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 2.

Step 4 (Optional) Click the **Device Pool** tab, enter the field values, and click **Save**. See Add or Remove Device From Device Pool.

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>
```

Gateway Settings

General Settings

After adding an IOS Gateway, you can execute a subset of IOS Gateway commands on the Gateway from the Operations Console.

The Ingress Gateway is the point at which an incoming call enters the Unified CVP solution. It terminates 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.

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 1: 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

Field	Description	Default	Value	Restart Required
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 and Add or Remove Device From Device Pool.

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 procedure.

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

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

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
!
```

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.

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 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:

- If you are using ACE, the server name is configured to the virtual IP (VIP) of the Call Server on ACE. For more information, see the *Configure High Availability for Unified CVP* section.
- 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.

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 and SIP Dialed Number Pattern Matching Algorithm 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
!
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
!
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.

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 6 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 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 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 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.

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.