting requires the Java plug-in. If the Java plug-in is not already installed on the PC on which you are viewing the reports, the Cisco VVB system automatically installs it when you choose **Tools** > **Real Time Reporting Tool**.

Note

- Use Mozilla Firefox and Internet Explorer for Real Time Reporting.
- If you are using Mozilla Firefox, you must manually install the correct version of JRE to use real-time reports.

The Application Reporting web page is a stand-alone component of the Cisco VVBAdministration interface. It has its own menu bar, which replaces the Cisco VVBAdministration menu bar.

To open real-time reporting, complete the following steps.

Procedure

Step 1 If you are running Real-Time Reporting for the **first time** on this system, log into Cisco VVBAdministration as an **Administrator**.

The system prompts you to download the Java plug-in; follow the prompt instructions.

Note After you perform the initial download of the Real-Time Reporting Java plug-in, non-Administrative users can access Real-Time Reporting on this system.

Step 2 Choose **Tools** > **Real-Time Reporting** from the Cisco VVBAdministration menu bar.

The Application Reporting web page opens in a new window. The real-time reporting tool requires a Java plug-in. If the plug-in is not installed on the machine you are using, the Cisco VVB system prompts you to accept the automatic installation of the plug-in. If you do not accept the installation, you cannot use real-time reporting.

Run Reports

Open the real-time reporting tool from the Cisco VVBAdministration web interface to run reports.

To run a real-time report, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Reports**.

Step 2 From the Reports menu, choose the report to run.

The report opens in the Application Reporting window.

View Detailed Subreports

You can view more detailed information for selected items in these four reports:

- Application Tasks report
- Contacts report
- Applications report
- Sessions report

To view detailed subreports, complete the following steps.

Procedure

Step 1 Run the Application Tasks, Contacts, Applications, or Sessions report.

Step 2 Click a line in the report for which you want to view more detailed information. For example, click an email address in the Contacts report.

Step 3 From the Application Reporting menu bar, choose **Views** and click the subreport that you want to run.

You can also open a subreport by right-clicking the selected item and choosing a subreport.

The subreport opens.

Print Reports

To facilitate printing, you can open a printable version of a report.

To print a report, complete the following steps.

Procedure

Step 1 Run a report.

Step 2 From the Application Reporting menu, choose **Tools** > **Open Printable Report**.

A printable version of the report opens in a separate window.

Step 3 Print the report using your browser print functionality.

Reset Report Statistics

The Cisco VVB system automatically resets all statistics each day at midnight. You can reset the accumulated statistics manually at any time. Resetting statistics does not reset active statistics, such as active contacts and active tasks.

To reset report statistics, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Tools** > **Reset All Stats**.

The Reset Stats dialog box opens for you to confirm the reset.

Step 2 Click **Yes**.

Accumulated statistics are reset.

Set Report Options

You can set the following reporting options:

- Refresh interval
- Number of times that the Cisco VVBAdministration web interface should attempt to reconnect to the Cisco VVB server

To set report options, complete the following steps.

Procedure

Step 1 From the Application Reporting menu bar, choose **Settings** > **Options**.

The Options dialog box opens.

Step 2 From the Polling Interval drop-down menu, choose the refresh rate in seconds.

Step 3 From the Server Connect Retry Count drop-down menu, choose the number of times that the Cisco VVBAdministration web interface should attempt to reconnect to the Cisco VVB server.

Step 4 Click **Apply** to apply the settings.

Set Report Appearance

You can select from three report appearances:

- Windows, which displays reports in colors based on your Windows settings
- Motif, which displays reports in purple and menu items in brown
- Metal, which displays reports in grey and menu items in black

To set the report appearance:

Procedure

Choose **Settings** from the Application Reporting menu bar and click the appearance that you want.

Application Reporting User Interface

When you choose **Tools** > **Real-Time Reporting** from the Cisco VVBAdministration menu, the Application Reporting tool opens a web page in a new window.

The Application Reporting tool menu bar contains the following options:

- **Report**—Choose this option to display a list of the available top-level real-time reports.
- **Tools**—Choose this option to reset all the statistics and refresh connections.
- **Settings**—Choose this option to set the look and feel of the real-time Reporting client, set the polling (refresh) interval times, and set the amount of times the server will attempt to reconnect.
- **Help**—Choose this option to display system information and to access Cisco VVB online help.

Report Menu

The Report menu provides access to a variety of top-level reports. It contains the following menu options:

Related Topics

Call Contacts Detailed Info Report, on page 312

Contacts Summary Real-Time Report

Use the Contacts Summary report to view specific contact information for call contacts, email contacts, HTTP contacts, and total number of contacts.

To access the Contacts Summary real-time report, choose **Reports** > **Contacts Summary** from the Application Reporting menu bar.

Note You display the data on this report as numbers or percentages by clicking the Display Value/Display % toggle button.

The following fields are displayed on the Contacts Summary report.

Field	Description
Active	Active contacts that are currently running.
Inbound	Number of inbound contacts since the statistics were last reset.
Connected	Number of connected contacts since the statistics were last reset. Provides a total for contacts that are connected to resources.
Terminated	Number of terminated contacts since the statistics were last reset.
Rejected	Number of rejected contacts since the statistics were last reset.
Aborted	Number of aborted contacts since the statistics were last reset.

Application Tasks Summary

Use the Application Tasks Summary report to display statistics that summarize the activity of specific applications.

To access the Application Tasks Summary real-time report, choose **Reports** > **Application Tasks Summary** from the Application Reporting menu bar.

The following fields are displayed on the Application Tasks Summary report.

Field	Description
Application Name	Names of the applications that are running or have run.
Running	Currently running applications.
Completed	Applications that have stopped running.
Total	Number of times an application was invoked since the statistics were last reset.

Application Tasks Real-Time Report

Use the Application Tasks real-time report to view information about currently active applications.

To access the Application Tasks report, choose **Reports** > **Application Tasks** from the Application Reporting menu bar. The following fields are displayed on the Application Tasks report.

Field	Description
ID	Unique application task ID.
Node ID	Unique ID for a server in the cluster. **Note** As Cisco VVB does not support clustering, you can ignore the value.
Application	Name of the application.
Start Time	Time when the application task started.
Duration	Length of time that the application has been active.

Note If this report indicates that an application is running for an unusually long time, there may be a problem with the application. The application script may not include error handling that prevents infinite retries if a call is no longer present. If the application does not receive a disconnect signal after a call, the application repeatedly retries to locate the call, and causes the application to run for an unusually long time. To prevent this problem, include the proper error handling in the application script.

Engine Tasks Real-Time Report

Use the Engine Tasks real-time report to view information about currently active Engine tasks.

To access the Engine Tasks report, choose **Reports** > **Engine Tasks** from the Application Reporting menu bar.

The following fields are displayed on the Engine Tasks report.

Field	Description
ID	Unique identifier of the engine task. If the engine task is the main task running the application and the parent ID is empty, its identifier will match the Application Task Identifier.
Parent ID	Unique identifier for the parent of the engine task (if any). **Note** This field is not relevant to Cisco VVB. You can ignore the value.
Node ID	Unique identifier for a server in the cluster. **Note** As Cisco VVB does not support clustering, you can ignore the value.
Server IP Address	IP address identifying the server in the cluster.

Field	Description
Script	Name of the script that is running the task (if the task is running a Cisco VVB script).
Start Time	Time that the task started.
Duration	Length of time the task has been active.

Contacts Report

Use the Contacts real-time report to view information for all the active contacts for all servers.

To access the Contacts report, choose **Reports** > **Contacts** from the Application Reporting menu bar.

You can access detailed information about specific contacts listed on the Contacts web page by performing one of the following procedures:

- Call Contacts Detailed Info Report, on page 312

The following fields are displayed on the Contacts report.

Field	Description
ID	Unique identifier representing a contact.
Type	Type of contact:
Impl ID	Unique identifier provided by the particular type of contact.
Node ID	Unique identifier for a server in the cluster. **Note** As Cisco VVB does not support clustering, you can ignore the value.
Start Time	Time stamp when the contact was created.
Duration	Length of time that the contact is active.
Handled	If True, the contact is handled; if False, the contact is not handled.
Aborting	If True, the contact is aborted with a default treatment; if False, the contact is not aborted.
Application	Name of the application currently managing the contact.
Task	Unique identifier of the application task that is currently responsible for the contact.
Session	Unique identifier of the session currently managing the contact (if any).

Note The information displayed is dependent on the type of contact selected. Depending on the type of call, some fields may not be supported and will appear blank.

Call Contacts Detailed Info Report

Use the Call Contacts Detailed Info real-time report to view all information related to the call contact.

To access the Call Contacts Detailed Info report, right-click a specific call contact record on the Contacts report; information for that specific record displays.

The following fields are displayed on the Call Contacts Detailed Info report.

Field	Description
State	Current state of the contact.
Inbound	If True, this call was received by the Cisco VVB server; if False, this call was placed as an outbound call by an application.
Language	The selected language context of the call.
Application ID	Unique identifier of the associated application.
Called Number	Called number for this call leg from the perspective of the called party.
Dialed Number	Dialed number for this call leg from the perspective of the calling party.
Calling Number	Calling number of the originator of this call.
ANI	Automatic number identification.
DNIS	Dialed number identification service.
CLID	Caller ID.
Arrival Type	Information on how the call contact arrived in the system.
Last Redirected Number	Number from which the last call diversion or transfer was invoked.
Original Called Number	Originally called number.
Original Dialed Number	Originally dialed number.
ANI Digits	Automatic Number Identification information indicator digit codes.
CED	Entered digits that were gathered by the network before the call was received. **Note** Calls running Unified ICME applications are also reported here.

Applications Report

Use the Applications real-time report to view all the applications loaded on the server.

To access the Applications report, choose **Reports** > **Applications** from the Application Reporting menu bar.

The following fields are displayed on the Applications report.

Field	Description
Name	Unique name of the currently loaded application.
ID	Application ID.
Type	Type of application that is currently running (for example, a Cisco Script Application).

Field	Description
Description	Description of the application as entered on the Cisco VVBAdministration web site.
Enabled	If True, the application is enabled; if False, the application is disabled.
Max. Sessions	Maximum number of simultaneous task instances that can run simultaneously on the Cisco VVB server.
Valid	If True, the application is valid; if False, the application is invalid.[4]

[4] An application is valid if it was successfully loaded and initialized from its configuration. At any time, an application can become invalid if it internally fails to be refreshed.

Sessions Report

Use the Sessions real-time report to view real-time information on all the active sessions.

To access the Sessions report, choose **Reports** > **Sessions** from the Application Reporting menu bar.

The following fields are displayed on the Sessions report.

Field	Description
ID	Session ID. **Note** This identifier is guaranteed to remain unique for a period of 12 months.
Mapping ID	User- or system-defined identifier that maps to this session.
Node ID	Unique identifier for a server in the cluster. **Note** As Cisco VVB does not support clustering, you can ignore the value.
Parent	Sessions that were created as a result of consult calls propagated in the system.
Creation Time	Creation time of the session.
State	Current state of the session. **Note** When marked IDLE, the session is subject to being “garbage collected” by the system after a specified period of time. In addition, a session is IN_USE if it still has a contact associated or a child session.

Tools Menu

The Tools menu gives you access to the following Application Reporting tools:

- **Reset All Stats**—Choose this option to reset all statistics.
- **Open Printable Report**—Choose this option to get a printable report of all currently active contacts in the system.
- **Refresh Connections**—Choose this option to refresh connections with the Cisco VVB system.

Reset All Statistics

Use the Reset All Stats option to reset all statistics accumulated since the last time the statistics were reset. It will not reset active statistics, such as active contacts, tasks, and so on.

Procedure

Choose **Tools** > **Reset All Statistics** from the Application Reporting menu bar.

Open Printable Report

Use the option to get a printable report of all currently active contacts in the system.

To get a printable report:

Procedure

Choose a real-time report from the Report menu option and then **Tools** > **Open Printable Report** from the Application Reporting menu bar.

Refresh Connections

To refresh connections with the Cisco VVB system:

Procedure

Choose **Tools** > **Refresh Connections** from the Application Reporting menu bar.

The Cisco VVB system refreshes all connections.

Views Menu

The Views menu allows you to access more detailed information for the following reports:

The Views menu contains different options, depending on the report you have chosen. Possible options are:

- **Contacts by Application Task ID**—Choose this option to view contacts according to Application Task ID numbers.
- **Engine Tasks by Application Task ID**—Choose this option to view Engine tasks according to Application Task ID numbers.
- **Detailed Info**—Choose this option to view more detailed information on selected reports.
- **Application Tasks by Application Name**—Choose this option to view application tasks by application name.
- **Contacts by Session ID**—Choose this option to view contacts by session ID.

Application Tasks

You can obtain reports based on the application task ID associated with application tasks.

Contacts by Application Task ID

This report displays the same report as the Contact report with the exception that the Contacts by Application Task ID report has been filtered using only the contact currently being managed by the selected application task.

Engine Tasks by Application Task ID

This report displays the same report as the Engine Task reports except that the Engine Tasks by Application Task ID report has been filtered to display only the engine tasks that are associated with the application task.

Contacts

When you use the Views options with the Contacts report, the Views menu contains only the Detailed Info option.

The Detailed Info option provides various detailed information, depending on the type of contact selected. For example, if the contact is a call, the Calling Party number, the Called Number, and so on, are displayed for that particular call.

Applications

When you use the Views options with the Application reports, the Views menu contains only the Application Tasks by Application Name option.

The Application Task By Application Name report displays the same report as the Application Task report except that the Application Task By Application Name report is filtered using only the active application tasks associated with this application.

Sessions

You can obtain reports based on the session ID associated with a session.

Contacts by Session ID

This report displays the same report as the Contact report with the exception that the Contacts By Session ID report is filtered using only the contacts associated with the selected session.

Detailed Info

Detailed info displays the time the session was created and its current state.

Settings Menu

The Settings menu of the Application Reporting menu bar allows you to adjust various settings of the Real Time Reporting tool.

The Settings menu contains the following menu options:

- **Options**—Choose this option to set the polling (refresh) interval times and to set the amount of times the server will attempt to reconnect and to enable the reset statistics at midnight .
- **Window**—Choose this option to display reports in colors based on your Windows settings.

- **Motif**—Choose this option to display reports in purple and menu items in brown.
- **Metal**—Choose this option to display reports in grey and menu items in black.

Options Menu

Choose **Settings** and click **Options** to access the Options dialog box. Use the Options dialog box to set the polling (refresh) interval time, set the number of times the server will attempt to reconnect.

The following fields are displayed in the Options dialog box.

Field	Description
Polling Interval	Time between two requests to the server for new statistics by the client.
Server Connect Retry Count	The number of times that the Cisco VVBAdministration web interface should attempt to reconnect to the Cisco VVB server. **Note** If an error occurs, an Error dialog box opens to alert you that the server is not communicating with the web interface.
Reset Statistics at Midnight	The statistics data gets cleared at midnight if enabled. **Note** This option is disabled either when client is not connected to the server or report is not selected. To connect to the server, select an option from Report menu.

Click **Apply** to submit configuration changes.

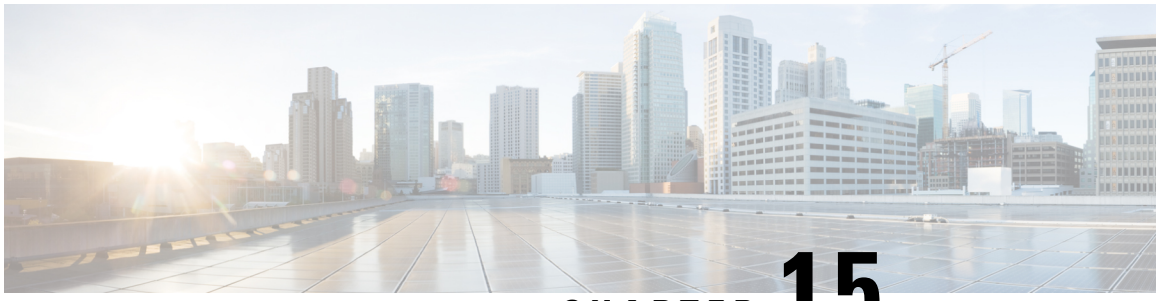
HTTP Proxy Setting for Dialogflow

For connecting with Google Dialogflow services, the Dialogflow SDK expects the proxy to be configured as tunnel mode to support the HTTP Connect method.

Procedure

Tunnel the Google request directly the Google Cloud. This ensures that the proxy transparently passes the client Hello to Google.

Note Without this configuration, the proxy needs to support h2/ALPN and HTTP2/0 protocols for GRPC, which most of the proxies do not support.



CHAPTER 15

SIP Proxy Server Configuration

Configure SIP Proxy Server

Procedure

Step 1 Log in to Operations Console and click **Device Management** > **SIP Proxy Server**.

Step 2 Click **Add New** to add a new SIP Proxy server or click **Use As Template** to use the existing SIP Proxy server from the list of available SIP Proxy servers.

Step 3 Click the following tabs and modify the default values of fields, if required:

a) **General**. See General Settings, on page 319.

b) **Device Pool**. See Add or Remove Device From Device Pool, on page 97. For information on Device Pool, see Device Pool, on page 97.

Step 4 Click **Save**.

Related Topics

General Settings, on page 319

Add or Remove Device From Device Pool, on page 97

Device Pool, on page 97

SIP Proxy Server Settings

General Settings

To configure the general settings of SIP Proxy server, on the **General** tab, enter or modify the field values, as listed in the following table:

Table 50: SIP Proxy Server General Tab Configuration Settings

Field	Description	Default	Range	Restart Required
General				
IP Address	The IP address of a SIP Proxy server.	None	Valid IP address	Not Applicable
Hostname	The host name of the SIP Proxy server.	None	Valid DNS name includes uppercase and lowercase letters, the numbers 0 through 9, and a dash.	Not Applicable
Device Type	The type of proxy server. **Note** Depending on the option selected, the **Enable Serviceability** fields change. See the **Enable Serviceability** options for details.	Cisco Unified SIP Proxy	Cisco Unified SIP Proxy and Cisco Unified Presence.	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. **Note** The user interface (UI) validates the URL for syntax errors. However, it cannot validate a URL for website existence.	Not Applicable
Enable Serviceability				
Enable Serviceability	Check this check box to enable serviceability for SIP Proxy server.	Not Applicable	Unchecked	Not Applicable

Field	Description	Default	Range	Restart Required
Username	The username required to log in to the proxy server Serviceability.	Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable	Not Applicable
Port	The port on which Serviceability is configured on the SIP Proxy.	1 to 65535	8443	Not Applicable
(For Device Type: Cisco Unified SIP Proxy)				
User Password	Enter a password. This is the first level of authentication for IOS.	Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.	Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable
Enable Password	The password required to log in to SIP Proxy Serviceability. This is the second level of authentication for IOS.	Must be same as password on the SIP Proxy.	Not Applicable	Not Applicable
(For Device Type: Cisco Unified SIP Presence)				
Password	Enter a password.	Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.	Valid names containing uppercase and lowercase alphanumeric characters, period, dash and underscore.	Not Applicable
Confirm Password	The password required to log in to SIP Proxy Serviceability.	Must be same as password on the SIP Proxy.	Not Applicable	Not Applicable

Add SIP Proxy Server to Device Pool

See Add or Remove Device From Device Pool, on page 97. For information on Device Pool, see Device Pool, on page 97.

Related Topics

Add or Remove Device From Device Pool, on page 97
Device Pool, on page 97

Configuration

If only a single SIP Proxy Server is needed for outbound call routing from the Call Server, choose the SIP Proxy configuration when configuring the SIP Service. In the Unified CVP Operations Console Server, configure the following:

- Add a SIP Proxy Server and specify the IP address of the server.

Under the Call Server SIP Service settings, configure the following:

- Enable Outbound Proxy = True
- Use DNS SRV type query = False
- Outbound Proxy Host = SIP Proxy Server configured above

When using multiple SIP Proxy Servers for outbound redundancy from the Call Server, configure the SIP Proxy with a DNS name and configure DNS SRV records in order to reach the SIP Proxy Servers. The DNS SRV records can exist on an external DNS Server, or they can be configured in a local DNS SRV record on each CVP server. In the OAMP Console, configure the following:

- Add a SIP Proxy Server and specify DNS name of the server.

Under SIP Service configuration, configure the following:

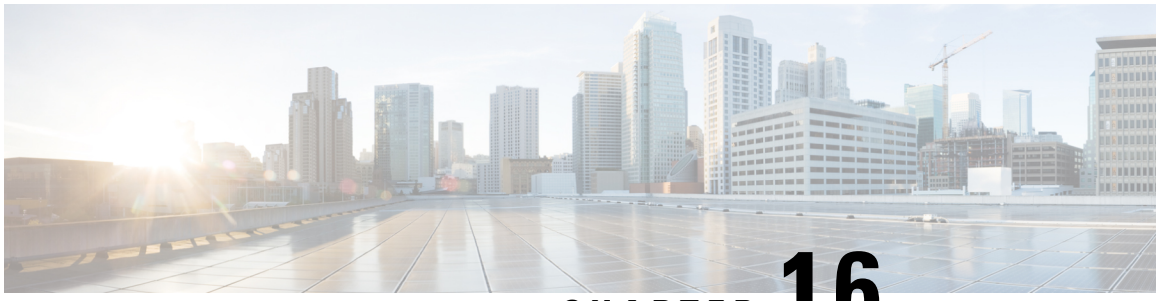
- Enable Outbound Proxy = True
- Use DNS SRV type query = True

  The DNS SRV record should then be configured with the list of SIP Proxy Servers.

To configure the Local DNS SRV record on each server, under the SIP service configuration, check **Resolve SRV records locally**.

To use a server group for redundant Proxy Servers:

1. Select **resolve SRV records locally** and enter the name of the server group for the outbound proxy domain name.
2. Under **System > Server Groups**, create a new server group with two proxy servers that have priority 1 and 2.
3. Deploy the server group configuration to the Call Server.



CHAPTER 16

Unified CM SME Configuration

Enable Session Refresh

Periodic session refresh helps to determine the downlink status and to trigger clear sessions from the gateway to release Unified CVP call server ports in case of Unified CM SME failures.

Perform the following steps to enable SIP session refresh globally.

Procedure

Step 1 Use putty or telnet to log in to the IOS gateway.

Step 2 From the command prompt, run the following command:

```
>enable
>configure terminal
>voice service voip
>sip
>session refresh
```

Enable Session Timer

To enable SIP session timer globally, set the `min-se` command in SIP configuration mode using the following steps.

Procedure

Step 1 Use putty or telnet to log in to the IOS gateway.

Step 2 From the command prompt, run the following command:

```
>enable
>configure terminal
>voice service voip
>sip
>min-se <seconds> session-expires <seconds>
```

Step 3 Check the min-se set value by typing the following command: `show sip-ua min-se`.

Configure Media Inactivity Timer in Cisco IOS Gateway

During Unified SME failure, the IOS(Cisco UBE or PSTN Gateway) does not receive a BYE message for any type of call flow. To avoid this scenario, you must use the following procedure to configure Media Inactivity Timer in the IOS Gateway.

Procedure

Step 1 Use Putty or Telnet to log in to the IOS gateway.

Step 2 From the command prompt, run the following command:

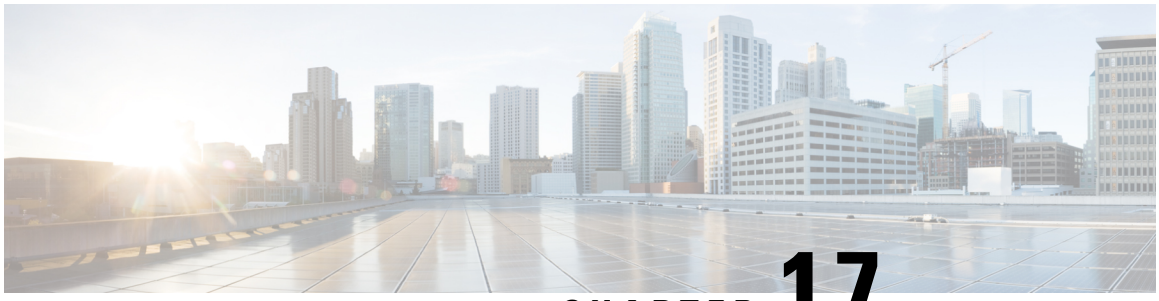
```
ip rtcp report interval <timer_value in msecs>
gateway
media-inactivity-criteria all
 timer receive-rtcp <timer_value in secs>
 timer receive-rtp <timer_value in secs>
```

Configure SIP Trunk from SME to Unified CM Leaf Cluster

For more information about configuring SIP trunk from SME to Unified CM Leaf Cluster, see *Cisco Collaboration System Solution Reference Network Designs (SRND)* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html.

Configure SIP Trunk from Unified CM Leaf Cluster to SME

For more information about configuring SIP trunk from Unified CM Leaf Cluster to SME, see *Cisco Collaboration System Solution Reference Network Designs (SRND)* available at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/design/guides/UCgoList.html.



CHAPTER 17

System Configuration

System Tab Options

Table 51: System Tab Options

System tab options	Use To
Control Center	View the status of the Cisco Unified Customer Voice Portal environment in a network control center. View the status and statistics by Device Type or Device Pools, logical groups of devices in the Cisco Unified Customer Voice Portal solution. Initiate Start, Shutdown, or Graceful Shutdown actions on devices in the control center.
Device Pool	Create, modify, and delete device pool names and descriptions for logical groups of devices (for example, all devices located in a geographical region). For details, see Device Pool, on page 97 and Add or Remove Device From Device Pool, on page 97.
Import System Configuration	Import a previously-saved Operations Console Server configuration file and apply it to the current system. For details, see Import System Configuration, on page 326.

System tab options	Use To
Export System Configuration	Save and export all configuration information for the Operations Console Server to a single file on your local computer. You can later use this file to restore an Operations Console Server during disaster recovery. For details on this option, see Export System Configuration, on page 327.
Location	Add, edit, synchronize, and delete Unified CM location information.
SIP Server Groups	Configure server groups for SIP and view Call Server deployment status. For details, see Location Configuration, on page 328.
Web Services	Configure Diagnostic Portal servlet credentials. For details, see Deploy Web Services, on page 343.
Dialed Number Pattern	Configure the Dialed Number Patterns for a destination. You can define the dialed numbers for the Error Tone, Ring Tone, and other destinations. For details, see Add and Deploy Dialed Number Pattern, on page 340.
IOS Configuration	**IOS Template Management** - Add, Delete, Edit, Copy, and View an IOS template configuration pushed to an IOS gateway. The template contains the IOS commands required for use in a Unified CVP deployment. **IOS Template Deployment** - Deploy a gateway configuration template to an IOS gateway. The template provisions the gateway and substitutes any variables in the template with the source devices that are chosen when it is deployed. For details, see IOS Configuration, on page 343.
Courtesy Callback	For details, see Configure Courtesy Callback, on page 353.

Related Topics

Add or Remove Device From Device Pool, on page 97
Device Pool, on page 97
Import System Configuration, on page 326
Export System Configuration, on page 327
Location Configuration, on page 328
Deploy Web Services, on page 343
Add and Deploy Dialed Number Pattern, on page 340
IOS Configuration, on page 343
Configure Courtesy Callback, on page 353

Import System Configuration

For disaster recovery, import the saved Operations Console configuration to your computer. To back up and restore Operations Console configuration, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*.

Note

- Operations Console supports the import of system-level configuration data.
- Operations Console cannot export the sip.properties file. To export the sip.properties file, manually copy the sip.properties file along with the CVP Operations Console configuration.
- When you import a database which was exported from an older version, the imported database is automatically upgraded to the latest version, as indicated in the confirmation message

Procedure

Step 1 Stop the **Cisco CVP WebServicesManager** Windows Service by performing the following steps:
a) Select **Start** > **All Programs** > **Control Panel Programs** > **Administrative Tools** > **Services**.

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

Step 3 Enter the file name in the **Enter Configuration File** text box or click **Browse to** to search for the file to import.

Step 4 Select **Import**.

Step 5 Perform Step 1(a).

Step 6 Perform the following steps:
a) Select **Cisco CVP OPSConsoleServer**, and click **Restart**.
b) Select **Cisco CVP WebServicesManager**, and click **Restart**.

Step 7 Log in to the Operations Console.

What to do next

If 12.5(1) or an earlier version of CVP configuration (exported) is imported on 12.6(x) Operations Console (OAMP), you need to run the command **mgr-init.bat -oamp** from the command prompt from CVP's bin folder:

1. Stop Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.
2. Go to the CVP bin folder.
3. Run the `mgr-init.bat -oamp` command from the command prompt.
4. Restart Cisco Unified CVP Operations Console and Cisco CVP WebServicesManager.

Export System Configuration

For back up, save and export the Operations Console configuration to a single file on your computer. This file can later be used to configure another Operations Console Server without having to individually reconfigure each module. For details, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*. You can export the database on a regular basis and also when you make major configuration changes to a device.

Note

- All Operations Console configuration data is exported, except for any files you have uploaded, includingapplication scripts. The Operations Console supports the export of system-level configuration data.
- Import and export operations do not back up or restore the CVP configuration of the VoiceBrowser or the SIP.properties files. If the backup and record of the Unified CVP configuration is required, manually back up the SIP.properties file and the result of the VoiceBrowser **sall** command along with the export of system configuration through the Operations Console.

Procedure

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

Step 2 On the **Export System Configuration** page, click **Export**.

Step 3 In the **Save As** dialog box, select a location to save the file.

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

Location Configuration

Configure a location to route calls locally to the agent available in the branch office instead of routing calls to centralized or non-geographical numbers. Use the location configuration feature to select a Unified Communication Manager (CM) Server and extract the Unified CM location information (location provider). After an administrator initiates the synchronization, the system retrieves the location information for all available Unified CM servers which have been identified as sources for location information.

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

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

The following table lists the location configuration settings:

Table 52: Location Configuration Settings

Property	Description	Default	Value	Restart Required
General				
Insert Site Identifier	Select one of the following options to identify the site information: • **Insert site identifier between the Network VRU label and the correlation ID** • **Insert site identifier at the beginning of the Network VRU label** • **Do not insert site identifier**	**Insert site identifier between the Network VRU label and the correlation ID**	Not applicable	No
Location				
Location Name (required)	This is a user defined field.	Not applicable	a-z, A-Z, 0-9, -_ Max length 128 characters	No
Site ID (required)	The Site ID is a unique user-defined field.	Null	0-9, # Max length 128 characters	No
Location ID (required)	The Location ID is a unique user-defined field.	Null	a-z, A-Z, 0-9 Max length 128 characters	No
Unified CM IP Address This field is not available for manually-configured locations.	Ensure to check the Enable Synchronization check box in the Unified CM Server Configuration screen's **General** tab to select Unified CM as a Unified CM location information provider. If a Unified CM server is removed from the Operations Console configuration, if the Unified CM server is unreachable, or if the synchronization check box is deselected, all locations stored in the Operations Console are automatically marked as invalid.	Not applicable	Not applicable	No

Property	Description	Default	Value	Restart Required
Associated Gateway	You can select Gateways from the Available list to deploy location information. You can configure multiple Gateways per location. An instance of a Gateway can only be assigned to one location. When a Gateway is associated with a location, the Gateway configuration window displays the location as a read-only field.	Not applicable	Not applicable	No

Property	Description	Default	Value	Restart Required

Status	The status indicates if the location information is valid or invalid:
	• **Invalid:** The location is invalid if any of the following scenarios apply:
	  • The location was previously synchronized with a Unified CM server. Later, you delete this location from the Unified CM server. When you perform the next synchronization with the Unified CM server, this location becomes invalid.
	  • The Unified CM server's Enable Synchronization check box remains unchecked. You can select and remove "Invalid" locations at any time. If a unified CM is deselected from the synchronization list after synchronizing with that Unified CM server, then all the locations synchronized from this Unified CM server become invalid.
	  • If a Unified CM server is not reachable when the next synchronization occurs, then all the locations associated with that Unified CM become invalid.
	• **Valid:** The location is valid if any of the following scenarios apply:
	  • the Enable Synchronization check box is checked
	  • the location is exists in a Unified CM server configuration, the last synchronization was successful with the Unified CM, and if that Unified CM is still selected.
		Not applicable	Valid or Invalid	No

Call Server Deployment				
Associate Call Servers	Select call servers from the Available list to deploy location information. One or more call servers can be selected and designated as Selected/Available.	Configuration is deployed to all selected call servers	Not applicable	No

Prerequisites for Location Configuration

- Configure the device type as a gateway.

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

- If the device location ID information is configured on the Location configuration page, ensure that it is displayed as a read-only field.
- Ensure that any configurable fields remain blank if they are not configured by a user.

Deploy Location Information

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

Procedure

Step 1 Select **System** > **Location** and make the enter or modify the location configuration field values.

Step 2 Click **Save & Deploy** to save the location information and initiate a deployment request to the selected Call Servers. Or, click **Save** to save the settings three components to the database: the location information, information in the General tab, and the associated Call Servers and deploy the location information later.

Caution The Deployment Status screen displays a warning message if you have:

- Saved only the configuration details and have not deployed them.
- Edited or deleted an existing configuration and have not deployed the changes.
- Changed the call server association.

Add Location

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

Procedure

Step 1 Log in to the Operations Console and select **System** > **Location**.

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

The Location Configuration window appears.

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

Step 4 (Optional) Select the required Gateway by moving it to the **Selected** column.

Step 5 Click **Save**.

SIP Server Group Configuration

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

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

Add SIP Server Groups

Procedure

Step 1 Log in to the Operations Console and select **System** > **SIP Server Groups**.

The SIP Server Groups window appears.

Step 2 Select **Add New**.

Step 3 Click the following tabs and enter or modify the default values of fields, if required:

a) **General**. See General Settings, on page 334.

b) **Heartbeat Properties**. See Heartbeat Properties Settings, on page 334.

c) **Call Server Deployment**. See Deploy Call Server, on page 338.

Step 4 (Optional) To remove an element from the group, select it and click **Remove**. To replace a selected element with a new element, edit the SIP Server Group Elements properties, select an existing element, and then click **Replace**

Step 5 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and configure the SIP Server group later.

Related Topics

General Settings, on page 334
Heartbeat Properties Settings, on page 334
Deploy Call Server, on page 338

General Settings

Table 53: SIP Server Group General Settings

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

Heartbeat Properties Settings

These properties enable Heartbeat communication between the SIP Server Group and the elements of the SIP Server Group. In case of element not responding to Heartbeat messages, the element is marked as unavailable; on receiving a successful response, it is marked as available again.

Table 54: SIP Server Group Heartbeat Properties Settings

Property	Description	Default	Value
Use Heartbeats to Endpoints	Select to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled. **Note** Endpoints that are not in a Server Group can not use the heartbeat mechanism.	Disabled (unchecked)	Enabled or Disabled **Note** Enable Heartbeat for high-availability and quick recovery of element in case of a failover.

Property	Description	Default	Value
Number of failed Heartbeats for unreachable status	The number of failed heartbeats before marking the destination as unreachable.	1	1 through 5
Heartbeat Timeout (ms)	The amount of time, in milliseconds, before timing out the heartbeat.	500 milliseconds	100 through 3000
Up Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is up.	5000 milliseconds	5000 through 3600000
Down Endpoint Heartbeat Interval (ms)	The ping interval for heart beating an endpoint (status) that is down.	5000 milliseconds	5000 through 3600000
Heartbeat Local Listen Port	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067	0 through 65000
Heartbeat SIP Method	The heartbeat SIP method. **Note** PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS **Note** If SIP Server Group has secure SIP port configured, OPTIONS messages are sent on non-secure 5060 port.	OPTIONS or PING

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

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

Server Group Heartbeat Settings

The Server Group heartbeat default setting tracks the ping interval between any two pings; it is not the interval between pings to the same endpoint. The Server Group does not ping at a specific interval and ping all elements because this approach would introduce a fluctuation on CPU usage. Also, it takes more resources when the system has to ping many endpoints. For example, to ping 3 elements across all groups at 30-second intervals, you have to set the ping interval at 10 seconds.

It is less deterministic for reactive mode because elements that are currently down can fluctuate, so the ping interval fluctuates with it.

Note

- **Heartbeat Behavior Settings for Server Groups.** To turn off pinging when the element is up, set the **Up Endpoint Heartbeat Interval** to zero (reactive pinging). To turn off pinging when the element is down, set the **Down Endpoint Heartbeat Interval** to zero (proactive pinging). To ping when the element is either up or down, set the heartbeat intervals to greater than zero (adaptive pinging).
- **Heartbeat Response Handling.** Any endpoint that CVP may route calls to should respond to OPTIONS with some response, either a 200 OK or some other response. Any response to a heartbeat indicates the other side is alive and reachable. A 200 OK is usually returned, but CUSP Server may return a 483 Too Many Hops response, because the max-forwards header is set to zero in an OPTIONS message. Sometimes the endpoints may not allow OPTIONS or PING, and may return 405 Method Not Allowed.

By default, Server Group heartbeats are monitored using a UDP socket connection. The transport type can be changed to TCP from the Operations Console Server Groups window.

Whenever an element has an unreachable or overloaded status, that element is marked as down completely, that is for both UDP and TCP transports. When the element is up again, transports are routed for both UDP and TCP.

Note

- TLS transport is not supported.
- If a heartbeat is coming from any proxy using TLS, it is supported and can be used over the same TCP port.

Duplicate Server Group Elements is not monitored because the primary element is already monitored.

Note See the *Configuration Guide for Cisco Unified Customer Voice Portal* for typical configurations for the Server Group feature, available at http://www.cisco.com/en/US/products/sw/custcosw/ps1006/products_installation_and_configuration_guides_list.html

Deploy Call Server

Procedure

Step 1 Log in to the Operations Console and select **System** > **SIP Server Groups**.

The SIP Server Groups Configuration window appears.

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

Step 3 From the **Associate Unified CVP Call Servers** screen, in the **Available** list box, select one or multiple Call Servers and click the **Add** arrow.

The added Call Servers appear in the **Selected** list box.

Note

- Add and deploy at least one Call Server before you configure a SIP Server group. A warning message is displayed if you try to add a SIP Server group without deploying a Call Server. For details on how to configure a Call Server, see Configure Call Server, on page 77.
- The Deployment Status screen displays a warning message In the following cases:
  - If you have only saved the SIP server details and have not deployed them.
  - If you have edited or deleted an existing configuration and have not deployed the changes.
  - If you changed the call server association.
- Only one deployment process can run at a time. If one process is already running, you cannot initiate another process and receive an error message.
- A message displays to indicate the successful start of deployment process. The Operations Console saves the Call Server configuration to the Operations Console database and returns to display the new configuration in the list page.

Step 4 Click **Save & Deploy**.

Note Click **Save** to save the changes on the Operations Console and deploy a Call Server for the SIP Server group later.

Related Topics

Configure Call Server, on page 77

Dialed Number Pattern Configuration

A dial plan essentially describes the number and pattern of digits that a user dials to reach a particular telephone number. Access codes, area codes, specialized codes, and combinations of the number of digits dialed are all part of a dial plan. For example, the North American Public Switched Telephone Network (PSTN) uses a 10-digit dial plan that includes a 3-digit area code and a 7-digit telephone number. Most PBXs support variable length dial plans that use 3 to 11 digits. Dial plans must comply with the telephone networks to which they connect. A Dialed Number (DN) pattern is dial plan configured on one or multiple Call Servers and provides details on the call flow of dialed digits.

Dial plans on Cisco routers are manually defined using dial peers. Dial peers are similar to static routes; they define where calls originate and terminate and what path the calls take through the network. Attributes within the dial peer determine which dialed digits the router collects and forwards to telephony devices. For more information on Dial plans, see https://www.cisco.com/en/US/docs/ios/12_2/voice/configuration/guide/vcf_bk.pdf.

Use the **System** menu to configure a DN pattern. Select the **Display Pattern Type** to display the configured SN patterns in a tree-hierarchy view. The Display Pattern Type list box includes the following options:

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

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

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

The column types are as follows:

Dialed Number Pattern - The actual dialed number pattern.

Description - The dialed number pattern description.

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

Add and Deploy Dialed Number Pattern

Procedure

Step 1 Log in to the Operations Console and select **System** > **Dialed Number Pattern**.

Step 2 Click **Add New**.

Step 3 Enter or modify the Dialed Number pattern configuration settings, as listed in the following table:

Table 55: Dialed Number Pattern Configuration Settings

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

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

Property	Description	Default	Value
Enable Post Call Survey for Incoming Calls	Enables post call survey for incoming calls. • **Survey Dialed Number Pattern -** Enter the survey dialed number pattern.	Disabled none	n/a Maximum length of 24 characters Can contain alphanumeric characters, wildcard characters such as exclamation point (!) or asterisk (*), single digit matches such as period (.) or X (not x), and can end with an optional greater than (>) wildcard character.

Step 4 Click **Save**.

The **Dialed Number Pattern** page appears.

Step 5 To deploy the Dialed Number Pattern configuration to all the Call Servers, click **Deploy**.

Note Click **Deployment Status** to view the status of DN pattern deployment.

Web Services Configuration

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

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

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

- **Web Services User Management:** The Operation Console administrator can configure new Web Services users (users with the Web Services user role type). The Operations Console administrator can also manually push any configured Web Services users using the procedure identified in Deploy Web Services, on page 343.

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

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

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

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

Related Topics

Deploy Call Server, on page 338

Deploy Web Services

Before you begin

Install Remote Operations on the third-party device.

Procedure

Step 1 Log in to the Operations Console and select **System** > **Web Services**.

Step 2 Click the **Remote Operations Deployment** tab and perform the following steps:

a) Enter the IP Address and Hostname.
b) (Optional) Enter the description of the third-party device.
c) Click **Add** to add the device to the list of devices associated with the Unified CVP deployment Web services.

Step 3 Click **Save & Deploy** to save and deploy the configuration to the impacted devices in the Operations Console database.

IOS Configuration

Configure IOS gateways using templates through Operations Console. Templates are text files that contain the IOS commands required for use in a Unified CVP deployment. You can edit the templates locally and then upload it to the Operation Console. You can deploy the configuration defined in the template to a gateway right from the Operations Console. You can also rollback the configuration on the gateway to the point immediately before the template was deployed.

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

IOS Configuration consists of:

- Template Management. See IOS Template Management, on page 346
- Template Deployment. See IOS Template Deployment, on page 348.

You can use the default templates or create custom templates.

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

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

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

Related Topics

IOS Template Management, on page 346
IOS Template Deployment, on page 348

IOS Template Format

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

- The first line of the template must be a comment that exactly matches the following format:

  ! Customer Voice Portal 9.0(1) IOS Template

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

  conf t

With the exception of variables, all of the commands use standard IOS syntax. The variables that can be used are listed in the following table:

Table 56: IOS Template Format

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

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

IOS Template Management

Manage IOS templates by adding, deleting, editing, copying, and viewing details about templates.

Add New Template

Procedure

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

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

The IOS Template Configuration page opens.

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

Note The file you select to upload must be of a valid file format or the upload fails. See the IOS Template Format, on page 344 section for details on the format required and the variables that you can use in your template.

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

Delete Template

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

Procedure

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

The IOS Template Management page opens.

Step 2 Select the check boxes next to the templates you want to delete.

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

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

Edit Templates

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

Procedure

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

The IOS Template Management window opens.

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

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

The IOS Template Configuration page appears.

Step 4 (Optional) Edit the description field.

Step 5 If this is a custom template, then you can check the **Enable template modification** check box to allow for editing of the template body. See IOS Template Format, on page 344 for details about template syntax. You can cancel any unsaved changes you made to the body by clicking **Undo Template Body Changes**.

Step 6 Click **Save**.

Related Topics

IOS Template Format, on page 344

Copy Templates

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

Procedure

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

The IOS Template Management window opens.

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

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

Step 4 Edit the name and description for the copy.

Step 5 (Optional) Check the **Enable template modification** check box and make changes to the copy. You can also make changes later. See Edit Templates, on page 347.

Step 6 Select **Save**.

Related Topics

Edit Templates, on page 347

IOS Template Deployment

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

From this page, you can:

- Preview the body of the template (and validate the template) and deploy to a gateway.
- Check the status of the template deployment.
- Rollback the configuration sent to a gateway to its previous state.

Related Topics

IOS Template Format, on page 344

Preview and Deploy Template

To preview (validate) and deploy a template:

Procedure

Step 1 Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

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

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

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

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

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

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

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

Check Deployment Status

To check the status of a template deployment:

Procedure

Step 1 Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

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

The IOS Template Deployment - Deployment Status window opens.

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

Roll Back Deployment

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

Procedure

Step 1 Log in to the Operations Console and select **System** > **IOS Configuration** > **IOS Template Deployment**.

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

The IOS Template Deployment - Deployment Status window opens.

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

- A confirmation dialog opens. Read the warning message and click **OK** to continue the rollback.
- A status message is displayed stating that the rollback is in progress. Refresh the status page by clicking **Refresh** to see the status of the rollback.

IOS Gateway Configuration

With CiscoIOS Gateways, dial peers are used to match phone numbers, and the destination can be a SIP Proxy Server, DNS SRV, or IP address. The following example shows a CiscoIOS Gateway configuration to send calls to a SIP Proxy Server using the SIP Proxy's IP address.

```
sip-ua
 sip-server ipv4:10.4.1.100:5060

dial-peer voice 1000 voip
 session target sip-server
 ...
```

The **sip-server** command on the dial peer tells the CiscoIOS Gateway to use the globally defined SIP Server that is configured under the **sip-ua** settings. In order to configure multiple SIP Proxies for redundancy, you can change the IP address to a DNS SRV record, as shown in the following example. The DNS SRV record allows a single DNS name to be mapped to multiple Reporting Servers.

```
sip-ua
 sip-server dns:cvp.cisco.com

dial-peer voice 1000 voip
 session target sip-server
 ...
```

Alternatively, you can configure multiple dial peers to point directly at multiple SIP Proxy Servers, as shown in the following example. This configuration allows you to specify IP addresses instead of relying on DNS.

```
dial-peer voice 1000 voip
 session target ipv4:10.4.1.100
 preference 1
 ...
dial-peer voice 1000 voip
 session target ipv4:10.4.1.101
 preference 1
 ...
```

In the preceding examples, the calls are sent to the SIP Proxy Server for dial plan resolution and call routing. If there are multiple Unified CVP Call Servers, the SIP Proxy Server would be configured with multiple routes for load balancing and redundancy. It is possible for CiscoIOS Gateways to provide load balancing and redundancy without a SIP Proxy Server. The following example shows a CiscoIOS Gateway configuration with multiple dial peers so that the calls are load balanced across three Unified CVP Call Servers.

```
dial-peer voice 1001 voip
 session target ipv4:10.4.33.131
 preference 1
 ...
dial-peer voice 1002 voip
 session target ipv4:10.4.33.132
 preference 1
 ...
dial-peer voice 1003 voip
 session target ipv4:10.4.33.133
 preference 1
 ...
```

DNS SRV records allow an administrator to configure redundancy and load balancing with finer granularity than with DNS round-robin redundancy and load balancing. A DNS SRV record allows you to define which hosts should be used for a particular service (the service in this case is SIP), and it allows you to define the load balancing characteristics among those hosts. In the following example, the redundancy provided by the three dial peers configured above is replaced with a single dial peer using a DNS SRV record. Note that a DNS server is required in order to do the DNS lookups.

```
ip name-server 10.4.33.200
 dial-peer voice 1000 voip
 session target dns:cvp.cisco.com
```

With CiscoIOS Gateways, it is possible to define DNS SRV records statically, similar to static host records. This capability allows you to simplify the dial peer configuration while also providing DNS SRV load balancing and redundancy. The disadvantage of this method is that if the SRV record needs to be changed, it must be changed on each gateway instead of on a centralized DNS Server. The following example shows the configuration of static SRV records for SIP services handled by cvp.cisco.com, and the SIP SRV records for cvp.cisco.com are configured to load balance across three servers:

```
ip host cvp4cc2.cisco.com 10.4.33.132
ip host cvp4cc3.cisco.com 10.4.33.133
ip host cvp4cc1.cisco.com 10.4.33.131
```

(SRV records for SIP/TCP)

```
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
ip host _sip._tcp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

(SRV records for SIP/UDP)

```
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc3.cisco.com
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc2.cisco.com
ip host _sip._udp.cvp.cisco.com srv 1 50 5060 cvp4cc1.cisco.com
```

Courtesy Callback

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

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

Use this page to identify the required Unified CVP Reporting Server for which Courtesy Callback data is stored and deploy them to the selected Unified CVP Call Servers. The configured values for Courtesy Callback are stored as cached attributes.

Configure the Courtesy Callback feature on the following servers/gateways:

- Ingress Gateway (IOS configuration)
- VXML Gateway (IOS configuration)
- Reporting Server (through the Unified CVP Operations Console)
- Media Server (upload of Courtesy Callback media files)
- Unified CVP VXML Server (upload of Call Studio Scripts)
- Unified ICM (through the ICM script)

Note Ensure that the registry is modified to use the CVP keystore. CCB uses CVP keystore instead of Java keystore in 12.0(1) and higher releases.

Callback Criteria

In your callback script, you can establish criteria for offering a caller a courtesy callback. Examples of callback criteria include:

- Number of minutes a customer is expected to wait in queue that exceeds a maximum number of minutes (based on your average call handling time per customer)

Note The included example scripts use this method for determining callback eligibility.

- Assigned status of a customer (for example, a callback can be given on the basis of status of a customer).
- The service a customer has requested (sales calls, or system upgrades, for example, may be established as callback criteria).

Note

- CCB does not support the use of SRTP.
- ANI provides a caller extension/number which is required for CCB. If ANI is null or anonymous, CCB cannot be offered to the callers.

Modifiable Example Scripts and Sample Audio Files

The courtesy callback feature is implemented using Unified CCE scripts. Modifiable example scripts are provided. These scripts determine whether or not to offer the caller a callback, depending on the callback criteria. Sample audio files are also provided.

The example scripts and audio files are located on the CVP installation media in the `\CVP\Downloads and Samples\` folder.

Following files are provided:

- `CourtesyCallback.ICMS`, the ICM script, in the `ICMDownloads` subfolder.
- `CourtesyCallbackStudioScripts.zip`, a collection of Call Studio scripts, in the `helloStudio` Samples subfolder.

  Following example scripts are provided:

  - BillingQueue: Plays queue music to callers. Can be customized.
  - Callback Engine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and hangs up) and when the caller actually receives the callback. Cannot be customized or modified.
  - CallbackEntry: Initial IVR when caller enters the system and is presented with opportunity for a callback. Can be customized.
  - **CallbackQueue:** Handles the keepalive mechanism for the call when callers are in queue and listening to the music played by BillingQueue. Do **not** modify this script.
  - CallbackWait: Handles IVR portion of call when caller is called back. Can be customized.

- `CCBAudioFiles.zip`, in the `CCBDownloads` subfolder, contains sample audio files that accompany the sample studio scripts.

Courtesy Callback Configuration

Configure Courtesy Callback

Procedure

Step 1 Log in to the Operations Console and select **System** > **Courtesy Callback**.

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

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

Step 3 (Optional) Check the **Enable secure communication with the Courtesy Callback database** check box to secure the communication between the Call Server and Reporting Server used for Courtesy Callback.

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

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

Table 57: Configuration Options for Dialed Number Configuration

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

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

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

Step 6 Click **Save & Deploy**.

Note Click **Save** to save the configuration to the Operations Console database and configure Courtesy Callback later.

Configure Ingress Gateway for Courtesy Callback

The ingress gateway where the call arrives is the gateway that processes the pre-emptive callback for the call, if the caller elects to receive a callback.

Note A sip-profile configuration is needed on ISR for the courtesy callback feature, only when deploying an IOS-XE version affected by CSCts00930. For more information on the defect, access the Bug Search Tool at https://sso.cisco.com/autho/forms/CDClogin.html.

For more information about sip-profile configuration, see *Design Guide for Cisco Unified Customer Voice Portal*, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-implementation-design-guides-list.html.

Procedure

Step 1 Login to the CVP OAMP Operations Console (from the CVP OAMP VM), using this syntax:
`https://<server_ip>:9443/oamp`.

Step 2 Copy survivability.tcl from the Operations Console to the flash memory of the gateway. Using the Operations Console, perform the following:

a) Select: **Bulk Administration** > **File Transfer** > **Scripts and Media**.
b) In Device Association, for **Select Device Type** select: **Gateway**.
c) Select all the Ingress gateways.
d) From the default gateway files, highlight: **survivability.tcl**.
e) Click **Transfer**.

Step 3 Log into the ingress gateway.

Step 4 Configure Call Survivability. See Call Survivability, on page 442 for details.

Step 5 To add services to the gateway, ensure that the enabled-config application mode is turned on. Type these commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 6 Add the following to the survivability service:

```
param ccb id:<host name or ip of this gateway>;loc:<location name>;trunks:<number of callback trunks>
```

Where the definitions of the preceding fields are:

- *id*: A unique identifier for this gateway and is logged to the database to show which gateway processed the original callback request.
- *loc*: An arbitrary location name specifying the location of this gateway.
- *trunks*: The number of DS0's reserved for callbacks on this gateway. Limit the number of T1/E1 trunks to enable the system to limit the resources allowed for callbacks.

The Courtesy Callback(CCB) *trunks* param configuration on the ingress gateway should be calculated based on CCB call parameters by including the *average CCB call duration* and the *fixed throttling period,* to ensure effective utilization of trunks between CCB and non-CCB calls.

The trunk value is given by the equation: Number of DS0 channels * (Throttling period/Average call duration)

Example

To dedicate a maximum of 10 DS0 channels for CCB calls, if you consider the following:

- The concurrent CCB calls at any given point is 10.
- The average CCB call duration is 900 seconds which includes the callback registration, callback offered, and talk time of called back user.
- The fixed throttling period is 1800 seconds.

Then, the trunk value will be 10 * (1800/900) = 20

The following example shows a basic configuration:

```
service cvp-survivability flash:survivability.tcl
param ccb id:10.86.132.177;loc:doclab;trunks:1
!
```

If you are updating the survivability service, or if this is the first time you created the survivability service, remember to load the application using the command:

```
call application voice load cvp-survivability
```

Step 7 Create the incoming dial peer, or verify that the survivability service is being used on your incoming dial peer. For example:

```
dial-peer voice 978555 pots
service cvp-survivability
incoming called-number 9785551234
direct-inward-dial
!
```

Note: We support both POTS and VoIP dial peers that point to a service provider.

Step 8 Create outgoing dial peers for the callbacks. These are the dial peers that place the actual call back out to the PSTN. For example:

```
dial-peer voice 978554 pots
destination-pattern 978554....
no digit-strip
port 0/0/1:23
!
```

Step 9 Use the following configuration to ensure that SIP is set up to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Note The default value for the estimated wait time (EWT) for Courtesy Callback is 90 minutes (5400 seconds). This can be configured up to four hours (14400 seconds). This is applicable for both static route and dynamic route configurations. For more information, see Configure Courtesy Callback up to Four Hours, on page 369.

Related Topics

Call Survivability, on page 442

Configure VXML Gateway for Courtesy Callback

Procedure

Step 1 Copy **cvp_ccb_vxml.tcl** from the Operations Console to the flash memory of the gateway. Using the Operations Console:

a) Select **Bulk Administration** > **File Transfer** > **Scripts and Media**.
b) On the **General** tab, select a device association by selecting **Gateway** from the **Select Device Type**drop-down box.**Gateway**.
c) From the default gateway files, highlight **cvp_ccb_vxml.tcl**.
d) Click **Transfer**.

Step 2 To add services to the gateway, ensure that the enabled-config application mode is turned on. Type the following commands at the gateway console:

```
GW81#en
GW81#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
GW81(config)#application
GW81(config-app)#
```

Step 3 Add the cvp_cc service to the configuration:

```
service cvp_cc flash:cvp_ccb_vxml.tcl
```

The service does not require any parameters.

Load the application with the command:

```
call application voice load cvp_cc
```

Note The media-activity detection feature should be turned off in the VXML Gateway to successfully callback the caller. With media-activity enabled on the VXML Gateway, the `cvp_cc` service disconnects the waiting callback calls after 'ip rtcp report interval' * 1000 milliseconds interval. This configuration becomes important in a co-located Ingress/VXML setup where media inactivity timers are always enabled. In such scenarios, the 'ip rtcp report interval' has to be increased to support the maximum allowable waiting for a callback call as defined by the solution requirements.

Step 4 On the VoIP dial-peer that defines the VRU leg from Unified ICM, verify that the codec can be used for recording. The following example shows that g711ulaw can be used for recording in Courtesy Callback:

```
dial-peer voice 123 voip
service bootstrap
incoming called-number 123T
dtmf-relay rtp-nte
codec g711ulaw
no vad
!
```

In other words, this example shows the g711ulaw codec set on the 123 voip dial-peer. Note that the codec must be specified explicitly. A codec class cannot be used because recording will not work.

Step 5 Use the following configuration to ensure that SIP is setup to forward SIP INFO messaging:

```
voice service voip
signaling forward unconditional
```

Step 6 VXML 2.0 is required to play the beep to prompt the caller to record their name in the BillingQueue example script. Add the following text to the configuration so the VXML Server uses VXML 2.0:

```
vxml version 2.0
```

Note Whenever vxml version 2.0 is enabled on the gateway,vxml audioerror is off by default. When an audio file cannot be played, error.badfetch will not generate an audio error event. To have the gateway generate an error.badfetch event when a file cannot be played, enable vxml audioerror in your gateway configuration. The following example uses config terminal mode to add both commands:

```
config t
vxml version 2.0
vxml audioerror
exit
```

Configure Reporting Server for Courtesy Callback

Before you begin

Install and configure a Reporting Server.

Note To install Reporting Server, see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*. To configure Reporting Server, see Reporting Server Configuration chapter.

Note The *RPT.DynamicEwtCalculationEnabled* variable is configured in the Unified CVP Reporting Server properties at `c:\cisco\cvp\conf`. This variable decides whether the dynamic calculation for estimated waiting time (EWT) is enabled or not. The variable is set to *false* by default. You may change the configuration, if needed:

- *RPT.DynamicEwtCalculationEnabled = true* – Unified ICM decides the EWT based on the average call handling time and the number of agents available. Unified CVP recalculates the EWT based on the dynamics of the contact center's incoming call rate and leaving rate.
- *RPT.DynamicEwtCalculationEnabled = false* – Unified ICM provides a static EWT, for example 15 minutes, and the Unified CVP uses this static EWT for calling back the caller. Unified CVP doesn't use the agent availability to alter the EWT.

Procedure

Step 1 On the Operations Console page, select **System** > **Courtesy Callback**.

On the **General** tab, you can:

- Select the Reporting Server for Courtesy Callback.
- Enable secure communication with the Courtesy Callback database.
- Configure allowed and disallowed dialed numbers.

Step 2 On the Courtesy Callback Configuration page, select the **Unified CVP Reporting Server** drop-down list, and select the Reporting Server to use for storing Courtesy Callback data.

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

Step 3 (Optional) Enable secure communication with the callback reporting database. Check the **Enable secure communication with the Courtesy Callback database** check box.

Step 4 Configure allowed and denied dialed numbers. These are the numbers that the system *should* and *should not* call when it is making a courtesy callback to a caller. Also, configure the Maximum Number of Calls Per Calling Number.

Use the following table to configure these fields:

Initially, there are **no** allowed dialed numbers for the Courtesy Callback feature. which means:

- **Allow Unmatched Dialed Numbers** is deselected.
- And, the **Allowed Dialed Numbers window** is empty.

This initial configuration is intentional; you must specifically enable the dialed numbers allowed for your deployment.

If you wish to allow **all** dialed numbers *except* those that are specifically listed in the Denied Dialed Numbers box, check **Allow Unmatched Dialed Numbers** .

Otherwise, add specific allowed number to the Allowed Dialed Numbers box. Refer to the Operations Console online help for detailson how to add specific allowed numbers, and for allowed valid dialed number shortcut patterns.

Note The Denied Dialed Numbers window is prepopulated if your local language is "en-us" (United States, English). Be sure to add any additional numbers you want to deny.

- Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character.
- Any of the wildcard characters in the set ">*!T" will match multiple characters but can only be used for trailing values because they will always match all remaining characters in the string.
- The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match.
- When the number of characters are matched equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.

Step 5 Adjust the “Maximum Number of Calls per Calling Number” to the desired number. By default, this is set to 0 and no limit is imposed.

This setting allows you to limit the number of calls, from the same calling number, that are eligible to receive a callback. If this field is set to a positive number (X), then the courtesy callback “Validate” element only allows X callbacks per calling number to go through the “preemptive” exit state at any time. If there are already X callbacks offered for a calling number, new calls go through the “none” exit state of the “Validate” element. In addition, if no calling number is available for a call, the call always goes through the “none” exit state of the “Validate” element."

Step 6 Click the **Call Server Deployment** tab and move the Call Server you want to use for courtesy callbacks from the **Available** box to the **Selected** box, as shown in the following screen shot :

Step 7 Click **Save & Deploy** to deploy the new Reporting Server configuration immediately.

If you click **Save**, the configuration is saved and is deployed after the Reporting Server restarts.

Note If you are updating the courtesy callback configuration (for example, changing to a different Reporting Server), perform deployment during a scheduled maintenance period. Otherwise, restarting the Reporting Server could cause the cancellation of currently scheduled courtesy callbacks.

Configure Media Server for Courtesy Callback

Several Courtesy-Callback-specific media files are included with the sample scripts for Courtesy Callback. During the Operations Console installation , the media files are placed in the following directory:

`%CVP_HOME%\OPSConsoleServer\CCBDownloads\CCBAudioFiles.zip`

After CVP installation, the media files are located on the Operations Console in *%CVP_Home%*\OPSConsoleServer\. A typical value for *%CVP_Home%* is C:\Cisco\CVP.

CCBAudioFiles.zip has callback-specific application media files in `C:\inetpub\wwwroot\en-us\app` and the media files for *Say it Smart* in `C:\inetpub\wwwroot\en-us\sys`.

Unzip the special audio files copy to a Media Server.

Note If you selected the Media File installation option, during the Unified CVP installation, the audio files are unzipped and copied to `C:\inetpub\wwwroot\en-us\app` on the installation server.

Note CCBAudioFiles.zip also contains media files for Say It Smart. During installation, these files are copied to `C:\inetpub\wwwroot\en-us\sys`. Copy these files to your media server, if you do not have them there already.

Note The sample scripts are set up to use the default location of `http://<server>:<port>/en-us/app` for the audio files. Later in this configuration process, change the <server> and <port> parameters in the default location of the audio files in the example scripts to be your media server IP address and port number.

Configure Call Studio Scripts for Courtesy Callback

The Courtesy Callback feature is controlled by a combination of Call Studio scripts and ICM scripts. See the *Configuration Guide for Cisco Unified Customer Voice Portal* for details of the script logic.

Note This example follows the BillingQueue example application.

Procedure

Step 1 Extract the example Call Studio Courtesy Callback scripts contained in CourtesyCallbackStudioScripts.zip to a folder on the computer that has Call Studio installed.

You can access the .zip file from the following two locations:

- From the Unified CVP install media in \CVP\Downloads and Samples\Studio Samples\CourtesyCallbackStudioScripts.
- From the Operations Console server in %CVP_HOME%\OPSConsoleServer\StudioDownloads.

Step 2 Each folder contains a Call Studio project having the same name as the folder. The five individual projects comprise the Courtesy Callback feature.

Do not modify the following scripts.

- CallbackEngine: Keeps the VoIP leg of the call alive when the caller elects to receive the callback (and hangs up) and when the caller actually receives the callback.
- CallbackQueue: Handles the keepalive mechanism for the call when callers are in queue and listening to the music played by BillingQueue.

Modify the following scripts to suit your business needs:

- BillingQueue: Determines the queue music played to callers.
- CallbackEntry: Modify the initial IVR treatment a caller receives when entering the system and is presented with an opportunity for a callback.
- CallbackWait: Modify the IVR treatment a caller receives when they respond to the callback.

Note Do not change the CCB application names.

Step 3 Start Call Studio by selecting **Start** > **Programs** > **Cisco** > **Cisco Unified Call Studio**.

Step 4 In Call Studio, select **File** > **Import**.

Step 5 In the **Import** dialog box, expand the Call Studio folder and select **Existing Call Studio Project Into Workspace** .

Step 6 Click **Next**.

Step 7 In the **Import Call Studio Project From File System** dialog, browse to the location where you extracted the call studio projects. For each of the folders that are unzipped, select the folder (for example BillingQueue), and click **Finish**.

The project is imported into Call Studio. Repeat this action for each of the five folders.

When you have imported the five folders, you should see five projects in the **Navigator** window in the upper left corner.

Step 8 Update the Default Audio Path URI field in Call Studio to contain the IP address and port value for your Media Server.

For each of the Call Studio projects previously unzipped, complete the following steps:

a) Select the project in the Navigator window of Call Studio.
b) Click **Project** > **Properties** > **Call Studio** > **Audio Settings**.
c) On the Audio Settings window, modify the Default Audio Path URI field by supplying your server IP address and port number for the <*Server*> and <*Port*> placeholders.
d) Click **Apply**, and then click **OK**.

Step 9 (Optional) Billing Queue Project: Change the music played to the caller while on hold.

You can also create multiple instances of this project if you want to have different hold music for different clients, for example, BillingQueue with music for people waiting for billing, and SalesQueue with music for people waiting for sales. You also need to point to the proper version (BillingQueue or SalesQueue) in the ICM script. In the ICM script, the parameter queueapp=BillingQueue would also have a counterpart, queueapp=SalesQueue.

The CallbackEntry Project (in the following step) contains a node called SetQueueDefaults. This node contains the value Keepalive Interval which must be greater than the length of the queue music you use.

Step 10 Callback Entry Project: If desired, in the CallbackEntry project, modify the caller interaction settings in the SetQueueDefaults node.

This step defines values for the default queue. You can insert multiple SetQueueDefaults elements here for each queue name, if it is necessary to customize configuration values for a particular queue. If you do not have a SetQueueDefaults element for a given queue, the configuration values in the default queue are used.

Note You can define a Callback_Set_Queue_Defaults node with **Queue Name** parameter set to default. Configuration defined in this default node will be picked whenever a queue type is encountered for which there are no explicitly defined values.

a) In the Call Studio Navigator panel, open the CallBackEntry project and double click **app.callflow** to show the application elements in the script window.
b) Open the Start of Call page of the script using the tab at the bottom of the script display window.
c) Select the SetQueueDefaults node.
d) In the **Element Configuration panel**, select the Setting tab and modify the following default settings as desired:

   For the SetQueueDefaults element, the caller interaction values in the Start of Call and the Wants Callback elements, may be edited. For more information on the caller interaction values, see the Settings table in Chapter 10, Callback_Set_Queue_Defaults, in the *Element Specifications for Cisco Unified CVP VXML Server and Cisco Unified Call Studio* guide.

Step 11 Perform the following steps.

a. Set the path for the storage of recorded caller names.

b. Select app.callflow.

c. In the CallbackEntry project, on the Wants Callback page, highlight the Record Name node and click the **Settings** tab in the Element Configuration window of Call Studio.

d. In the Path setting, change the path to the location where you want to store the recorded names of the callers.

By default, Call Studio saves the path string in your VXML Server audio folder. If you are using the default path, you can create a new folder called Recordings in the `%CVP_HOME%\VXMLServer\Tomcat\webapps\CVP\audio\` folder on the VXML Server. If you are using IIS as your Media Server, create a new folder called Recordings in `C:\Inetpub\wwwroot\en-us\app` and set that as the path for recordings.

Step 12 Set the name of the Record name file.

From the CallbackEntry project on the Wants Callback page, highlight the **Add Callback to DB** node and select the **Settings** tab in the Element Configuration window of Call Studio.

Change the **Recorded name file** setting to match the location of the recording folder you created.

This setting references the URL of the recordings folder, whereas the Path setting references the file system path.

The AddCallback element setting in the CallbackEntry project is configured to do automatic recorded file deletions. If automatic recorded file deletion is not desired, then remove the value of the Recorded name path setting in the AddCallback element. This removal action assumes that you will be doing the deletion or management of the recorded file yourself.

Step 13 In the CallbackEntry project on the Callback_Set_Queue_Defaults node, be sure the keepalive value (in seconds) is greater than the length of the queue music being played. The default is 120 seconds.

Step 14 Save the **CallbackEntry** project.

Step 15 CallbackWait Project: Modifying values in the CallbackWait application.

In this application, you can change the IVR interaction that the caller receives at the time of the actual callback. The caller interaction elements in **CallbackWait** > **AskIfCallerReady (page)** may be modified. Save the project after you modify it. The WaitLoop retry count can also be modified from the default of six retries in the Check Retry element. This will allow a larger window of time to pass before the call is dropped from the application. It is used in a failure scenario when the CallbackServlet on the reporting server cannot be reached.

For instance, in a reboot or a service restart, this allows more time for the reporting server to reload the entry from the database when it is initializing. If the reporting server is not online within the retry window, then the entry will not be called back.

Step 16 Validate each of the five projects associated with the Courtesy Callback feature by right-clicking each Courtesy Callback project in the Navigator window and selecting **Validate**.

Step 17 Validate each of the five projects associated with the Courtesy Callback feature and deploy them to your VXML Server.

a) Right-click each Courtesy Callback project in the Navigator window and select **Validate**.
b) Right click each of the projects and click **Deploy**, then click **Finish**.

Step 18 Using windows explorer, navigate to `%CVP_HOME%\VXMLServer\applications`.

Step 19 For each of the five Courtesy Callback applications, open the project's admin folder in `%CVP_Home%\VXMLServer\applications`, and double-click **deployApp.bat** to deploy the application to the VXML Server.

Step 20 Verify that all the applications are running by going into `%CVP_HOME%\VXMLServer\admin` and double-clicking **status.bat**. All five applications should be listed under Application Name, and the status for each one should be Running.

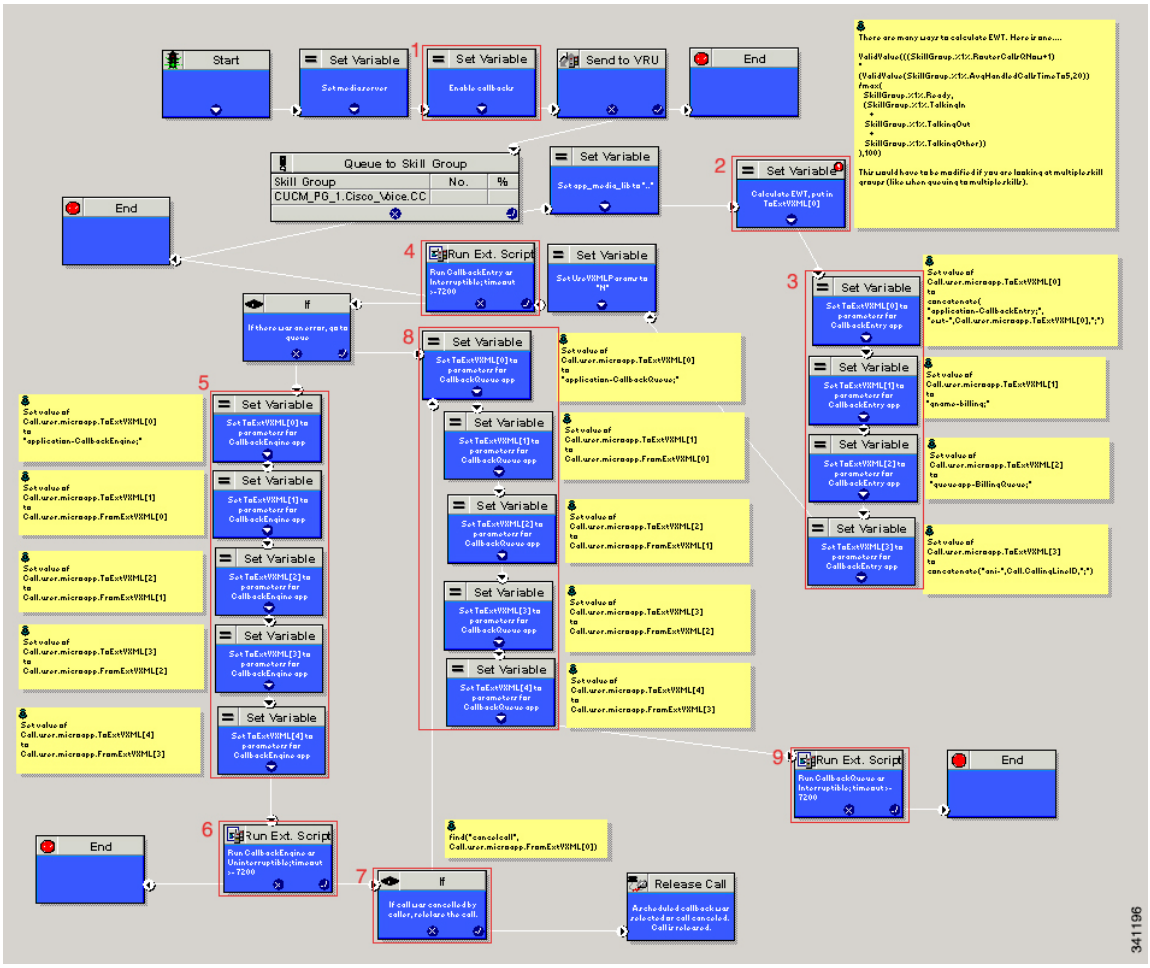
Note As an alternative to following steps 16-19 above, to deploy a VXML application to the VXML Server, you can also use the Bulk Administration VXML Applications feature. This way, you can deploy all the applications into a single archive, and then deploy them from OAMP in one click. This process is simpler and saves time. Bulk Administration deploys the application to the VXML Server, runs update-all-apps batch file, and then runs deploy-all-new-apps batch file.

CCE Script for Courtesy Callback

This section describes of the scripts used for the courtesy callback feature. There are nine numbered blocks or sets of blocks as identified below.

Note In the following example, the yellow comment blocks describe the value being set and the location where the value is being sent.

Figure 16: Setting Value for Courtesy Callback



The numbered blocks in the above figure as described as follows:

- Block 1: Enable callback or shut it off.
- Block 2: Compute average wait time. Once the caller is *in queue*, calculate the Estimated Wait Time (EWT) for that queue and place the value in ToExtVXML[0].

  If there is poor statistical sampling because of sparse queues and the wait time cannot be calculated in the VXML Server, use the ICM-calculated estimated wait time.

  One method of calculating EWT (the method used in this example) is:

```
    ValidValue(((SkillGroup.%1%.RouterCallsQNow+1)
    *
(ValidValue(SkillGroup.%1%.AvgHandledCallsTimeTo5,20))

    /max(
    SkillGroup.%1%.Ready,
    (SkillGroup.%1%.TalkingIn
    +
    SkillGroup.%1%.TalkingOut
    +
    SkillGroup.%1%.TalkingOther))
```

```
),100)
```

Modify this method if you are looking at multiple skill groups (when queuing to multiple skills).

- Block 3: Set up parameters to be passed.
- Block 4: Run this block and prompt the caller. If the caller does not accept the offer for a callback, keep the caller in the queue and provide queue music.
- Block 5: Set up variables. Call flow returns to this block if the caller elects to receive a callback. Otherwise, the call remains queuing in the queuing application (BillingQueue in this example) on the VXML Server.
- Block 6: Run external to Callback engine to keep the call alive. If the agent becomes available and there is no caller, then agent can't interrupt (do not want an agent to pick up and have no one there).
- Block 7: Has the caller rejected the callback call? If no, then go to block 8.
- Block 8: Set up variables.
- Block 9: Put caller briefly into queue (after caller accepts the actual callback call)

Overview of CCE Script Configuration for Courtesy Callback

The CCE script elements needed to enable Courtesy Callback are on the CVP Installation CD in *CVP\Downloads and Samples\ICM Downloads*. The script sample found there (CourtesyCallback) contains the necessary sample elements for the courtesy callback feature. However you must merge this script into your existing CCE scripts.

As a starting point and to run a simple test, import the script into the CCE script editor, validate it with the CCE script editor validation tool to locate nodes that need extra configuration (such as for Network VRU scripts and expanded call variables), and then modify the script according to your existing CCE environment.

1. Locate each queue point in every CCE script. For example: Queue To Skill Group, Queue to Enterprise Skill Group, Queue to Scheduled Target or Queue to Agent.
2. Categorize each queue point according to the pool of resources that it is queuing for. Each unique pool of resources will ultimately require a queue in VXML Server if Courtesy Callback is going to be offered for that resource pool. For example, using the following example, QueueToSkill X and QueueToSkill Z are queuing for the exact same resource pool (despite the different queuing order). Queue to Skill Y, however, is queuing to a different pool because it includes Skill Group D.
    - QueueToSkillGroup X is queuing for Skill Group A, B, C in that order.
    - QueueToSkillGroup Y is queuing for Skill Group A, C and D in that order.
    - QueueToSkillGroup Z is queuing for Skill Group C, B, A in that order.
3. Assign a unique name to each unique resource pool. In the above example, we can use names ABC and ACD as example names.
4. For each resource pool, decide whether callbacks will be allowed in that resource pool. If yes, then every occurrence of that resource pool in all ICM scripts must be set up to use VXML Server for queuing. This is to ensure that the Courtesy Callback mechanism in the VXML Server gets a full, accurate picture of each resource pool's queue.

5. For any queue point where Courtesy Callback will be offered, modify all CCE scripts that contain this queue point according to the guidelines in the following CCE script examples.

Configure CCE Script for Courtesy Callback

Many of the configuration items below relate to the numbered blocks in the diagram and provide understanding for CCE Script for Courtesy Callback. See CCE Script for Courtesy Callback, on page 364 for details. Steps that refer to specific blocks are noted at the beginning of the each step.

To configure CCE to use the sample Courtesy Callback CCE script, perform the following steps:

Procedure

Step 1 Copy the CCE example script, **CourtesyCallback.ICMS** to the CCE Admin Workstation.

The example CCE script is available in the following locations:

- On the CVP install media in `\CVP\Downloads and Samples\`.
- From the Operations Console in **%CVP_HOME%\OPSConsoleServer\ICMDownloads**

Step 2 Map the route and skill group to the route and skill group available for courtesy callback.

a) In Script Editor, select **File** > **Import Script...**.
b) In the script location dialog, select the **CourtesyCallback.ICMS** script and click **Open**.
c) In the Import Script - Manual Object Mapping window, map the route and skill group to the route and skill group available for courtesy callback (identified previously).

Step 3 Once the script is open in Script Editor, open the **Set media server** node and specify the URL for your VXML Server.

For example: **http://10.86.132.139:7000/CVP**

Step 4 **Refer to Block #1:** A new ECC variable is used when determining if a caller is in queue and can be offered a callback. Define the **user.CourtesyCallbackEnabled** ECC variable for courtesy callback.

a)
b) On the CCE Admin Workstation, in the ICM Configuration Manager, use the Expanded Call Variable List tool.
c) Create **user.CourtesyCallbackEnabled**.
d) Set **Maximum Length** to 1.
e) Check **Enabled**.
f) Check **Persistent**.

This step assumes you have already created the standard ECC variables required for any Unified CVP installation. See Define Unified CVP ECC Variables, on page 181.

Step 5 **Block #2:** If you wish to use a different estimated wait time (EWT), modify the calculation in block #2; you will need to do this if you use a different method for calculating EWT or if you are queuing to multiple skill groups.

Step 6 **Block #3:** Set up the parameters that will be passed to CallbackEntry (VXML application).

Note This step assumes you have already configured the CCE and expanded call variables not related to Courtesy Callback. Ensure that the **user.media.id** variable is enabled and configured with a length of 36 characters.

Variable values specific to Courtesy callback include:

ToExtVXML[0] = concatenate("application=CallbackEntry",";ewt=",Call.user.microapp.ToExtVXML[0])

ToExtVXML[1] = "qname=billing";

ToExtVXML[2] = "queueapp=BillingQueue;"

ToExtVXML[3] = concatenate("ani=",Call.CallingLineID,";");

Definitions related to these variables are:

- CallbackEntry is the name of the VXML Server application that will be run.
- ewt is calculated in **Block #2** .
- qname is the name of the VXML Server queue into which the call will be placed. There must be a unique qname for each unique resource pool queue.
- queueapp is the name of the VXML Server queuing application that will be run for this queue.
- ani is the caller's calling Line Identifier.

Step 7 Create Network VRU Scripts.

Using the ICM Configuration Manager, Network VRU Script List tool, create the following Network VRU Scripts:

Block #4: Interruptible Script (agent can interrupt the caller on hold):

- Name: **VXML_Server_Interruptible**
- Network VRU: Select your Type 10 CVP VRU
- VRU Script Name: **GS,Server,V,interrupt**
- Timeout: **9000 seconds**
- Interruptible: **Checked**

Block #6: Noninteruptible Script (agent cannot interrupt because no caller is available):

- Name: **VXML_Server_Noninterruptible**
- Network VRU: Select your Type 10 CVP VRU
- VRU Script Name: **GS,Server,V,nointerrupt**
- Timeout: **9000 seconds** (must be greater than the maximum possible call life in Unified CVP)
- Interruptible: **Not Checked**

Step 8 Verify that the **user.microapp.ToExtVXML ECC** variable is Enabled,Persistent, with at least 60 (chars) for the maximum length setting, set up as an array with a maximum array size of 5 elements.

Check **Array** and then a subfield for **Maximum array size** appears.

Step 9 Verify that the **user.microapp.FromExtVXML** variable is Enabled, Persistent, with at least 60 (chars) for the maximum length setting, set up as an array with a maximum array size of 4 elements.

Check **Array** and then a subfield for **Maximum array size** appears.

Step 10 Verify that you have at least one available route and skill group to map to the route and skill group in the example script.

Step 11 Save the script, then associate the call type and schedule the script.

Note For an example of scheduling the script refer to *Getting Started with Cisco Unified Customer Voice Portal* , the *Create a Call Type Manager Entity Routing Script and Call Schedule* topic.

Related Topics

CCE Script for Courtesy Callback, on page 364
Define Unified CVP ECC Variables, on page 181

Configure Courtesy Callback up to Four Hours

The default value for the estimated wait time (EWT) for Courtesy Callback is 90 minutes (5400 seconds). This can be configured up to four hours (14400 seconds). This is applicable for both static route and dynamic route configurations. To configure EWT for Courtesy Callback for more than two hours, you need to change CVP, ICM, and Gateway configurations.

These configurations work with Cisco Virtualized Voice Browser (VVB).

Procedure

Step 1 To configure **CVP**, perform the following steps:

a) Go to **C:\Cisco\CVP\conf** folder.

b) Edit the *ivr.properties* file:

Set the following parameters to the desired value:

- **IVR.LastAccessTimeout=** <value between 5400 and 14400>
- **IVR.VBCallTimeout=** <value between 5400 and 14400>

c) Restart Call Server and VXML service from the Call Server.

Step 2 To configure **ICM**, perform the following steps:

a) Open **ICM Configuration Manager**.

b) Go to **Configuration Manage**, and then open **Network VRU Script List**.

Set the **Timeout Attributes**: **VXML_Server_Interruptible** and **VXML_Server_Noninterruptible** to the desired value.

c) Go to **Configuration Manage**, and then open **Media Routing Domain List**.

Set the **Max time in queue** attribute to the desired value.

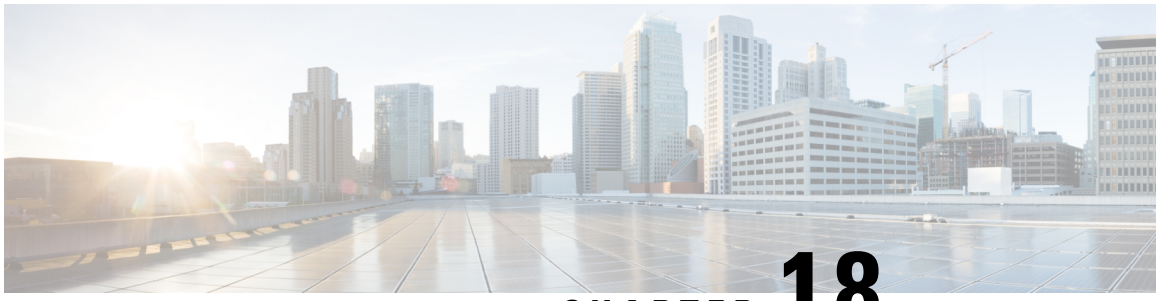
d) Go to **regedit Router** > **CurrentVersion** > **Configuration** > **Queuing**.

Set the **MaxTimeInQueue** attribute to to the desired value.

e) Restart the **VRU PG** in **ICM**.

Step 3 To configure **Ingress Gateway**, run the following commands from the command prompt:

```
router# configure terminal
router(config)# sip-ua
router(config)#voice service voip
router(conf-voi-serv)#sip
router(conf-serv-sip)#session refresh
```



CHAPTER 18

Unified CVP Security

This chapter describes security considerations for Unified CVP call flow model deployments.

Note

- This release supports only TLS 1.2. For more information, see *Contact Center Enterprise Solution Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/tsd-products-support-series-home.html.
- As per security guidelines, limit the validity of the generated or the requested SSL certificates to 2-3 years or shorter.
- If you are testing with the self-signed TLS certificates that are generated as a part of the installation, ensure that you map the CN/SANs on the certificate to the corresponding IP through DNS or hosts file entries.
- For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Secure JMX Communication between OAMP and Call Server using Mutual Authentication

You can secure JMX communication by:

- Exchanging the CA-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificates

On Call Server or VXML Server or Reporting Server

Log in to the CVP/Reporting Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Export the following certificates:

a) WSM certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm_security.cer`

b) Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\callserver_security.cer`

c) VXML Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vxml_certificate -file %CVP_HOME%\conf\security\vxml_security.cer`

Note VXML certificate is not applicable for Reporting Server.

Step 2 Enter the keystore password when prompted.

Step 3 Copy all the generated certificates from the `%CVP_HOME%\conf\security\` folder of the Call/VXML/Reporting Server machine to the `%CVP_HOME%\conf\security\` folder on the OAMP machine.

Step 4 On the OAMP machine, export the OAMP Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_certificate -file %CVP_HOME%\conf\security\oamp_security.cer`

Step 5 Enter the keystore password when prompted.

Step 6 Copy the generated OAMP Server certificate from the `%CVP_HOME%\conf\security\` folder of the OAMP machine to the `%CVP_HOME%\conf\security\` folder of the CVP/Reporting Server machine.

Step 7 On the CVP/Reporting Server machine, import the OAMP Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore`

```
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_certificate
-file %CVP_HOME%\conf\security\oamp_security.cer
```

Step 8 Enter the keystore password when prompted.

Step 9 Trust this certificate? [no]: **yes**

Step 10 Configure WSM in CVP:

a) Go to `c:\cisco\cvp\conf\jmx_wsm.conf`

Add or update the file as shown and save it:

```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore= C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

Step 11 Run the regedit command.

a) Append the following to the file at: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\Webservices Manager\Parameters\Java`

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=<keystore_password>
Djavax.net.ssl.trustStoreType=JCEKS
```

Step 12 Configure JMX of callserver in CVP.

Go to `c:\cisco\cvp\conf\jmx_callserver.conf`.

Update the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2098
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 2097
javax.net.ssl.keyStore= C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

Step 13 Configure JMX of VXMLServer in CVP.

Go to `c:\cisco\cvp\conf\jmx_vxml.conf`.

Edit the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword = <keystore_password>
```

Step 14 Run the regedit command.

a) Append the following to the file at: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXML\Parameters\Java`

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=<keystore_password>
Djavax.net.ssl.trustStoreType=JCEKS
```

Step 15 Restart the Operation Console Server and the Call Server machines.

On OAMP

Log in to the Operations Console Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Import the following certificates:

a) WSM certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_wsm_certificate -file %CVP_HOME%\conf\security\wsm_security.cer`

b) Call Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_callserver_certificate -file %CVP_HOME%\conf\security\callserver_security.cer`

c) VXML Server certificate by running `%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_vxml_certificate -file %CVP_HOME%\conf\security\vxml_security.cer`

Step 2 Enter the keystore password when prompted.

Step 3 Trust this certificate? [no]: **yes**

Step 4 Restart OAMP service.

Step 5 Log into OAMP. To enable secure communication between OAMP and Call Server or VXML Server or Reporting Server, navigate to **Device Management** > **Call Server**. Check the **Enable secure communication with the Ops console** check box. Save and deploy both Call Server and VXML Server.

Generate CA-Signed Certificate for WSM Service in Call Server/VXML Server/Reporting Server/WSM Server

Log in to the Call Server or VXML Server or Reporting Server or WSM Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Go to `%CVP_HOME%\conf\security` and delete the WSM certificate from by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore**

%CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate. Enter the keystore password when prompted.

Step 2 Repeat Step 1 for Call Server, VXML Server, and Reporting Server.

Step 3 Generate a CA-signed certificate for WSM server by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA`.

a) Enter the details at the prompts and type *Yes* to confirm.
b) Enter the keystore password when prompted.

Note Note the CN name for future reference.

Step 4 Generate the certificate request for the alias by running the following command and saving it to a file (for example, wsm.csr): `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm_certificate`.

a) Enter the keystore password when prompted.

Step 5 Sign the certificate on a CA.

Note Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority.

Step 6 Copy the root certificate and the CA-signed WSM certificate to `%CVP_HOME%\conf\security\`.

Step 7 Import the root certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cer>`.

a) Enter the keystore password when prompted.
b) At **Trust this certificate** prompt, type *Yes*.

Step 8 Import the CA-signed WSM certificate by running `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>`. Enter the keystore password when prompted.

Step 9 Repeat Step3, 4, and 8 for Call Server, VXML Server, and Reporting Server.

Step 10 Configure WSM in CVP:

a) Go to `c:\cisco\cvp\conf\jmx_wsm.conf`

Add or update the file as shown and save it:

```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword=< keystore_password >
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
```

b) Run the **regedit** command.

Append the following to the file at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\WebServicesManager\Parameters\Java`:

```
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

Step 11 Configure JMX of callserver in CVP:

a) Go to `c:\cisco\cvp\conf\jmx_callserver.conf`

Update the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2098
com.sun.management.jmxremote.ssl = true
 com.sun.management.jmxremote.rmi.port = 2097
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword = <keystore password>
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
```

Step 12 Configure JMX of VXMLServer in CVP:

a) Go to `c:\cisco\cvp\conf\jmx_vxml.conf`

Edit the file as shown and save the file:

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true
com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword = <keystore password>
```

b) Run the **regedit** command.

Append the following to the file at `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java`:

```
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

c) Restart WSM service.

Note When secure communication is enabled with JMX, it forces the keystore to be *%CVP_HOME%\conf\security\.keystore*, instead of *%CVP_HOME%\jre\lib\security\cacerts*.

Therefore, the certificates from *%CVP_HOME%\jre\lib\security\cacerts* should be imported to *%CVP_HOME%\conf\security\.keystore*.

Generate CA-Signed Client Certificate for WSM

Log in to the Call Server or VXML Server or Reporting Server or WSM. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Go to `%CVP_HOME%\conf\security` and generate a CA-signed certificate for client authentication with callserver by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA**

a) Enter the details at the prompts and type *Yes* to confirm.
b) Enter the keystore password when prompted.

Note The alias will be the same as the CN used for generating WSM server certificate.

Step 2 Generate the certificate request for the alias by running the following command and saving it to a file (for example, jmx_client.csr): **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr**

a) Enter the keystore password when prompted.
b) Verify that the CSR was generated successfully by running **dir jmx_client.csr**

Step 3 Sign the certificate on a CA.

Note Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority.

a) Enter the keystore password when prompted.
b) At **Trust this certificate** prompt, type *Yes*.

Step 4 Copy the root certificate and the CA-signed JMX Client certificate to `%CVP_HOME%\conf\security\`.

Step 5 Import the CA-signed JMX Client certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\<filename of CA-signed JMX Client certificate>**

a) Enter the keystore password when prompted.

Step 6 Restart Cisco CVP VXMLServer service.

Note Repeat the same procedure for Reporting Server, if any.

Generate CA-Signed Client Certificate for OAMP (to be done on OAMP)

Log into the OAMP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Go to `%CVP_HOME%\conf\security` and generate a CA-signed certificate for client authentication with callserver WSM by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalg RSA**.

a) Enter the details at the prompts and type *Yes* to confirm.

b) Enter the keystore password when prompted.

Note The alias will be the same as the CN of the Call Server or the VXML Server.

Step 2 Generate the certificate request for the alias by running the following command and saving it to a file (for example, jmx.csr): **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr**.

a) Enter the keystore password when prompted.

Step 3 Sign the certificate on a CA.

Note Follow the procedure to create a CA-signed certificate using the CA authority. Download the certificate and the root certificate of the CA authority.

Step 4 Copy the root certificate and CA-signed JMX Client certificate to `%CVP_HOME%\conf\security\`.

Step 5 Import the root certificate of the CA by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

a) Enter the keystore password when prompted.

b) At **Trust this certificate** prompt, type *Yes*.

Step 6 Import the CA-signed JMX Client certificate of CVP by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>**.

a) Enter the keystore password when prompted.

Step 7 Restart OAMP service.

Step 8 Log into OAMP. To enable secure communication between OAMP and Call Server or VXML Server, navigate to **Device Management** > **Call Server**. Check the **Enable secure communication with the Ops console** check box. Save and deploy both Call Server and VXML Server.

Step 9 Run the **regedit** command.

a) Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java`.

b) Append the following to the file sand save it:

```
-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
-Djavax.net.ssl.trustStorePassword=<keystore_password>
-Djavax.net.ssl.trustStoreType=JCEKS
```

Note After securing the ports for JMX, JConsole can be accessed only after performing the defined steps for JConsole listed in the OpenJDK docs.

Note After securing the ports for JMX, JConsole can be accessed only after performing the defined steps for JConsole listed in the Oracle docs.

[Optional] Blocking JConsole Login to OAMP

This section is needed if you want to block JConsole login to OAMP.

Note OAMP will stop the JMX communication with the following procedure but OAMP to Call Server/VXML Server / Reporting Server/WSM will continue to work.

Procedure

Step 1 Go to `c:\cisco\cvp\conf\jmx_oamp.conf`.

Add the following to the file and save it:

```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 10001
com.sun.management.jmxremote.ssl = true
#com.sun.management.jmxremote.ssl.config.file=
com.sun.management.jmxremote.rmi.port = 10000
```

Step 2 Restart the OpsConsoleServer service.

Step 3 Go to `c:\cisco\cvp\conf\jmx_wsm.conf`.

Add the following to the file and save it:

```
javax.net.debug = all
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
#com.sun.management.jmxremote.ssl.config.file=
com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore= C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.keyStorePassword= <keystore_password>
```

Step 4 Restart the WSM service.

With the aforesaid steps, unsecure JConsole login to OAMP will stop from remote machines but JConsole will continue to work from the OAMP host.

Securing System CLI

To run the System CLI command on Cisco CVP CallServer, perform the following steps:

Procedure

Step 1 Import the root CA certificate in the JRE keystore:

a) Run the `%CVP_HOME%\jre\bin\keytool.exe -keystore %CVP_HOME%\jre\lib\security\cacerts -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>` command.

b) Enter the keystore password when prompted.

The default keystore password is *changeit*.

a) Type *Yes* when the **Trust this certificate** prompt appears.

Step 2 Restart the Cisco CVP CallServer service.

Secure SIP Communication between Call Server and Cisco VVB

You can secure SIP communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Note

- To support AES 256 bit encryption-based ciphers (for example, TLS_RSA_WITH_AES_256_CBC_SHA256), JRE version in the Unified CVP server needs to be upgraded to Java 1.8u275.
- If you are using SHA1 after upgrading the JRE version, then edit `C:\Cisco\CVP\jre\lib\security\java.security` file to remove the `SHA1 jdkCA & usage TLSServer` parameter from `jdk.certpath.disabledAlgorithms` configuration.

Self-Signed Certificates

Note When the Unified CVP Call Server, Media Server, and Unified CVP VXML Server are co-resident on the same server and use self-signed certificates, you can use a single self-signed certificate for all these services. This simplifies the certificate management process and ensures secure communication within the co-resident environment.

On Call Server

Log in to the Call Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Export the Call Server certificate by running **%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate.cer>**.

Step 2 Enter the keystore password when prompted.

Step 3 Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running **%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate>**.

Note See Step 5 of the *On Cisco VVB* section to download a VVB certificate.

Step 4 Enter the keystore password when prompted.
A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

Step 5 Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**.

On Cisco VVB

Procedure

Step 1 Copy the CVP CallServer self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.

Step 2 Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**.

Step 3 In **Certificate Purpose**, select **tomcat-trust**.

Step 4 Select the self-signed certificate of the Call Server and click **Upload**.

Step 5 Download the self-signed certificate of the VVB.

Step 6 Go to **OS Admin** > **Security** > **Certificate Management**.

Step 7 In the **Certificate** column, find the certificate named **tomcat**.

Step 8 Select the self-signed tomcat certificate and click **Download** .

Step 9 After the new certificate is uploaded, restart the node(s) using the CLI command **utils system restart**.

Step 10 Go to **Cisco VVB Administration** > **System Parameters** > **TLS**.

Step 11 Check TLS as **Enable**.

Step 12 Select the supported TLS version and click **Update**.

Step 13 Restart Cisco VVB Engine from the **VVB Serviceability** page.

CA-Signed Certificate

On Call Server

Log in to the Call Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Attention Repeat this procedure if you have multiple Call Servers.

On Cisco VVB

Procedure

Step 1 To generate the CSR certificate on VVB, open the administration page. From the **Navigation** drop-down list, choose **Cisco Unified OS Administration** and click **Go**.

Step 2 Go to **Security** > **Certificate Management** > **Generate CSR Generate Certificate signing Request**. Create the CSR against tomcat with the key-length as 2048.

Step 3 To download the generated CSR, click **Download CSR**. After the **Generate Certificate signing Request** dialog opens, click **Download CSR**.

Step 4 Open the certificate in Notepad, copy the contents and sign the certificate with CA.

Step 5 Upload the root certificate generated from the CA into VVB against tomcat-trust:

a) Go to **Security** > **Certificate Management** > **Generate CSR** > **Upload certificate/certificate chain**.
b) Choose **tomcat-trust** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload** to upload the root certificate of the Certificate Authority.

Step 6 Upload the signed certificate into VVB against tomcat.

a) Go to **Security** > **Certificate Management** > **Upload certificate/certificate chain**.
b) Choose **tomcat** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload**.

After the certificate is uploaded successfully, VVB displays the certificate signed by <CA hostname>.

Step 7 Restart the Tomcat service and the VVB engine.

For the configuration steps, see the *Manage System Parameters* section.

Secure HTTP Communication between VXML Server and Cisco VVB

You can secure HTTP communication by:

- Exchanging the self-signed certificates between the VXML Server and VVB or VXML Gateway.

- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

On VXML Server

Log in to the VXML Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Export the VXML SERVER certificate by running **%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vxml_certificate -file %CVP_HOME%\conf\security\<vxml_certificate.cer>**.

Step 2 Enter the keystore password when prompted.

Step 3 Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running **keystore.%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate>**.

Note See Step 5 of the following Section, *On Cisco VVB* to download a VVB certificate.

Step 4 Enter the keystore password when prompted.
A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

Step 5 Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**.

On Cisco VVB

Procedure

Step 1 Copy the VXML Server self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.

Step 2 Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**.

Step 3 In **Certificate Purpose**, select **tomcat-trust**.

Step 4 Select the self-signed certificate of the VXML Server and click **Upload**.

Step 5 Download the self-signed certificate of the VVB.

Step 6 Go to **OS Admin** > **Security** > **Certificate Management**.

Step 7 In the **Certificate** column, select the **tomcat** certificate.

Step 8 Select the tomcat certificate and click **Download** .

Step 9 After the new certificate uploads, restart the Cisco Tomcat service.

Step 10 Go to **Cisco VVB Administration** > **System Parameters** > **TLS**.

Step 11 Check the **TLS** check box as **Enable**.

Step 12 Select the supported TLS version and click **Update**.

Step 13 Restart the Cisco VVB Engine from the **VVB Serviceability** page.

Note To enable secured connection in Application Management from the Cisco VVB UI, see *Cisco Virtualized Voice Browser Administration and Configuration Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-series-home.html.

CA-Signed Certificate

On VXML Server

Log in to the VXML Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Procedure

Step 1 Remove the existing certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias vxml_certificate**.

Step 2 Generate a new key pair for the alias with selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias vxml_certificate -v -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <specify the CVP host name appended with "VXML_Server"> E.g
cisco-cvp-211_VXML_Server
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN
Specify 'yes' for the inputs.
```

Step 3 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias vxml_certificate -file %CVP_HOME%\conf\security\vxmlserver.csr** and save it to a file (for example, oamp.csr).

Step 4 Enter the keystore password when prompted.

Step 5 Download the vxmserver.csr from `CVP %CVP_HOME%\conf\security\` and sign it from CA.

Step 6 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

Step 7 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 8 Enter the keystore password when prompted.

Step 9 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias vxml_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Step 10 Enter the keystore password when prompted.

Step 11 Restart the VXML Server.

On Cisco VVB

Procedure

Step 1 Upload the root certificate generated from the CA into VVB against tomcat-trust. Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**, select **tomcat-trust** and upload the root certificate of the Certificate Authority.

Note If you use the same root certificate that was used in the Call Server configuration as described in Section, Secure Communication between Call Server and Cisco VVB and the certificate is already imported, then you can skip this step.

Step 2 Generate the CSR against tomcat with the key-length as 2048.

Step 3 Open the certificate in Notepad. Copy the contents and sign the certificate with CA.

Step 4 Restart the Tomcat service and the VVB engine.

To enable secure communications on the VXML Server, see Unified CVP VXML Server Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

To enable secure communications on the VXML Server (standalone), see Unified CVP VXML Server (Standalone) Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Secure HTTPS Communication between Media Server and Cisco VVB

This section describes how to import certificate from IIS MediaServer to Cisco VVB and how to import IIS CA-signed certificate.

Procedure

Step 1 Enter **https://<mediaserver>:443/** in the address bar of the web browser.

Step 2 In the **Security Alert** dialog box, click **View Certificate**.

Step 3 Click the **Details** tab

Step 4 Click **Copy to File**.

Step 5 In the **Certificate Export Wizard** dialog box, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6 In the **File to the Export** dialog box, specify a file name, and then click **Next**.

Step 7 Click **Finish**.
A message indicates that the export was successful.

Step 8 Click **OK** and close the **Security Alert** dialog box.

Step 9 Copy the CVP MediaServer self-signed certificate downloaded from the CVP and upload into VVB against **tomcat-trust**.

Step 10 Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain** > **In Certificate Purpose*** select **tomcat-trust**, choose the self-signed certificate of the Call Server and press **Upload** button.

Step 11 Restart Cisco VVB Engine.

Secure HTTP Communication between OAMP Server and Cisco VVB

Self-Signed Certificate

Procedure

Step 1 Sign in to Cisco Unified OS Administration on the VVB server (https://<FQDN of VVB server>/cmplatform).

Step 2 Go to **Security** > **Certificate Management**.

Step 3 Click **Find**.

Step 4 Perform one of the following steps.

- If the tomcat certificate for your server is not on the list, click **Generate Self-signed**. When the certificate is generated, reboot your server.
- If the tomcat certificate for your server is on the list, click the certificate to select it.

Note Ensure that the certificate you select includes the hostname for the server.

Step 5 Click **Download .PEM File** and save the file to your desktop.

Step 6 Copy the certificate to `%CVP_HOME%\conf\security\` in OAMP Server.

Step 7 Run the following command to import the certificate to the CVP Call Server keystore.

```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias VVB_cert -file
%CVP_HOME%\conf\security\<VVB certificate.pem>
```

Log in to the Call Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 8 Go to **Services** and restart **Cisco CVP OPSConsoleServer**.

CA-Signed Certificate

On OAMP Server

Procedure

Step 1 Log in to the OAMP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Remove the existing certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias oamp_certificate**.

Step 3 Generate a new key pair for the alias with selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <specify the CVP host name appended with "OAMP_Server"> E.g
cisco-cvp-211_OAMP_Server
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN
Specify 'yes' for the inputs.
```

Step 4 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias oamp_certificate -file %CVP_HOME%\conf\security\oampserver.csr** and save it to a file (for example, `oamp.csr`).

Step 5 Enter the keystore password when prompted.

Step 6 Download `oamp.csr` from `CVP %CVP_HOME%\conf\security\` and sign it from CA.

Step 7 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

Step 8 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 9 Enter the keystore password when prompted.

Step 10 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias oamp_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Step 11 Enter the keystore password when prompted.

Step 12 Restart the Cisco **CVP OpsConsoleServer** service.

On Cisco VVB

Procedure

Step 1 To generate the CSR certificate on VVB, open the administration page. From the **Navigation** drop-down list, choose **Cisco Unified OS Administration** and click **Go**.

Step 2 Go to **Security** > **Certificate Management** > **Generate CSR Generate Certificate signing Request**. Create the CSR against tomcat with the key-length as 2048.

Step 3 To download the generated CSR, click **Download CSR**. After the **Generate Certificate signing Request** dialog opens, click **Download CSR**.

Step 4 Open the certificate in Notepad, copy the contents and sign the certificate with CA.

Step 5 Upload the root certificate generated from the CA into VVB against tomcat-trust:

a) Go to **Security** > **Certificate Management** > **Generate CSR** > **Upload certificate/certificate chain**.
b) Choose **tomcat-trust** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload** to upload the root certificate of the Certificate Authority.

Step 6 Upload the signed certificate into VVB against tomcat.

a) Go to **Security** > **Certificate Management** > **Upload certificate/certificate chain**.
b) Choose **tomcat** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload**.

After the certificate is uploaded successfully, VVB displays the certificate signed by <CA hostname>.

Step 7 Restart the Tomcat service and the VVB engine.

Secure HTTP Communication between VXML Server and Dialogflow

This procedure explains how to configure proxy settings for VXML Server to communicate with Dialogflow. This is required if VXML Server is not connected to cloud-based services.

Procedure

Step 1 Log in to VXML Server.

Step 2 Run the **regedit** command.

Step 3 Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java\Options`.

Step 4 Append the following lines to the file:

```
-Dhttps.proxyHost=<Your proxy IP/Host>
-Dhttps.proxyPort=80
```

Note If proxy requires credentials, add the following:

```
-Dhttps.proxyUser=<username>
-Dhttps.proxyPassword=<password>
```

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

Secure HTTP Communication between OAMP Server and Call Server

Self-Signed Certificate

Procedure

Step 1 Log in to the CVP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Run the following command to export the WSM certificate.

```
%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore
-storetype JCEKS -alias wsm_certificate -file
%CVP_HOME%\conf\security\{CVPServerName}_wsm.cer>
```

Step 3 Enter the keystore password when prompted.

Step 4 Copy the certificate to `%CVP_HOME%\conf\security\` in OAMP Server.

Step 5 Log in to the OAMP Server.

For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 6 Run the following command to import the certificate to the OAMP Server:

```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias {CVPServername}_wsm -file
%CVP_HOME%\conf\security\{CVPServername}_wsm.cer>
```

For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 7 Enter the keystore password when prompted.

Step 8 Repeat all the steps for all the Cisco Unified CVP Servers in the deployment.

Step 9 Go to **Services** and restart **Cisco CVP OPSConsoleServer** and **CVP WebServices** on CVP OAMP Server.

Step 10 Download the OAMP WSM certificate (OAMP_wsm) from https://<oampserverip>:8111 on the Cisco Unified CVP Server to `%CVP_HOME%\conf\security\`

Step 11 Run the following command to import the certificate to the Cisco Unified CVP Server:

```
%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore
%CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias oamp_wsm -file
%CVP_HOME%\conf\security\oamp_wsm.cer>
```

Step 12 Enter the keystore password when prompted.

Step 13 Repeat all the steps for all the Cisco Unified CVP Servers in the deployment.

Step 14 Go to **Services** and restart **Cisco Web Services**, **Cisco VXML Service**, and **Cisco Call Service** on each Cisco Unified CVP Server.

CA-Signed Certificate

On OAMP Server

Procedure

Step 1 Log in to the OAMP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Remove the existing certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias oamp_certificate**.

Step 3 Generate a new key pair for the alias with selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias oamp_certificate -v -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <specify the CVP host name appended with "OAMP_Server"> E.g
cisco-cvp-211_OAMP_Server
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN
Specify 'yes' for the inputs.
```

Step 4 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias oamp_certificate -file %CVP_HOME%\conf\security\oampserver.csr** and save it to a file (for example, `oamp.csr`).

Step 5 Enter the keystore password when prompted.

Step 6 Download `oamp.csr` from `CVP %CVP_HOME%\conf\security\` and sign it from CA.

Step 7 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

Step 8 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 9 Enter the keystore password when prompted.

Step 10 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias oamp_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Step 11 Enter the keystore password when prompted.

Step 12 Restart the Cisco **CVP OpsConsoleServer** service.

On Call Server

Procedure

Step 1 Log in to the Call Server or Reporting Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Remove the existing WSM certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias wsm_certificate**.

Step 3 Remove the existing Call Server certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security.keystore -delete -alias callserver_certificate**.

Step 4 Generate a new key pair for the alias with selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -v -validity <duration in days> -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <specify the  CVP hostname or FQDN, appended with "wsm"> E.g cisco-cvp-211_wsm>
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN
Specify 'yes' for the inputs.
```

Note When a certificate is generated to be used in PCCE SPOG, provide the FQDN of the host without appending _wsm.

The default duration for `validity` is 90 days.

Step 5 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr** and save it to a file (for example, `wsm.csr`).

Step 6 Enter the keystore password when prompted.

Step 7 Download `wsm.csr` from `CVP %CVP_HOME%\conf\security\` and sign it from CA.

Step 8 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

Step 9 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -validity <duration in days> -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 10 Enter the keystore password when prompted.

Step 11 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -validity <duration in days> -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Step 12 Enter the keystore password when prompted.

Step 13 Restart the **Cisco CVP WebServicesManager** service.

Configure Cloud Connect

Before you begin

CVP interacts with Webex Experience Management through Cloud Connect for receiving the SIP URI of the Survey Application. Follow this procedure to configure a CVP device for Cloud Connect via the Operations Console.

1. Import the certificate from the Call Server to the Operations Console server. For details on how to do this, see *Secure HTTPS Communication between OAMP Server and Call Server* section in *Configuration Guide for Cisco Unified Customer Voice Portal*.
2. Import the Cloud Connect certificate to the Call Server. For details on how to do this, see Import the Cloud Connect Certificate, on page 392.
3. Ensure Unified CVP hostname is DNS resolvable from OAMP Server.
4. Restart the CVP OPSConsoleServer service.

Procedure

Step 1 To open the Operations Console, enter `https://<FQDN>:9443/noamp` in the web-browser, where *FQDN* is the fully qualified domain name of the machine on which Operations Console is installed.

Step 2 Navigate to **Integration** > **Cloud Connect**.

Step 3 From the **Device** drop-down list, select the CVP device.

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

Step 5 In the **Subscriber IP Address / Hostname** text box, enter the FQDN / IP address of the subscriber.

Step 6 In the **User Name** text box, enter the username.

Step 7 In the **Password** text box, enter the password.

Step 8 Click **Save**.

Step 9 Restart the Cisco CVP Call Server.

Import the Cloud Connect Certificate

Follow this procedure to import the Cloud Connect (publisher and subscriber) certificates to CVP call servers:

Note Ensure that you import both the Cloud Connect Publisher and Subscriber certificates to all the CVP call servers.

Procedure

Step 1 To export the Cloud Connect certificates:

a) Enter the following URL to access the **Cisco Unified Communications Operating System Administration** page.

```
https://<FQDN of CloudConnect:8443/cmplatform
```

b) Navigate to **Security** > **Certificate Management** and find the Cloud Connect publisher and subscriber certificates in one of your tomcat-trust folders.

c) Select the certificates and click **Download .PEM File** to save the certificates to a local folder.

Step 2 Copy the Cloud Connect certificates into the call server folder at `c:\cisco\cvp\conf\security`.

Step 3 Open the Command Prompt as an administrator.

Step 4 Enter the following command in the keystore to import the Cloud Connect certificate to the call server.

```
c:\Cisco\CVP\jre\bin\keytool.exe -import -keystore .keystore -storetype JCEKS -trustcacerts

   -alias <cloud connect publisher or cloud connect subscriber> -file <filepath>
```

Step 5 Enter the keystore password when prompted. To retrieve the keystore password, do the following:

Go to `%CVP_HOME%\bin`. Generate the keystore password by running the `DecryptKeystoreUtil.bat` file.

Step 6 Restart the CVP call server.

Step 7 Repeat steps 1 through 6 for all the CVP call servers.

For more details on how to obtain a third-party CA certificate for Cloud Connect, see the *Obtain and Upload Third-party CA Certificate* topic in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Secure Communication on CUCM

You can secure communication on CUCM by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

Procedure

Step 1 Log in to the CUCM OS Administration page.

Step 2 Go to **Security** > **Certificate Management**.

Step 3 Click **Generate Self-signed**.

Step 4 On the pop-up window, click **Generate** button.

Step 5 Restart Tomcat from CUCM CLI by running **utils service restart Cisco Tomcat**.

Note Tomcat will take a few minutes to stop and then start. If you access the CUCM UI during this time, you may receive a 404 error.

Step 6 When the CUCM UI is available, open the CUCM OS Administration page.

Step 7 Go to **Security** > **Certificate Management**.

Step 8 Click **Find** and identify the Self-signed certificate generated by the system.

Step 9 Click the CallManager Certificate name.

Step 10 In the dialog box, click **Download**.

CA-Signed Certificate

To configure TLS and SRTP, see *Security Guide for Cisco Unified Communications Manager 11.6* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Procedure

Step 1 Enter the following command in the CLI to set the CUCM in the mixed mode, and to register the endpoints in the encrypted mode:

```
admin: utils ctl set-cluster mixed-mode

This operation will set the cluster to Mixed mode.  Auto-registration is enabled on at least
 one CM node. Do you want to continue? (y/n):y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
You must reset all phones to ensure they received the updated CTL file.
You must restart Cisco CTIManager services on all the nodes in the cluster that have the
service activated.
admin:
```

Step 2 Choose **CUCM Admin Page** > **System** > **Enterprise Parameters**. Check if **Cluster Security Mode** is set to 1.

Step 3 Set the minimum TLS version command from the CLI:

```
admin:set tls client min-version 1.2
```

```
**WARNING** If you are lowering the TLS version it can lead to security issues **WARNING**

Do you really want to continue (yes/no)?y
Run this command in the other nodes of the cluster.

Restart the system using the command 'utils system restart' for the changes to take effect

Command successful
admin:set tls ser
admin:set tls server mi
admin:set tls server min-version?
Syntax:
set tls server min-version

admin:set tls server min-version 1.2

**WARNING** If you are lowering the TLS version it can lead to security issues **WARNING**

Do you really want to continue (yes/no)?y
Run this command in the other nodes of the cluster.

Restart the system using the command 'utils system restart' for the changes to take effect

Command successful
admin:
```

Step 4 Create an encrypted phone profile and the SIP trunk profile. Associate them with the phone and CUCM SIP trunk.

Step 5 Go to **System** > **Security** > **SIP Trunk Security Profile** and create a new SIP trunk security profile.

Step 6 On CUCM SIP Trunk, check the **SRTP Allowed** check box.

Step 7 From **SIP Trunk Security Profile** drop-down list, choose **TLS Secure Profile**.

Step 8 Restart the TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Step 9 Upload the root certificate generated from the CA to CUCM against CUCM-trust.

Step 10 Generate the CSR against CallManager and select the key-length as 2048.

Step 11 Sign the certificate on a CA https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118731-configure-san-00.html.

Step 12 Upload the root certificate generated from the CA to CUCM against CUCM-trust.

Step 13 Click **Upload Certificate** on CUCM by selecting the certificate name as **CallManager**.

On successful completion, CUCM displays the description as *Certificate signed by <CA hostname>*.

Step 14 Restart TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Secure Communication between Ingress Gateway and Call Server

You can secure communication between the Ingress Gateway and the Call Server by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

To secure SIP connection between Cisco Ingress Gateway and Call Server, import the Call Server certificate on the IOS device during the device configuration.

Procedure

Step 1 Open the certificate that was exported in Step 1, on page 381.

Step 2 Click **View Certificate**.

Step 3 Click the **Details** tab.

Step 4 Click **Copy to File**.
The **Certificate ExportWizard** window appears.

Step 5 Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6 Specify a file name in the **File to the Export** dialog box, and then click **Next**.

Step 7 Click **Finish**. A message indicates that the export was successful.

Step 8 Click **OK** and close the **Security Alert** dialog box.

Step 9 Open the certificate in Notepad.

Step 10 Access the IOS ingress GW in the privileged EXEC mode.

Step 11 Access the global configuration mode by entering the configuration terminal.

Step 12 Import the CVP CallServer Certificate to Cisco IOS Gateway by entering the following commands:

```
crypto pki trustpoint <Call Server trust point name>
enrollment terminal

exit
```

Step 13 Open the exported Call Server certificate in Notepad and copy the certificate information that appears between the -BEGIN CERTIFICATE and END CERTIFICATE tags to the IOS device.

Step 14 Enter the following command:

```
crypto pki auth <Call Server  trust point name>
```

Step 15 Paste the certificate from Notepad and end with a blank line or the word *quit* on a line by itself.

Step 16 To generate the self-signed certificate of the Gateway, first generate 2048-bit RSA keys:

```
crypto key generatersageneral-keys Label <Your Ingress GW trustpointname> modulus 2048
```

Step 17 Configure a trustpoint:

```
crypto pkitrustpoint<Your Ingress GW trustpointname>
enrollment selfsigned
fqdn none
subject-name CN=SIP-GW
rsakeypair <Your Ingress GW trustpoint name>

Router(config)# crypto pkienroll<Your Ingress GW trustpointname>
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

Step 18 View the certificate in PEM format, and copy the Self-signed CA certificate (output starting from "----BEGIN" to "CERTIFICATE----") to a file named *ingress_gw.pem*.

```
Router(config)# crypto pki export <Your Ingress GW trustpoint name> pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----END CERTIFICATE-----
```

Step 19 Test your certificate.

```
show crypto pkicertificates
```

Step 20 To configure TLS version on the Gateway:

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>


v1.2 Enable TLS Version 1.2

Note: SIP TLS version 1.2 is available in Cisco IOS Software Release 15.6(1)T and higher.
```

Step 21 To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

Step 22 To enable SRTP on the incoming/outgoing dial-peer, specify SRTP:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp

Note: This command is supported in Cisco IOS Software Release 15.6(1)T and higher.
```

Step 23 Configure the SIP stack in Cisco IOS GW to use the self-signed certificate of the router to establish a SIP TLS connection from/to the CVP Call Server.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address> <peer subnet mask>
trustpoint <Your Ingress GW trustpoint name> strict-cipher

Example:
sip-ua
 crypto signaling remote-addr 10.48.54.89 255.255.255.255 trustpoint VG-SIP-1 strict-cipher
```

Step 24 Configure an outbound VoIP dial-peer to route calls to the CVP Call Server.

```
session target ipv4:<Call Server IP address>:5061
 session transport tcp tls

Example:
dial-peer voice 3 voip
 destination-pattern 82...
 session protocol sipv2
 session target ipv4:10.48.54.89:5061
 session transport tcp tls
 dtmf-relay rtp-nte
 codec g711ulaw
```

Step 25 To import GW or CUSP certificate into the CVP Call Server:

a) Copy the Ingress GW/CUSP self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserverkeystore. **%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetypeJCEKS -alias gw_cert -file %CVP_HOME%\conf\security\<ingress GW\CUSP certificate name>**

b) Enter the keystore password when prompted.

c) A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

d) Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**

Step 26 To change the supported TLS version from the OAMP UI, see *Administration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Step 27 Restart the Call Server.

CA-Signed Certificate

For the configuration steps, see the latest *Cisco Unified Border Element Configuration Guide* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html.

Before you begin

- To configure SIP TLS and SRTP on the gateway, apply a security-k9 license on the gateway.
- Time sync all the nodes (CVP, VVB, Gateway) with an NTP server.

Procedure

Step 1 Create a 2048-bit RSA key.

```
Router(config)# crypto key generate rsa general-keys Label <name of the key pair> modulus
2048
   Generates 2048 bit RSA key pair.
```

Step 2 Create a trustpoint. A trustpoint represents a trusted CA.

Example:

```
Router(config)# crypto pki trustpoint ms-ca-name
     Creates the trustpoint.

Router(config-pki-trustpoint)# enrollment terminal
    Specifies cut and paste enrollment with this trustpoint.

Router(config-pki-trustpoint)# subject-name CN=sslvpn.mydomain.com,OU=SSLVPN,O=My Company
Name,C=US,ST=Florida
    Defines x.500 distinguished name.

Router(config-pki-trustpoint)# rsakeypair keypairname
    Specifies key pair generated previously

Router(config-pki-trustpoint)# fqdn sslvpn.mydomain.com
   Specifies subject alternative name (DNS:).

Router(config-pki-trustpoint)# exit
```

Step 3 Create a CSR (Certificate Request) to give to the MS Certificate Server.

Example:

```
Router(config)# crypto pki enroll ms-ca-name
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=Webvpn.cisco.com
% The subject name in the certificate will include: webvpn.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
! Displays the PKCS#10 enrollment request to the terminal.
! You will need to copy this from the terminal to a text
! file or web text field to submit to the 3rd party CA.

Certificate Request follows:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Redisplay enrollment request? [yes/no]: no

Router(config)#
```

Step 4 Sign the CSR with the root CA.

Step 5 Install the root certificate.

```
Router(config)# crypto pki authenticate ms-ca-name
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

```
-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit

Certificate has the following attributes:
Fingerprint MD5: D5DF85B7 9A5287D1 8CD50F90 232DB534
Fingerprint SHA1: 7C4656C3 061F7F4C 0D67B319 A855F60E BC11FC44
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Step 6 Install the signed certificate for the gateway:

```
Router(config)# crypto pki import ms-ca-name certificate
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

Step 7 Test your certificate.

```
show crypto pki certificates
```

Note

- To configure TLS version on the gateway:

```
router#
router# config terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>


  v1.2  Enable TLS Version 1.2
```

- To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

- To enable SRTP on the incoming/outgoing dial-peer, specify srtp:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

Step 8 Associate the created trustpoint in Step 2 with sip-ua.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address>
<peer subnet mask> trustpoint <trust point name created in step2>
```

Note Installing CVP Call/VXML Servers enables IIS (for media server functionality), which opens port 443 by default for TLS connections. This port allows TLSv1.0 and TLSv1.1 connections. To close these connections, change the **Enabled** value to 0 by selecting the **Decimal** option in the following registry keys:

- **TLSv1.0:** `HKEY-LOCAL-MACHINE \SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Protocols\TLS1.0\Server\Enabled`
- **TLSv1.1:** `HKEY-LOCAL-MACHINE\ SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Protocols\TLS1.1\Server\Enabled`

This disables ports 443 and 3389 for TLSv1.0 and TLSv1.1 server-side connections. While Windows 8 and Windows Server 2012 remote desktop clients work by default, Windows 7 and Windows Server 2008 remote desktop clients cannot connect to these servers for the RDP port (3389). To re-enable this port, install the patch available at https://support.microsoft.com/en-us/help/3080079/update-to-add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-7-or-wind.

Secure Communication on CUSP

You can secure communication on CUSP by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

For the configuration steps, see the latest *CLI Configuration Guide for Cisco Unified SIP Proxy* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel9_0/cli_configuration/cusp_cli_config/configuration.html#72360.

CA-Signed Certificate

Procedure

Step 1 Create an RSA keypair in CUSP. From the CUSP foundation, enter the config mode and create the keypair:

democusp48(config)# crypto key generate rsa label <key-label> modulus 1024 default

Example

```
democusp48# conf terminal
democusp48(config)# crypto key generate rsa label cusp48-ca modulus 1024 default
```

```
Key generation in progress. Please wait...
The label name for the key is cusp48-ca
```

Step 2 Generate CSR signed by CA by running **democusp48(config)# crypto key certreq label <key-label> url ftp:**

An FTP or HTTP server is required to export the CSR. Make sure the label in the command matches the label used to create the rsa private key.

Example

```
democusp48(config)# crypto key certreq label cusp48-ca url ftp:
Address or name of remote host? 10.64.82.176
Username (ENTER if none)? test
Password (not shown)?
Destination path? /cusp48-ca.csr Uploading CSR file succeed
democusp48(config)#
```

Step 3 Import the CA server root certificate into CUSP by running: **crypto key import trustcacert label <rootCA-label> terminal**.

Example

```
democusp48(config)# crypto key import trustcacert label rootCA terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIEdTCCA12gAwIBAgIQaO1+pgDsy5lNqtF3E
epB4TANBgkqhkiG9w0BAQUFADBC MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYK
CZImiZPyLGQBGRYHQVJUR1NPTDES MBAGA1UEAxMJU0lQUEhPTklYMB4XDTA3MDc
xMzExNTAyMVoXDTEyMDcxMzExNTgz MVowQjETMBEGCgmSJomT8ixkARkWA2NvbT
EXMBUGCgmSJomT8ixkARkWB0FSVEdT T0wxEjAQBgNVBAMTCVNJUFBIT05JWDCCA
SIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAKbepxqDVZ5uWUVMWx8VaHVG
geg4CgDbzCz8Na0XqI/0aR9lImgx1Jnf ZD0nP1QvgUFSZ2m6Ee/pr2SkJ5kJSZo
zSmz2Ge4sKjZZbgQHmljWv1DswVDw0nyV F71ULTaNpsh81JVF5t2lqm75UnkW4x
P5qQn/rgfXv/Xse9964kiZhZYjtt2Ixt2V3imhh1i228YTihnTY5c3L0vD30v8dH
newsaCKd/XU+czw8feWguXXCTovvXHIbFeHvLCk9FLDoV8n9PAIHWZRPnt+HQjsD
s+jaB3F9MPVYXYElpmWrpEPHUPNZG4LsFi 6tQtiRP2UANUkXZ9fvGZMXHCZOZJi
FUCAwEAAaOCAWUwggFhMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA
1UdDgQWBBR39nCk+FjRuAbWEof5na/+Sf58STCCAQ4GA1UdHwSCAQUwggEBMIH+o
IH7oIH4hoG4bGRhcDovLy9DTj1TSVBQSE9O SVgsQ049U0lQUEhPTklYLUlORElB
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBT ZXJ2aWNlcyxDTj1TZXJ2aWNlcyx
DTj1Db25maWdlcmF0aW9uLERDPUFSVEdTT0ws REM9Y29tP2NlcnRpZmljYXRlUm
V2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz cz1jUkxEaXN0cmlidXRpb25Qb
2ludIY7aHR0cDovL3NpcHBob25peC1pbmRpYS5h cnRnc29sLmNvbS9DZXJ0RW5y
b2xsL1NJUFBIT05JWC5jcmwwEAYJKwYBBAGCNxUB BAMCAQAwDQYJKoZIhvcNAQE
FBQADggEBAHua4/pwvSZ48MNnZKdsW9hvuTV4jwtGErgc16bOR0Z1urRFIFr2NCP
yzZboTb+ZllkQPDMRPBoBwOVr7BciVyoTo7AKFheqYm9asXL18A6XpK/WqLjlCcX
rdzF8ot0o+dK05sd9ZG7hRckRhFPwwj5Z7z0Vsd/jcO51QjpS4rzMZZXK2FnRvng
d5xmp4U+yJtPyr8g4DyAP2/UeSKe0SEYoTV5x5FpdyF4veZneB7+ZfFntWFf4xwi
obf+UvW47W6pCj5nGLMBzOiaxeQ8pre+yjipL2ucWK4ynOfKzz4XlkfktITDSogQ
A1AS1quQVbKTKk+qLGD6Ml2P0LrcKQkk=
-----END CERTIFICATE-----
Certificate info
****************************************
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03
Do you want to continue to import this certificate, additional validation will be perfom?
[y/n]: y
democusp48(config)#
```

Step 4 Import the signed certificate into CUSP by running **crypto key import cer label <key-label> url terminal**.

Example

```
democusp48(config)# crypto key import cer label cusp48-ca terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIFITCCBAmgAwIBAgIKGI1fqgAAAAAAEDAN
BgkqhkiG9w0BAQUFADBCMRMwEQYK CZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZ
PyLGQBGRYHQVJUR1NPTDESMBAGA1UE AxMJU0lQUEhPTklYMB4XDTA4MTIwOTA5M
DExOVoXDTA5MTIwOTA5MTExOVowYTEL MAkGA1UEBhMCJycxCzAJBgNVBAgTAicn
MQswCQYDVQQHEwInJzELMAkGA1UEChMC JycxCzAJBgNVBAsTAicnMR4wHAYDVQQ
DExVTT0xURVNUQ0MuYXJ0Z3NvbC5jb20w gZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAOZz88nK51bJYjWgvuv4Wx1CGxTN YWGyNg+vDyQgKBXlL7b1CqBx1Yjl4
eetO4LiKkW/y4jSv3nCxCAdOrMvVF5lxFmY baMlR1R/qMCLzAMvmsWlH6VY4rcf
FGkjed3zCcI6BJ6fG9H9dt1J+47iM7SdZYz/ NrEqDnrpoHaUxdzlAgMBAAGjggJ
8MIICeDAdBgNVHQ4EFgQUYXLxMfiZJP29UZ3w Mpj0e79sk4EwHwYDVR0jBBgwFo
AUd/ZwpPhY0bgG1hKH+Z2v/kn+fEkwggEOBgNV HR8EggEFMIIBATCB/qCB+6CB+
IaBuGxkYXA6Ly8vQ049U0lQUEhPTklYLENOPVNJ UFBIT05JWC1JTkRJQSxDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMs Q049U2VydmljZXMsQ049Q29
uZmlndXJhdGlvbixEQz1BUlRHU09MLERDPWNvbT9j ZXJ0aWZpY2F0ZVJldm9jYX
Rpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz dHJpYnV0aW9uUG9pbnSGO
2h0dHA6Ly9zaXBwaG9uaXgtaW5kaWEuYXJ0Z3NvbC5j b20vQ2VydEVucm9sbC9T
SVBQSE9OSVguY3JsMIIBIgYIKwYBBQUHAQEEggEUMIIB EDCBqAYIKwYBBQUHMAK
GgZtsZGFwOi8vL0NOPVNJUFBIT05JWCxDTj1BSUEsQ049 UHVibGljJTIwS2V5JT
IwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJh dGlvbixEQz1BUlRHU
09MLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0 Q2xhc3M9Y2VydGlm
aWNhdGlvbkF1dGhvcml0eTBjBggrBgEFBQcwAoZXaHR0cDov L3NpcHBob25peC1
pbmRpYS5hcnRnc29sLmNvbS9DZXJ0RW5yb2xsL1NJUFBIT05J WC1JTkRJQS5BUl
RHU09MLmNvbV9TSVBQSE9OSVguY3J0MA0GCSqGSIb3DQEBBQUA A4IBAQAXm0MPu
eXcMYxQhVlPR/Yaxw0n2epeNRwsPP31Pr9Ak3SYSzhoMRVadJ3z K2gt4qiVV8wL
tzTO2o70JXKx+0keZdOX/DQQndxBkiBKqdJ2Qvipv8Z8k3pza3lN jANnYw6FL3/
Yvh+vWCLygEHfrUfKj/7H8GaXQVapj2mDs79/zgoSyIlo+STmwFWT GQy6iFO+pv
vMcyfjjv2dsuwt1Ml0nlict0LtkIKnRGLqnkA6sJo1P6kE+WK7n3P2 yho/Lg98q
vWl+1FRC18DrkUhpNiKXsP1ld9TcJGrdJP9zG7lI5Mf3Q/2NIAx2JZd ZVAsXZMN
smOsOrgXzkcU/xU3BXkX -----END CERTIFICATE-----  Import succeeded
democusp48(config)#exit
democusp48#
```

Step 5 You can list the certificates by running **show crypto key all**.

Example

```
democusp48# sh crypto key all
Label name: rootca
Entry type: Trusted Certificate Entry
Creation date: Sat Jul 01 14:13:14 GMT+05:30 2017
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Valid from: Wed Mar 22 14:23:10 GMT+05:30 2017 until: Tue Mar 22 14:33:09 GMT+0
5:30 2022
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03

Label name: cusp48-ca
Entry type: Key Entry
Creation date: Tue Jul 04 10:47:40 GMT+05:30 2017
Owner: CN=democusp48.cvpvb.cisco.com, OU='', O='', L='', ST='', C=''
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
SubjectAltName: DNS:democusp48.cvpvb.cisco.com
Valid from: Tue Jul 04 10:41:56 GMT+05:30 2017 until: Thu Jul 04 10:41:56 GMT+0
5:30 2019
Certificate fingerprint (MD5): 91:ED:83:CA:3B:37:16:E8:AB:07:EA:85:04:1A:D1:05
```

Configurable HTTP Security Headers

Tomcat Level Configuration

You can configure standard HTTP(S) security headers like Strict-Transport-Security, X-XSS-Protection, X-FRAME-OPTIONS, X-Content-Type-Options in CVP to protect from typical attack vectors like MITM (Man-In-The-Middle) attacks, XSS (Cross-Site Scripting), Clickjacking, and MIME-sniffing.

You can configure any of the standard HTTP(S) security headers to include with every response at a blanket level for all apps via the Tomcat-level web.xml file in the `$CATALINA_HOME/conf` folder. For more information, refer https://tomcat.apache.org/tomcat-9.0-doc/config/filter.html#HTTP_Header_Security_Filter

Cisco Customer Voice Portal ships with these headers enabled with standard recommended values pre-configured by default in all its Tomcat instances; Ops Console Server, Web Service Manager, VXML Server; as follows.

```
<filter>
    <filter-name>httpHeaderSecurity</filter-name>
    <filter-class>org.apache.catalina.filters.HttpHeaderSecurityFilter</filter-class>
    <async-supported>true</async-supported>
 <init-param>
  <param-name>hstsEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>hstsMaxAgeSeconds</param-name>
  <param-value>31536000</param-value>
 </init-param>
 <init-param>
  <param-name>hstsIncludeSubDomains</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>antiClickJackingEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>antiClickJackingOption</param-name>
  <param-value>SAMEORIGIN</param-value>
 </init-param>
 <init-param>
  <param-name>blockContentTypeSniffingEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
 <init-param>
  <param-name>xssProtectionEnabled</param-name>
  <param-value>true</param-value>
 </init-param>
</filter>
```

Note By default, HSTS is disabled in the VXML Server Tomcat instance because using HTTPS impacts the performance. You can enable it by uncommenting the documented section of the Tomcat instance's web.xml.

For protocol redirection from HTTP to HTTPS, perform the following steps:

1. Test the HTTP and HTTPS connectors, and make sure that you can access your web application via both connectors before you proceed.
2. Edit the `<tomcat_root_dir>/conf/web.xml` file (where, <tomcat_root_dir> is the base directory of Tomcat, for example: `C:/Cisco/CVP/OPSConsoleServer/Tomcat`) and add the following in the <web-app> container element:

```
<!-- Requires HTTPS for everything except /img (favicon) and /css. -->
<security-constraint>
 <web-resource-collection>
  <web-resource-name>HTTPSOnly</web-resource-name>
  <url-pattern>/</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
  <transport-guarantee>CONFIDENTIAL</transport-guarantee>
 </user-data-constraint>
</security-constraint>
<security-constraint>
 <web-resource-collection>
    <web-resource-name>HTTPSOrHTTP</web-resource-name>
    <url-pattern>.ico</url-pattern>
    <url-pattern>/img/</url-pattern>
    <url-pattern>/css/</url-pattern>
 </web-resource-collection>
 <user-data-constraint>
  <transport-guarantee>NONE</transport-guarantee>
 </user-data-constraint>
</security-constraint>
```

Note This configuration can be done at the container level (recommended) or application level, as per your preference. For application level, add it to the web.xml file in the WEB-INF folder of the web application. For example: `C:\Cisco\CVP\OPSConsoleServer\Tomcat\webapps\oamp\WEB-INF\web.xml`

3. Restart the web application server (or Tomcat).

Note The above configuration declares that the entire web application is for HTTPS only, and the container intercepts HTTP requests and redirect them to the equivalent https:// URL.

Application Level Configuration

You can enable application-level filters at application-level web.xml in the `$CATALINA_HOME/webapps/<app_name>/WEB-INF` folder. You can use the filters to override the configuration made in Tomcat container level web.xml or to set some application-specific behaviours.

Tomcat instances in CVP are shipped with an application-level filter to enable the Content-Security-Policy header for XSS protection. They are pre-configured with following standard values:

The application-level filter internally checks the HTML/JS encoding.

Another application-level filter in OAMP allows customization of X-Frame-Options value if required.

```
<filter>
    <filter-name>XSSFilter</filter-name>
    <filter-class>com.cisco.cvp.filter.XSSFilterCommon</filter-class>
    <init-param>
        <param-name>mode</param-name>
       <param-value>frame-ancestors 'self'; default-src 'self'; script-src * 'unsafe-inline'
 'unsafe-eval'; style-src * 'unsafe-inline'; img-src * data: 'unsafe-inline'; font-src *
data:;</param-value>
    </init-param>
</filter>
```

You can customize the param-value as per your security preferences/standards/deployment. If param-value is left blank, the default value is used.

For more information, refer https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

XSS Protection - Query Parameter Validation

As part of measures to protect CVP from XSS (Cross-Site Scripting) attacks, the following Tomcat filter helps to validate/sanitize all query parameters in REST/HTTP(S) requests in a standard, generic, and configurable manner.

The Parameter Validation Filter (PVF) provided by OWASP (Open Web Application Security Project) is available for web applications hosted on Web Services Manager.

The filter definition for each web application is present in the `WEB-INF/web.xml` file, and the filter's configuration file is `WEB-INF/xml/pvf.xml`.

For more information on how the filter can be customized or enabled/disabled as required per web application, see https://www.owasp.org/index.php/Parameter_Validation_Filter.

Configuration for Ghostcat Vulnerability

To fix the Apache Tomcat AJP Local File Inclusion vulnerability (Ghostcat), configuration changes need to be done in OAMP and VXML server.

OAMP

Procedure

Step 1 Go to `C:\Cisco\CVP\OPSConsoleServer\Tomcat\conf\server.xml`.

Step 2 Update the following line as highlighted and save the file:

```
Connector enableLookups="false" port="9009" protocol="AJP/1.3" redirectPort="9443"
address="127.0.0.1"
```

Step 3 Go to `C:\Cisco\CVP\wsm\Server\Tomcat\conf\server.xml`.

Step 4 Update the following line as highlighted and save the file:

```
Connector port="8101" protocol="AJP/1.3" redirectPort="8443" address="127.0.0.1"
```

Step 5 Restart the Web Services Manager and Operations Console services.

VXML Server

Procedure

Step 1 Go to `C:\Cisco\CVP\VXMLServer\Tomcat\conf\server.xml`.

Step 2 Update the following line as highlighted and save the file:

```
Connector enableLookups="false" port="7009" protocol="AJP/1.3" redirectPort="7443"
address="127.0.0.1"
```

Step 3 Go to `C:\Cisco\CVP\wsm\Server\Tomcat\conf\server.xml`.

Step 4 Update the following line as highlighted and save the file:

```
Connector port="8101" protocol="AJP/1.3" redirectPort="8443" address="127.0.0.1"
```

Step 5 Restart the Web Services Manager and VXML services.

Generate CVP ECDSA Certificate with OpenSSL

Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of Digital Signature Algorithm which can be enabled in CVP and VVB.

CVP supports either ECDSA or RSA. RSA will continue to be used as the default cryptography algorithm. However, based on the requirements we can enable and disable ECDSA.

For disabling ECDSA, you have to delete the existing ECDSA aliases and generate RSA certificates again.

Note Use the CVP keystore password when prompted for *Export Password*, *Destination Keystore Password* or *Source Keystore Password*.

Before you begin

Follow the below steps before you generate the ECDSA Certificate with OpenSSL.

Procedure

Step 1 Install the latest ES patch from https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/customer_voice_portal/ES_MR/ES/ccvp_b_ccvp-eng-es-spl.html.

Step 2 Update OpenJDK to the 8u342 version or higher. For detailed steps, see Java Runtime Environment Minor Update, on page 489.

Step 3 Go to `C:\Cisco\CVP\conf\security` and take a backup of the existing `.keystore` file.

Step 4 For enabling ECDSA, add the ciphers through OAMP. Go to **OAMP** > **Device Management** > **Unified CVP Call Server**. Select the Call Server. Go to **SIP** > **Advanced Configurations** > **Security Proprieties**. Add the following ciphers here:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Step 5 Add the above ciphers in VXML server, OAMP, and WSM Tomcat in `server.xml` files and restart the services.

For example, for adding the ciphers in VXML server, go to `C:\Cisco\CVP\VXMLServer\Tomcat\conf\server.xml` and add the ciphers within the `Connector` tag:

```
<Connector SSLEnabled="true" acceptCount="1500"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256" clientAuth="false"
disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="vxml_certificate" keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="<pass>" keystoreType="JCEKS" maxHttpHeaderSize="8192" port="7443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslImplementationName="org.apache.tomcat.util.net.jsse.JSSEImplementation" sslProtocol="TLS"
 sslEnabledProtocols="TLSv1.2"/>
```

Self-Signed Certificates

Follow this procedure to generate self-signed ECDSA certificates for Call server, VXML server, WSM server, and OAMP server to be used in CVP.

On Call Server

Procedure

Step 1 Log into the Call Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Download OpenSSL (64 bit) and install on your CVP machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys for Call server, VXML server, and WSM server respectively:

Call server:

```
openssl ecparam -name prime256v1 -genkey -noout -out callserver-private-key.pem
```

VXML server:

```
openssl ecparam -name prime256v1 -genkey -noout -out vxml-private-key.pem
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
```

Step 6 Run the following commands to generate the self-signed certificates for Call server, VXML server, and WSM server:

Call server:

```
openssl req -new -key callserver-private-key.pem  -x509 -nodes -days 365
 -out callserver-cert.pem
```

VXML server:

```
openssl req -new -key vxml-private-key.pem  -x509 -nodes -days 365
 -out vxml-cert.pem
```

WSM server:

```
openssl req -new -key wsm-private-key.pem  -x509 -nodes -days 365
 -out wsm-cert.pem
```

Step 7 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 8 Run the following commands to append the keys and certificates in one file:

```
cat callserver-private-key.pem callserver-cert.pem > callserver-certificate-private.pem
cat vxml-private-key.pem vxml-cert.pem > vxml-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 9 Run the following commands to export the certificates to the Call server:

```
openssl pkcs12 -export -inkey callserver-private-key.pem -in
callserver-certificate-private.pem -out cert_callserver.p12 -name callserver_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey vxml-private-key.pem -in vxml-certificate-private.pem -out
cert_vxml.p12 -name vxml_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 10 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for Call server, VXML server, and WSM servers:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
callserver-certificate -storepass <CVP keystore password>
```

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
vxml_certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 11 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_callserver.p12
-srcstoretype PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias
callserver_certificate
Importing keystore cert_callserver.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_vxml.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias vxml_certificate
Importing keystore cert_vxml.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 12 Restart the Call server, VXML server, and WSM services from Windows services.

Step 13 In new browser tabs, type the following and check the certificates:

```
https://<callserver ip>:8443
https://<vxmlserver ip>:7443
https://<wsm ip>:8111
```

What to do next

Generate ECDSA certificates on the OAMP server.

On OAMP Server

Procedure

Step 1 Log into the OAMP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Install OpenSSL (64 bit) on your machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys for the OAMP server and WSM server respectively:

OAMP server:

```
openssl ecparam -name prime256v1 -genkey -noout -out oamp-private-key.pem
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
```

Step 6 Run the following commands to generate the self-signed certificates for OAMP server and WSM server:

OAMP server:

```
openssl req -new -key oamp-private-key.pem  -x509 -nodes -days 365 -out oamp-cert.pem
```

WSM server:

```
openssl req -new -key wsm-private-key.pem  -x509 -nodes -days 365 -out wsm-cert.pem
```

Step 7 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 8 Run the following commands to append the keys and certificates in one file:

```
cat oamp-private-key.pem oamp-cert.pem > oamp-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 9 Run the following commands to export the certificates to the OAMP server:

```
openssl pkcs12 -export -inkey oamp-private-key.pem -in oamp-certificate-private.pem -out
cert_oamp.p12 -name oamp_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 10 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for OAMP server and WSM server:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
oamp_certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 11 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_oamp.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias oamp_certificate
Importing keystore cert_oamp.p12 to .keystore...
Enter destination keystore password:
```

```
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 12 Restart the OAMP and WSM servers from Windows services.

Step 13 In new browser tabs, type the following and check the certificates:

```
https://<wsm ip>:8111
https://<oamp ip>:9443
```

What to do next

Generate ECDSA certificates on the Reporting server.

On Reporting Server

Procedure

Step 1 Log into the Reporting Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Install OpenSSL (64 bit) on your machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys for the Call server and WSM server:

Call server:

```
openssl ecparam -name prime256v1 -genkey -noout -out callserver-private-key.pem
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
```

Step 6 Run the following commands to generate the self-signed certificates for Call server and WSM server:

Call server:

```
openssl req -new -key callserver-private-key.pem  -x509 -nodes -days 365 -out
callserver-cert.pem
```

WSM server:

```
openssl req -new -key wsm-private-key.pem  -x509 -nodes -days 365 -out wsm-cert.pem
```

Step 7 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 8 Run the following commands to append the keys and certificates in one file:

```
cat callserver-private-key.pem callserver-cert.pem > callserver-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 9 Run the following commands to export the certificates to the Reporting server:

```
openssl pkcs12 -export -inkey callserver-private-key.pem -in
callserver-certificate-private.pem -out callserver-cert.p12 -name callserver_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 10 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for the Call server and WSM server:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
callserver-certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 11 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore callserver-cert.p12
-srcstoretype PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias
callserver_certificate
Importing keystore callserver-cert.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 12 Restart the Call server and WSM server from Windows services.

Step 13 In new browser tabs, type the following and check the certificates:

```
https://<callserver ip>:8443
https://<wsm ip>:8111
```

CA-Signed Certificates

Follow this procedure to generate CA-signed ECDSA certificates for Call server, VXML server, WSM server, and OAMP server to be used in CVP.

On Call Server

Procedure

Step 1 Log into the Call Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Download OpenSSL (64 bit) and install on your CVP machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys and the CSRs (for Call server, VXML server, and WSM server) respectively:

Call server:

```
openssl ecparam -name prime256v1 -genkey -noout -out callserver-private-key.pem
openssl req -new -key callserver-private-key.pem -out callserver-cert.csr -days 360
```

VXML server:

```
openssl ecparam -name prime256v1 -genkey -noout -out vxml-private-key.pem
openssl req -new -key vxml-private-key.pem -out vxml-cert.csr -days 360
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
openssl req -new -key wsm-private-key.pem -out wsm-cert.csr -days 360
```

Step 6 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

This information is incorporated in your certificate request. Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 7 Run the following commands to see the certificate requests:

```
openssl cat callserver-cert.csr
openssl cat vxml-cert.csr
openssl cat wsm-cert.csr
```

The encoded certificate request details are displayed.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBCjCBsQIBADBPMQswCQYDVQQGEwJJTjESMBAGA1UECAwJS0FSTkFUQUtBMQ0w
CwYDVQQHDARCR0xSMQ4wDAYDVQQKDAVDaXNjbzENMAsGA1UECwwEQ0NCVTBZMBMG
ByqGSM49AgEGCCqGSM49AwEHA0IABP3MPDdzf56f+9uuv6e0f7mqVuVOeM4JVaq0
B0Fx6PtKPiby3K85A36F16Ueh81Br5DUueMfnexlwl4RdIbiMn+gADAKBggqhkjO
PQQDAgNIADBFAiEA/z4mjLovTAWUzIHKm3yO5N//At9SBNoJnB8Uz5loRVUCIArL
FjU79myKyC90iJqWyL7b8xPqGrhk4pdNdGaOP/0j
-----END CERTIFICATE REQUEST-----
```

Step 8 Request for the CA-signed certificates:

a) Submit the `callserver-cert.csr`, `vxml-cert.csr`, and `wsm-cert.csr` to your CA (who can provide signed ECDSA certificates).

Note
- Details may vary from one CA to another. You can submit your request via a website, then the CA contacts you to verify your identity.
- CAs can send signed files in various formats and filenames. Typically, you receive the CA-signed files in **PEM** format.
- Request the CA for the **intermediate** certificates. One or more intermediate certificates are often, but not always, necessary to complete the chain of trust between your CA and a root CA-trusted client.

b) Wait for the CA's reply.

c) Rename the certificate files received from the CA to `callserver-cert.pem`, `vxml-cert.pem`, and `wsm-cert.pem` respectively.

Step 9 From the command prompt, run the following commands to append the keys and certificates in one file:

```
cat callserver-private-key.pem callserver-cert.pem > callserver-certificate-private.pem
cat vxml-private-key.pem vxml-cert.pem > vxml-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 10 Run the following commands to export the certificates to the Call server:

```
openssl pkcs12 -export -inkey callserver-private-key.pem -in
callserver-certificate-private.pem -out cert_callserver.p12 -name callserver_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey vxml-private-key.pem -in vxml-certificate-private.pem -out
cert_vxml.p12 -name vxml_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 11 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for Call server, VXML server, and WSM servers:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
callserver-certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
vxml_certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 12 Go to `c:\cisco\cvp\conf\security` and import the root certificate to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -keystore .keystore -storetype JCEKS -import -alias root
-trustcacerts -file <filename_of_root_cert>
```

Note Also, import the intermediate certificates shared by the CA to the keystore.

Step 13 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_callserver.p12
-srcstoretype PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias
callserver_certificate
Importing keystore cert_callserver.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_vxml.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias vxml_certificate
Importing keystore cert_vxml.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 14 Restart the Call server, VXML server, and WSM services from Windows services.

Step 15 In new browser tabs, type the following and check the certificates:

```
https://<callserver ip>:8443
https://<vxmlserver ip>:7443
https://<wsm ip>:8111
```

What to do next

Generate ECDSA certificates on the OAMP server.

On OAMP Server

Procedure

Step 1 Log into the OAMP Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Download OpenSSL (64 bit) and install on your machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys and the CSRs (for the OAMP server and WSM server) respectively:

OAMP server:

```
openssl ecparam -name prime256v1 -genkey -noout -out oamp-private-key.pem
openssl req -new -key oamp-private-key.pem -out oamp-cert.csr -days 360
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
openssl req -new -key wsm-private-key.pem -out wsm-cert.csr -days 360
```

Step 6 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

This information is incorporated in your certificate request. Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 7 Run the following commands to see the certificate requests:

```
openssl cat oamp-cert.csr
openssl cat wsm-cert.csr
```

The encoded certificate request details are displayed.

Step 8 Request for the CA-signed certificates:

a) Submit the `oamp-cert.csr` and `wsm-cert.csr` files to your CA (who can provide signed ECDSA certificates).

Note
- Details may vary from one CA to another. You can submit your request via a website, then the CA contacts you to verify your identity.
- CAs can send signed files in various formats and filenames. Typically, you receive the CA-signed files in **PEM** format.
- Request the CA for the **intermediate** certificates. One or more intermediate certificates are often, but not always, necessary to complete the chain of trust between your CA and a root CA-trusted client.

b) Wait for the CA's reply.
c) Rename the certificate files received from the CA to `oamp-cert.pem` and `wsm-cert.pem` respectively.

Step 9 From the command prompt, run the following commands to append the keys and certificates in one file:

```
cat oamp-private-key.pem oamp-cert.pem > oamp-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 10 Run the following commands to export the certificates to the OAMP server:

```
openssl pkcs12 -export -inkey oamp-private-key.pem -in oamp-certificate-private.pem -out
cert_oamp.p12 -name oamp_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 11 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for OAMP server and WSM server:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
oamp_certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 12 Go to `c:\cisco\cvp\conf\security` and import the root certificate to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -keystore .keystore -storetype JCEKS -import -alias root
-trustcacerts -file <filename_of_root_cert>
```

Note Also, import the intermediate certificates shared by the CA to the keystore.

Step 13 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_oamp.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias oamp_certificate
Importing keystore cert_oamp.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 14 Restart the OAMP and WSM servers from Windows services.

Step 15 In new browser tabs, type the following and check the certificates:

```
https://<wsm ip>:8111
https://<oamp ip>:9443
```

What to do next

Generate ECDSA certificates on the Reporting server.

On Reporting Server

Procedure

Step 1 Log into the Reporting Server. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Step 2 Download OpenSSL (64 bit) and install on your machine.

Step 3 Add OpenSSL bin path to the Windows environment path variable.

Example: `path=C:\Program Files\OpenSSL-Win64\bin`

Step 4 Go to `C:\Cisco\CVP\conf\security`.

Step 5 From the command prompt, run the following commands to generate the private keys and the CSRs for the Call server and WSM server:

Call server:

```
openssl ecparam -name prime256v1 -genkey -noout -out callserver-private-key.pem
openssl req -new -key callserver-private-key.pem -out callserver-cert.csr -days 360
```

WSM server:

```
openssl ecparam -name prime256v1 -genkey -noout -out wsm-private-key.pem
openssl req -new -key wsm-private-key.pem -out wsm-cert.csr -days 360
```

Step 6 Enter the values for the following fields when prompted:

```
Country Name (2 letter code) []:<>
State or Province Name (full name) []:<>
Locality Name (eg, city) []:<>
Organization Name (eg, company) []:<>
Organizational Unit Name (eg, section) []:<>
Common Name (eg, server FQDN or your name) []:.
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:.
```

This information is incorporated in your certificate request. Some fields (*Common Name*, *Email Address*, *A challenge password*, and *An optional company name*) can be left blank by entering a period (.). The certificate is generated after all the details are entered.

Step 7 Run the following commands to see the certificate requests:

```
openssl cat callserver-cert.csr
openssl cat wsm-cert.csr
```

The encoded certificate request details are displayed.

Step 8 Request for the CA-signed certificates:

a) Submit the `callserver-cert.csr` and `wsm-cert.csr` files to your CA (who can provide signed ECDSA certificates).

Note
- Details may vary from one CA to another. You can submit your request via a website, then the CA contacts you to verify your identity.
- CAs can send signed files in various formats and filenames. Typically, you receive the CA-signed files in **PEM** format.
- Request the CA for the **intermediate** certificates. One or more intermediate certificates are often, but not always, necessary to complete the chain of trust between your CA and a root CA-trusted client.

b) Wait for the CA's reply.

c) Rename the certificate files received from the CA to `callserver-cert.pem` and `wsm-cert.pem` respectively.

Step 9 From the command prompt, run the following commands to append the keys and certificates in one file:

```
cat callserver-private-key.pem callserver-cert.pem > callserver-certificate-private.pem
cat wsm-private-key.pem wsm-cert.pem > wsm-certificate-private.pem
```

Step 10 Run the following commands to export the certificates to the Reporting server:

```
openssl pkcs12 -export -inkey callserver-private-key.pem -in
callserver-certificate-private.pem -out callserver-cert.p12 -name callserver_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

```
openssl pkcs12 -export -inkey wsm-private-key.pem -in wsm-certificate-private.pem -out
cert_wsm.p12 -name wsm_certificate
Enter Export Password:<CVP keystore password>
Verifying - Enter Export Password:<CVP keystore password>
```

Step 11 Go to `c:\cisco\cvp\conf\security` and run the following commands to delete the existing RSA certificates for the Reporting server and WSM server:

```
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
callserver-certificate -storepass <CVP keystore password>
c:\cisco\CVP\jre\bin\keytool.exe -storetype JCEKS -keystore .keystore -delete -alias
wsm_certificate -storepass <CVP keystore password>
```

Step 12 Go to `c:\cisco\cvp\conf\security` and import the root certificate to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -keystore .keystore -storetype JCEKS -import -alias root
-trustcacerts -file <filename_of_root_cert>
```

Note Also, import the intermediate certificates shared by the CA to the keystore.

Step 13 Run the following commands to import the ECDSA certificates to the keystore:

```
c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore callserver-cert.p12
-srcstoretype PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias
callserver_certificate
Importing keystore callserver-cert.p12 to .keystore...
Enter destination keystore password:
```

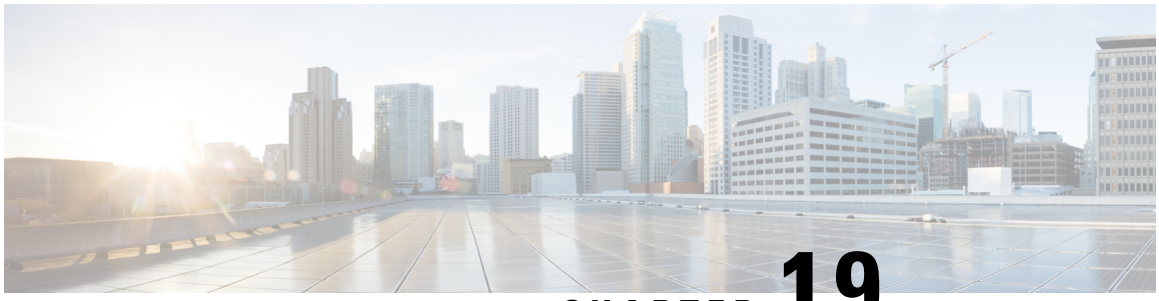
```
Enter source keystore password:
[Storing .keystore]

c:\cisco\CVP\jre\bin\keytool.exe -v -importkeystore -srckeystore cert_wsm.p12 -srcstoretype
 PKCS12 -destkeystore .keystore -deststoretype JCEKS -alias wsm_certificate
Importing keystore cert_wsm.p12 to .keystore...
Enter destination keystore password:
Enter source keystore password:
[Storing .keystore]
```

Step 14 Restart the Reporting and WSM servers from Windows services.

Step 15 In new browser tabs, type the following and check the certificates:

```
https://<callserver ip>:8443
https://<wsm ip>:8111
```



CHAPTER 19

Unified ICME Warm Consult Transfer/Conference

When an agent attempts a warm consultative transfer/conference to another agent, but there is no agent available in the skill group to service the request, the first agent is placed in a queue to wait for the availability of an agent in the desired skill group. To place the first agent in queue, a call is initiated from Unified CM to Unified Customer Voice Portal (CVP), via a Translation Route to VRU, to provide queue music to the first agent. To Unified CVP, this appears as a new call from an IP phone.

Optionally, customer business call flows may require that IP phone users call Unified CVP directly. For example, you may have a corporate IP phone network that is serviced by a Unified CVP help desk call center. IP phone users with problems would call a Unified CVP number to open trouble tickets.

This chapter provides information about the minimal software component release requirements for the Unified ICME Warm Consult Transfer and Conference to Unified CVP feature for Type 7 VRUs. Resource sizing and configuration requirements are also included.

Note For information about using the Warm Consult Transfer feature with SIP and Type 10 VRUs, see Warm Transfer with SIP Calls, on page 425. For configuration procedure of Call Director and Comprehensive call flow models using SIP, see Unified CVP Call Flow Models, on page 13.

Configure Unified ICME Warm Consult Transfer/Conference to Unified CVP

Procedure

Step 1 Install a new Call Server (see *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* for detailed information).

Note It can be configured identically to all other Unified CVP machines, with the exception that you must add each Translation Route DNIS.

- Define it as a Type 7 VRU in the Network VRU Explorer tool in Unified ICME.
- **Network Transfer Preferred** must be disabled for this peripheral.
- Add a new DNIS in the **Add DNIS** box on the ICM tab in the Operations Console. Ensure to add each translation route DNIS.

Step 2 If the Unified CVP machine resides in a different location from the Unified CM cluster initiating the calls, WAN bandwidth is a consideration because the prompts are played G.711 from the Unified CVP machine. In this case, size and configure the network appropriately. Wherever possible, Unified CVP should be co-located with Unified CM to eliminate these bandwidth requirements.

Step 3 Define a SIP trunk in the Unified CM, using the Unified CVP machine IP address as the Destination address in **Device** > **Trunk** > **SIP Information**.

Step 4 (Perform this step for IP-originated calls only). Determine if customer business call flows require that IP phone users call Unified CVP directly. In Unified CM administration, in "Route Plan" using route groups/lists/patterns, route Unified CVP DNIS's to the Unified CVP gateway installed in Step 1.

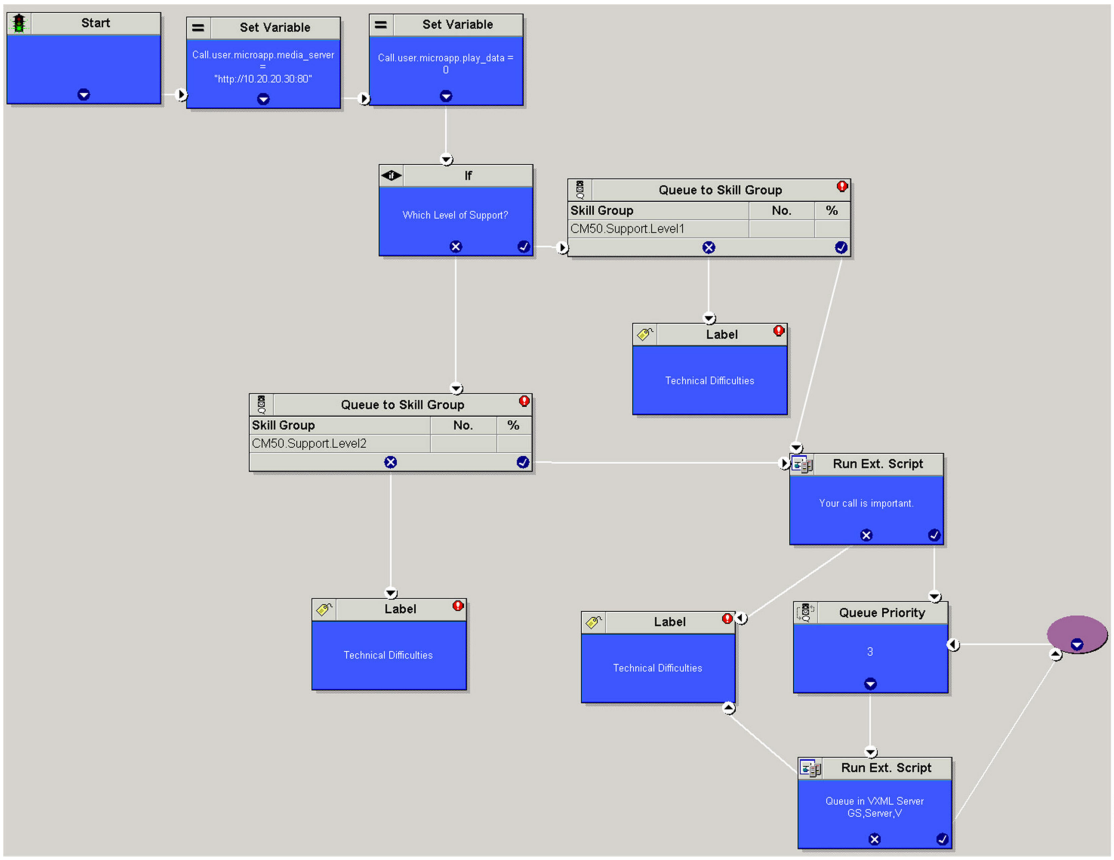
If you want to load-balance between two Unified CVP systems:

- Create a route group and put both of the Unified CVP gateways in the route group, both with order priority 1.
- Create a route list and put the route group in the route list.
- Create a route pattern and assign the route list to the route pattern.
- In Service Parameters for Unified CM, set **Reorder Route List** to **True** and the **H225 TCP timer** to **5**.

Note The Reorder Route List setting applies only for Unified CM 3.3 and earlier.

Step 5 Create a Unified ICME script similar to the script below. (See the Unified ICME documentation for details). This script should be tied to the Dialed number and call type that the agent invokes to do a warm consultative transfer/conference. This dialed number's Routing Client should be associated with a Unified CM peripheral from which the agent will be invoking the transfer or conference.

Figure 17: Unified ICME Script



Minimal Component Version Requirement

See the https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html for the list of component versions that are required to use the Unified ICME Warm Consult Transfer and Conference to Unified CVP feature.

Warm Transfer with SIP Calls

If an agent performs a warm transfer to another agent and then that agent is queued, or a SendToVRU label returns to Unified CM using jtapi on the Unified CM PG connection, then you must associate a Route Pattern for that label with a SIP TRUNK to send to Unified CVP or the Proxy Server to ensure the call returns to Unified CVP. Unified CVP then sends the **request instruction** message back to Unified ICME on the Unified CVP routing client and starts the queuing.

Note These SIP calls do not require MTP enablement on the SIP trunks.

When using the Warm Transfer feature for SIP Calls with queuing, and the agent completes a consult transfer to ther caller while the call is still in the queue (VXML Gateway), then the call flow does not require MTP enabled on the SIP trunk that is associated with the VRU label route pattern.

Note The MTP is not required if VXML GW version is IOS 12.4.(15)T8 or 12.4(20)T2 or later versions on these T releases. In cases, where there is SIP DTMF capability mismatch, MTP is required between Unified Customer Voice Portal (CVP) and Cisco Unified Communications Manager (CUCM).

Set Up Unified ICME Warm Consult Transfer

Note Unified CVP with a Type 10 VRU does not support multiple Network VRUs on the same Unified CVP peripheral device. Multiple customer instances can be used in order to address multiple Network VRUs, but they must then address different physical Unified CVP Call Servers as well. Calls that originate from an ACD or Unified CM, such as Warm Transfer/Conference, Helpdesk, or Outbound calls, are also limited to one Network VRU on any given Unified CVP Call Server. Note that the reverse is supported - multiple Unified CVP Call Servers can share the same Network VRU.

In this scenario, an agent transfers a call to another agent by dialing that agent's ID. If the agent is unavailable, the originating agent is placed in a queue to wait for the second agent to pick up the call.

For the first agent to be queued while waiting for another agent, set up the following configuration:

Procedure

Step 1 In the ICM Configuration Manager's PG Explorer tool Routing Client tabs, uncheck the **NetworkTransferPreferred** check box for Unified CM and Unified CVP routing clients.

Step 2 On the **Advanced** tab for the Unified CM routing client, select **None** for the Network VRU and the Type 10 VRU for the Unified CVP routing client.

Step 3 For the Type 10 VRU, in the ICM Configuration Manager's Network VRU Explorer tool, define a label for the Unified CM routing client as well as the Unified CVP routing client, and associate them with a customer instance.

Step 4 In the ICM Configuration Manager's Dialed Number List Tool, associate the dialed numbers for the incoming call as well as the transfer dialed number with the same customer instance.

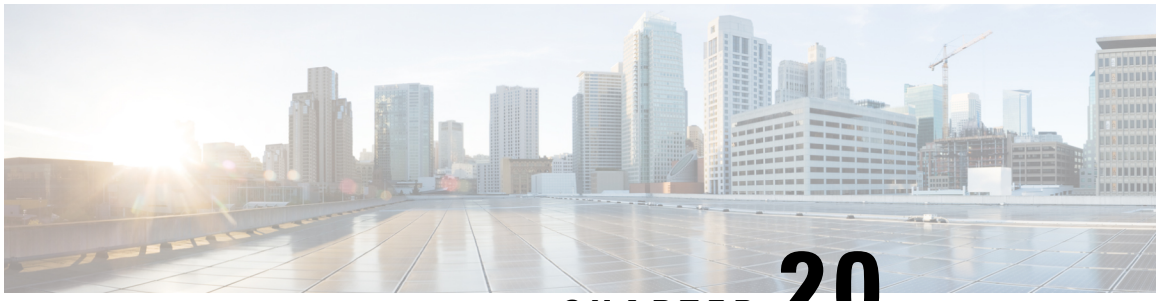
When the second call is placed for the warm transfer and no agent is available, the label defined on the Unified CM RC plus the correlation ID will be sent back via EAPIM/JGW to Unified CM. For example, if the label is 7777777777, with a correlation ID it could be 777777777712345 because the call originated from the Unified CM RC, and also because the **NetworkTransferPreferred** check box is not checked.

Step 5 In Unified CM, select **Call Routing** > **Route/Hunt** > **Route Pattern** > **Add New**. Add a new route pattern to route the call to Unified CVP using the SIP trunk if you are adding from the Device Management menu (for example, 777! where ! allows label plus arbitrary length correlation ID).

When Unified CVP sees this call, it perceives it as a pre-routed call with a correlation ID and sends it back to Unified ICME to continue the script.

Unified ICME sends a temporary connection back to Unified CVP, which queues the agent call while the caller hears music on hold (MoH) from Unified CM.

Note When customized CTI clients are used, consult transfer mechanism is utilized to check if the second agent is really answering the call before the call is being finally transferred automatically by the customized CTI client. In this scenario, it is not required for the agents transferring the call to complete the transfer manually as customized CTI client automatically transfers the calls. However, this is applicable only when the second agent (called agent) answers the call and not before. Customized clients should wait for five seconds before completing the automatic consult transfer to avoid race conditions.



CHAPTER 20

Transfer and Queue Calls with Unified CVP

IVRs From Perspective of Unified ICME

Unified ICME categorizes IVRs into one of the following two types:

- **Intelligent Peripheral IVRs** (in control of Unified ICME) - the carrier network routes calls to the IVR and then removes calls from the IVR for delivery to agents. With Intelligent Peripheral IVRs, once the prompting or queuing treatment of IVR is complete, the IVR has no further role to play for that call.
- **Service Node IVRs** (following prompting/queuing treatment) - the IVR initiates call delivery to agents, who are in control of Unified ICME. When functioning as a Service Node IVR, Unified CVP can stay involved with a call even after it is transferred to another VoIP endpoint.

Unified CVP can act as either IVR type.

Note For information about the call flow models for Unified CVP, see the chapter "Unified CVP Call Flow Models".

Call Transfer Using Unified CVP in Comprehensive Mode

This section provides examples of Unified CVP call transfer scripts.

Note The Script Editor Busy and Ring nodes are not supported.

Call Transfer Using SIP Service

You can configure the SIP Service to operate in two modes to perform Unified CVP transfers. Unified CVP remains in the signaling path for the duration of the call, and in this usual mode it uses SIP re-INVITE messages to perform the transfers. This causes Unified CVP to hold the port license for the call duration.

To operate in standard re-INVITE mode, you do not need to modify the Unified ICME script. However, to send a REFER transfer, send a dynamic label with the letters “rf” prepended to it. Or, when using a Queue node in the Unified ICME script, define an ECC variable called "user.sip.refertransfer" and set it to the value of the lowercase "y." Unified CVP then uses the REFER method to blind transfer to agent labels.

Alternatively, Unified CVP can perform a SIP REFER type transfer where it moves out of the signaling path after sending a referral to the caller to the label that Unified ICME provides. This allows Unified CVP to release the port license after the REFER is sent. Unified CVP receives notification of the outcome of the call using SIP NOTIFY messages, and this is included in the reporting database.

Note If Unified CVP is configured to redirect calls to the ingress gateway for 9292 DN and the SIP REFER type transfer fails, then the ingress gateway must be configured to handle the failure by using the survivability script or by creating a 9292 dial peer directed to VVB.

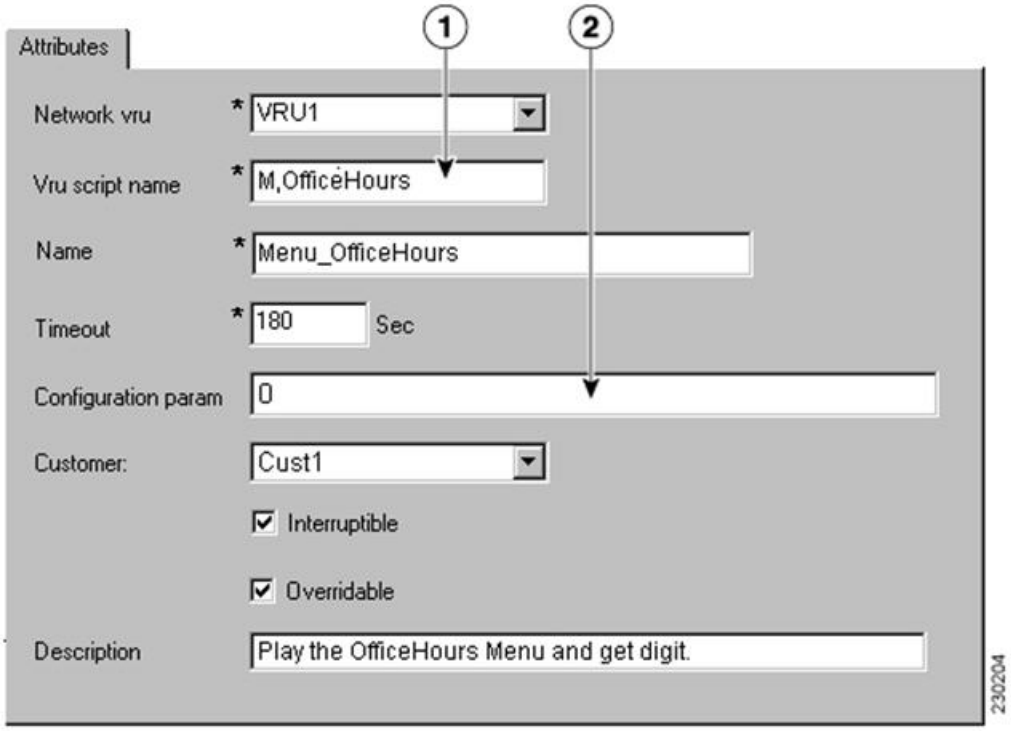
Caution When using REFER, do not apply the survivability script for TDM callers on the Ingress gateway. Also, SIP transfers to VoiceXML gateways for micro-applications do not use the REFER method. It is only used for non-"SEND TO VRU" type transfers. When using REFERs, note that the survivability script does not currently support REFER messaging events, so when using REFER with TDM calls on the IOS gateway, the survivability service must be removed from the pots dial peer for those calls. REFER is used as a "blind refer" operation and can typically be used when sending calls to third-party ACD agents. However, it can also be used to send calls to the Cisco Unified Communications Manager (Unified CM) extensions as well, if desired.

Example: Transfer Call to a Label

This example shows sample ICM Configuration Manager and Script Editor screen captures for a Menu application that plays a prompt presenting a menu ("Our office hours are between 8 AM and 6 PM. If you would like to talk to a customer service representative, press 0 at any time.") and then performs one of the following actions:

- If the caller presses 0, the system collects the digit, and then routes and queues the call.
- If the caller does not press 0, the system releases the call.

Figure 18: Call Transfer to a Label



The **Attributes** tab of the Network VRU Script List tool in the figure above shows:

1. The VRU Script Name field contains two Unified CVP parameters:

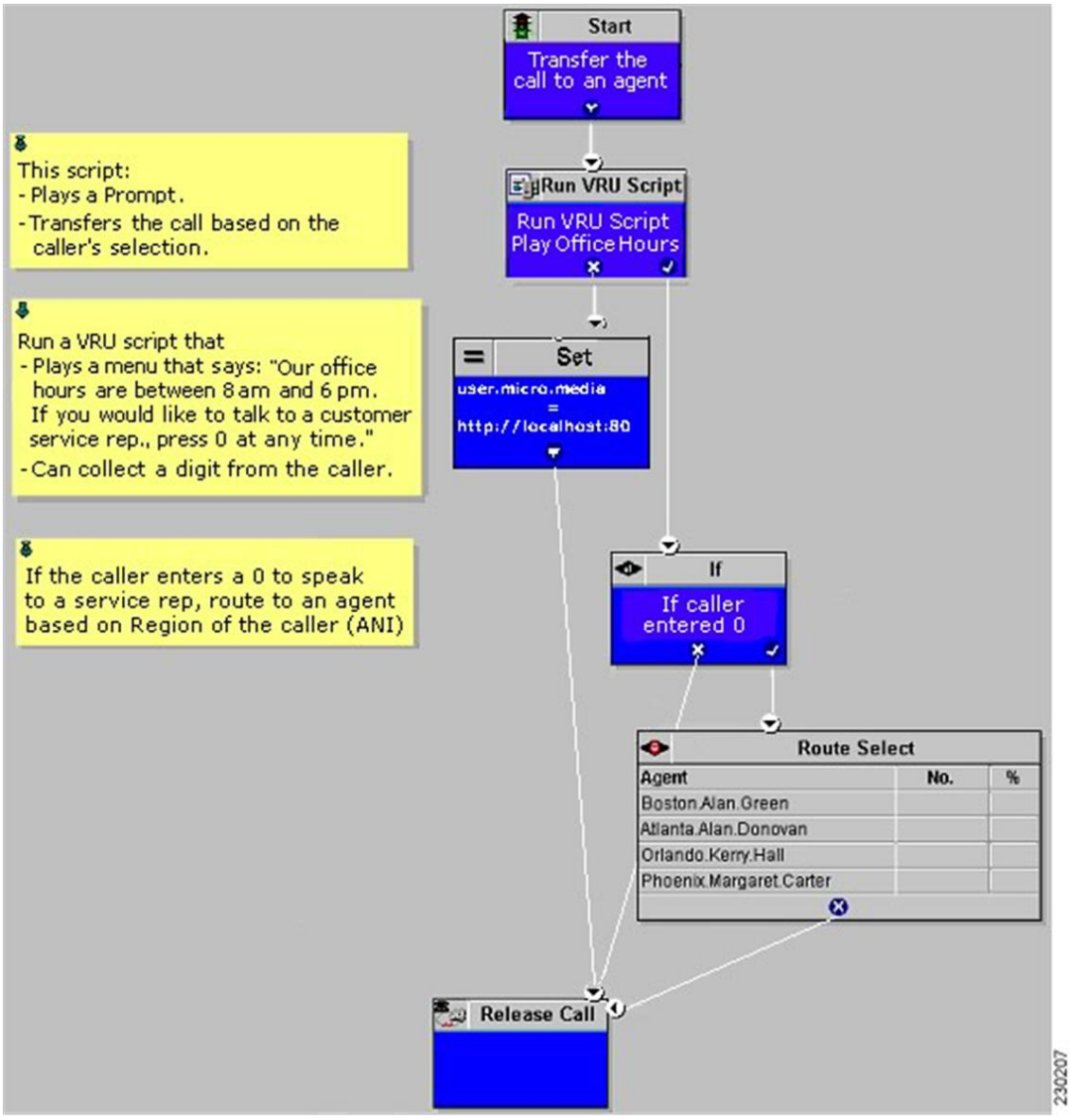
   M: Menu

   OfficeHours: Media File name

2. The Config Params field contains the following Unified CVP parameter:

   0: The number 0 is the only valid option.

Figure 19: Network VRU Script



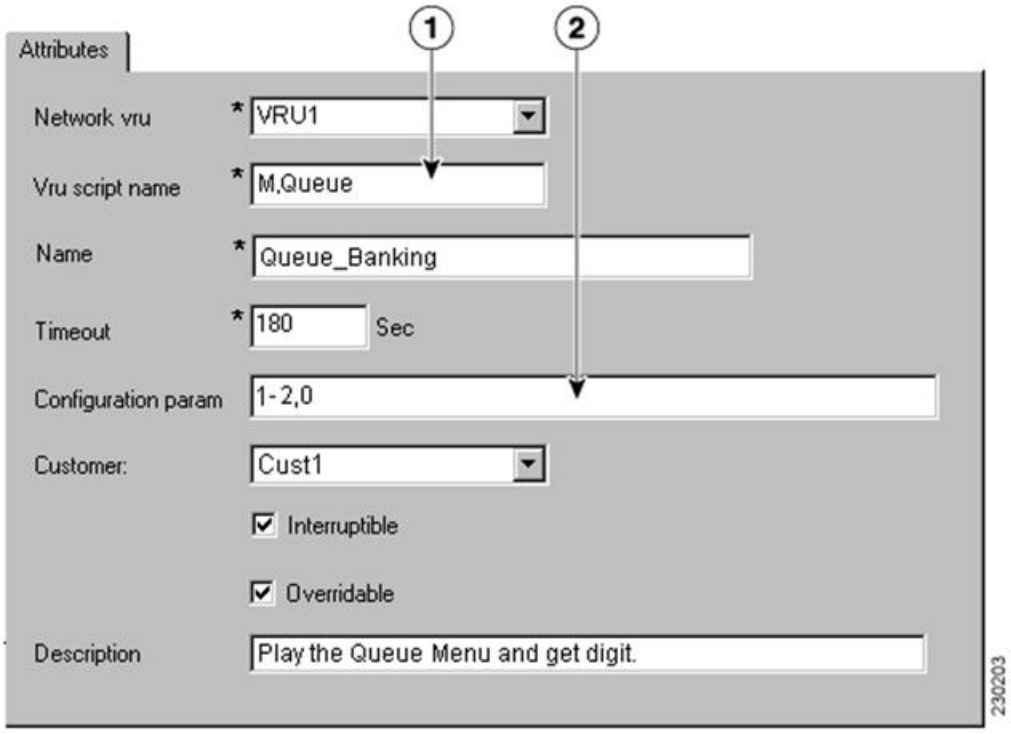
Example: Queue and Transfer Call to a Skill Group

Use Unified ICME to queue a call to an agent group and instruct Unified CVP to entertain the caller with IVR scripting using the Run VRU Script and other nodes. When the resource becomes available, Unified ICME and Unified CVP perform the following tasks:

1. Unified ICME tells Unified CVP to cancel the original request.
2. Unified CVP then confirms the cancel request.
3. Unified ICME sends the label for the destination.
4. Unified CVP or the network transfers the call to a freed-up agent.

This example shows sample ICM Configuration Manager and Script Editor screen captures for a Menu application that plays a prompt presenting a menu ("For Checking, press 1. For Savings, press 2. To speak to a customer service representative, press 0."), retrieves any caller-entered digits, and then routes and queues the call.

Figure 20: Sample ICM Configuration Manager and Script Editor Screen



The Network VRU Script List tool's Attribute tab in the figure above shows:

1. The VRU Script Name field containing two Unified CVP parameters:

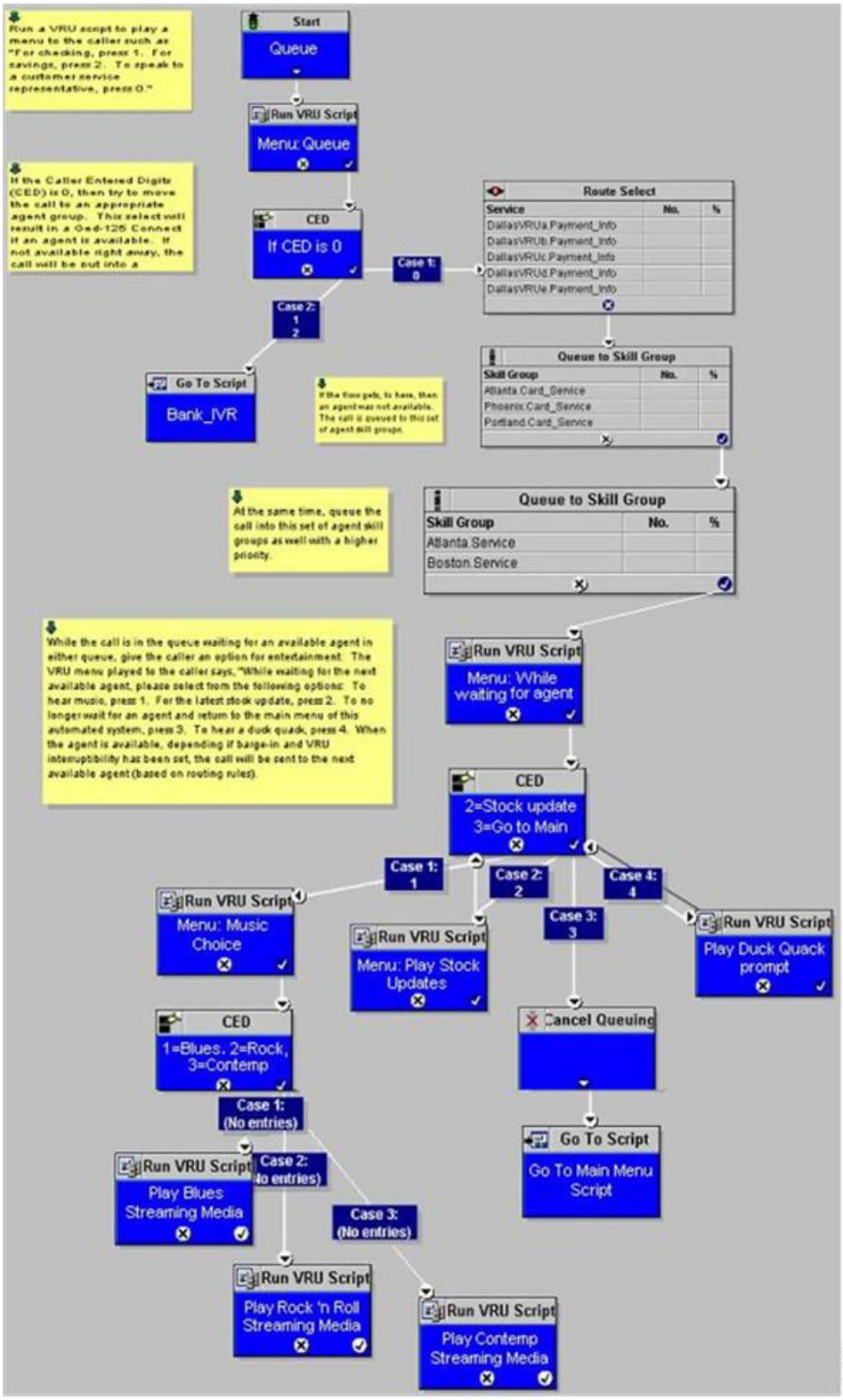
   M: Menu

   Queue: Media File name

2. The Configuration Param field containing the following Unified CVP parameters:

   1-2,0: The numbers. 1, 2, and 0 are valid options

Figure 21: Running VRU Script



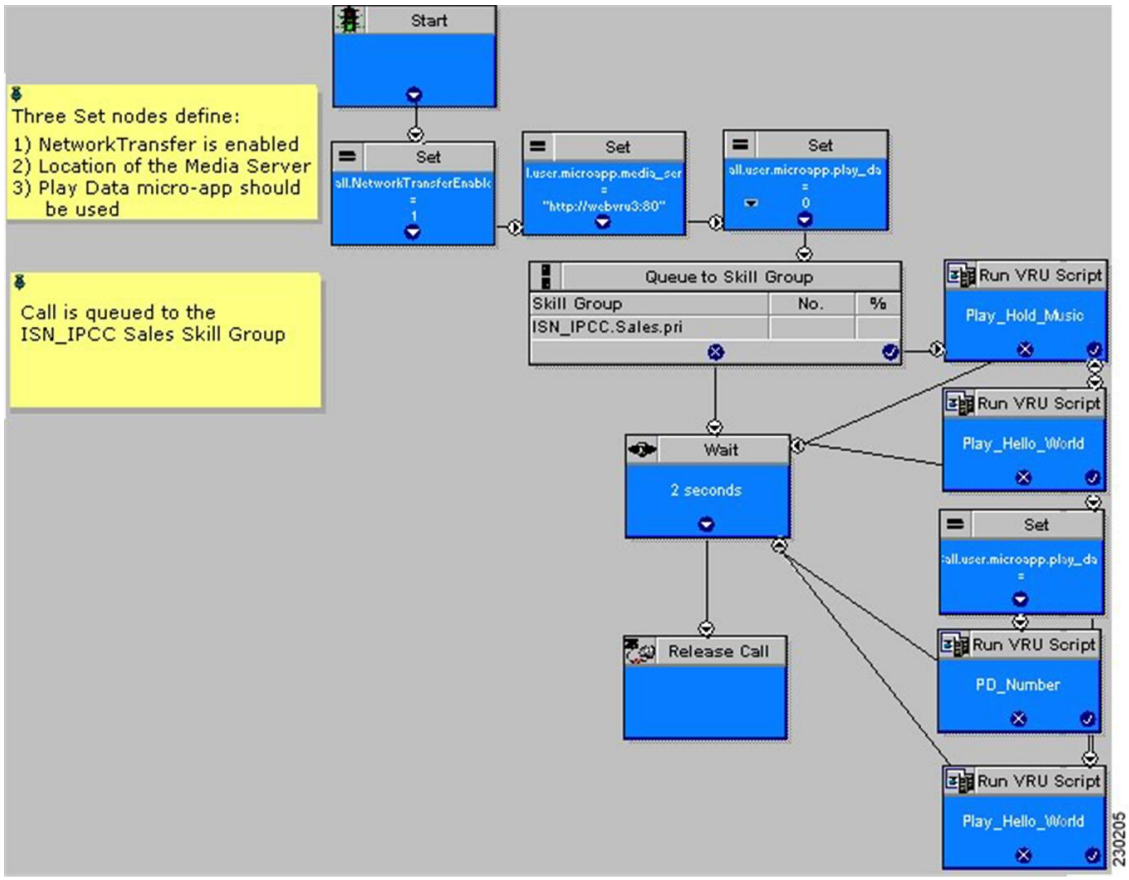
Example: Network Transfer Script

Unified CVP provides capabilities to transfer calls to another destination after they an agent answers them. These capabilities are referred to as Network Transfer. The Network Transfer feature does not require any special installation on the part of Unified CVP. By default, the feature is disabled for all PG types except Enterprise Agent (EA).

To change the Network Transfer setting, perform the following steps:

1. Use Set node of the Script Editor to specify the **Call.NetworkTransferEnabled** variable. If you set this variable to 1, Network Transfer is enabled and if you set it to 0, Network Transfer is not enabled.
2. In EA PG setups where the EA is behind a PBX, use the **Network Transfer Preferred** check box on the Routing Client tab of the PG Explorer. Network Transfer is enabled only if this check box is checked.

Figure 22: Network Transfer Setting



Call Transfer From Agent to Agent

When a call is transferred from Unified CVP to an agent, and that agent wants to transfer the call to another agent, the agent can make the transfer using either the agent IP phone or agent desktop. Transfers from the IP phone are made using CTI route points that point to a Unified ICME script. Transfers from the agent desktop are made using the Dialed Number Plan.

For network transfer from either the IP phone or CTI OS Agent Desktop, you must Queue the call to skill group in the first Unified ICME script, for example "NetXfer1", to create the call context. In this script, the "networkTransferEnabled" flag must be set to "1".

Note The **NetworkTransferEnabled** setting must explicitly be set to 1 in all postroute scripts.

Configure Network Transfer From IP Phone

Procedure

Step 1 In Unified CM, define a CTI Route Point, for example "9999." Associate it with the JTAPI user that is connected to Unified CCE PIM in Unified ICME.

Step 2 In the ICM Admin Workstation, define a Dialed Number with a call Type for Unified CCE PIM. This call type can then be associated with a Unified ICME Script, for example, "NetXfer2".

Note Avoid defining the labels of agents for the Unified CCE PIM. Define the labels for VRU PIM so that the route result is returned to VRU instead of Unified CCE PIM. If you define the agent labels for the Unified CCE PIM, the Unified ICME router returns the route result to the VRU PIM if "Network Transfer Preferred" is enabled on the Unified CCE PIM and VRU PIM and returns the route result to the Unified CCE PIM if "Network Transfer Preferred" is disabled on the Unified CCE PIM and VRU PIM.

Step 3 When the call is delivered to Agent 1 using the Unified ICME Script "NetXfer1", the agent can dial the number 9999 to send the call to another script, "NetXfer2."

Configure Network Transfer From CTI OS Agent Desktop

Procedure

Step 1 Define a Dialed Number Plan in Unified ICME.

The routing client is the Unified CCE PIM and dialed number is the one defined before for the Unified CCE PIM, that is, IPCC_PIM.9999.

Step 2 Set Post Route to **Yes** and Plan to be **international**.

Step 3 In the Agent Desk Settings, check all the **Outbound access** check boxes.

Example of IP Transfer

An IP transfer to an Unified CCE agent is very similar to an IP transfer to an ACD (TDM) agent with the following exceptions:

- The egress Gateway for this case is Unified CM.
- When Unified CM receives the new call, it uses the “Skinny protocol” to connect to the agent at an IP phone. The voice channels are then connected from the Ingress Gateway to the IP phone.

CLI Field on Outgoing Transfers

Calling Line Identification (CLI) is a set of digits and related indicators (type of number, numbering, plan identification, screening indicator, and presentation indicator) that provide numbering information related to the calling party. This feature allows customers to override the CLI field on outgoing transfers, using either a Label node or an ECC variable in the Unified ICME routing script. This feature is required for transfers into Unity, which uses both Automatic Number Identification (ANI) and Dialed Number Identification Service (DNIS) to determine the appropriate mailbox to access. CLI is passed through most networks and into most call-handling devices, so this feature provides a back-door method to transmit arbitrary data during transfers when translation routing is not feasible.

The following section describes how to enable the **call.user.microapp.override_cli** ECC variable, which you must configure to enable this feature.

Configure CLI Override

CLI override is controlled from the Unified ICME routing script.

Note For IP originated calls, you need to check the "Asserted-Identity" check box on the Unified Communications Manager, SIP Trunk configuration.

Note For SIP calls, the CLI Override feature is only supported using the ECC variable as shown in second method. Using a dynamic label as in Method #1 with "CLI" prepended is not supported.

You can configure CLI override one of following two ways:

- **First method:** Append **CLI=NNNNNNNN** to the label in a LABEL node. Setting NNNNNNNN to the word **null** will blank out the CLI on the transfer.

  Example: Setting a label node to **1111;CLI=9876543** results in a transfer to 1111 using a CLI of 9876543.

  Example: Setting a label node to **1111;CLI=null** results in a transfer to 1111 using an empty CLI.

- **Second method:**Set the **call.user.microapp.override_cli** ECC variable before invoking a transfer using Queue to Skill Group, Label node, and so on. For the **call.user.microapp.override_cli** Expanded Call Variable List, set the maximum length to the maximum length of the data that will be used for CLI override. The Unified CVP Call Server must be restarted after adding this variable to Unified ICM. Setting the variable to " " will blank out the CLI on the transfer.

  Example: Setting **call.user.microapp.override_cli** ECC variable to **9876543** prior to a Queue to SkillGroup where agent **1111** becomes available, results in a transfer to 1111 using a CLI of 9876543.

Example: Setting **call.user.microapp.override_cli=" "** ECC variable *prior* to a Queue to Skill Group where agent **1111** becomes available, results in a transfer to 1111 using an empty CLI.

If both of the methods are used in one routing script, the LABEL node CLI value takes precedence over the ECC variable.

CLI override takes precedence over the SetSetupCallingNum command in VBAdmin. That is, the new CLI is always be propagated to the transfer call leg regardless of the value of ShowSetupCallingNum.

CLI override also forces the presentationIndicator to presentationAllowed on the transfer call leg.

Note For SIP calls, the CLI Override feature is only supported using the ECC variable. Using a dynamic label with "CLI" prepended is not supported.

Unified CCE Reroute on No Answer Configuration for Unified CVP

This section describes how to use the Reroute On No Answer function when using Unified CVP as a queue point for Unified CCE.

When you use Unified CCE with Unified CVP as a queuing point and routing client, configure the Reroute On No Answer function differently than when you use it with Unified IP IVR. The difference is when you use Unified IP IVR the call control is with Unified CM, whereas with Unified CVP, the call control is with Unified CVP.

Reroute on No Answer Operation for Unified CCE with Unified IP IVR

The Reroute On No Answer function ensures that when an agent does not answer a call, the call is taken away after ringing for a configurable number of seconds and presented to another agent or put back in queue, and the agent who did not answer the call is put in "Not Ready" state. An example of an agent not answering a call is when the agent is not at the desk and the presence of agent is not changed to the "Not Ready" state.

This function is implemented by setting a Reroute On No Answer timeout in the agent desk settings. When the call has been ringing for the configured number of seconds, the Unified CM PG makes the agent unavailable and send a postroute request to Unified ICME using a dialed number that is also configured in the Agent Desk Settings. A routing script is run that determines a new destination for the call. This can be another agent, or the script can put the call back in a queue. When using Reroute On No Answer with Unified IP IVR, Unified ICME software responds back to Unified CM with the new destination for the call. Unified CM is responsible for sending the call to the right destination (IP IVR for queuing or new agent).

Reroute on No Answer Operation with Unified CVP

When you use Unified CCE with Unified CVP, Unified CM does not control the queuing platform (Unified CVP), and hence cannot send the call back to Unified CVP for requeuing. Instead, Unified CVP controls the call and needs to take action.

The solution is to use the Reroute On No Answer function only to make the agent state “Ready” or “Not_Ready” when the agent does not answer the call, and to use the ICM Router Requery function to take the call away from the non-answering agent.

Reroute on No Answer Agent Desk Settings Configuration

For Agent state to be READY after CVP RNA expires:

- In Agent Desk Settings, the Ring no answer dialed number field is set to blank.
- Enter a value in the Ring No Answer time field. Set the timeout to the maximum time you want to allow the agent to answer a call; for example, 2 rings = 8 seconds. This value must be at least 2 seconds more than the timeout configured at Unified CVP for RNATimeout.

For Agent state to be NOT_READY after CVP RNA expires:

- In Agent Desk Settings, the Ring no answer dialed number field is set to blank.
- Do not enter a value in the Ring No Answer time field.

Router Requery Configuration

Router Requery is triggered by the routing client (Unified CVP) when a No Answer timer expires (a different timer than the Reroute On No Answer timer in the Agent Desk Settings).

- The No Answer timer for Router Requery is not controlled by Unified ICME, but by the switching fabric that is Unified CVP in this case. CVP 1.0 has a fixed No Answer timer of 15 seconds. The Unified CVP SIP has a configurable No Answer timer (RNATimeout) with a default value of 15 seconds.

  When using Unified CVP, set RNATimeout to the desired number of seconds that the agent phone should ring before being taken away. In any case, this timeout **must be at least 2 seconds shorter than the Re-route On No Answer timeout** if it was set in the Agent Desk Settings.

  After the Unified CVP VB RNATimeout expires, the VB/AS/PG sends an **EventReport=NoAnswer** to the router. The router picks another target according to the routing script and sends the Connect message to Unified CVP. The target might be another agent or it might be a VRU label to requeue the call. When the call disappears from the first agent, this agent is put in "Ready" or "Not Ready" based on No Answer Timeout in the desk setting.

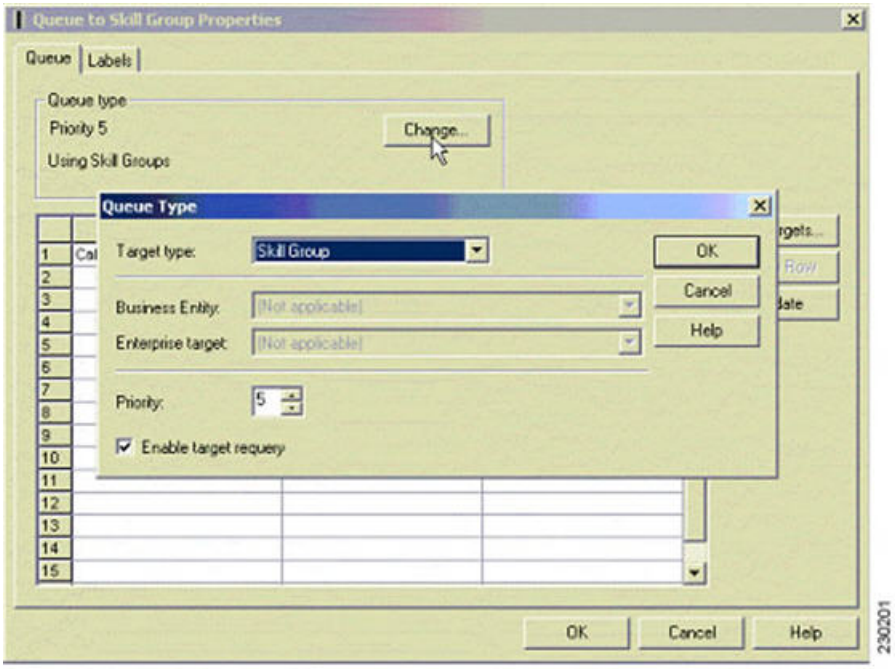
Note Do not set the No Answer DN in the desk setting, because this is a global Unified ICME setting for all scripts. The No Answer DN may not be suitable for all scripts depending on the complexity of the deployment. Instead, each script should have the X path of the queue node set appropriately for each script.

- Enable Requery on the node in the script that selects the first agent. Depending on the type of node used, the Requery mechanism selects a new target from the available agents or will require additional scripting. The Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted describes how Requery works for the different nodes.

In most cases Unified CCE uses the Queue node. The Queue node requires additional scripting to handle the requeuing of the call in front of the queue. The script example below provides a standard way of handling the requeuing of the call.

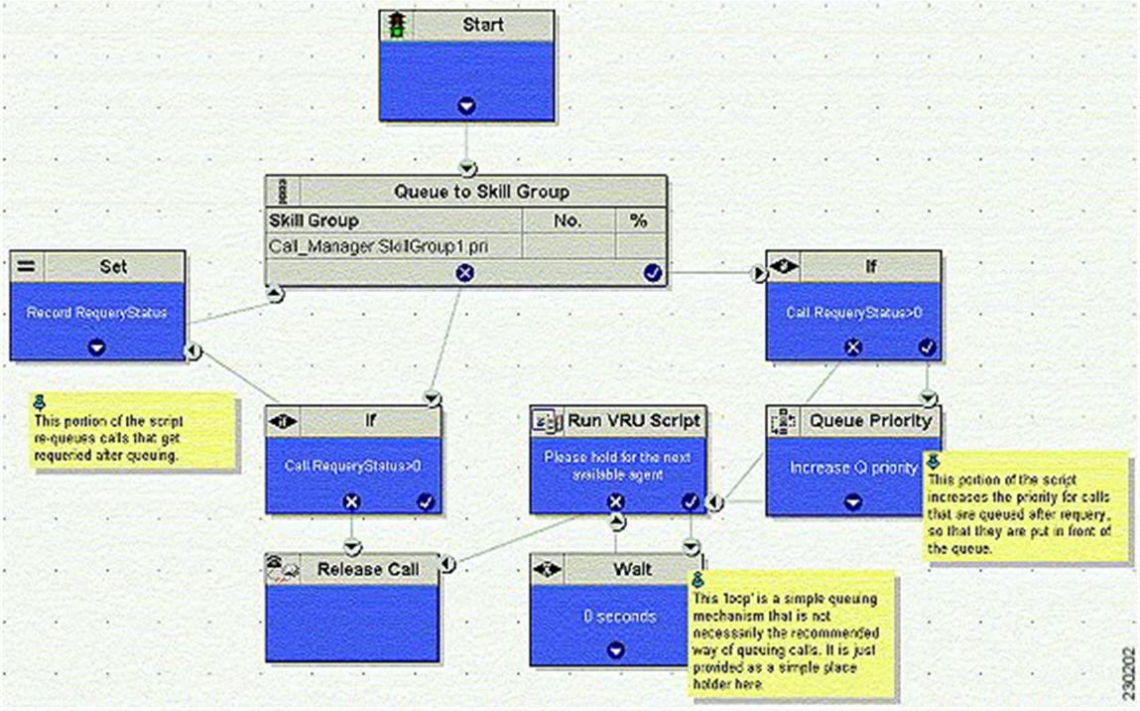
If there is an available agent, the Queue node selects the longest available agent from the skill groups. If there is no available agent, it queues the call with a priority set in the node (see the following figure) and continues down the success exit of the node. When an agent becomes available, Unified ICME always selects the longest queued call from the ones with the highest priority. When the Queue node connects the call to an agent and the agent does not answer the call, Unified CVP Ring-No-Answer timeout expires causing the Requery mechanism to start.

Figure 23: Queue to Skill Group Properties



When this happens, the script immediately continues through the failure exit of the Queue node with the Requery Status variable set to ‘No Answer’ (= 3). The typical treatment is to put the call back into the same queue but with a higher priority than all other calls, since the call needs to go in the front of the queue, not the back.

Figure 24: Requery Mechanism



In this script, when the Queue node selects an agent who does not answer the call, the script exits through the failure exit (X) of the Queue node. The If node tests the RequeryStatus variable. If it has value of greater than zero, this is a requery call, and the script requeues the call. In the preceding example, it also sets a flag using a call variable for reporting purposes. Assuming that there are no agents available, the Queue node immediately exits through the success exit (Checkmark). The node checks to see if this is a requeried call. If so, it increases the Queue Priority of the call so that it is handled before any other calls in queue. It then enters the usual wait loop with RunScripts.

The call flow is as follows:

- Script connects call to agent by sending connect message to Unified CVP (with requery enabled).
- Agent phone rings.
- After the Unified CVP VB RNATimeout expires, the VB/AS/PG sends an EventReport=No Answer to the router. The router picks another target according to the routing script and sends the Connect message to Unified CVP. The target might be another agent or it might be a VRU label to requeue the call.
- When the call disappears from the first agent, this agent is put in "Ready" or "Not Ready" state based on No Answer Timeout in the desk setting.

Limitations

The only limitation for the configuration described in this section is that each call that is redirected by this mechanism is counted twice in the Skill Group—once as redirected, and next as handled (if the call is finally handled). However, the Call Type is only count this call once. Although it is counted Handled and Requeried, Requeried is not used to balance CallsOffered in the Call Type. If you want to see this call counted twice in the Call Types, address this by changing the call type in the error path before the second queue to skill group node.

Reroute Configuration on No Answer for Unified CM with Unified CVP

In case of an agent transfer, when calls are originated from Unified CM to a CTI Route Point, routing client responsibilities should be passed back to Unified CVP as soon as possible upon entering the Unified ICM script. To ensure that Unified ICM Router directs calls to Unified CVP, include a SendtoVRU node in the Unified ICM script before any Runscript or SkillGroup node is run. When the routing script runs the SendToVRU node, the ICM Router instructs Unified CVP to become the routing client to handle for any subsequent transfers or VRU call processing.

RONA Operation to a script CTI Route Point Transfer

The "Go to Script" node is used as a RONA destination when "enable target requery" is configured on the Queue to Skill Group node and the agent does not answer. When the ICM script runs the "Go To Script" node, script proceeds to the specified script. For example, when an agent does not answer a call, the X-path out of the Queue to Skill Group Node will target a "Go To Script" node with the "CTI_Route_Point_Transfer" script specified. Script processing then continues from the beginning of the CTI_Route_Point_Transfer"script and proceeds as usual.

Following are the valid destinations out of the X-path of Queue to Skill Group node:

- Another skill group
- A prompt
- GoTo node (do not use "Dynamic Label")

Limitations

The limitation for the configuration described in this section is that the disposition of the requeried call is not correctly reported. The **Redirect No Answer** field in the agent and skill group reports do not show calls that are redirected by this mechanism. Each call that is redirected by this mechanism is counted twice—Once as abandoned, and next as handled (if the call is finally handled). There are two Unified CCE TerminationCallDetail records for this call—One for the rerouted call (with CallDisposition ‘Abandoned while Ringing’, code 3), and other for the handled call with a CallDisposition depending on how the call was finally handled. The scripting example above shows how a Peripheral Call Variable can be used to mark and count calls Requeried because of no answer. A custom reporting template can be written to report on this data.

Call Survivability

This section describes how to install and configure Unified CVP with a script that allows the gateway to transfer a call in the event of a critical Unified CVP application error or WAN failure. Place this application on the incoming pots dial-peer or the incoming VOIP dial-peer that is destined for Unified CVP. Call survivability is supported in all Unified CVP call flow models except the VRU-Only call flow model. In the Unified CVP Standalone call flow model, survivability is invoked if the gateway encounters an error from the CVP Voice Server, the "param survive" parameter is included and a survivability service is defined.

In the event of critical Unified CVP application errors or a WAN failure that would usually disconnect the caller, this script allows the gateway to attempt a transfer to some alternate location after the failure occurs instead of disconnecting the caller. In the event that the call cannot be transferred to an alternate agent, the script plays a "call-back-later" message and disconnects the call.

This script provides the following capabilities:

- Perform multiple types of transfer in call failure conditions:

- *8 transfer connect (outpulse)
- Hairpin
- SRST
- Hookflash Relay
- Two B-Channel Transfer (TBCT)

- Differentiate call recovery behavior by incoming DNIS.
- Differentiate call recovery behavior by incoming DNIS and how long the call had been in Unified CVP prior to failure.
- Differentiate call recovery behavior based on time of day and date.
- Hand off to an auto-attendant type application in the event of some downstream failure (for example, WAN failure, Unified ICME failure, Unified CVP failure). This auto-attendant functionality can be BACD of CME, a Unified CVP Standalone call flow model, a VXML Server application, or a custom-written VXML application.

Caution This script is a component of the Unified CVP software. Hence, do not make any modifications to this script. Modifications to this script not made as part of an official Unified CVP release nullify Cisco support responsibility for this script.

Install Call Survivability Script

Procedure

Step 1 Log in to the Operations Console, and copy all script and prompt files to the gateway.

Step 2 On the gateway, perform the following:

For a **Unified CVP Comprehensive** call flow model, define the following services:

```
application
service survive flash:survivability.tcl
paramspace callfeature med-inact-det enable
service handoff flash:handoff.tcl
```

And, then add the following parameters:

```
ip rtcp report interval 2000
gateway
timer receive-rtcp 4
```

Note This causes survivability to be invoked between 8 and 16 seconds ((2000 ms *4) * 2) for an active call after a WAN failure. If IOS detects the absence of both RTP and RTCP packets after 8 to 16 seconds, it raises an error event and survivability is invoked. (The **factor of 2** is a built-in IOS factor that cannot be configured. Do not adjust these values lower as this can cause the survivability event to be prematurely invoked.)

Note The timer **receive-rtcp** command configures a media activity timer for SIP calls.

For a **Unified CVP Standalone** call flow model, first define one service:

```
  application
service my-survivability-service flash:survivability.tcl
```

Note You can replace `my-survivability-service` with any desired name.

Then associate the my-survivability-service that you just created as a parameter on the CVPSelfService.tcl service associated with the incoming pots dial-peer. Note that the text "param survive" must be entered exactly as shown, but the `my-survivability-service` service can be renamed to the service name of your choice. For example:

```
  dial-peer voice XXXX pots
  service my-CVP-service
  incoming called-number NNNNN
  service my-CVP-service flash:CVPSelfService.tcl
  param CVPPrimaryVXMLServer my-VXML-server-IP
  param CVPBackupVXMLServer my-backup-VXML-server-IP
  param CVPSelfService-app my-VXML-server-app
  param keepalive my-CVP-service
  param survive my-survivability-service
service my-survivability-service flash:survivability.tcl
```

Optionally, start a background keepalive service to the VXML Server. For example, for a service name of "my-standalone-service":

```
  service my-standalone-service
  param keepalive my-standalone-service
```

Note This service prevents the caller from hearing a period of silence at the start of each call if the VXML Server is down, as the gateway will know the current status of the VXML Server.

Step 3 On the gateway, perform a "call appl voice load my-survivability-service" and "call appl voice load handoff."

Step 4 Perform the following:

On a **Unified CVP Comprehensive** call flow model:

- Create a Unified CVP pots dial-peer on the gateway, placing the Unified CVP called number on an incoming-called-number parameter.
- Assign the my-survivability-service service to this dial-peer.

On a **Unified CVP Standalone** call flow model, no special survivability dial-peer needs to be created. However, the parameter "param survive my-survivability-service" must be included on the CVPSelfService.tcl service.

This parameter indicates which service to run in the event of a system failure. In this way, different survivability services can be invoked depending on the incoming pots dial-peer invoked.

Configure the Gateway for Call Survivability

Configure the following parameters on the gateway for call survivability:

- **open-hours-agent**—The destination recovery target DNIS to be used when the current time matches any open-hours-time parameter. The script cycles through all agents sequentially until an agent answers. If no agent answers, (or in the case of a takeback transfer, the PSTN does not take back the call), the script cycles through all after-hours-agents (maximum of 50 agents).
  - **Syntax:** open-hours-agentX DNIS
  - **Arguments:** X = a number from 0 to 49, DNIS = target destination for the recovery transfer.
  - **Example 1:** DTMF*8,9875551212 (When PSTN *8 takeback is desired), where **DTMF** - Indicates takeback and transfer via DTMF tones ***8** - The sequence the switch recognizes to perform the takeback. **Zero or more commas** - Each comma represents a pause of 100 ms. Some switches require a pause between the takeback sequence and the DNIS. **9875551212** - The actual DNIS to which the PSTN should transfer the call.
  - **Example 2:** HF,,,,,9875551212 (when hookflash transfer is desired) where: **HF** - Indicates takeback and transfer via hookflash relay **Zero or more commas** - Each comma represents a pause of 100 ms. Some switches require a pause between the hookflash and the DNIS. **9875551212** - The actual DNIS to which the switch should transfer the call. **Note:** When using either DTMF or hookflash takeback, you need to configure the following additional parameters on the gateway voice ports:

    ```
    voice-port 7/1:0
    no echo-cancel
    enable no non-linear
    no vad
    playout-delay maximum 250
    playout-delay nominal 200
    playout-delay minimum high
    playout-delay mode fixed
    ```

  - **Example 3:** 9875551212 (when hairpin or SRST transfer is desired)
  - **Example 4:** TBCT9875551212 (when TBCT is desired)
  - **Example 5: <retry>** (when a retry to the original CVP DNIS is desired) - Assuming the original Unified CVP DNIS was *4444:*, **<retry>** will send the call to CVP using DNIS. 4444 **56<retry>78** will send the call to CVP using DNIS 56444478.
- **after-hours-agent**—The destination recovery target DNIS to be used when the current time matches any after-hours-time parameter or as a default destination if transfers to the open-hours-agent's fail. The script will cycle through all agents sequentially until one answers (maximum of 50 agents). If no one answers, a call-back-later message will be played to the caller and then disconnected.
  - Syntax: identical to open-hours-agent

- **open-hours-time**—A string representing the date or days of week and time of day that open-hours-agent's will be used for the recovery transfer (maximum of 20 values). Month/day has higher selection priority than days of the week.
  - **Syntax:** open-hours-timeX {month/day | days-of-week}[:HHMM-HHMM]
  - **Arguments:X** = a number from 0 to 19, **month/day** = month of year and day of month (no year), **days-of-week** = a string of up to seven digits representing the days of the week (Sunday = 0, Saturday = 6), **HHMM-HHMM** = the starting and ending time of the period, expressed in 24-hour clock notation.
  - **after-hours-time**—A string representing the date or days of week and time of day that after-hours-agents use for the transfer. These do not explicitly need to be listed. If the current date/time does not fall in an open-hours-time slot, it defaults to an after-hours agent. A typical use is to specify holidays that would fall on working weekdays. A maximum of 20 values are allowed.
  - **Syntax:** identical to open-hours-time
- **open-hours-cvptime**—You may want to choose a particular recovery agent based on how long the call had been in Unified CVP before the failure occurred. If no open-hours-cvptime is specified, the associated open-hours-agent will be used regardless.
  - **Syntax:** number-of-seconds
  - **Arguments: X** = a number from 0 to 19, corresponding to the associated open-hours-agent **number-of-seconds**55 would use open-hours-agent0 only when the call had been in Unified CVP less than 55 secs.
- **after-hours-cvptime**—Same as open-hours-cvptime, but applies instead to after-hours-agents.
- **alert-timeout**—A numeric value indicating the maximum number of seconds the destination phone should ring before stopping the call attempt.
  - **Syntax:** alert-timeout 20
- **setup-timeout**—A numeric value indicating the maximum number of seconds that the tcl script will wait in establishing a tcp connection to Unified CVP before stopping the call attempt. This value should be greater than the "h225 timeout tcp establish" parameter under the voice class h323 configuration on the gateway.
  - **Syntax:** setup-timeout 7
- **aa-name**—If non-blank, indicates that when a failure occurs, the Unified CVP survivability script hands off the caller to the BACD auto-attendant application. Enter the following:

```
service <survivability-servicename>
param aa-name <BACD-servicename>
service <BACD-servicename>
param isn-name <survivability-servicename>
```

Where servicename is the service name of the BACD auto-attendant script to which control should be passed.

Procedure

- **standalone**—If non-blank, indicates that when a failure occurs, this Unified CVP survivability script passes control to the service name specified. Typically, that service would reference the CVPSelfService.tcl script to invoke a Call Studio application to provide IVR treatment to the caller; for example:

```
service survivability flash:survivability.tcl
param standalone vxmlapp
service vxmlapp flash:CVPSelfService.tcl
```

- **standalone-isntime**—Select the standalone option depending on how long the call had been in Unified CVP before the failure occurred. If no standalone-isntime is specified, the standalone option is invoked if it is *non-blank*.
  a) **Syntax**: standalone-isntime {> OR <}number-of-seconds
  b) **Arguments**: **number-of-seconds** = number of seconds the call was in Unified CVP before the call failed, prefixed with > or <. For example, standalone-isntime <2 would use standalone only when the call had been in Unified CVP less than 2 seconds.
- **icm-tbct**—A numeric boolean value (0 or 1) indicating whether or not Unified ICME scripts will issue TBCT transfers. Default is 0 (by default, Unified ICME does not handle TBCT transfers). Set this value to 1 to enable TBCT transfers issued from a TBCT label in an Unified ICME script.
  a) **Syntax Example:** icm-tbct 1
- **disableDnisStrip**—By default survivability.tcl will strip of all leading zeros from the dialed number. To disable this, you can set the disableDnisStrip parameter to a value of 1.
  a) **Syntax Example:** disableDnisStrip 1

  Configure the following parameters on the gateway for call survivability in case of REFER call flow:

  - **refer-prefix**—A numeric array value of 3 digits indicating whether to handle transfers as SIP REFER pass-through or SIP REFER consume on the gateway. If the transfer number matches this prefix then SIP REFER pass-through is used, otherwise SIP REFER consume is used.
  - • **Syntax Example**: refer-prefix "800 888 877 866 855"

Note If survivability is configured for REFER pass-through scenario, then the gateway must have outbound dial-peer for the referred DN.

What to do next

Configure the following parameters on the gateway for call survivability in case of REFER call flow:

- **refer-prefix**—A numeric array value of 3 digits indicating whether to handle transfers as SIP REFER pass-through or SIP REFER consume on the gateway. If the transfer number matches this prefix then SIP REFER pass-through is used, otherwise SIP REFER consume is used.

  Syntax Example: refer-prefix "800 888 877 866 855"
- **refer-pass-setup-timeout**—A numeric value indicating the maximum number of seconds that the tcl script will wait in establishing a call that is a refer pass-through. To disable the timer, you can set the refer-prefix parameter to a value of 0. The default value is 7.

Syntax Example: refer-pass-setup-timeout 7

Examples of Call Survivability

In the first Call Survivability example, the following configurations are used:

```
service survivability flash:survivability.tcl

param open-hours-agent0 9777123400
param open-hours-agent1 4444888
param open-hours-time0 12345:0900-1730
param open-hours-time1 12/18:0600-2300

param after-hours-agent0 7777008
param after-hours-agent1 8766008
param after-hours-time0 7/21:0700-0800
param after-hours-time1 11/25

param setup-timeout 7
param alert-timeout
dial-peer voice 800232 pots
application survivability
incoming called-number 8002321765
direct-inward-dial
```

Using the above survivability configurations, review the following cases:

- Case 1: Assume today is a holiday, Thursday, 11/25 at 1300 hours. Since 11/25 is defined as a specific after-hours-time, it is selected before the 12345:0900-1730 open-hours-time, which also falls on a Thursday. If the WAN fails, this script first tries a transfer to 7777008, and then to 8766008.
- Case 2: Assume today is Saturday, 12/18 at 0900 hours, peak of the holiday shopping season. Since 12/18 is defined as a specific open-hours-time, it is selected for an open-hours-agent even though it falls on a Saturday, which would usually be after hours time. If the WAN fails, this script first tries a transfer to 9777123400, then try 4444888, 7777008, and 8766008.
- Case 3: If time-of-day routing is not important, but you need a last-resort transfer mechanism, put one or more DNIS in the after-hours-agent slots and do not define any times. Any failed call is always directed to the list of after-hours-agents.

The next example illustrates how to organize call survivability functionality by incoming DNIS, create a separate application for each DNIS and apply desired call recovery properties to each application. For example:

- Assume billing callers dial 45XX and sales callers dial 55XX to access Unified CVP.
- Assume that a billing call fails somewhere in the course of the call:
  - If the call fails and the call had been in Unified CVP less than 30 seconds (this would also include the case where the call had *never* made it to Unified CVP; for example, 0 seconds), send the caller back through the PSTN via a *8 takeback to 8005556666.
  - If the call fails and the call had been in Unified CVP greater than or equal to 30 seconds, send the caller back through the PSTN via a *8 takeback to 8007778888.
- Assume that a sales call fails somewhere in the course of the call:

- If the call fails (in this case, the amount of time the call had been in Unified CVP is irrelevant), send the caller back through the PSTN via a hairpin transfer to 8009990000.

- Assume the PSTN switch is sending ANI and DNIS in such a way that the ANI and DNIS are concatenated together in the DNIS field. Assume that ANI length is 10 and DNIS length is 4. Also assume that ANI can be blank; for example, blocked callerID.

The IOS configuration elements necessary to accomplish these cases are shown below.

Note Dial-peers 2 and 4 are necessary in the event of no ANI (blocked caller ID). The lower preferences of dial-peers 2 and 4 is to protect against the case where a caller's ANI begins with 45, for example. For example, assume caller with ANI 4521111111 dials the sales DNIS. Without lower preferences, the caller would have matched dial-peer 2 and gone to the billing application instead of sales (you wanted it to match dial-peer 3).

The following are the configuration elements for the second example:

```
dial-peer voice 1 pots
preference 1
application billing
incoming called-number 45..
#----------------------------------------
dial-peer voice 2 pots
preference 2
application billing
incoming called-number 45..
#----------------------------------------
dial-peer voice 3 pots
preference 1
application sales
incoming called-number 55..
#----------------------------------------
dial-peer voice 4 pots
preference 2
application sales
incoming called-number 55..
#----------------------------------------
dial-peer voice 5 pots
destination-pattern 8009990000
port 7/0:D (or whatever port is desired)
#----------------------------------------
dial-peer voice 6 voip
incoming called-number 8009990000
codec g711ulaw (To force the call to g711ulaw on the outgoing
hairpin)
#----------------------------------------
service billing flash:survivability.tcl
param after-hours-agent0 DTMF*8,,,8005556666
param after-hours-cvptime0 <30
param after-hours-agent1 DTMF*8,,,8007778888
param after-hours-cvptime1 >29
param ani-dnis-split 10:4
#----------------------------------------
service sales flash:survivability.tcl
param after-hours-agent0 8009990000
param ani-dnis-split 10:4
```

Enhanced Location Call Admission Control

Enhanced Location Call Admission Control (ELCAC) is used to maximize local branch resources, keeping a call within the branch whenever possible and limiting the number of calls that go over the WAN. Unified CVP supports queue-at-the-edge, a simpler and more effective configuration of ELCAC than the transfer and queue calls with Unified CVP. Using the queue-at-the-edge functionality, the call originating from a specific branch office is deterministically routed to a local VXML Gateway based on priority, which means that ELCAC always selects a local branch agent, if possible.

ELCAC Topic Definitions

The following definitions are used in the configuration of ELCAC:

- **Phantom Location**: A default location with unlimited bandwidth used when calculating calls that are hairpinned over a SIP trunk or when the SIP call is queued at the local branch, to enable correct bandwidth calculations. The Phantom location should be assigned to the gateway or trunk for CVP.
- **SiteID**: The SiteID is a string of numbers that is appended to the label from Unified ICM so that the dial plan can be configured to route the call to a specific destination, such as the branch VXML gateway or egress gateway, or Unified CM node. The SiteID can be appended at the front of the label, at the end, or not at all. This configuration is separate from the Unified CM location configuration, and is specific to Unified CVP. The SiteID is used to indicate the real location of the call and allow the bandwidth to be deducted from the correct location.
- **Shadow Location**: This new location is used for inter-cluster trunks between two Cisco Unified Communications Manager clusters. This location is not used as inter-cluster ELCAC is not supported in Unified CVP 9.0(1).

Note The CVP server does not calculate bandwidth when using the ELCAC feature. This calculation is performed on the CUCM server.

ELCAC Queue-at-the-Edge Configuration

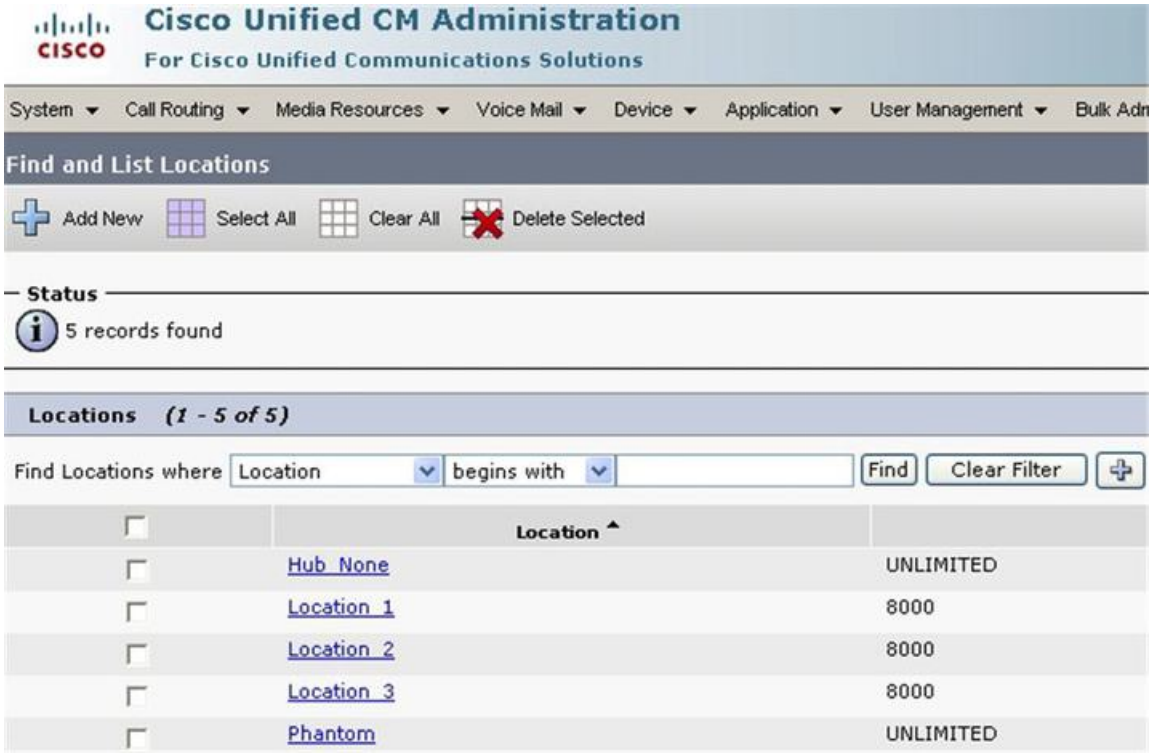
The following steps provide an example configuration for ELCAC with queue-at-the-edge functionality.

Through the Unified CM, configure all branches so that Location and Bandwidth are defined:

1. From Unified CM Administration, select **System** > **Location**. Click **Find** to list the locations and add new ones as appropriate.

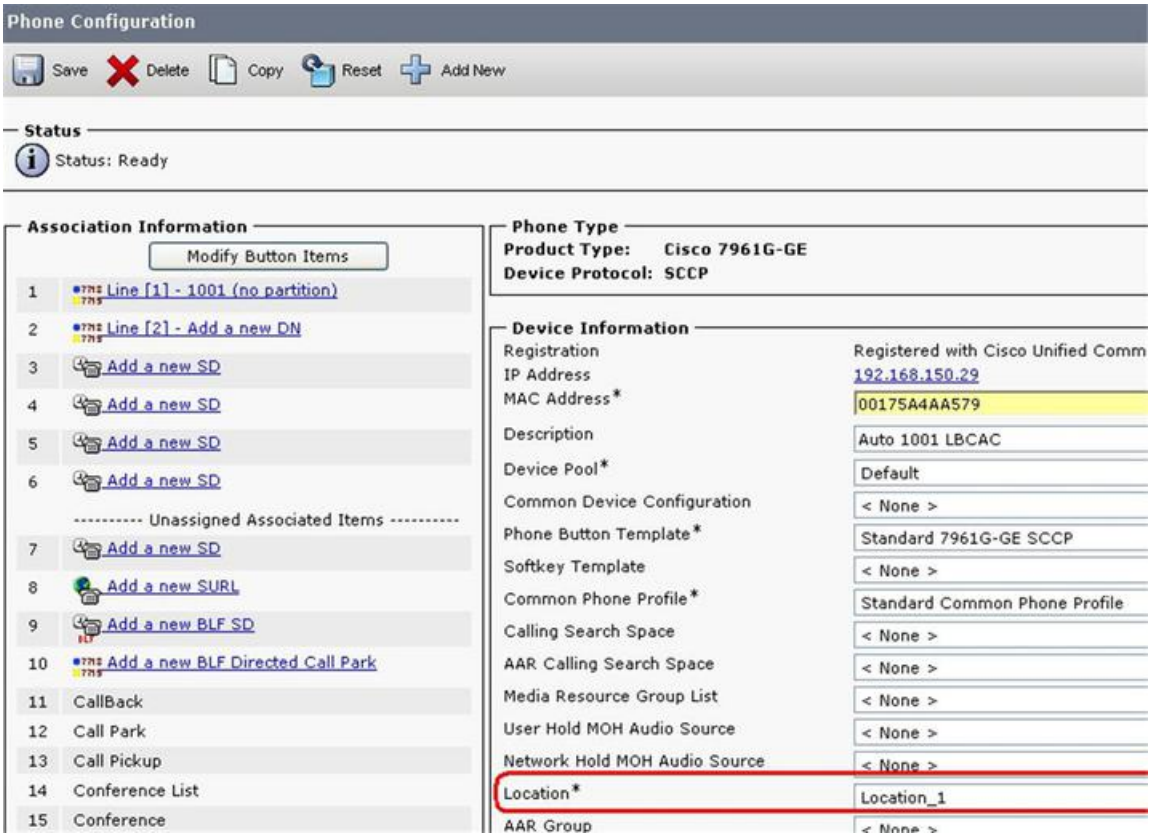
Note **Unlimited** must be unchecked for each branch (the box to the left of the location name); otherwise bandwidth is not deducted for that branch. (The Phantom location still has unlimited bandwidth even when unchecked.)

Figure 25: Cisco Unified CM Administration—Find and List Locations



2. For the branch phones, configure each phone so that it is assigned the branch location for that phone.
   - Select **Device** > **Phone**. Click **Find** to list the phones.
   - Select a phone and set the **Location** field.

Figure 26: Phone Configuration Screen



3. Verify that the Cisco AXL Web Service is started and that an Application User is defined and has a role of *Standard AXL API Access*.
   - From Cisco Unified Servicability, select **Tools** > **Control Center** > **Feature Services**
   - Start the Cisco AXL Web Service, if it is not started.
   - From Cisco Unified CM Administration, select **User Management** > **Application User**. Verify you have a user with the role of *Standard AXL API Access*, or create a new one and add that user to a group that has the role of Standard AXL API Access.

On Unified CVP, perform the following steps using the Operations Console:

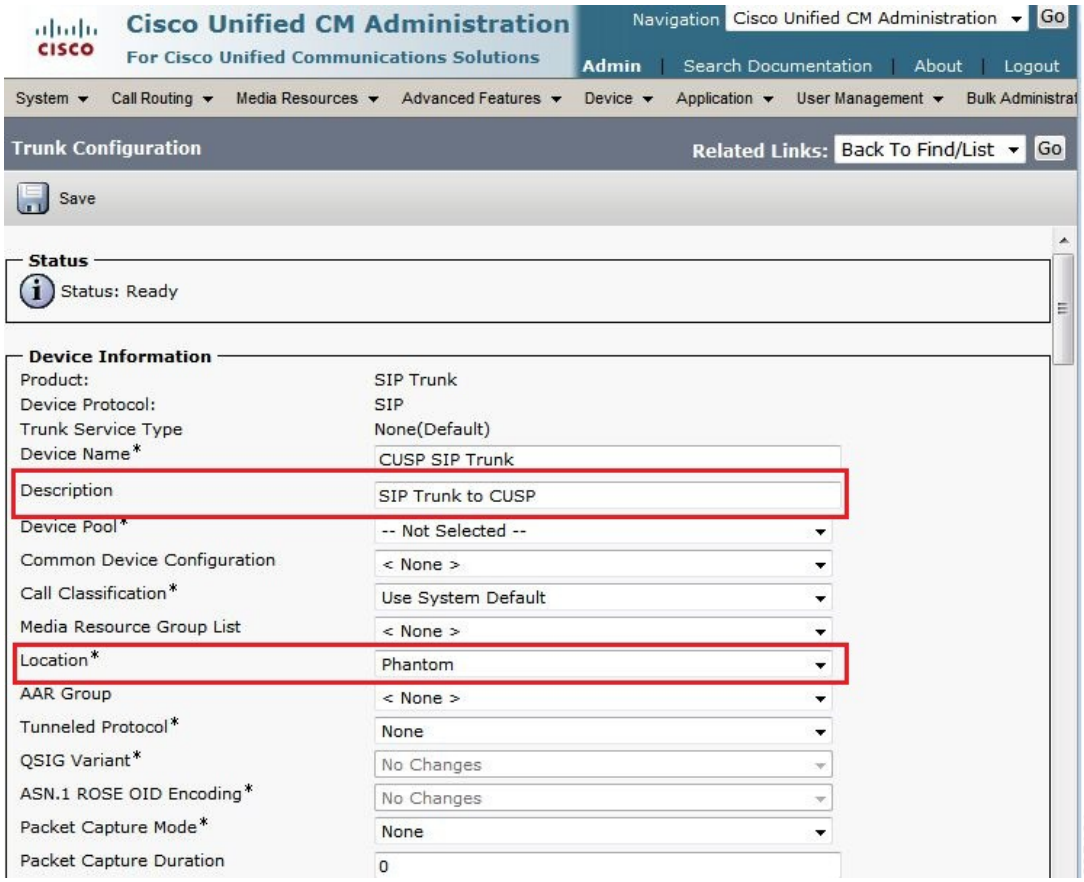
1. In **Device Management** > **Unified CM**, in the section **Enable Synchronization for Location** , enable synchronization and provide the credentials required to log in.
2. In **System** > **Location**, click **Synchronize** to retrieve the locations defined on Unified CM.

   Select **System** > **Location** and verify that the locations have been synchronized from Unified CCM.
3. In **Device Management** > **Gateway**, define the Ingress and VXML gateways.
4. **Assign IDs.** In **System** > **Location**, select a location.
   - Assign a Site ID and Location ID to the location, then add the associated gateways to the location.
   - Repeat for each of the locations.

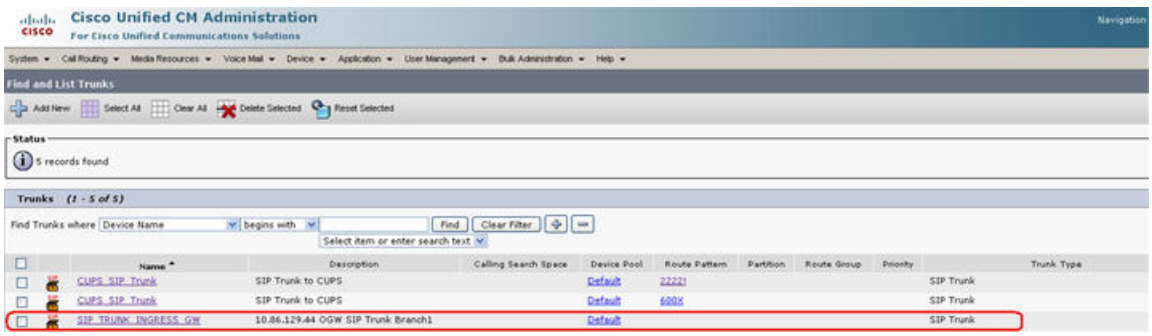
5. In **System** > **Location**, navigate to **Call Server Deployment** and select the Call Servers where the configuration is to be deployed. Click **Save and Deploy**.
6. For the insertion point of the SiteID, use the default location *between the Network VRU label and the correlation ID* as shown in the following screenshot.

SIP Deployments—Unified CM Steps:

1. Using Unified CM, create a SIP trunk toward the SIP proxy server and select the *Phantom* location.



2. Create a SIP trunk for each ingress gateway and make the location of these ingress TDM-IP gateways the actual branch location.



3. Create a route pattern pointing the Network VRU Label of the CCM routing client to the SIP trunk toward the SIP proxy you created in Step 1.

The SIP proxy should route the Network RRU label of CCM routing client to the farm of CVP Call Servers.

4. For any IP-originated calls, the CCM route pattern should be associated with the SIP trunk created in Step 1.
5. Associate the new SIP profile from Step 3 with the trunk defined in Step 1 and each Ingress gateway defined in Step 2.

Locations-Based Call Admission Control Configuration

Locations-based call admission control (CAC) is used in the Unified CCE branch-office call flow model, which is also known as the Centralized Model. This means that all servers (Unified CVP, Unified ICME, Unified CM, SIP Proxy server, and Media Servers) are centralized at one or two data centers, and each branch office (of which there can hundreds or thousands) contains only a gateway and IP phones.

This section provides an overview on how to configure Unified CVP to perform the following tasks:

- Accommodate Unified CM locations-based CAC.
- Minimize bandwidth usage on the WAN.

This section also describes other call flow and bandwidth usage issues to consider.

The following sections do not include detailed installation and configuration instructions. They are intended to provide you with guidance as you set up the Unified CVP solutions in your network. For additional information about how to install, set up, run, and administer Unified CVP, see the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal*.

Unified CM Service Configuration Settings

Set the following configuration parameters to make Unified CM use the Ingress gateway instead of Unified CVP as the originating location of the call.

- Set "Accept Unknown TCP connection" in Unified CM Service parameters.
- Set the Unified CM Service parameter "GK controlled trunk that will listen to 1720" to “None”.
- Do not define Unified CVP as a gateway device in Unified CM.
- Define the Ingress gateways as gateway devices in Unified CM. Assign the correct location to the devices.

These settings ensure that CAC can be adjusted based on the locations of the calling endpoint and the phone.

Unified CVP Bandwidth Utilization

The following factors contribute to WAN bandwidth usage by Unified CVP in a CAC with Distributed Queuing call flow model:

- VoiceXML documents. See VoiceXML Documents, on page 455.
- Prompt retrieval. See Prompt Retrieval, on page 455.

The following sections describe the bandwidth requirements of these factors in an example Centralized Call Control with Distributed Queuing call flow model. The examples in these sections are based on data that Cisco obtained from testing.

In these examples, assume that:

- Each call begins with some IVR treatment followed by a transfer to an agent.
- Each branch has 20 agents and each agent handles 30 calls per hour. Thus, the total number of calls is as follows:

  20 * 30 = 600 calls per hour = 0.166 calls per second (CPS).

Related Topics

VoiceXML Documents, on page 455
Prompt Retrieval, on page 455

VoiceXML Documents

A VoiceXML document corresponds approximately to a Run External node in a Unified ICME script.

A round trip of a VoiceXML document between Unified CVP and the gateway consumes an average of 7 KB (7000 bytes). If each call includes approximately 20 VoiceXML documents, the WAN bandwidth consumed by VoiceXML documents can be calculated as follows:

- 7000 bytes * 20 VoiceXML documents * 8 bits = 1,120,000 bits per call
- 0.166 CPS * 1,120,000 bits per call = 185.9 Kbps per remote site

Prompt Retrieval

Store the voice prompts at the following locations:

- In flash memory on each local site gateway - In this way, gateways do not need to retrieve .wav files for prompts and WAN bandwidth is not affected. However, if a prompt needs to change, you must change it on every gateway.
- On an HTTP media server - In this way, each local site gateway (if properly configured) can cache many or all prompts, depending on the number and size of the prompts.

When prompts are stored on an HTTP media server, the refresh period for the prompts is defined on that server. The bandwidth consumed by prompts consists of the initial loading of the prompts at each gateway and of the periodic updates at the expiration of the refresh interval.

As an example of determining the bandwidth consumed by prompts, assume that a call flow has 50 prompts with an average size of 50 KB (50,000 bytes) each. Also, assume that the refresh period for the prompts is defined as 15 minutes (900 seconds) on the HTTP media server.

The WAN bandwidth required for prompts in this call flow can be calculated as follows:

- 50 prompts * 50,000 bytes * 8 bits = 20,000,000 bits
- 20,000,000 bits / 900 seconds = 22.2 Kbps per branch

Gateway Prompt Caching Considerations

When you store audio prompts on an HTTP media server, proper gateway prompt caching methods are necessary to optimize both the performance of the gateway and network bandwidth consumption. Gateway performance decreases by approximately 35-40% if caching is disabled entirely.

Configure Caching on the Gateway

Procedure

Step 1 Set the following settings on the gateway:

a) ivr prompt memory 15000
b) http client cache memory file 500
c) http client cache memory pool 15000

Note The 'http client cache memory file' represents the largest size prompt file (in Kbytes) that can be cached. In general, break up customer prompts larger than 500K (about a minute in length) into smaller, more manageable pieces to facilitate loading and caching. For example, queue music could be a repetitive loop of a 30 second prompt. Note also that because the prompts are streamed, the prompt will not be cached unless the whole prompt is played. Therefore, you must make prompts a manageable size.

Step 2 Synchronize the datetime between the gateway and the HTTP media server.

Note Synchronization does not have to be exact, but at least within a minute or two. Times that are not synchronized can cause prompts to never refresh or they will refresh with every call, both of which are undesirable behaviors.

Step 3 On the media server, set the content expiration (for example 15 minutes).

Determine Gateway Caching

To determine if you have properly configured gateway caching, perform one of the following actions:

Procedure

- The IIS log on the media server records every time a client requests a prompt. If caching is set up correctly, these requests appear approximately every X minutes, where "X" is the number of minutes defined as the refresh interval for any particular prompt. The log is located at **C:\WINNT\system32\LogFiles\W3SVC1\ex***.
- Run 'show http client cache' on the gateway. The 'Fresh Time' column equals the refresh time period set on the HTTP media server. For example, if the refresh period was set to 15 minutes, it says 900 seconds. The 'Age' column shows how many seconds have passed since the prompt was last refreshed. In general, this number will be less than the 'Fresh Time'. However, if no call has ever accessed the prompt recently, this number could be greater than the fresh time. Prompts are only refreshed when triggered by a call *and* the prompt 'Fresh Time' has expired. If the Fresh Time is a very high value, the only way to remove the prompt from cache is to reload the gateway.

UUI as Correlation ID

Unified CVP uses the User-to-User Information (UUI) from the incoming call as a Correlation ID in the VRU-Only call flow model. This feature allows customers to transfer Correlation IDs through their network; for example, using a Call Routing Service Protocol (CRSP) NIC for call control.

Note This feature applies only to the Unified CVP VRU-Only call flow model.

The network has no place to store a Correlation ID, so it must be "hidden" in the ISDN setup that arrives at the IOS gateway and then is extracted by the gateway. The UUS parameter, also known as the User-to-User Information (UUI) of the Generic Transparency Descriptor (GTD) data, can be used to "hide" the Correlation ID, provided the call control client has the capability of inserting a Correlation ID value into the GTD.

When the call arrives at the gateway from the network, the call control client extracts the value and appends it to the DNIS before sending an HTTP request to the Type3 Unified CVP Call Server.

How It Works

The call control client (such as the CRSP NIC) inserts the desired Correlation ID value into the dat field of the UUS parameter of the NSS IAM message. These NSS messages are used as the basis of building the GTD data that ultimately arrives at the IOS gateway from the PSTN. See the ITU-T Narrowband Signaling Syntax spec (Q.1980.1) for a detailed description of the IAM message and UUS parameter, included below for convenience. Note that the dat field contains pairs of hexadecimal digits, meaning that if the Correlation ID is "12345", the dat field must be populated as "3132333435". The gateway bootstrap.tcl script converts back to "12345" before appending to the DNIS and passing to the Unified CVP Call Server in the HTTP URL.

To configure a gateway, see Configure Gateway, on page 249.

Related Topics

Configure Gateway, on page 249

Debugging Tips

Debug Trace Settings for the Gateway

On the gateway, enter the following code:

```
debug voip application script
debug gtd
```

GTD Values in the Gateway Log

In the gateway log, look for the following GTD values:

```
6616806: *Jan 31 17:12:41.220: cdapi_find_tsm:
Found a gtdmsg of length144:6616807: *Jan 31 17:12:41.220:
gtd msg = "IAM,PRN,isdn*,,
ATT5*,USI,rate,c,s,c,1USI,lay1,ulawTMR,00CPN,00
```

```
                                    ,,u,5900CPC,09FCI,,,,,,,y,UUS,3,3132333435

                                    ---> This is the UUI that will become the Correlation
ID12345GCI, 87c0c79d91dd11daa9c4000bfda207f2"
```

External Transfers in Unified ICME

Unified ICM Script Label for Outpulse Transfer

Labels in Unified ICM scripts for Unified CVP calls that require outpulse transfer mode must be prepended with the characters DTMF followed by *8 and some number of commas, where each comma represents a pause of 100 milliseconds. By configuring the target label with the form DTMFnnnnn (where nnnnn are the digits to outpulse), Unified CVP sends the digits out-of-band using H.245 signaling to the Ingress gateway for outpulsing.

To use the AT&T Transfer Connect feature to transfer the call to the number “4441234”, configure the label as DTMF*8,,,4441234.

Note Usually the PSTN switch expects a delay between the *8 and the phone number. Each comma represents 100ms by default. It can be changed with the SetTakebackDelay command in VBAdmin.

Note In outpulse transfer mode, Unified CVP sends whatever digits are in the label to the Gateway for outpulsing. It is the customer’s responsibility to confirm interoperability with the target switch.

Note In your Unified ICM script, when using outpulse transfers with SIP calls, digits can only be outpulsed on a call that has already been established. This means that it is necessary to transfer the call to the VXML gateway with a run external script node *before* you can send the DTMF*8 label. The Unified ICM script cannot send the DTMF*8 label back to Unified CVP for the first connect message in the call because the call has not been answered at this point. The Unified CVP Call Server uses SIP INFO messages to send the digits to the gateway for outpulsing.

Note When using outpulse transfers with SIP, you can also use the comma duration as the default interdigit pause duration.

For example, with the default 100 msec comma duration, a label such as "DTMF*8,,,8009785001" will have 300 msecs between the first 8 and the second 8. The interdigit pause will also be 100 msecs. The tone duration is also configurable and defaults to 100 msecs.

Note Outpulse transfer with SIP uses SIP INFO messages being sent to the TDM gateway, where the outpulsing of digits occurs. If the agent using the CTI desktop performs a blind transfer (single step transfer), and the scheduled script for the transfer DN returns a DTMF type label, the Unified Communications Manager SIP Trunk can loop the CVP DTMF label through the bridged call using an UPDATE message. Unified CVP can get the label back and convert the digits to SIP INFO messages to forward to the ingress gateway. This only works on blind transfers, and is not supported on consult transfers.

Unified ICME Script Label for Two B-Channel Transfer

For Unified CVP calls that require Two B-Channel Transfer (TBCT) mode, add a label node to your Unified ICME script with the following syntax:

TBCT99#8005551212#

Replace "8005551212" with your transfer destination target; TBCT99 and the # sign are mandatory.

By configuring the target label in this form, Unified CVP sends the digits to the Ingress endpoint for Two B-Channel transfer.

Unified ICME Script Label for Hookflash Transfer

Prepend labels in Unified ICME scripts for Unified CVP calls that require hookflash transfer mode with the characters HF. By configuring the target label with the form HFnnnnn (where nnnnn are the digits to call), Unified CVP sends the digits to the Ingress endpoint for hookflash transfer.

If the switch requires a pause after the hookflash, insert commas between the HF and the transfer number. (Each comma represents 100 milliseconds.)

For example, to use the hookflash feature to transfer the call to the number “4441234” with a 500- millisecond pause after the hookflash, configure the Unified ICME label as "HF,,,,,4441234."

Multicast Music on Hold (MMoH)

Multicasting may be used for Music On Hold with supplementary services on Unified CM as an alternative to the unicast MoH.

There are two ways to deploy this feature:

- With the Unified CM multicasting the packets on the local LAN.
- With the branch gateway(s) multicasting on their local LANs.

The latter is used when survivable remote site telephony (SRST) is configured on the gateway, and allows the deployment to utilize MOH locally and avoid MOH streaming over the WAN link.

Note Associate the SIP Trunk for Unified CVP (configured on Unified CM) with a Media Resource Group List (MRGL) that supports MMOH resources. Access the following links for configuration details and on how to create the MRGL:

- Configuring Music on Hold
- Integrating Cisco CallManager and Cisco SRST to Use Cisco SRST as a Multicast MoH Resource

Multicast MOH Usage Guidelines

The following guidelines apply when using Multicast MOH:

- Do not use this setting globally, or on a dial peer on the Ingress or Egress Gateway:

  ```
  modem passthrough nse codec g711ulaw
  ```

  This setting might cause Unified CM to stop the MOH after a timeout period of 10 to12 seconds.

- Do not set media inactivity on the Ingress Voice Gateway because multicast MOH does not send RTP or RTCP, and the call might get disconnected due to media-inactivity configuration. The setting media-inactivity criteria does not support multicast traffic.

- SIP-based multicast MOH is not supported on a 5400 platform because CCM-manager-based MOH subsystems are not supported on 5400 platform. This limitation also affects the ability of a TDM caller to hear multicast packets broadcasted from the Unified CM MOH server.

Mixed G.729 and G.711 Codec Support

Transcoders (DSPs) are required if the two endpoints participating in the call cannot negotiate a common codec. Therefore, midcall codec negotiation greatly reduces the need for transcoders.

CVP supports mixed G.711 and G.729 codecs in Standalone and Comprehensive SIP deployments with Cisco Unified Border Element Enterprise Edition (CUBE) and Cisco Unified Communications Manager (Unified CM). Calls that are ingressed through a SIP trunk from the carrier to a CUBE require Cisco IOS 15.1(2)T or later for mixed codec support. You can use any combination of codecs on the legs of a call. For example, a caller can place a call using the G.729 codec, hear an IVR prompt played using the G.711 codec, be transferred to the first Agent using the G.729 codec, and then transferred to the second agent using the G.711 codec.

A typical use case where transcoders may be required is when phones in a WAN connected location only support the G729 codec, and CVP is set up for G711 support. In this case, when these phones call into CVP, Unified Communications Manager engages transcoders. For inbound calls that arrive from a gateway or CUBE can start with G711 at CVP, then later renegotiate to G729 with the agents without the need for transcoders.

Transcoders (DSPs) are controlled by CUBE and Unified Communications Manager depending on the call flow. Because most of the service providers support midcall codec negotiation, transcoders in CUBE are not necessary. You commonly need transcoders controlled by Unified Communications Manager to support call flows, in which the phone supporting G729 is calling into CVP supporting G711.

Post Call Survey for SIP

A Post Call Survey takes place after usual call treatment. It is used to determine whether customers are satisfied with their call center experiences. This feature lets you configure a call flow that, after the agent disconnects from the caller, optionally sends the call to a Dialed Number configured for a Post Call Survey.

The Unified CCE script can enable and disable Post Call Survey on a per-call basis by testing for conditions and setting an expanded call variable that controls post call survey. For example, the script can invoke a prompt that asks callers whether they want to participate in a survey. Based on the caller's response, the script can set the expanded call variable that controls whether the call gets transferred to the Post Call Survey dialed number.

The Post Call Survey call works like a regular call from the Unified CCE point of view. Scripts can be invoked and the customer can use the keypad on a touch tone phone and voice with ASR/TTS to respond to questions asked during the survey. During Post Call Survey, the call context information is retrieved from the original customer call.

Note For reporting purposes, the Post Call Survey call has the same CallGUID and call context as the original inbound call.

Note Unified CVP can only send call variables and predefined ECC variables and ECC array like ToExtVXML and FromExtVXML in the call context to the NEW_CALL for PCS.

If you wish to use the Post Call Survey feature through Unified CVP, you must configure it on the Call Server. Also, you can configure the Unified ICM script to toggle the use of Post Call Survey off and on. The two configuration topics that follow, explain these methods.

Configure Call Server for Post Call Survey

In the following procedure, enter a dialed number pattern for the inbound call and a dialed number pattern for the post call survey. In both cases, the patterns can use alphanumeric characters and wildcard characters such as the exclamation point (!), asterisk (*), and single digit matches, such as the letter X (not x) or period (.). The pattern can end with an optional greater than (>) wildcard character. The maximum length of the dialed number pattern is 24 characters.

Procedure

Step 1 Access the CVP Operations Console by typing **https://<OAMP_server_IP>:9443/oamp**.

Step 2 Log in to the Operations Console and select **Device Management** > **Unified CVP Call Server**.

The **Find, Add, Delete, Edit Call Servers** window opens.

Step 3 Click the Call Server for which you want to configure Post Call Survey.

The **Edit CVP Call Server Configuration** page displays.

Step 4 Click the **SIP** tab. Verify the **Override System Dialed Number Pattern Configuration** is not checked.

Step 5 Click **Save** and **Deploy** to deploy the Unified CVP Call Server device.

Step 6 Select **System** > **Dialed Number Pattern**.

The Dialed Number Pattern window opens.

Step 7 Click **Add New**.

Step 8 Enter a pattern in the **Dialed Number Pattern** field. This is the incoming Dialed Number for calls that you want to direct to a Post Call Survey. Make sure that dialed number patterns entered here are unique. (An incoming dialed number can not be associated with multiple survey numbers.)

Step 9 Check **Enable Post Call Survey for Incoming Calls**. This action enables post call surveys for all incoming calls with the specified dialed number pattern.

The **Survey Dialed Number Pattern** field appears.

Step 10 In the **Survey Dialed Number Pattern** field, enter a dialed number for the Post Call Survey. This is the dialed number to which the calls should be transferred to after completing the usual call flow.

Record the number you have entered. In the next task, you create this dialed number in CCE Administration and create a call type to associate with this dialed number.

Step 11 Click **Save** to save the Dialed Number Pattern.

You are returned to the **Dialed Number Pattern** page.

Step 12 Click **Deploy** to deploy the configuration to all Call Servers.

Configure ICM for Post Call Survey

Configuration is not required on Unified ICM to use Post Call Survey, however, you can turn the feature off (and then on again) within an ICM script by using the ECC **variableuser.microapp.isPostCallSurvey** and a value of n or y (value is case insensitive) to disable and re-enable the feature.

Configure the ECC variable to a value of n or y before the label node or before the Queue to Skillgroup node. This sends the correct value to Unified CVP before the agent transfer. This ECC variable is not needed to initiate a Post Call Survey call, but you can use it to control the feature once Post Call Survey is configured using the Operations Console. As long as a DN is mapped in the Operations Console for Post Call Survey, the call will be automatically transferred to the configured Post Call Survey DN.

Note

- The Post Call Survey DN is called if the Unified CVP has received at least one CONNECT message from ICM (either from the VRU leg or from the Agent leg). Use the END node in your ICM script if the Post Call Survey is not required for the calls disconnected from the IVR.
- If Router Requery is configured incorrectly and the Ring-No-Answer timeout expires, the caller is still transferred to the Post Call Survey DN. This can occur if a Queue node is used and Enable target requery is not checked.

Procedure

Step 1 On the Unified ICM Administration Workstation, using configuration manager, select the **Expanded Call Variable List** (ECC) tool.

Step 2 Create a new ECC variable with **Name:**`user.microapp.isPostCallSurvey`.

Step 3 Set **Maximum Length:** to 1.

Step 4 Check the **Enabled** checkbox. Then click **Save**.

In your Unified ICM scripts, remember that, at script start, the default behavior of Post Call Survey equals **enabled**, even if **user.microapp.isPostCallSurvey** has not yet been set in the script. You can turn **off** Post Call Survey in the script by setting **user.microapp.isPostCallSurvey** to *n*. You can later re-enable Post Call Survey in the same path of the script by setting this variable to *y*.

Step 5 Select **Manage** > **Call Types**.

Step 6 Add the call type for Post Call Survey, and click **Save**.

Step 7 Select **Manage** > **Dialed Numbers**.

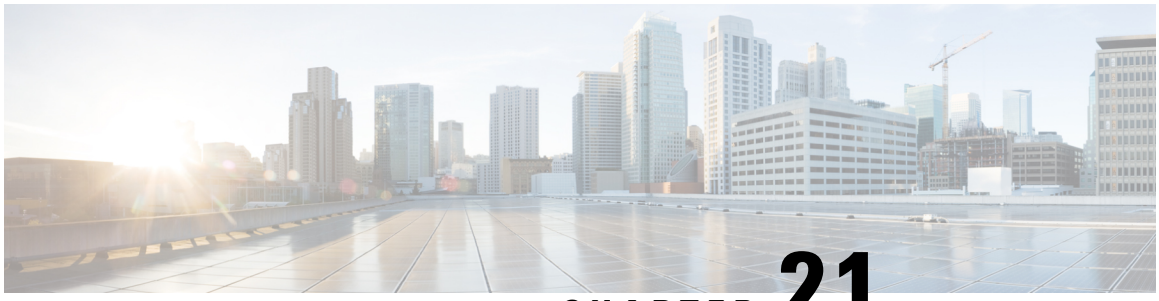
Step 8 Create Dialed Numbers with Routing Type External Voice for each of the Post Call Survey Dialed Number Patterns created in CVP and associate them to the Post Call Survey Call Type you just added.

Step 9 Click **Save**.

Step 10 If you added the new expanded call variable, you must restart the active generic PG (side A or B) to register the new variable.

If the expanded call variable already existed, you can skip this step.

Note The **user.microapp.isPostCallSurvey** setting takes effect on CVP only when it receives a connect or temporary connect message. Therefore, if you do not want the survey to run, without first reaching an agent (such as 'after hours of treatment'), you must set the isPostCallSurvey to *n* before the initial 'Run script request'.



CHAPTER 21

Configure High Availability for Unified CVP

Server Groups

A Server group is a dynamic routing feature that enables the originating endpoint to have knowledge of the status of the destination address before attempting to send the SIP INVITE. Whether the destination is unreachable over the network, or is out of service at the application layer, the originating SIP user agent can have fore-knowledge of the status through a heartbeat mechanism.

The Server Groups add a heartbeat mechanism with endpoints for SIP. This feature enables faster failover on call control by eliminating delays due to failed endpoints.

The following list is a summary of important configuration items:

- Server Groups are not automatically added to your configuration. You must explicitly configure Server Groups for their deployment and turn on this feature.
- If you have already configured the **local SRV** feature and therefore created a srv.xml file, you must run the **srvimport.bat** command before you configure Server Groups using the Operations Console. Otherwise, your existing definitions will be overwritten. This process is explained in the configuration details that follow.
- You define Server Groups using the Operations Console. You must always configure at least one Call Server first, because you will not be able to save the Server Groups configuration without assigning it to at least one Call Server.

Configure Server Groups

Complete the following steps to configure Server Groups:

1. If you have previously created an srv.xml file, after you upgrade your Unified CVP installation, run the batch file **srvimport.bat** to transfer your prior configuration to the new Server Groups feature.

The srvimport.bat file is located in the **CVP bin directory**. This batch file takes your **srv.xml** file as an argument. Copy this file from your Call Server configuration directory. Running srvimport.bat brings this configuration data into the Operations Console.

Note You must **stop** the OAMP (Operations Console) service before you run the .bat file.

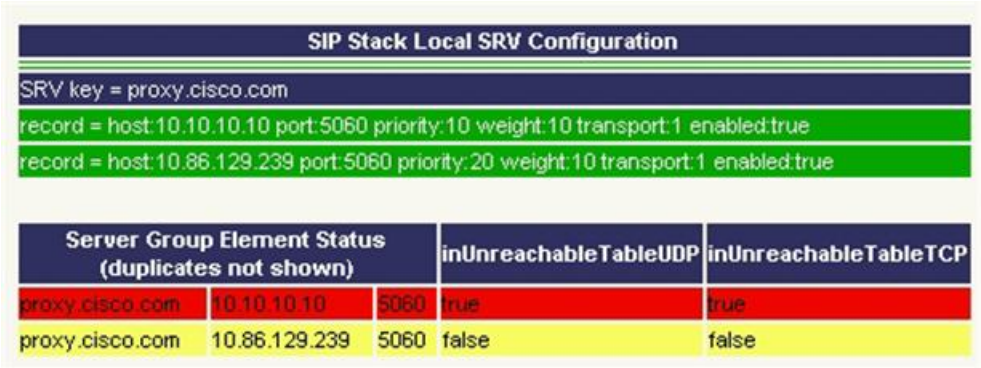
2. If you have not defined a Call Server using the Operations Console, refer to *Configuring a Call Server* in the Operations Console online help.
3. From the Operations Console, click **System** > **SIP Server Groups** > **Add New SIP Server Group**.
4. A Server Group consists of one or more destination addresses (endpoints) and is identified by a Server Group domain name. This domain name is also known as the SRV cluster name, or Fully Qualified Domain Name (FQDN). Define the FQDN and add it to the list. Refer to Configuring Server Groups in the Operations Console online help.
5. Refer to SIP Server Group Configuration Settings in the Operation Console online help to complete the Server Group configuration.
6. Click the **Call Server Deployment** tab and select the Call Server(s) that you want to associate with the Server Group(s). Then click **Save & Deploy** .

Note When you associate the Call Server(s) configuration, all the SIP Server Group configurations are applied to the Call Server(s), but individual deployment of SIP Server Group is not supported.

Server Groups Diagnostics

The CVP log file has traces which show endpoint status events. From the diagnostic servlet, click on the link for *dump SIP state machine* to display information as shown in the following example:

Figure 27: Server Group Diagnostics



Redundancy and Failover for Unified CVP

This section describes redundancy and failover mechanisms for ASR, TTS, Media, and VXML Servers in the Unified CVP solution.

Redundancy for VXML Server Applications

VXML Server applications rely on the gateway's configured default for ASR and TTS servers, which allow only a single host name or IP address to be specified for each. This differs from the Unified CVP micro-applications based applications, which support automatic retries to specifically named backup ASR and TTS servers.

Use the following configuration on the gateway if you are using Nuance or Scansoft ASR/TTS servers:

```
ip host asr-en-us 10.10.10.1
ip host tts-en-us 10.10.10.2
```

Use the following configuration on the gateway if you are using Nuance or Scansoft ASR/TTS servers:

```
mrcp client rtpsetup enable
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
http client cache memory pool 15000
http client cache memory file 500
ivr prompt memory 15000
ivr prompt streamed none
mrcp client timeout connect 5
mrcp client timeout message 5
rtsp client timeout connect 10
rtsp client timeout message 10
vxml tree memory 500
http client connection idle timeout 10
no http client connection persistent
```

The URL configured by the above ivr commands defines the gateway's default target for ASR and TTS services, and is in effect for all calls handled by that gateway. You can override it dynamically in your VXML Server application by populating the Cisco-proprietary VoiceXML properties **com.cisco.asr-server** or **com.cisco.tts-server**.

Redundancy for Micro-App-Based Applications

When a load balancer is used for ASR or TTS servers, the IVR Service plays a significant role in implementing a failover mechanism for Media Servers, ASR/TTS Servers and micro-app-based applications. Up to two of each such servers are supported, and the IVR Service orchestrates retries and failover between them.

Note This redundancy mechanism is only available for Unified CVP micro-applications.

Note For information about setting up the IVR Service to accommodate failover, see the *Administration Guide for Cisco Unified Customer Voice Portal*.

IVR Service Failover Mechanism

The IVR Service failover mechanism applies to:

- Connections between the IVR Service and the IOS Voice Browser, only.
- All communication between the IOS Voice Browser and an ASR Server, TTS Server, or Media Server.
- Media Server, when the ICM Script ECC variable, **user.microapp.media_server**, is set to mediaserver. When **user.microapp.media_server** is set to mediaserver, the IVR Service uses the IP Address defined on the gateway as:
  - ip host mediaserver 10.86.129.50
  - ip host mediaserver-backup 10.86.129.51

Note If **user.microapp.media_server** is configured as the hard-coded IP Address of the media server, then the IVR Service will not perform any failover for the media server.

If the IVR Service receives a Call Result error code value of **9** (MEDIA_FILE_NOT_FOUND), **33** (GENERAL_ASR_TTS), **31** (MEDIA_RESOURCE_ASR) or **32** (MEDIA_RESOURCE_TTS), it does the following:

- When attempting to connect to a *Media Server* , the IVR Service:
  - Resends the request the number of times defined in the IVR Service Configuration's **Media Server Retry Attempts** field.
  - If the connection is not successful after the specified number of attempts, and the IVR Service Configuration's **Use Backup Media Servers** field is set to **Yes** (the default), the IVR Service makes the same number of attempts to retrieve the media from a backup media server before failing and generating an error.

Note The backup media server is defined on the gateway as <mediaserver>-backup.

  - Passes the error in a Call State Event to the ICM Service, which then passes it to Unified ICME.
- When attempting to connect to an *ASR/TTS Server*, the IVR Service:
  - Resends the request the number of times defined in the IVR Service Configuration's **ASR/TTS Server Retry Attempts** field.
  - If the connection is not successful after the specified number of attempts, and the IVR Service Configuration's **Use Backup ASR/TTS Servers** field is set to **Yes** (the default), the IVR Service

makes the same number of attempts to connect to a backup ASR/TTS server before failing and generating an error.

Note The backup ASR and TTS servers are defined on the gateway as asr-<locale>-backup and tts-<locale>-backup.

- Passes the error in a Call State Event to the ICM Service, which then passes it to Unified ICME.

Each new call attempts to connect to the primary server. If failover occurs, the backup server is used for the duration of the call; the next new call will attempt to connect to the primary server.

Note This failover mechanism differs from that used in prior releases of Unified CVP software. Legacy releases used a *sticky* connection. In a sticky connection, if failover occurs to a backup server, subsequent new calls automatically connect to the backup server, rather than attempt to connect with the primary server.

If the Unified CVP IVR Service fails, the following conditions apply to the call disposition:

- Calls in progress are default-routed to an alternate location on the originating gateway. (Survivability does not apply in NIC-routing models.)
- New calls are directed to an in-service Unified CVP IVR Service.

ASR and TTS Server Location Setup

There are two ways to specify an external media server for TTS and ASR operations:

- Specify an ASR and TTS Server Location Globally on the Gateway, on page 469
- Specify an ASR and TTS Server Location with an Individual VoiceXML Document, on page 470

Note While using ASR/TTS, use a single version of MRCP (v1/v2) instead of using it in mixed mode.

Related Topics

Specify an ASR and TTS Server Location Globally on the Gateway, on page 469
Specify an ASR and TTS Server Location with an Individual VoiceXML Document, on page 470

Specify an ASR and TTS Server Location Globally on the Gateway

Media server sessions are created for each call to IVR applications, regardless of whether an application needs to communicate with the media server. Follow these steps to specify an ASR and TTS server location globally on the gateway.

Procedure

Step 1 Define the Hostname to IP Address mapping for the ASR and TTS servers.

```
ip host asr-en-us 10.78.26.31
ip host tts-en-us 10.78.26.31
```

Step 2 Define the Voice class URI that matches the SIP URI of the ASR Server in the dial-peer.

```
voice class uri TTS sip
pattern tts@10.78.26.31
```

Step 3 Define the Voice class URI that matches the SIP URI of TTS server in the dial-peer. Syntax - voice class uri tag sip.

```
voice class uri ASR sip
pattern asr@10.78.26.31
```

Step 4 Define the SIP URI of the ASR and TTS Server. Syntax -sip:server-name@host-name | ip-address.

```
ivr asr-server sip:asr@10.78.26.31
ivr tts-server sip:tts@10.78.26.31
```

Step 5 Set up a SIP VoIP dial-peer that is an outbound dial-peer when the Gateway initiates an MRCP over SIP session to the ASR server.

```
dial-peer voice 5 voip
session protocol sipv2
destination uri ASR
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

Step 6 Set up a SIP VoIP dial-peer that is an outbound dial-peer when the Gateway initiates an MRCP over SIP session to the TTS server.

```
dial-peer voice 6 voip
session protocol sipv2
destination uri TTS
dtmf-relay rtp-nte
codec g711ulaw
no vad
```

Step 7 Specify the name or IP address of a SIP server; usually a proxy server. You can then configure the dial-peer session target as session target sip-server. Syntax - sip-server {dns:[host-name] |ipv4: ip-addr[:port-num]}.

```
sip-ua
sip-server ipv4:10.78.26.31
```

Specify an ASR and TTS Server Location with an Individual VoiceXML Document

Media server sessions occur for each call to that application. If only a small number of applications require TTS/ASR media sessions, use the <property> extensions within those applications to define the external media server URL in the VoiceXML script.

Note Specifying the URL of media servers in a VoiceXML document takes precedence over the gateway configuration. Any value that is configured on the gateway is ignored if the same attribute is configured with a VoiceXML property.

com.cisco.tts-server

The “com.cisco.tts-server” allows the document to specify an external media server for text-to-speech operations. The media server is specified in the form of an URI, and is used in all consecutive TTS operations until the next media server is specified. An external media server specified by a property in the script takes precedence over being specified by a command through the CLI.

It can be defined for:

- An entire application or document at the <vxml> level
- A specific dialog at the form or menu level
- A specific form item

You can format the media server URI for Media Resource Control Protocol version 1 (MRCP v1), which uses Real Time Streaming Protocol (RTSP), IP Address or Hostname; or MRCP v2, which uses Session Initiation Protocol (SIP), IP Address or Hostname for example:

<property name="com.cisco.tts-server" value="rtsp://tts-server1/synthesizer" />

<property name="com.cisco.tts -server" value="sip:mresources@mediaserver.com" />

<property name="com.cisco.tts-server" value=“10.10.10.10" />

<property name="com.cisco.tts-server" value=“ttsserver.com" />

com.cisco.asr-server

The “com.cisco.asr-server” allows the document to specify an external media server for recognize operations. The media server is specified in the form of an URI, and is used in all consecutive ASR operations until the next media server is specified. An external media server specified by a property in the script takes precedence over being specified by a command through the CLI.

You can format the media server URI for Media Resource Control Protocol version 1 (MRCP v1), which uses Real Time Streaming Protocol (RTSP), IP Address, or Hostname, or MRCP v2 which uses Session Initiation Protocol (SIP), IP Address or Hostname for example:

<property name="com.cisco.asr-server" value="rtsp://asr-server/synthesizer" />

<property name="com.cisco.asr -server" value="sip:mresources@mediaserver.com" />

<property name="com.cisco.asr-server" value=“10.10.10.10" />

<property name="com.cisco.asr-server" value=“asrserver.com" />

Set Up the VoiceXML Document Properties

Procedure

Step 1 In Unified Call Studio, view the properties for the AgeIdentification.

Step 2 Specify the VoiceXML document properties at either the root or node level.

Step 3 Select **Properties** > **General Settings** > **Language**, and specify “en–us” as the language.

Certain third-party software and hardware are compatible only with US English.

Example Gateway Configuration for MRCPv2 with Failover

```
-----------------Primary Server-----
ip host asr-en-us 10.78.26.83
ip host tts-en-us 10.78.26.83
ivr asr-server sip:asr@asr-en-us
ivr tts-server sip:tts@tts-en-us

voice class uri ASR sip
pattern asr@asr-en-us*
voice class uri TTS sip
pattern tts@tts-en-us*

dial-peer voice 5 voip
destination uri ASR
session target ipv4:10.78.26.83
session protocol sipv2
dtmf-relay rtp-nte
codec g711ulaw
no vad

dial-peer voice 6 voip
destination uri TTS
session target ipv4:10.78.26.83
session protocol sipv2
dtmf-relay rtp-nte
codec g711ulaw
no vad

-------Backup --------------------
dial-peer voice 7 voip
destination uri ASR
session target ipv4:10.78.26.20
session protocol sipv2
dtmf-relay rtp-nte
codec g711ulaw
preference 2
no vad

dial-peer voice 8 voip
destination uri TTS
session target ipv4:10.78.26.20
session protocol sipv2
dtmf-relay rtp-nte
codec g711ulaw
```

```
preference 2
no vad
```

Unified CVP Call Servers

Note Call Server load balancing is only supported on *IVR only* deployments.

Probes

The probe below is used to determine whether the Call Server is up and in service. The probe passes only if the Call Server is *In Service*. This probe is an HTTP probe using the load balancer.

The load balancer Call Server probe sends an HTTP request to **/cvp/VBServlet?MSG_TYPE=HEARTBEAT&TIMEOUT=0**. This probe takes a little more than 4 seconds to send back a response. If the Call Server is *In Service*, the HTTP 200 OK response returns.

To create the Call Server HTTP probe, place the following lines in the configuration for the load balancer:

```
    probe http PROBE_CALLSERVER_HTTP
    port 8000
    interval 6
    faildetect 1
    passdetect interval 6
    passdetect count 1
    receive 5
request method get url /cvp/VBServlet?MSG_TYPE=HEARTBEAT&TIMEOUT=0

    open 1
    expect status 200 200
```

Related Topics

Create Policy Based QoS, on page 123

Unified CVP VXML Servers

Real Servers: Configure the Physical Servers

Create a real server for every physical VXML Server you would like to load balance. Associate the probe with each server by creating a section, as shown in the following example, for each VXML server in the server farm.

```
rserver host vxml1
probe PROBE_SERVICE_ICMP
ip address 10.1.1.15
inservice
rserver host vxml2
probe PROBE_SERVICE_ICMP
ip address 10.1.1.16
inservice
```

HTTP Probe Configuration

The probe below is used to determine whether the VXML Server is up and in service. The probe passes only if the VXML Server is *In Service* . To create the VXML Server HTTP probe, place the following lines in the configuration for the load balancer.

The VXML Server probe sends an HTTP request to /CVP/Server?probe=true. If the VXML Server is up and inservice, HTTP 200 OK is returned. In the HTTP probe below, the http request is made to the port specified in the probe and the IP of the real server that this probe is associated with.

```
probe http PROBE_VXMLSERVER_HTTP
port 7000
interval 5
receive 3
faildetect 1
passdetect interval 5
passdetect count 1
request method get url /CVP/Server?probe=true
expect status 200 200
open 1
```

Note In order to get the "?", press CTRL-V before pressing the question mark.

Server Farm Configuration

```
serverfarm host vxmlserver
probe PROBE_VXMLSERVER_HTTP
rserver vxml1 7000
inservice
rserver vxml2 7000
inservice
```

Sticky Server Farm

For a VXML Server to preserve HTTP session information, you must ensure that, once the load balancer has chosen a particular VXML Server from the list of servers in a server farm, the load balancer continues to send all traffic for that session to the same VXML Server. To accomplish this, use a *sticky group* .

The following definitions apply to the settings shown below:

- **http-cookie:** Sticky method being used. In this method, when the load balancer examines a request for content, and determines through policy matching that the content is sticky, the load balancer examines any cookie or URL present in the content request. The load balancer uses the information in the cookie or URL to direct the content request to the appropriate server.
- **Cookie insert:** The load balancer inserts the cookie on behalf of the VXML Server upon the return request, so that the load balancer can perform cookie stickiness even when the VXML servers are not configured to set cookies. The cookie contains information that the load balancer uses to ensure persistence to a specific real server.

Class map Configuration

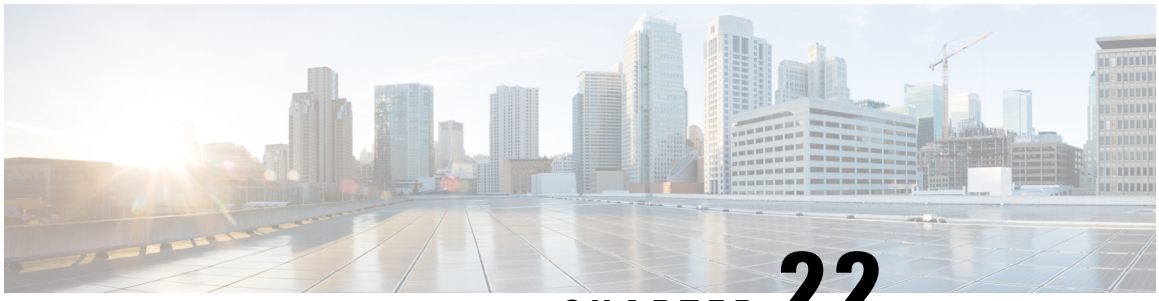
```
class-map match-all vxmlserver_HTTP_CLASS_L3
2 match virtual-address 10.1.1.17 tcp eq 7000
```

Policy map Configuration

```
policy-map type loadbalance first-match vxmlserver_HTTP_POLICY_L7

  class L7_HTTP_CLASS
  sticky-serverfarm VXMLServer_HTTP_STICKY

  policy-map multi-match POLICY
  class vxmlserver_HTTP_CLASS_L3
  loadbalance vip inservice
  loadbalance policy vxmlserver_HTTP_POLICY_L7
  loadbalance vip icmp-reply active
```



CHAPTER 22

IPv6 Configuration

Configure IPv6 on Unified CVP Call Server

For IPv6-enabled deployments, you must add an IPv6 address to your Unified CVP Call Server's existing network interface.

Procedure

Step 1 On the Unified CVP Call Server, navigate to **Control Panel** > **Network and Sharing**.

Step 2 Click **Ethernet**.

Step 3 From the **Ethernet Status** window, select **Properties**.

Step 4 Check the **Internet Protocol Version 6 (TCP/IPv6)** check box, and choose **Properties**.

Step 5 Choose **Use the following IPv6 address** radio button.

Step 6 Enter values in the **IPv6 address**, **Subnet prefix length**, and **Default gateway** fields.

Step 7 Click **OK** and restart Windows when prompted.

Configure IPv6 on Unified Communications Manager

Enable IPv6 in Unified Communications Manager

Perform the following procedure to enable IPv6 on all the Unified Communications Manager in your cluster.

Procedure

Step 1 From **Cisco Unified Operating System Administration**, navigate to **Settings** > **IP** > **Ethernet IPv6**.
Step 2 Check the **Enable IPv6** check box.
Step 3 Enter the values in the **IPv6 Address**, **Prefix Length**, and the **Default Gateway** fields.
Step 4 Click **Save**.

Cluster-Wide Configuration in Unified CM Administration

Perform the following procedure to set IPv6 as the addressing mode preference for media and signaling cluster-wide.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **System** > **Enterprise Parameters** > **IPv6 Configuration Modes** to configure the cluster-wide IPv6 settings for each Unified Communications Manager server.
Step 2 From the **Enable IPv6** drop-down list, choose **True**.
Step 3 From the **IP Addressing Mode Preference for Media** drop-down list, choose **IPv6**.
Step 4 From the **IP Addressing Mode Preference for Signaling** drop-down list, choose **IPv6**.
Step 5 From the **Allow Auto-configuration for Phones** drop-down list, choose **Off**.
Step 6 Save your changes.

Add a Common Device Configuration Profile in Unified Communications Manager

In an IPv6-enabled environment, you may have both IPv4 and IPv6 devices.

Perform the following procedure to add an IPv4, IPv6, or dual stack common device configuration profile in Unified Communications Manager.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **Common Device Configuration**.
Step 2 Click **Add New** and enter the name of the new common device configuration profile.
Step 3 From the **IP Addressing Mode** drop-down list:

- To add an IPv6 common device configuration profile in Unified Communications Manager, choose **IPv6 only**.

- To add an IPv4 common device configuration profile in Unified Communications Manager, choose **IPv4 only**.
- To add a dual stack common device configuration profile in Unified Communications Manager, choose **IPv4 and IPv6**. Then choose **IPv4** from the **IP Addressing Mode Preference for Signaling** drop-down list.

Step 4 Save your changes.

Associate the Common Device Configuration Profile with Gateway Trunk

Perform the following procedure to associate the common device configuration profile with the Gateway trunk. This procedure applies to the Ingress Gateway.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list:

- To associate the IPv6 common device configuration profile with the Gateway trunk, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile with the Gateway trunk, choose the IPv4 common device configuration profile.

Note Unified CM gateway trunk supports only an IPv4 or IPv6 trunk. You cannot associate a dual stack common device configuration profile to a Unified CM gateway trunk.

Step 4 Enter the IPv6 address in the **Destination Address IPv6** field.

Note Unified CM to Gateway trunk supports only standard SIP Profile and does not support ANAT enabled dual-stack SIP trunk.

Step 5 Save your changes.

Associate the Common Device Configuration Profile with an IPv4 or IPv6 Phone

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list: choose the IPv6 common device configuration profile.

- To associate the IPv6 common device configuration profile to an IPv6 phone, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile to an IPv4 phone, choose the IPv4 common device configuration profle.

Step 4 Save your changes.

Configure SIP trunk from Unified Communications Manager to Unified CVP

The following sections describe the steps to configure the SIP trunk from Unified Communications Manager to Unified CVP.

Add a SIP Profile in Unified CM

This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Perform this procedure for IPv6-enabled deployments only.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Click **Add New** and enter the name of the SIP profile.

Step 3 Check the **Enable ANAT** check box on the SIP Profile.

Step 4 Save your changes.

Associate the Dual Stack Common Device Configuration Profile with SIP Trunk

You only need to perform this procedure if you have an IPv6 enabled deployment.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**. Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list, choose the Dual Stack Common Device Configuration Profile.

Note For more information on how to add a Dual Stack Common Device Configuration Profile, see Add a Common Device Configuration Profile in Unified Communications Manager, on page 478.

Step 4 Save your change.

Related Topics

Add a Common Device Configuration Profile in Unified Communications Manager, on page 478

Gateway Configuration

Configure an Interface to Support IPv6 Protocol Stack

This procedure applies to both the Ingress and the VXML gateway.

Procedure

Configure the following on the Gateway:

```
>Enable
>configure terminal
>interface type number
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

Enable ANAT in Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>voice service voip
>SIP
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

Enable Dual Stack in the Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
```

```
>sip-ua
>protocol mode dual-stack preference ipv6
```

Transcoder Configuration in Unified CM and IOS Gateway

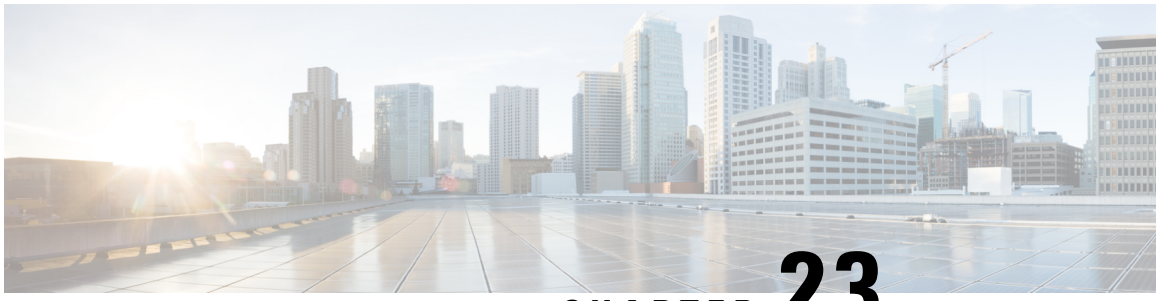
A transcoder is required in the following scenarios

- An agent logged in to an IPv6 endpoint needs to send or receive transfers from an agent logged in to an IPv4 endpoint.
- An agent logged in to an IPv6 endpoint needs to connect to a VXML Gateway for self service.
- A multicodec scenario to convert a stream from a G.711 codec to G.729 codec.

For more information about transcoder configuration in Unified Communications Manager and gateway, see the section "Configure Transcoders and Media Termination Points" in the *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Configure the CVP Call Server Dial Peers in Ingress Gateway

The Ingress Gateway to Unified CVP outbound dial peer configuration uses the IPv4 address of Unified CVP as the session target.



CHAPTER 23

Network-based Recording Configuration

CUCM Configuration

Network- based recording is configured using Cisco Unified Communications Manager Administration. Network-based recording is controlled by using a recording profile assigned to the line. The recording can be selective or full-time audio-only recording. You can either configure CUBE or phone as the forking device and you can change the forking device during a call.

Create a Recording Profile

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Device** > **Device Settings** > **Recording Profile**.

Step 2 To add a new recording profile, click **Add New**.

Step 3 In the **Name** field, enter a name to identify the recording profile.

Step 4 In the **Recording Destination Address** field, enter the directory number (DN) or the URL of the recorder that associates with this recording profile. This field allows any characters except the following characters: double quotation marks (“), back quote (‘), and space ( ).

Step 5 Click **Save**.

Configure the SIP Trunk from CUCM to Recording Server

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Device** > **Trunk**.

Step 2 To add a new SIP trunk, click **Add New**.

Step 3 In the **Device Name** field, enter a unique identifier for the trunk (which is the IP address of the Recording server).

Note For Call Transcript, the IP address should be that of the Call Server.

Step 4 In the **Description** field, enter a name for the trunk.

Step 5 From the **SIP Profile** drop-down list, choose **Standard SIP Profile** for this SIP trunk.

Step 6 In the **Recording Information** section, click **None**.

Step 7 Click **Save**.

Creating a Recorder Route Group

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Call Routing** > **Route/Hunt** > **Route Group**.

Step 2 In the **Available Devices** drop-down list, choose a device to add and click **Add to Route Group** to move it to the **Selected Devices** list box. Repeat this step for each device that you want to add to this route group.

Note If an SIP trunk is already configured for CVP, **Route Group** does not list that trunk.

Step 3 In the **Selected Devices** drop-down list, choose the order in which the new device or devices must be accessed in this route group. To change the order of devices, click a device and use the **Up** and **Down** arrows to the right of the list box.

Step 4 To add the new device or devices, and to update the device order for this route group, click **Save**.

Add a Route Group to a Route List

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, select **Call Routing** > **Route/Hunt** > **Route List**.

Step 2 Select the route list to which you want to add the route group.
The **Route List Configuration** page is displayed.

Step 3 Click **Add Route Group**.
The **Route List Details Configuration** page is displayed.

Step 4 Select/enter values for the fields.

Step 5 Click **Save**.
A confirmation message is displayed.

Step 6 Click **OK**.
The route list configuration is saved and the route group is added.

Create a Route Pattern Based on the DN for the Recorder

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.
The **Find and List Route Patterns** page is displayed.

Step 2 Select the route list for which you are adding a route pattern.
The **Route Pattern Configuration** page is displayed.

Step 3 Select/enter values for the fields.

Step 4 Click **Save**.
A confirmation message is displayed.

Step 5 Click **OK**.

Configure the Device Phone for Recording

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Device** > **Phone**. Click **Find** to list the phones.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Association Information** area, click the link associated with your phone.

Step 4 From the **Recording Option** drop-down list, choose one of the following options:

- **Call Recording Disabled**—The calls that the agent makes on this line appearance are not recorded.
- **Automatic Call Recording Enabled**—The calls that the agent makes on this line appearance are automatically recorded.
- **Application Invoked Call Recording Enabled**—The calls that the agent makes on this line appearance are recorded if an application invokes calling recording.
- **Device Invoked Call Recording Enabled**—This option supports the external call control feature. If the policies on the policy server dictate that a chaperone must monitor and record calls, choose this option.

Step 5 From the **Recording Profile** drop-down list, choose an existing recording profile.

Step 6 Set the **Recording Media Source** preference (either Phone Preferred or Gateway Preferred) when enabling recording on the line appearance of the device.

Step 7 Click **Save**.

Enable the Device Phone for Recording

Procedure

Step 1 To enable phone-based recording, choose **Device** > **Phone** from **Cisco Unified Communications Manager Administration**.

Step 2 From the **Built In Bridge** drop-down list, choose **On**.

Step 3 If the recorder does not support codecs (for example, G.722, ILIBC), enable Cisco Unified CM to ignore the preference if audio codecs.

a) Choose **System** > **Service Parameters**.
b) From the **Server** drop-down list, choose the server.
c) From the **Server** drop-down list, choose the service that contains the **Accept Audio Codec Preferences in Received Offer** parameter.
d) From the **Accept Audio Codec Preferences in Received Offer** drop-down list, choose **Off**.
e) Click **Save**.

Configure the Ingress Gateway for Recording

Procedure

Step 1 From **Cisco Unified Communications Manager Administration**, choose **Device** > **Trunk**.

Step 2 In the **Device Name** field, enter the IP address of the Ingress Gateway.

Step 3 From the **Device Pool** drop-down list, choose **Default**.

Step 4 From the **Call Classification** drop-down list, choose **Use System Default**.

Step 5 From the **Location** drop-down list, choose **Hub_None**.

The locations feature does not track the bandwidth that this device consumes.

Step 6 From the **AAR Group** drop-down list, choose **None**.

Step 7 From the **Tunneled Protocol** drop-down list, choose **None**.

Step 8 From the **QSIG Variant** drop-down list, choose **No Changes.**.

Step 9 From the **ASN.1 ROSE OID Encoding** drop-down list, choose **No Changes**.

Step 10 From the **Packet Capture Mode** drop-down list, choose **None**.

Step 11 In the Recording Information area, click the **This trunk connects to a recording-enabled gateways** radio button.

Step 12 Click **Save**.

Configure the Outgoing Trunk from CVP to CUCM

Procedure

Step 1 To create a new SIP profile for recording, choose **Device** > **Device Settings** > **SIP Profile** from **Cisco Unified Communications Manager Administration**.

Step 2 To add a new SIP profile, click **Add New**.

Step 3 In the **Name** field, enter a name to identify the SIP profile.

Step 4 In the **Default MTP Telephony Event Payload Type** field, enter the default value, 101.

Step 5 From the **Early Offer for G.Clear Calls** drop-down list, choose **Disabled** to disable Early Offer for G.Clear Calls.

Step 6 From the **User-Agent and Server header information** drop-down list, choose **Send Unified CM Version Information as User-Agent Header**.

Step 7 From the **Version in User-Agent and Server Headers** drop-down list, choose **Major and Minor**.

Step 8 From the **Dial String Interpretation** drop-down list, choose **Phone number**.

Step 9 From the **Confidential Access Level Headers** drop-down list, choose **Disabled**.

Step 10 From the **SDP Session-level Bandwidth Modifier for Early Offer and Re-invites** drop-down list, choose **TIAS and AS**.

Step 11 From the **Accept Audio Codec Preferences in Received Offer** drop-down list, choose **Default**.

Step 12 Click **Save**.

Gateway Setup for Network-based Recording

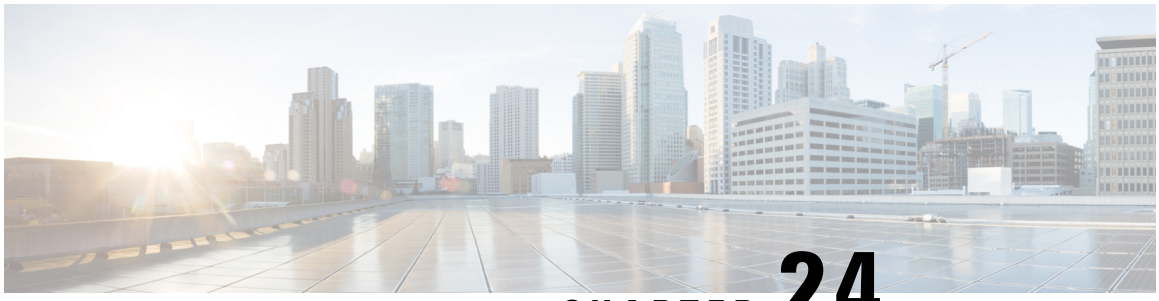
To set up the gateway for network-based recording, use the following Telnet command in CLI Enable mode:

```
uc wsapi
  message-exchange max-failures 100
  response-timeout 300
  source-address <IP address of gateway>
  probing interval negative 20
  probing interval keepalive 255

  provider xmf
  remote-url 1 http://<IP address of CUCM>:8090/ucm_xml
```

Note

- When using ISR G2 for network-based recording, ensure that the VXML Voice Gateway functionality is not enabled on the same gateway.
- In case of multiple subscribers, specify the URL for each subscriber and select the **Run on All Active CM Nodes** check box in CUCM SIP trunk.
- For more information, please refer the section **Network-Based Recording** in **Cisco Unified Border Element Configuration Guide** at https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html.



CHAPTER 24

Java Runtime Environment Minor Update

Java Runtime Environment Minor Update

Use the *JREUpdate.bat* script to install a minor update of Java Runtime Environment (JRE) version on your Unified CVP Server. For example, you can install a minor update of JRE version 1.8.0_275 to 1.8.0_x.

Note The script does not support a major upgrade of JRE versions. For example, the script does not allow a major upgrade of JRE Version 1.8 to 1.9/1.10.

Note From **12.6(1)** ES-12 and higher releases, only OpenLogic OpenJDK is supported.

Procedure

Step 1 Download and unzip the Java Development Kit (JDK) folder on your CVP machine.

Step 2 Copy the JRE folder from the JDK root folder to a known location on the Unified CVP Server. For example, `C:\JRE`.

Note The *jre* folder is available in the JDK root folder. For example: `C:\openlogic-openjdk-8u332-b09-windows-64\jre`.

Step 3 Go to the *bin* folder within the JDK root folder. For example *C:\openlogic-openjdk-8u332-b09-windows-64\bin*. Copy the *jconsole* application file and paste it in the path mentioned in Step 2 (*C:/JRE*).

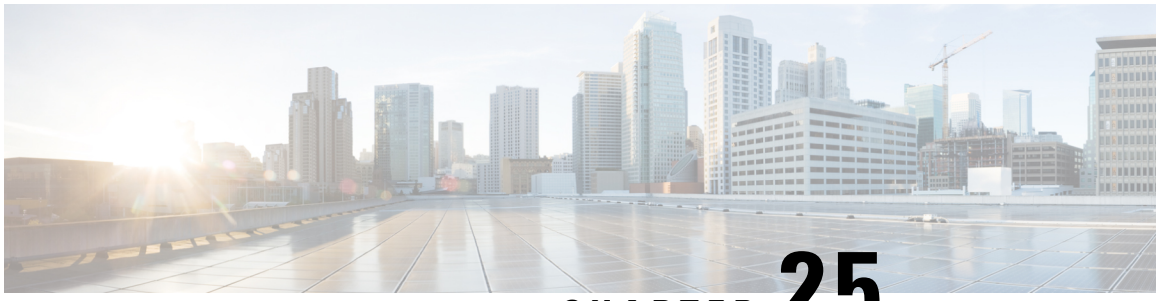
Step 4 Go to the *lib* folder within the JDK root folder. For example *C:\openlogic-openjdk-8u332-b09-windows-64\lib*. Copy the *jconsole* executable jar file and paste it in the same path mentioned in Step 2 (*C:/JRE*).

Step 5 Go to *C:/Cisco/CVP/bin* and right-click the *JREUpdate.zip* file and extract the files to a known location on your Unified CVP Server. For example, `C:\Cisco\CVP\bin`.

Step 6 Run this script from the command prompt: **C:\Cisco\CVP\bin >JREUpdate.bat apply C:\JRE**.
The script runs and Unified CVP JRE is updated to the new version.

Step 7 Ensure that the script output displays the updated JRE version.

The *JREUpdate.bat* script takes a backup of the old JRE to `C:\Cisco\CVP\jre.old` folder location. To revert to the previous backup version of JRE, run this script from the command prompt: **C:\Cisco\CVP\bin>JREUpdate.bat revert**.



CHAPTER 25

Tomcat Update

Tomcat Update

Perform the following procedure to update Tomcat version on Call Server, Operations Console, VXML Server, and Web Services Manager (WSM). For example, you can update from Tomcat version 9.0.8 to 9.0.x.

Perform the following procedure to update Tomcat version on Call Server, Operations Console, VXML Server, and Web Services Manager (WSM). For example, you can update from Tomcat version 9.0.43 to 9.0.x.

Before you begin

- Save a backup copy of the Tomcat folder from the following locations:
  - For Call Server: `C:\Cisco\CVP\CallServer`
  - For VXML Server: `C:\Cisco\CVP\VXMLServer`
  - For Operations Console: `C:\Cisco\CVP\OPConsoleServer`
  - For WSM: `C:\Cisco\CVP\wsm\Server`

Note Save a backup copy of the Tomcat folder on a directory path that is different from the default destination folder (C:\Cisco\CVP).

- Rename the Tomcat folders with a different name. For example: Tomcat_backup.

Procedure

Step 1 Stop the following Tomcat services:

- Cisco CVP Call Server
- Cisco CVP Operations Console Server

- Cisco CVP VXML Server
- Cisco CVP Web Services Manager

Step 2 Remove the Tomcat folder from the following locations:

- For Call Server: `C:\Cisco\CVP\CallServer`
- For VXML Server: `C:\Cisco\CVP\VXMLServer`
- For Operations Console: `C:\Cisco\CVP\OPConsoleServer`
- For WSM: `C:\Cisco\CVP\wsm\Server`

Step 3 Download the Tomcat binary apache-tomcat-9.0.x-windows-x64.zip file from the following location: https://archive.apache.org/dist/tomcat/tomcat-9/.

Step 4 Right-click the apache-tomcat-9.0.x-windows-x64.zip file and extract the files to a known location on the local drive.

Step 5 Rename the folder apache-tomcat-9.0.x to Tomcat.

Step 6 Copy the Tomcat folder to the following locations:

- For Call Server: `C:\Cisco\CVP\CallServer`
- For VXML Server: `C:\Cisco\CVP\VXMLServer`
- For Operations Console: `C:\Cisco\CVP\OPConsoleServer`
- For WSM: `C:\Cisco\CVP\wsm\Server`

Step 7 Copy the webapps file from the Tomcat_backup folder (`...\Tomcat_backup\webapps`) and paste it in the following folder locations:

- For Call Server: `C:\Cisco\CVP\CallServer\Tomcat`
- For VXML Server: `C:\Cisco\CVP\VXMLServer\Tomcat`
- For Operations Console: `C:\Cisco\CVP\OPConsoleServer\Tomcat`
- For WSM: `C:\Cisco\CVP\wsm\Server\Tomcat`

Step 8 Copy the missing jar files from the Tomcat_backup folder (`..\Tomcat_backup\lib`) to the following locations:

- For Call Server: `C:\Cisco\CVP\CallServer\Tomcat\lib`
- For VXML Server: `C:\Cisco\CVP\VXMLServer\Tomcat\lib`
- For Operations Console: `C:\Cisco\CVP\OPConsoleServer\Tomcat\lib`
- For WSM: `C:\Cisco\CVP\wsm\Server\Tomcat\lib`

Note Copy the contents of the `..\Tomcat_backup\Shared folder` to `C:\Cisco\CVP\OPSConsoleServer\Tomcat\`.

Step 9 Copy the `context.xml` file from the Tomcat_backup folder (`..\Tomcat_backup\conf`) to the following locations:

- For Call Server: `C:\Cisco\CVP\CallServer\Tomcat\conf`
- For VXML Server: `C:\Cisco\CVP\VXMLServer\Tomcat\conf`
- For Operations Console: `C:\Cisco\CVP\OPConsoleServer\Tomcat\conf`
- For WSM: `C:\Cisco\CVP\wsm\Server\Tomcat\conf`

Step 10 Update the new server.xml files with the existing properties from the backed up server.xml files.

Step 11 For wsm Tomcat upgrade, ensure the`jaas.conf` from the backed up Tomcat folder is copied to the new `Tomcat/conf` folder.

Step 12 Back up **connector.property** that was created before starting the process from:.

- For Operations Console:
  `C:\Cisco\CVP\OPConsoleServer\Tomcat_backup\bin\connector.property`
- For VXML Server:
  `C:\Cisco\CVP\VXMLServer\Tomcat_backup\bin\connector.property`

Step 13 Restore these to:

- For Operations Console:
  `C:\Cisco\CVP\OPConsoleServer\Tomcat\bin\connector.property`
- For VXML Server: `C:\Cisco\CVP\VXMLServer\Tomcat\bin\connector.property`

Step 14 Restart the following Tomcat services:

- Cisco CVP CallServer
- Cisco CVP OPSConsoleServer
- Cisco CVP VXMLServer
- Cisco CVP WebServicesManager

Step 15 Ensure that the CVP Diag portal is up and running.

Step 16 Check Tomcat and CVP logs for any exceptions.

Running Tomcat Service without Administrator Privileges

Procedure

Step 1 Create a Windows user, for example, *cvp_guest*.

Step 2 In `C:\Cisco` folder, grant read, write, modify permission to cvp_guest.

Step 3 Grant permission to cvp_guest to access the machine remotely (to allow remote connection capability in future) by right clicking **This Computer** from `File Explorer > Properties > Remote Settings > Allow remote connections to this computer > Select Users > Add, type the name of the new user (eg. cvp_guest) > Check Names > OK`.

Step 4 Log out as the current user, and log on as cvp_guest.

Step 5 Get the SID of the cvp_guest user to grant cvp_guest the required permissions to start and stop the Windows services.

a) Go to `Start > regedit > HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\`.

b) Browse to the folder that has the **ProfileImagePath** value as `C:\Users\cvp_guest`.

c) Right-click that folder and select **Copy Key Name** to copy the key name to Notepad. By default, the key name appears with the full path. Copy only the last part (for example, S-1-5-21-1386459338-4158420048-3623644462-1067).

Step 6 Log out as cvp_guest and log in as Administrator to assign permission to cvp_guest for starting and stopping the Tomcat service(s) that are to be run on that node.

a) Go to command prompt and run: sc.exe sdshow **<service_name>**. For example, on a Call Server node, type **sc.exe sdshow callserver** in the command prompt. Refer to the following table for all possible values of <service_name>.

Sample Output:

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA) (A;;CCLCSWLOCRRC;;;IU)
(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

This output lists the permissions for each user and group on this system.

Copy this output for reference and use in the following steps.

b) Suffix the key to **A;;RPWPCR;;;** (for example: A;;RPWPCR;;;<KEY_NAME>) and insert it in the output from Step 6a just before 'S:' as shown:

Example:

```
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
(A;;RPWPCR;;;S-1-5-21-1386459338-4158420048-3623644462-1067)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Step 7 Go to command prompt and run **sc.exe sdset <service_name> <Output from Step 6b>**

Example:

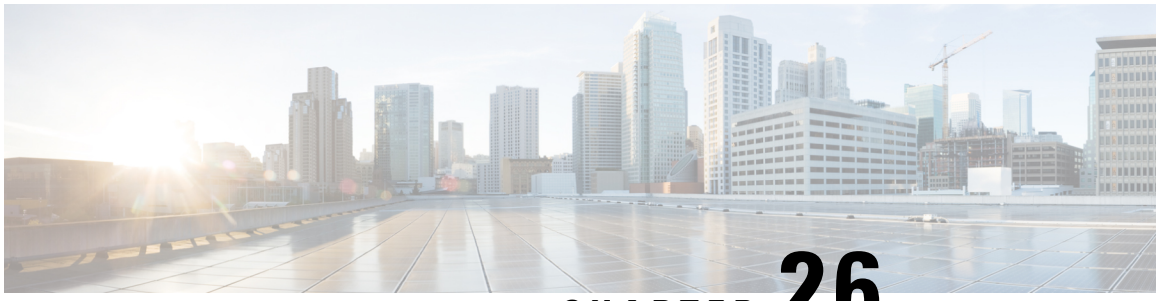
```
sc.exe sdset callserver "D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPCR;;;S-1-5-21-1386459338-4158420048-3623644462-1067)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
```

Depending on which CVP services are to be run on a node, grant permissions to the cvp_guest as follows. For example: on a Call Server node, run Steps 6 and 7 for 'callserver' and 'vxmlserver' Tomcat services.

Use the following table to refer to the possible values of <service_name> in the above commands to be run on each node:

Node	Service	<service_name>
Call Server/VXML Server	Call Server	callserver
	VXML Server	vxmlserver
	Web Services Manager	WebServicesManager
	SNMP Management	"Cisco CVP SNMP Management"
OAMP	OPS Console Server	OPSConsoleServer
	Web Services Manager	WebServicesManager
	SNMP Management	"Cisco CVP SNMP Management"

Node	Service	<service_name>
Reporting Server	Call Server	callserver
	Web Services Manager	WebServicesManager
	SNMP Management	"Cisco CVP SNMP Management"
	Informix IDS	cvp



CHAPTER 26

Webex Experience Management Configuration

Import Experience Management Certificate to Unified CVP Call Server

CVP VXML server fetches the authorization token from the Cloud Connect server and reaches the Experience Management platform to download the desired questionnaire. To succesfully interact and download the information from Experience Management, CVP server requires the Experience Management certificate in its keystore. Perform the following steps to export the certificate and to import it in CVP server.

Procedure

Step 1 Export the Experience Management platform certificate:

a) Open a Chrome browser session and navigate to https://api.getcloudcherry.com/api/Questions/Questionnaire.

b) Click the lock icon in the address bar and click **Certificate (Valid)**.

c) Under the **Details** tab, click **Copy to File** to export the certificate and save it as a *Base-64 encoded X.509 (.CER)* file with the name *CloudcherryAPI.cer* (the file to be imported in the next step).

Step 2 Import the certificate into the CVP keystore:

a) Copy the exported certificate to the following directory of all CVP call servers: *C:\Cisco\CVP\conf\security*

b) Import these certificates using the command: `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -trustcacerts -alias {apicloudcherry_name} -file c:\cisco\cvp\conf\security\CloudcherryAPI.cer`

Step 3 Export the Experience Management platform Azure certificate:

a) Open a Chrome browser, navigate to https://learn.microsoft.com/en-us/azure/security/fundamentals/azure-ca-details, and download the `DigiCert Global Root G2` certificate.

b) Check the certificate which is downloaded as `DigiCert Global Root G2.crt`.

Step 4 Import the certificate into the CVP keystore:

a) Copy the exported certificate to the following directory of all CVP call servers: *C:\Cisco\CVP\conf\security as DigiCert_Global_Root_G2.crt*
b) Import this certificate using the command: `%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -trustcacerts -alias {apicloudcherry_azure} -file c:\cisco\cvp\conf\security\DigiCert_Global_Root_G2.crt`

Step 5 Restart the CVP server.

Note While importing the certificate, CVP requests for a password. For generating the keystore password, go to the `%CVP_HOME%\bin` folder and run the `DecryptKeystoreUtil.bat` file.

Note If the Certificate Authority (CA) signed certificate on Cloud expires as per policy, the new certificate needs to be imported to the CVP Server.

Experience Management Voice Survey Thresholds

Experience Management voice survey is used for getting feedback on the overall customer journey experience.

The following default configurations are used for this feature:

In `c:\cisco\cvp\conf\ivr.properties` file:

Property	Description	Configurable/ Non-Configurable?	Value
IVR.AuthTokenRefresh TimeOut	Time in seconds after which AuthToken is refreshed	Yes	1800
IVR.SurveyTokenRefresh TimeOut	Time in seconds after which SurveyToken is refreshed	Yes	43200
IVR.SurveyQuestionRefresh TimeOut	Time in seconds after which SurveyQuestions is refreshed	Yes	43200
IVR.WxmSurveyToken ApiUrl	Url to connect to fetch the survey token from Wxm	Yes	https://api.getcloudcherry.com/api/SurveyToken
IVR.WxmSurveyQuestions ApiUrl	Url to connect to fetch the questionnaire from Wxm	Yes	https://api.getcloudcherry.com/api/Questions/Questionnaire

Property	Description	Configurable/ Non-Configurable?	Value
IVR.WxmSurveyAnswers SubmitApiUrl	Url to connect to submit the answers to Wxm	Yes	https://api.getcloudcherry.com/api/Survey ByToken/
IVR.WxmSurveySettings ApiUrl	Url to connect to fetch the settings of the questionaire from Wxm	Yes	https://api.getcloudcherry.com/api/Settings/
IVR.WxmAudio Url	Url to connect to fetch the audio files from Wxm	Yes	https://api.getcloudcherry.com/api/Stream UserAsset/
IVR.WxmSurveyQuestionnaire Url	Url to connect to fetch the questionnaire settings from Wxm	Yes	https://api.getcloudcherry.com/api/surveyquestionnaire/

In `c:\cisco\cvp\conf\sip.properties` file:

Property	Description	Configurable/Non-Configurable?	Value
SIP.CloudCherrySurveyValidity Time	Time in seconds for which the survey is active	Yes	60000
SIP.CloudConnectSurveyDispatch EndPointApi	Url for connecting Cloud Connect to get the SurveyDispatch EndPoint	Yes	/cherrypoint/surveydispatch
SIP.CloudConnect.Auth TokenApi	Url for connecting Cloud Connect to get AuthToken for Wxm	Yes	/cherrypoint/authtoken

Procedure

Sample

Experience Management SMS/Email Thresholds

Experience Management SMS/Email-based survey is used to send the survey link to the callers for getting feedback on the overall customer journey experience.

The following batch threshold properties which trigger the SMS/Email Cloud Connect API have to be configured (if not already configured) for this feature:

In `c:\cisco\cvp\conf\ivr.properties` file:

Property	Description	Configurable/ Non-Configurable?	Default Value
IVR.CloudCherryBatchSize	Batch size for triggering the Email/SMS Cloud Connect API	Yes	100
IVR.CloudCherryBatch Timeout	Batch timeout (in seconds) for triggering the Email/SMS Cloud Connect API	Yes	60

Note Customers can optimize these values based on their deployment requirements.

In `c:\cisco\cvp\conf\sip.properties` file:

Property	Description	Configurable/ Non-Configurable?	Value
SIP.CloudConnect.Request Timeout	HTTP request connection timeout (in milliseconds) towards Cloud Connect component	Yes	10000 **Note** The timeout value can be increased as per environment.

Procedure

Sample

HTTP Proxy Settings in VXML Server

For Experience Management to function, the VXML server must be connected to the internet. Enable direct access to the internet or configure HTTP proxy settings in the VXML server. To configure HTTP proxy settings in VXML server, perform the following steps:

Procedure

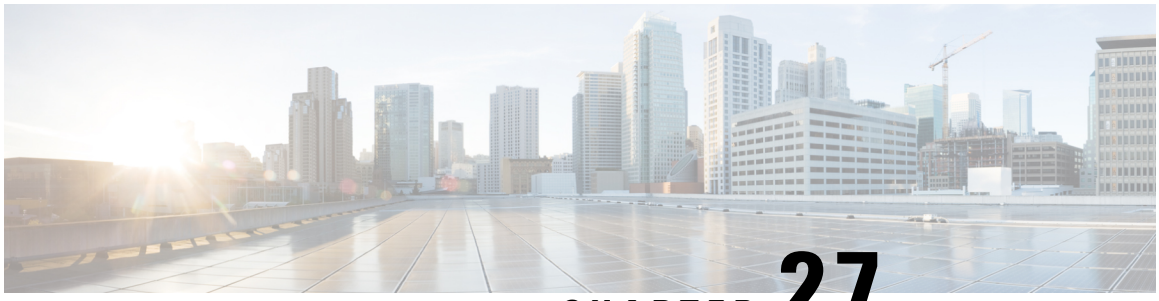
Step 1 Open Windows regedit in the VXML server.

Step 2 Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java\Options`.

Step 3 Add the following entries:

```
-Dhttp.proxyHost=<proxy IP>
-Dhttp.proxyPort=<proxy port>
-Dorg.asynchttpclient.useProxyProperties=true
-Dhttp.nonProxyHosts=<hostname>
```

Step 4 Restart the CVP VXML server from Windows services.



CHAPTER 27

CCAI Services Configuration

HTTP Proxy Settings in Call Server

For Agent Answers and other CCAI services to function, the Call server must be connected to the internet. Enable direct access to the internet or configure HTTP proxy settings in the Call server. To configure HTTP proxy settings in Call server, perform the following steps:

Procedure

Step 1 Open Windows regedit in the Call server.

Step 2 Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\CallServer\Parameters\Java\Options`.

Step 3 Add the following entries:

```
-Dhttp.proxyHost=<proxy IP>
-Dhttp.proxyPort=<proxy port>
-Dorg.asynchttpclient.useProxyProperties=true
-Dhttp.nonProxyHosts=<hostname>
```

Step 4 Restart the CVP Call server from Windows services.

HTTP Proxy Settings in OAMP Server

For Agent Answers and other CCAI services to function, the OAMP server must be connected to the internet. Enable direct access to the internet or configure HTTP proxy settings in the OAMP server. To configure HTTP proxy settings in OAMP server, perform the following steps:

Procedure

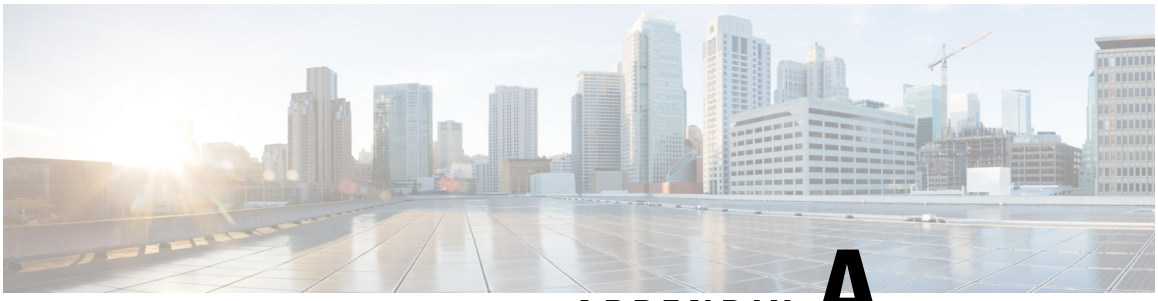
Step 1 Open Windows regedit in the OAMP server.

Step 2 Go to `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java\Options`.

Step 3 Add the following entries:

```
-Dhttp.proxyHost=<proxy IP>
-Dhttp.proxyPort=<proxy port>
-Dorg.asynchttpclient.useProxyProperties=true
-Dhttp.nonProxyHosts=<hostname>
```

Step 4 Restart the OAMP server from Windows services.



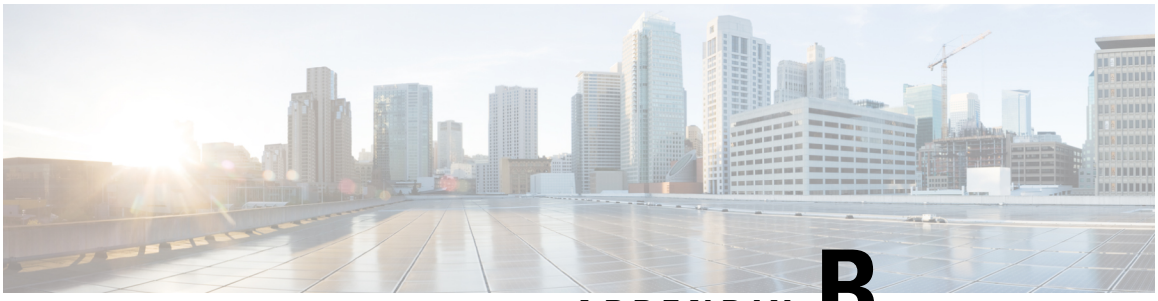
APPENDIX A

Internal REST API Endpoints

Following authenticated REST API endpoints are exposed for internal invocation from within the solution. These REST API endpoints are listed for information purposes only, and not intended for external consumption currently. If you have a valid use case to know more, please get in touch with the product team.

```
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/sipservergroup
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/sipservergroup/properties
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/location
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/location/properties
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/dialednumber
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/routepattern
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/cvpconfig
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/cloudconnectconfig
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/callserver/associatereporting
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/reporting/associatecallservers
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/reporting/deploy
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/reporting/undeploy
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/callserver/deassociatereporting
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/vxmlapplications
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/cvpconfig/properties
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/stats
https://<CVP_HOSTNAME_OR_IP>:8111/cvp-orm/rest/smartlicense/smartlicenseinfo
```

Internal REST API Endpoints



APPENDIX B

New Properties for WXM, VAV, Agent Answers, and Smart Licensing

Webex Experience Management

```
SIP.CloudCherry.SurveyValidityTime = 60000
SIP.CloudConnect.SurveyDispatchEndPointApi = /cherrypoint/surveydispatch
```

VAV Onboarding

```
IVR.CcaiOrgUrl = /cloudconnectmgmt/config
IVR.CcaiConfigUrl = cms/api/auxiliary-data/resources/ccai-config
IVR.CcaiCredentialUrl = _config/organization/%s/credentials/%s/access-token
IVR.CcaiCatalogUrl = /u2c/api/v1/user/catalog
IVR.CcaiConfigFlushTimeoutInMinutes = 60
```

Agent Answers

```
SIP.CloudConnect.AgentAssistAuthTokenApi = /cloudconnectmgmt/token
SIP.CloudConnect.AgentAssistAuthTokenScopes = cjp-ccai:read,cjp-ccai:write
SIP.MediaForking.DestinationUrl =
SIP.UseSecureMediaForking = true
SIP.MediaForking.DestinationPort = 443
SIP.UseSIPINFOForking = true
SIP.CloudConnect.AgentAssistAuthTokenRefreshRateInPercent = 10
```

Smart Licensing

```
SL.eventLogPath = C:/Cisco/CVP/logs/WSM
SL.eventLogMaxSize = 1000000
```

New Properties for WXM, VAV, Agent Answers, and Smart Licensing

INDEX